

]HackingTeam[

RCS 9.3

La suite de hacking para interceptación gubernamental

Guía del técnico



Propiedad de la información

© COPYRIGHT 2014, HT S.r.l.

Todos los derechos reservados en todos los países.

Está prohibido traducir a otros idiomas, adaptar, reproducir en otros formatos, procesar mecánica o electrónicamente, fotocopiar o registrar de cualquier otra forma cualquier parte de este manual sin la autorización previa por escrito de HackingTeam.

Todos los nombres de empresas o productos pueden ser marcas comerciales o registradas, propiedad de sus respectivos dueños. Específicamente, Internet Explorer™ es una marca registrada de Microsoft Corporation.

Aunque los textos y las imágenes se seleccionen con sumo cuidado, HackingTeam se reserva el derecho de cambiar y/o actualizar la presente información para corregir errores de tipeo u otros tipos de errores sin previo aviso y sin responsabilidad alguna.

Cualquier referencia a nombres, datos o direcciones de empresas ajenas a HackingTeam es mera coincidencia y, a menos que se indique lo contrario, se incluyen como ejemplos para aclarar el funcionamiento del producto.

NOTA: las solicitudes de copias adicionales de este manual o de la información técnica del producto se deben enviar a:

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

Correo electrónico: info@hackingteam.com

Contenido

Glosario	xiii
Introducción a esta guía	1
Nuevas funciones de la guía	2
Documentación incluida	4
Convenciones tipográficas de notas	4
Convenciones tipográficas de formato	5
Destinatarios del producto y de esta guía	5
Datos de identificación del autor del software	6
RCS Console para el técnico	7
Pantalla inicial de RCS Console	8
Cómo se ve la página de inicio de sesión	8
Acceso a RCS Console	8
Descripción de la página principal	9
Introducción	9
Cómo se ve	9
Asistentes en la página principal	10
Introducción	10
Cómo se ve	10
Investigación rápida	11
Elementos y acciones comunes de la interfaz	12
Cómo se ve RCS Console	12
Acciones siempre disponibles en la interfaz	14
Cambiar el idioma de la interfaz o la contraseña	14
Cambiar la fecha y la hora de RCS Console a su zona horaria	14
Acciones relacionadas con las tablas	14
Procedimientos del técnico	16
Introducción	16
Procedimientos	16
Inyección en las conexiones HTTP	16
Infectar una computadora no conectada a Internet	16
Infectar una computadora conectada a Internet	17
Mantener actualizado el software del agent	18
Operation y target	19
Qué debería saber acerca de las operations	20
Qué es una operation	20
Qué debería saber acerca de los targets	20
Qué es un target	20
Administración de operations	20

Propósito	20
Cómo se ve la función	20
Para obtener más información	21
Ver los targets de la operation	22
Datos de la operation	22
Página de la operation	22
Propósito	22
Cómo se ve la función	22
Para obtener más información	24
Crear una factory	24
Datos de la página de la operation	24
Targets	26
Página del target	27
Propósito	27
Cómo se ve la función	27
Para obtener más información	29
Crear una factory	29
Cerrar una factory o agent	29
Eliminar una factory o agent	30
Importar evidencia del target	30
Datos de la página del target	30
Vista de íconos	31
Vista en tabla	31
Qué debería saber acerca de las factories y los agents	32
Métodos de infección	32
Componentes de la estrategia de infección	32
Factories	32
Cómo crear factories	33
Vectores de instalación	33
Agents	33
Módulos de obtención de datos	34
Compilación de una factory	34
Propósito	34
Próximos pasos	34
Cómo se ve la función	34
Para obtener más información	35
Crear un agent	35
Creación de un agent que se probará en el modo de demostración	36
Agents	37
Qué debería saber acerca de los agents	38

Introducción	38
Proceso de instalación de agents	38
Íconos de agents	38
Agent scout	39
Agent soldier	39
Agent elite	39
Sincronización de agents	39
Agents en línea y sin conexión	40
Desactive temporalmente un agent	40
Prueba de un agent	40
Configuración de agents	41
Página del agent	41
Propósito	41
Cómo se ve la función	41
Para obtener más información	43
Datos del registro de configuración de un agent	43
Datos de registro de los eventos de un agent	44
Datos del registro de sincronización de un agent	44
Página de comandos	45
Propósito	45
Cómo se ve la función	45
Para obtener más información	46
Transferencia de archivos hacia y desde el target	46
Propósito	46
Cómo se ve la función	46
Para obtener más información	49
Factory y agent: configuración básica	50
Qué debería saber acerca de la configuración básica	51
Configuración básica	51
Exportar e importar las opciones de configuración	51
Guardar la configuración como una plantilla	51
Configuración básica de una factory o un agent	52
Propósito	52
Próximos pasos	52
Cómo se ve la función	52
Para obtener más información	54
Configurar una factory o un agent	55
Datos de la configuración básica	55
Factory y agent: configuración avanzada	57
Qué debería saber acerca de la configuración avanzada	58

Configuración avanzada	58
Componentes de configuración avanzada	58
Lectura de secuencias	59
Eventos	59
Acciones	60
Relaciones entre las acciones y los módulos	60
Relaciones entre las acciones y los eventos	61
Módulos	61
Exportar e importar las opciones de configuración	61
Guardar la configuración como una plantilla	61
Configuración avanzada de una factory o un agent	62
Propósito	62
Próximos pasos	62
Cómo se ve la función	62
Para obtener más información	65
Creación de una secuencia de activación simple	65
Crear una secuencia de activación compleja	65
Datos globales del agent	66
El Network Injector	68
Qué debería saber acerca del Network Injector y sus reglas	69
Introducción	69
Tipos de Network Injectors	69
Tipos de recursos que pueden ser infectados	69
Cómo crear una regla	69
Reglas de identificación automática o manual	70
Qué sucede cuando una regla está activada/desactivada	70
Inicio de la infección	70
Administración de los Network Injector	70
Propósito	70
Qué puede hacer	70
Cómo se ve la función	71
Para obtener más información	72
Agregar una nueva regla de inyección	72
Enviar las reglas al Network Injector	73
Datos de la regla de inyección	73
Verifique el estado del Network Injector	79
Introducción	79
Identificar cuándo se sincroniza Network Injector	79
Qué debería saber acerca de Appliance Control Center	79
Introducción	79

Funciones de Appliance Control Center	80
Sincronización con el RCS Server	80
Actualización de las reglas de infección	80
Uso de las interfaces de red	80
Dirección IP de la interfaz de inyección	81
Infección mediante identificación automática	81
Infección mediante identificación automática	81
Qué debería saber acerca de Tactical Control Center	82
Introducción	82
Funcionamiento del Tactical Control Center	82
Sincronización con el RCS Server	82
Actualización de las reglas de infección	83
Uso de las interfaces de red	83
Infección mediante identificación automática	83
Infección mediante identificación manual	84
Obtención de la contraseña de una red Wi-Fi protegida	84
Forzar la autenticación de los dispositivos desconocidos	84
Infección mediante identificación automática	85
Infección mediante identificación manual	85
Establecer filtros en el tráfico interceptado	85
Filtro con expresiones regulares	85
Filtro de red BPF (Berkeley Packet Filter)	86
Identificar el target analizando el historial	86
Emulación de un Punto de acceso conocido por el target	86
Qué debería saber acerca de la identificación de contraseñas de redes Wi-Fi	86
Introducción	86
Ataque de diccionario para WPA/WPA2	87
Ataque de fuerza bruta para WEP	87
Ataque de fuerza bruta de PIN para WPS	87
Progreso del ataque	87
Qué debería saber acerca del desbloqueo de las contraseñas del sistema operativo	88
Introducción	88
Requisitos del Tactical Network Injector	88
Requisitos de la computadora del target	88
Proceso estándar	89
Qué debería saber acerca del acceso remoto al Control Center	89
Introducción	89
Contraseña del disco (solo para Tactical Control Center)	90
Módem 3G para la conexión	90
Dirección IP del dispositivo	91

Correo electrónico con modo de envío a dirección IP	91
Protocolo de red	91
Otras funciones útiles	91
Comandos de Tactical Control Center y Appliance Control Center	91
Introducción	91
Comandos	92
Appliance Control Center	92
Propósito	92
Solicitud de contraseña	93
Cómo se ve la función	93
Para obtener más información	93
Activar la sincronización con RCS Server para recibir nuevas reglas	94
Hacer una prueba a la red	94
Infectar targets por medio de la identificación automática	95
Configurar el acceso remoto a las aplicaciones	97
Ver los detalles de una infección	98
Datos de Appliance Control Center	99
Datos de la pestaña Network Injector	99
Datos de la pestaña Administración del sistema	99
Tactical Control Center	100
Propósito	100
Solicitud de contraseña	100
Cómo se ve la función	100
Para obtener más información	101
Activar la sincronización con RCS Server para recibir nuevas reglas	101
Hacer una prueba a la red	102
Obtener una contraseña de red Wi-Fi protegida	103
Infectar targets por medio de la identificación automática	105
Forzar la autenticación de los dispositivos desconocidos	107
Infectar targets por medio de la identificación manual	108
Establecer filtros en el tráfico interceptado	110
Identificar el target analizando el historial web	111
Limpiar dispositivos infectados por error	112
Emulación de un Punto de acceso conocido por el target	112
Desbloquear una contraseña del sistema operativo.	113
Configurar el acceso remoto a las aplicaciones	114
Apagar el Tactical Network Injector	117
Ver los detalles de una infección	117
Datos del Tactical Control Center	117
Datos de la pestaña Network Injector	117

Datos encontrados del dispositivo	117
Datos de la pestaña Wireless Intruder	118
Datos de la pestaña Fake Access Point	119
Datos de la pestaña Administración del sistema	119
Otras aplicaciones instaladas en Network Injectors	119
Introducción	119
Aplicaciones	120
Monitoreo del sistema	121
Monitoreo del sistema (monitor)	122
Propósito	122
Cómo se ve la función	122
Para obtener más información	123
Datos de monitoreo del sistema (Monitor)	123
Datos del monitoreo de los componentes del sistema	123
Datos de monitoreo de la licencia	124
Anexo: acciones	126
Lista de subacciones	127
Descripción de los datos de las subacciones	127
Descripción de tipos de subacciones	127
Acción Destroy	127
Propósito	127
Parámetros	128
Acción Execute	128
Propósito	128
Referencia a la carpeta del agent	128
Datos importantes	129
Acción Log	129
Propósito	129
Parámetros	129
Acción SMS	129
Propósito	129
Parámetros	129
Acción Synchronize	130
Propósito	130
Configuración de escritorio	130
Configuración móvil	131
Criterio de selección del tipo de conexión (Windows Phone)	131
Acción Uninstall	131
Propósito	131
Anexo: eventos	133

Lista de eventos	134
Descripción de los datos de los eventos	134
Descripción de los tipos de eventos	134
Evento AC	135
Propósito	135
Evento Battery	135
Propósito	135
Parámetros	135
Evento Call	136
Propósito	136
Parámetros	136
Evento Connection	136
Propósito	136
Configuración de escritorio	136
Evento Idle	137
Propósito	137
Parámetros	137
Evento Position	137
Propósito	137
Parámetros	137
Evento Process	137
Propósito	137
Parámetros	138
Evento Quota	138
Propósito	138
Parámetros	138
Evento Screensaver	138
Propósito	138
Evento SimChange	139
Propósito	139
Evento SMS	139
Propósito	139
Parámetros	139
Evento Standby	139
Evento Timer	140
Propósito	140
Parámetros	140
Evento Window	140
Propósito	140
Evento WinEvent	140

Propósito	140
Parámetros	141
Anexo: módulos	142
Lista de módulos	143
Módulo Addressbook	145
Propósito	145
Módulo Application	145
Propósito	145
Módulo Calendar	145
Propósito	145
Módulo Call	145
Propósito	145
Datos importantes	145
Módulo Camera	146
Propósito	146
Datos importantes	146
Módulo Chat	146
Propósito	146
Módulo Clipboard	147
Propósito	147
Módulo Conference	147
Propósito	147
Datos importantes	147
Módulo Crisis	147
Comportamiento en dispositivos de escritorio	147
Comportamiento en dispositivos móviles	148
Datos importantes de los dispositivos de escritorio	148
Datos importantes de los dispositivos móviles	148
Módulo Device	149
Propósito	149
Datos importantes de los dispositivos móviles	149
Módulo File	149
Propósito	149
Datos importantes	149
Módulo Keylog	150
Propósito	150
	150
Módulo Livemic	150
Propósito	150
Datos importantes	151

Módulo Messages	151
Propósito	151
Datos importantes	151
Módulo Mic	152
Propósito	152
Datos importantes de los dispositivos de escritorio	152
Módulo Money	153
Propósito	153
Módulo Mouse	153
Propósito	153
Datos importantes	153
Módulo Password	154
Propósito	154
Módulo Position	154
Propósito	154
Datos importantes de los dispositivos móviles	154
Módulo Screenshot	154
Propósito	154
Datos importantes	154
Módulo URL	155
Propósito	155
Apéndice: vectores de instalación	156
Lista de vectores de instalación	157
Qué debería saber acerca de Android	158
Privilegios raíz	158
Obtención de un certificado Code Signing	159
Introducción	159
Instalación de un certificado Code Signing	159
Vector Exploit	159
Propósito	159
Instalación de dispositivos de escritorio	159
Instalación de dispositivos móviles	160
Ejemplo de comandos para copiar el instalador en un dispositivo con iOS	160
Eliminar los archivos que ya no están en uso	160
Parámetros	160
Vector Installation Package	160
Propósito	160
Notas para los sistemas operativos Android (preparación del vector)	161
Notas para los sistemas operativos Android (instalación)	161
Notas para los sistemas operativos Windows Phone (preparación del vector)	162

Notas para los sistemas operativos Windows Phone (instalación)	162
Notas para los sistemas operativos Windows Mobile	163
Notas para los sistemas operativos BlackBerry	163
Notas para los sistemas operativos Symbian	163
Parámetros de Android, WinMobile, Windows Phone	163
Parámetros para BlackBerry	164
Parámetros para Symbian	164
Preparación de Installation Package para Windows Phone	164
Introducción	164
Secuencia recomendada	165
Cómo leer estas instrucciones	165
Obtener un código ID de Symantec	165
Obtener un certificado de Symantec	166
Instalación del certificado de Symantec	167
Genere los archivos .pfx y .aetx	168
Cargue los archivos .pfx y .aetx en el servidor de base de datos de RCS	169
Vector Local Installation	169
Propósito	169
Vector Melted Application	170
Propósito	170
Parámetros	171
Dispositivos de escritorio	171
Dispositivos móviles	171
Vector Network Injection	171
Propósito	171
Vector Offline Installation	172
Propósito	172
Parámetros	172
Vector de instalación persistente	172
Propósito	172
Preparar el vector	172
Instalación del agent	173
Condiciones de activación de la infección	174
Verificar la instalación	174
Parámetros	175
Vector QR Code/Web Link	175
Propósito	175
Operations	175
Eliminar los archivos que ya no están en uso	175
Parámetros	176

Vector Silent Installer	176
Propósito	176
Vector U3 Installation	177
Propósito	177
Vector WAP Push Message	177
Propósito	177
Operations	177
Instalación	177
Eliminar los archivos que ya no están en uso	177
Parámetros	178

Glosario

A continuación se detallan las definiciones utilizadas en este manual.

A

Accounting

Sección de la consola en la que se administra el acceso a RCS.

Administrador

Es la persona que permite el acceso al sistema, crea grupos de trabajo y define las operations, los targets y los tipos de datos que se recopilarán.

Administrador del sistema

Persona que instala los servidores y las consolas, actualiza el software y restaura los datos en caso de alguna falla.

Agent

Software de sondeo instalado en los dispositivos a monitorear. Está diseñado para reunir evidencia y transmitirla al Collector.

Agent elite

Agent instalado en dispositivos seguros. Le permite recopilar todos los tipos de evidencia disponibles.

Agent scout

Reemplaza al agent enviado al dispositivo para verificar el nivel de seguridad antes de instalar agents reales (elite o soldier).

Agent soldier

Agent instalado en dispositivos que no son completamente seguros. Solo le permite recopilar algunos tipos de evidencia.

alertas de evidencia

Alertas, usualmente en forma de correos electrónicos, que se envían a los analistas cuando hay nueva evidencia que coincide con las reglas establecidas.

Alerting

Sección de la consola en la que se administran las alertas de nueva evidencia.

Analista

Persona encargada de analizar los datos recopilados durante las operaciones.

Anonymizer

(opcional) Protege al servidor contra ataques externos y permite permanecer anónimo durante las investigaciones. Transfiere los datos del agent a los Collectors.

Audit

Sección de la consola que reporta las acciones de todos los usuarios y el sistema. Se utiliza para controlar el abuso de RCS.

B

back end

Entorno diseñado para descifrar y guardar la información que se recopila. En una arquitectura distribuida, incluye el Master Node y las bases de datos shard.

BRAS

(Broadband Remote Access Server) Dirige el tráfico hacia o desde el DSLAM a la red del ISP y administra la autenticación de los suscriptores del ISP.

BSSID

(Basic Service Set Identifier) Punto de acceso y su identificador cliente.

C

Carrier

Servicio del Collector: envía los datos recibidos de los Anonymizers a las bases de datos shard o al Master Node.

Collector

Servicio de Collector: recibe los datos que envían los agents a través de la cadena de Anonymizers.

consola

Computadora en la que se instala RCS Console. Accede directamente a RCS Server o al Master Node.

D

Dashboard

Sección de la consola utilizada por el analista. Se usa para tener un resumen rápido del estado de las operations, targets y agents más importantes.

DSLAM

(Digital Subscriber Line Access Multiplexer) Dispositivo de red que usualmente se encuentra en la central telefónica de los operadores de telecomunicaciones. Conecta varias interfaces de líneas de abonados digitales (DSL) a un canal de comunicaciones de alta velocidad digital usando técnicas de multiplexión.

E

Emisor de RCS

Sistema RCS que recibe evidencia de los agents y la transfiere a otros sistemas RCS (consultar) a través de las reglas de conexión. Es un sistema RCS completo.

entidad

Grupo de información de Intelligence vinculada con el target y con las personas y lugares involucrados en la investigación.

ESSID

(Extended Service Set Identifier) También conocido como SSID. Permite identificar la red Wi-Fi.

evidencia

Evidencia de datos recopilados. El formato depende del tipo de evidencia (p. ej.: imagen).

Exploit

Código que se aprovecha de un error o vulnerabilidad y ejecuta un código imprevisto. Se utiliza para infectar a los dispositivos de los targets.

F

factory

Una plantilla para la configuración y compilación de un agent.

front end

Entorno diseñado para comunicarse con los agents para recopilar información y establecer su configuración. En una arquitectura distribuida, incluye el Collector y el Network Controller.

G

Grupo

Entidad de Intelligence que agrupa a varias entidades.

grupo de alerting

Grupo de usuarios que reciben notificaciones por correo cuando se activa una alarma del sistema (por ejemplo, cuando la base de datos excede los límites de espacio disponible). Usualmente este grupo no está vinculado con ninguna operación.

M

Monitor

Sección de la consola en la que se monitorea el estado de los componentes y la licencia.

N

Network Controller

Servicio del Collector: verifica el estado del Network Injector y el Anonymizer y les envía nuevos parámetros de configuración y actualizaciones de software.

Network Injector

Componente de hardware que controla el tráfico de la red del target e inyecta un agent en los recursos web seleccionados. Viene en dos versiones, Appliance o Tactical: la primera es para la implementación en el ISP, la segunda se usa en el campo.

Network Injector Appliance

Versión apilable del Network Injector, para instalarlo en el ISP. Consulte: Tactical Network Injector.

O

operation

Investigación dirigida a uno o más targets, cuyos dispositivos tendrán agents.

P

Person

Entidad de Intelligence que representa a una persona involucrada en la investigación.

Position

Entidad de Intelligence que representa a un lugar involucrado en la investigación.

R

RCS

(Remote Control System). El producto que aquí se documenta.

RCS Console

Software diseñado para interactuar con RCS Server.

RCS Server

Una o más computadoras, según la arquitectura de instalación, donde se instalan los componentes esenciales de RCS: las bases de datos shard, los Network Controller y el Collector.

Receptor de RCS

Sistema RCS que recibe evidencia de otros sistemas RCS emisores (consultar) pero nunca directamente de los agents. En comparación con un RCS completo, el receptor de RCS solo cuenta con las funciones de procesamiento de evidencia.

reglas de alerta

Reglas que crean alertas cuando se almacena nueva evidencia o los agents se comunican por primera vez.

reglas de inyección

Opciones de configuración que definen cómo identificar el tráfico HTTP, qué recurso debe inyectarse y qué método se usará para la inyección.

S

secuencia de obtención

Grupo de eventos, acciones y módulos de obtención complejos, que forman parte de la configuración avanzada de agents.

SSH

(Secure SHell) Protocolo de red para la transmisión segura de datos, los servicios del intérprete de comandos remoto o la ejecución de comandos.

System

Sección de la consola en la que se administra el sistema.

T

Tactical Network Injector

Versión portátil del Network Injector, para uso táctico. Consulte: Network Injector Appliance.

TAP

(Test Access Port) Dispositivo de hardware que se instala en una red y que monitorea de forma pasiva el flujo de datos transmitido.

target

La persona física bajo investigación. En la sección Intelligence está representada por una entidad Target.

Técnico

Persona designada por el administrador para crear y administrar agents.

V

Virtual

Entidad de Intelligence que representa a una ubicación virtual (p. ej.: sitio web) involucrado en la investigación.

VPS

(Virtual Private Server) Servidor remoto en el que se instala el Anonymizer. Usualmente se alquila.

W

WPA

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

WPA 2

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

Introducción a esta guía

Presentación

Objetivos de este manual

Este manual sirve como guía para el *Técnico* sobre cómo usar RCS Console para:

- crear agents e instalarlos en un target definido por el administrador
- crear las reglas de inyección de conexiones HTTP para los Network Injectors

A continuación se muestra la información necesaria para consultar el manual.

Contenido

En esta sección se incluyen los siguientes temas:

Nuevas funciones de la guía	2
Documentación incluida	4
Convenciones tipográficas de notas	4
Convenciones tipográficas de formato	5
Destinatarios del producto y de esta guía	5
Datos de identificación del autor del software	6

Nuevas funciones de la guía

Lista de notas publicadas y actualizaciones a esta ayuda en línea.

<i>Fecha de publicación</i>	<i>Código</i>	<i>Versión de software.</i>	<i>Descripción</i>
23 de junio de 2014	Manuale del tecnico Guía del técnico	9.3	<p>En Tactical Control Center se agregó una función para desbloquear la contraseña del sistema operativo, consulte "Qué debería saber acerca del desbloqueo de las contraseñas del sistema operativo" En la página 88 , "Qué debería saber acerca de Tactical Control Center" En la página 82 .</p> <p>Se agregó una identificación y una regla de inyección que permite controlar a través del Control Center.</p> <p>Se agregó una lista de aplicaciones de terceros instalada en el Network Injector, consulte "Otras aplicaciones instaladas en Network Injectors" En la página 119 .</p> <p>Se agregó un vector de instalación persistente, consulte "Vector de instalación persistente" En la página 172</p> <p>Se actualizó la sección de registro de sincronización de agents ,consulte "Datos del registro de sincronización de un agent" En la página 44</p>

<i>Fecha de publicación</i>	<i>Código</i>	<i>Versión de software.</i>	<i>Descripción</i>
19 de febrero de 2014	Guía del técnico 1.6 FEB-2014	9.2	<p>Se eliminó la información relacionada con los sistemas operativos que soportan cada acción, módulo y evento en la configuración avanzada. En caso de necesitarla, debe ponerse en contacto con el servicio técnico.</p> <p>Se agregó el módulo Money consulte "Módulo Money" En la página 153 .</p> <p>Se actualizó la documentación del vector de instalación, consulte "Apéndice: vectores de instalación" En la página 156 .</p> <p>Se agregó el agent de nivel soldier, consulte "Qué debería saber acerca de los agents" En la página 38 .</p> <p>Se agregó la configuración de acceso remoto a las aplicaciones Tactical Control Center y Appliance Control Center, consulte "Tactical Control Center" En la página 100 , "Qué debería saber acerca del acceso remoto al Control Center" En la página 89</p> <p>Se agregó la prueba de las redes en Appliance Control Center, consulte "Appliance Control Center" En la página 92 .</p> <p>Se eliminó la regla INJECT-UPGRADE, consulte "Datos de la regla de inyección" En la página 73 .</p> <p>Se agregó lo que debería saber acerca de la función Wireless Intruder, consulte "Qué debería saber acerca de la identificación de contraseñas de redes Wi-Fi" En la página 86 .</p> <p>Se agregó la descripción de los comandos de terminal para las aplicaciones Tactical Control Center y Appliance Control Center, consulte "Comandos de Tactical Control Center y Appliance Control Center" En la página 91</p>
30 de septiembre de 2013	Guía del técnico 1.5 SEP - 2013	9	<p>Se agregó la plataforma Windows Phone, consulte "Vector Installation Package" En la página 160</p> <p>Se actualizó la documentación para administrar los privilegios de raíz de los dispositivos Android, consulte "Qué debería saber acerca de Android" En la página 158 .</p> <p>Se actualizó la documentación sobre la administración de Network Injector, consulte "El Network Injector" En la página 68 .</p> <p>Se actualizó la documentación debido a las mejoras a la interfaz de usuario.</p> <p>Se mejoró el contenido.</p>

Documentación incluida

Los siguientes manuales se incluyen con el software RCS:

<i>Manual</i>	<i>Destinatarios</i>	<i>Código</i>	<i>Formato de distribución</i>
Guía del administrador del sistema	Administrador del sistema	Guía del administrador del sistema 1.6 JUN-2014	PDF
Guía del administrador	Administradores	Guía del administrador 1.5 FEB-2014	PDF
Guía del técnico (este manual)	Técnicos	Guía del técnico 1.7 JUN-2014	PDF
Guía del analista	Analistas	Guía del analista 1.6 JUN-2014	PDF

Convenciones tipográficas de notas

Las notas previstas en este documento se detallan a continuación (Manual de estilo de Microsoft):



ADVERTENCIA: indica una situación de riesgo que, si no se evita, podría causar lesiones físicas en el usuario o daños en el equipo.



PRECAUCIÓN: indica una situación de riesgo que, si no se evita, puede causar la pérdida de datos.



IMPORTANTE: indica las acciones necesarias para realizar una tarea. Si bien pueden pasarse por alto algunas notas sin que esto afecte a la realización de la tarea, no se deberían omitir las indicaciones importantes.



NOTA: información neutral y positiva que enfatiza o complementa la información del texto principal. Proporciona información que puede aplicarse solo en casos especiales.



Sugerencia: recomendación para la aplicación de técnicas y procedimientos descritos en el texto de acuerdo a ciertas necesidades especiales. Puede sugerirse un método alternativo y no es esencial para la comprensión del texto.



Llamada al servicio: la operation solo puede completarse con la ayuda del servicio técnico.

Convenciones tipográficas de formato

A continuación se muestran las explicaciones de algunas convenciones tipográficas:

<i>Ejemplo</i>	<i>Estilo</i>	<i>Descripción</i>
Consulte " Datos del usuario "	<i>cursiva</i>	indica el título de un capítulo, una sección, una subsección, un párrafo, una tabla o una imagen de este manual u otra publicación a la que se hace referencia.
<ddmmaaaa>	<aaa>	indica un texto que el usuario debe ingresar de acuerdo a cierta sintaxis. En el ejemplo, <ddmmaaaa> es una fecha y un posible valor podría ser "14072011".
Seleccione uno de los servidores de la lista [2] .	[x]	indica el objeto citado en el texto que aparece en la imagen adyacente.
Haga clic en Agregar . Seleccione el menú Archivo, Guardar datos .	negrita	indica el texto en la interfaz del operador, que puede ser un elemento gráfico (como una tabla o pestaña) o un botón en la pantalla (como mostrar).
Presione Entrar	primera letra mayúscula	indica el nombre de una tecla en el teclado.
Consulte: Network Injector Appliance.	-	sugiere que compare la definición de una palabra en el glosario o contenido con otra palabra o contenido.

Destinatarios del producto y de esta guía

A continuación se muestra una lista de los profesionales que interactúan con RCS.

<i>Destinatario</i>	<i>Actividad</i>	<i>Habilidades</i>
Administrador del sistema	<p>Sigue las indicaciones de HackingTeam que se suministran durante la fase contractual. Instala y actualiza los RCS Servers, los Network Injectors y las RCS Cosoles. Programa y se encarga de realizar las copias de seguridad. Restaura las copias de seguridad si se reemplazan los servidores.</p> <p> ADVERTENCIA: el administrador del sistema debe tener las habilidades necesarias. HackingTeam no se hace responsable en caso de mal funcionamiento del equipo o de posibles daños ocasionados por la instalación por parte de una persona no profesional.</p>	Técnico de red experto
Administrador	<p>Crea cuentas y grupos autorizados. Crea operations y targets. Monitorea el estado del sistema y de las licencias.</p>	Administrador de investigación
Técnico	<p>Crea agents y los configura. Establece las reglas de Network Injector</p>	Técnico especialista en interceptaciones
Analista	<p>Analiza la evidencia y la exporta.</p>	Operativo

Datos de identificación del autor del software

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

Correo electrónico: info@hackingteam.com

RCS Console para el técnico

Presentación

Introducción

RCS (Remote Control System) es una solución que soporta investigaciones por medio de la interceptación activa y pasiva de los datos y la información de los dispositivos bajo investigación. De hecho, RCS crea, configura e instala agents de software de forma anónima que recopilan datos e información y envían los resultados a la base de datos central para decodificarlos y guardarlos.

Rol del técnico

El rol del técnico es:

- crear reglas de inyección para cada Network Injector
- crear agents de infección para los distintos dispositivos del target
- mantener actualizado el software del agent

Funciones a las que el técnico tiene acceso

Para realizar sus actividades, el técnico tiene acceso a las siguientes funciones:

- **Operations**
- **System**

Contenido

En esta sección se incluyen los siguientes temas:

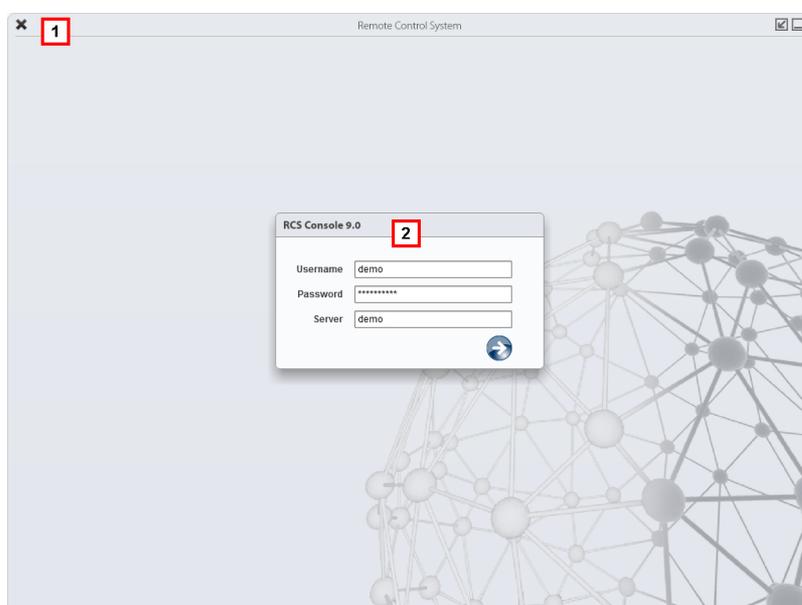
Pantalla inicial de RCS Console	8
Descripción de la página principal	9
Asistentes en la página principal	10
Elementos y acciones comunes de la interfaz	12
Procedimientos del técnico	16

Pantalla inicial de RCS Console

Cuando se abre RCS Console, se le pide que ingrese sus datos de inicio de sesión que estableció el administrador.

Cómo se ve la página de inicio de sesión

Así es como se ve la página de inicio de sesión:



Área Descripción

- 1 Barra de título con botones de comando:
 - ✕ Cierra RCS Console.
 -  Botón para ampliar la ventana.
 -  Botón para minimizar la ventana.
- 2 Ventana de diálogo para ingresar al sistema.

Acceso a RCS Console

Para acceder a las funciones de RCS Console:

Paso Acción

- 1 En **Nombre de usuario** y **Contraseña**, ingrese sus datos de inicio de sesión asignados por el administrador.

Paso Acción

- 2 En **Servidor**, ingrese el nombre del equipo o la dirección del servidor al que desea conectarse.
- 3 Haga clic en : aparecerá la página principal con los menús activados según los privilegios de su cuenta. Consulte "[Descripción de la página principal](#)" abajo .

Descripción de la página principal

Para ver la página principal:

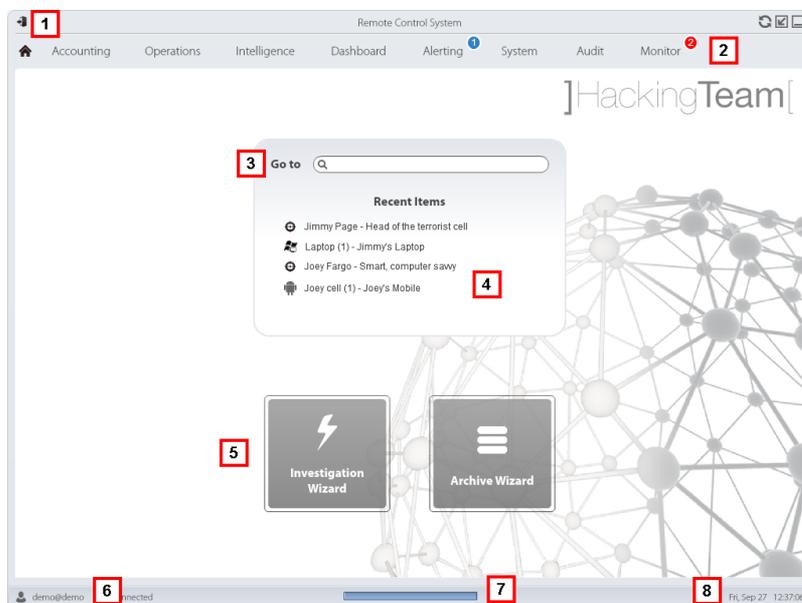
- haga clic en 

Introducción

Al abrir RCS Console se mostrará la página principal. Todos los usuarios verán la misma página. Los menús se verán activos según los privilegios asignados a la cuenta.

Cómo se ve

Así es como se ve la página principal, con elementos guardados que se abrieron recientemente. Detalle de los elementos y las acciones comunes:



Área Descripción

- 1 Barra de título con botones de comando.

Área Descripción

- 2 Menú de RCS con las funciones activas para el usuario.
- 3 Cuadro de búsqueda para buscar operations, targets, agents y entidades, por nombre o descripción.
- 4 Enlaces a los cinco elementos abiertos (operation en la sección **Operations**, operation en la sección **Intelligence**, target, agent y entidad).
- 5 Botones del asistente.
- 6 Usuario conectado con opciones para cambiar el idioma y la contraseña.
- 7 Área de descarga con una barra de progreso durante la exportación o compilación.
- 8 Fecha y hora actuales con opciones para cambiar la zona horaria.

Asistentes en la página principal

Para ver la página principal:

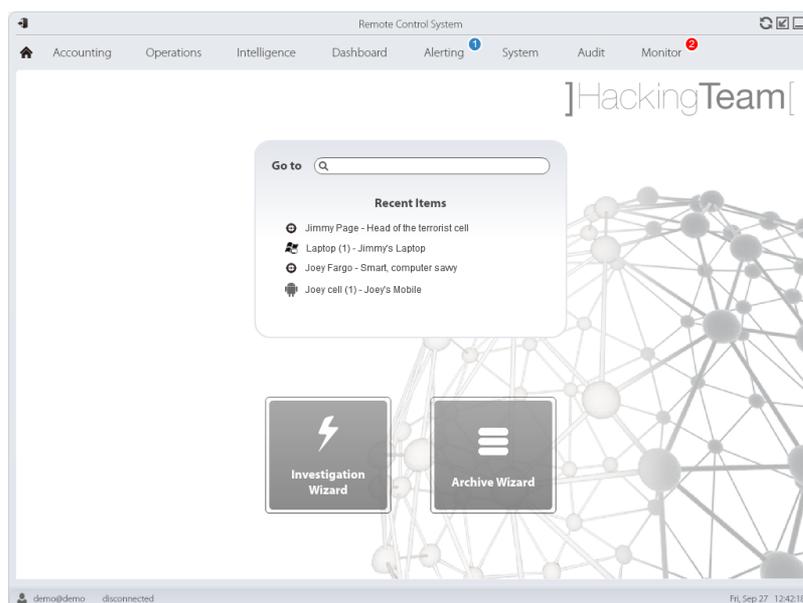
- haga clic en 

Introducción

Para los usuarios con ciertos privilegios, en RCS Console se muestran los botones que permiten abrir los asistentes.

Cómo se ve

Así es como se ve la página principal con los asistentes activados:



Botón	Función
-------	---------



Abre el asistente para crear rápidamente un agente.



NOTA: el botón solo se activa para los usuarios con privilegios Administrador y Técnico.



Abre el asistente para guardar rápidamente los datos de operation y target.



NOTA: el botón solo se activa para los usuarios con privilegios Administrador y Administrador del sistema.

Investigación rápida

Este asistente permite crear rápidamente un agente. El asistente le pide que ingrese el nombre (por ejemplo: "AveNocturna") y el tipo de agente que se desea crear (de escritorio o móvil) y crea lo siguiente, en este orden:

1. una operation "AveNocturna"
2. un target "AveNocturna"
3. una factory "AveNocturna"
4. un grupo de usuarios "AveNocturna" en el cual el usuario actual es el único miembro

A continuación se abre la página de configuración de la factory. Consulte "[Configuración básica de una factory o un agente](#)" En la página 52

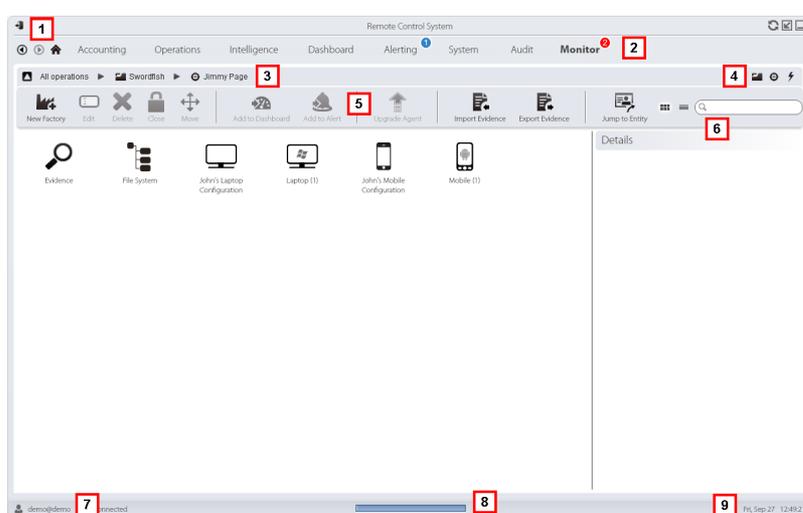
Para incluir otros elementos en esta operation, target o grupo de usuarios, simplemente entre a la página de detalles.

Elementos y acciones comunes de la interfaz

Cada página del programa usa elementos comunes y permite realizar acciones similares. Para facilitar la comprensión del manual, en este capítulo se describirán los elementos y acciones compartidos por ciertas funciones.

Cómo se ve RCS Console

Así es como se ve usualmente la página de RCS Console. En este ejemplo se muestra la página de un target:



Área Descripción

- 1 Barra de título con botones de comando:
 - Salir de RCS.
 - Botón para volver a cargar la página.
 - Botón para ampliar la ventana.
 - Botón para minimizar la ventana.
- 2
 - Botón Anterior del historial de navegación
 - Botón Siguiente del historial de navegación
 - Botón para regresar a la página principal
 - Menú de RCS con las funciones activas para el usuario.

Área Descripción

- 3 Barra de navegación de la operation. A continuación se muestra la descripción de cada elemento:

Ícono Descripción

-  Regresar al nivel superior.
-  Muestra la página de la operation (sección **Operations**).
-  Muestra la página del target.
-  Muestra la página de la factory.
-  Muestra la página del agent.
-  Muestra la página de la operation (sección **Intelligence**).
-  Muestra la página de la entidad.

- 4 Botones que permiten mostrar todos los elementos, independientemente del grupo al que pertenecen. A continuación se muestra la descripción de cada elemento:

Ícono Descripción

-  Muestra todas las operations.
-  Muestra todos los targets.
-  Muestra todos los agents.
-  Muestra todas las entidades.

- 5 Barra de herramientas de la ventana.

- 6 Botones y cuadro de búsqueda:

Objeto

Descripción

- | | |
|---|---|
|  | Cuadro de búsqueda. Escriba parte del nombre para que aparezca una lista con los elementos que contienen esas letras. |
|  | Muestra los elementos en una tabla. |
|  | Muestra los elementos como íconos. |

- 7 Usuario conectado con opciones para cambiar el idioma y la contraseña.

Área Descripción

- 8** Área de descarga con una barra de progreso durante la exportación o compilación. Los archivos se descargan en el escritorio, en la carpeta RCS Download.
 - Barra superior: porcentaje de generación en el servidor
 - Barra inferior: porcentaje de descarga desde el servidor a RCS Console.

- 9** Fecha y hora actuales con opciones para cambiar la zona horaria.

Acciones siempre disponibles en la interfaz

Cambiar el idioma de la interfaz o la contraseña

Para cambiar el idioma de la interfaz o la contraseña:

Paso Acción

- 1** Haga clic en **[7]** para que aparezca una ventana de diálogo con los datos del usuario.
- 2** Cambie el idioma o la contraseña y haga clic en **Guardar** para confirmar y salir.

Cambiar la fecha y la hora de RCS Console a su zona horaria

Para convertir todas las fechas y horas a su zona horaria:

Paso Acción

- 1** Haga clic en **[9]** para que aparezca una ventana de diálogo con la fecha y la hora actuales:
 - Hora UTC:** hora media de Greenwich (GMT)
 - Hora local:** fecha y hora donde se encuentra instalado el RCS Server
 - Hora de la consola:** fecha y hora de la consola que se está utilizando y que se puede cambiar.
- 2** Cambie la zona horaria y haga clic en **Guardar** para confirmar y salir: todas las fechas y horas se cambiarán según lo que haya indicado.

Acciones relacionadas con las tablas

RCS Console muestra varios datos en forma de tablas. Las tablas le permiten:

- ordenar los datos por columna en orden ascendente o descendente
- filtrar datos por columna

Acción**Descripción**

Ordenar por columna Haga clic en el encabezado de la columna para ordenarla de forma ascendente o descendente.

Event	Path
SYNC	Swordfish
INSTANCE	Swordfish > J
EVIDENCE	*

Filtrar un texto

Escriba una parte del texto que desea buscar: se mostrarán solo los elementos que contengan esas letras.

 Info

Al escribir el mismo texto que en el ejemplo se mostrarán elementos con una descripción como:

- "my**boss**"
- "**boss**anova"

Filtrar en base a una opción

Seleccione una opción: se mostrarán los elementos que coincidan con la opción seleccionada.

 Acquired
 Last 24 Hours
 Last Week
 From / To
 Action
 User

Filtrar en base a varias opciones

Seleccione una o más opciones: se mostrarán los elementos que coincidan con las opciones seleccionadas.

 Type
 Untagged
 Low
 Medium
 High
 Critical
Cambiar el tamaño de la columna

Seleccione el borde de la columna y arrástrelo.

Procedimientos del técnico

Introducción

El técnico está a cargo de las reglas de infección para recuperar información importante. A continuación se describen los procedimientos típicos, con referencias a los capítulos relacionados. Estas solo son simples indicaciones. Las habilidades y la competencia son esenciales para explotar la flexibilidad de RCS y adaptarla a las necesidades de investigación.

Procedimientos

Inyección en las conexiones HTTP

Para la inyección de conexiones HTTP debe utilizarse el Network Injector.

Paso Acción

- 1 En la sección **System, Network Injector** , cree las reglas de identificación e infección para Network Injector Appliance y Tactical Network Injector.

Consulte "[Administración de los Network Injector](#)" En la página 70



NOTA: no se requiere instalar ningún agent.

- 2 Al utilizar Network Injector Appliance, el sistema aplica las reglas de identificación para el tráfico de datos. Una vez que se encuentran los dispositivos del target, se los infecta con las reglas de inyección.

O se los puede identificar e infectar de forma automática o manual por medio del Tactical Network Injector.

Consulte "[Tactical Control Center](#) " En la página 100 .

Infectar una computadora no conectada a Internet

Para infectar una computadora no conectada a Internet:

Paso Acción

- 1 Cree una factory y desactive la sincronización a nivel operation, consulte "[Página de la operation](#)" En la página 22 .

O cree un una factory a nivel target, siempre sin sincronización, consulte "[Página del target](#)" En la página 27

Paso Acción

- 2 Compile la factory seleccionando el vector de instalación adecuado para la plataforma del dispositivo y el método de instalación, luego cree un agent.
Consulte "[Compilación de una factory](#)" En la página 34 .
- 3 Instale el agent en el dispositivo del target con los métodos seleccionados.
Consulte "[Lista de vectores de instalación](#)" En la página 157 .
- 4 Después del tiempo necesario, recupere la evidencia generada en el dispositivo del target.
- 5 Importe la evidencia del agent y analícela.
Consulte "[Página del agent](#)" En la página 41 .

Infectar una computadora conectada a Internet

Para infectar una computadora conectada a Internet:



Sugerencia: estos pasos son esenciales cuando no sabe desde un principio qué actividades del target va a registrar o si desea evitar registrar una cantidad excesiva de datos.

Paso Acción

- 1 Cree una factory: el sistema activará automáticamente la sincronización.
Consulte "[Página de la operation](#)" En la página 22
- 2 Compile la factory seleccionando el vector de instalación adecuado para la plataforma del dispositivo y el método de instalación, luego cree un agent.
Consulte "[Compilación de una factory](#)" En la página 34 .
- 3 Instale el agent en el dispositivo del target con los métodos seleccionados.
Consulte "[Lista de vectores de instalación](#)" En la página 157 .
- 4 El agent se mostrará en la página del target en la primera sincronización.
Consulte "[Página del target](#)" En la página 27
- 5 Restablezca los parámetros del agent usando la configuración básica o avanzada. El agent aplica la nueva configuración en la siguiente sincronización.
Consulte "[Configuración básica de una factory o un agent](#)" En la página 52
Consulte "[Configuración avanzada de una factory o un agent](#)" En la página 62 .

Mantener actualizado el software del agent

HackingTeam actualiza cíclicamente su software. Para actualizar los agents instalados:

Paso Acción

- 1
 - En la sección **Operations, Target** actualice los agents. Consulte "[Página del target](#)" En la página 27
 - o
 - En la sección **Operations, Target** abra un agent y actualícelo. Consulte "[Página del agent](#)" En la página 41 .

Operation y target

Presentación

Introducción

La administración de operations establece los targets que serán interceptados.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de las operations	20
Qué debería saber acerca de los targets	20
Administración de operations	20
Datos de la operation	22
Página de la operation	22
Datos de la página de la operation	24

Qué debería saber acerca de las operations

Qué es una operation

Una operation es una investigación que se llevará a cabo. Una operation contiene uno o más targets, es decir, las personas físicas que se van a interceptar. El técnico asigna uno o más agents, de *escritorio* o *móviles*, al target. Por lo tanto, es posible instalar agents en una computadora o teléfono móvil.

Qué debería saber acerca de los targets

Qué es un target

Un target es una persona física que va a ser investigada. El técnico asigna uno o más agents, de escritorio o móviles, al target. Por lo tanto, es posible instalar agents en una computadora o teléfono móvil.

Administración de operations

Para administrar
operations:

- Sección Operations

Propósito

Esta función le permite:

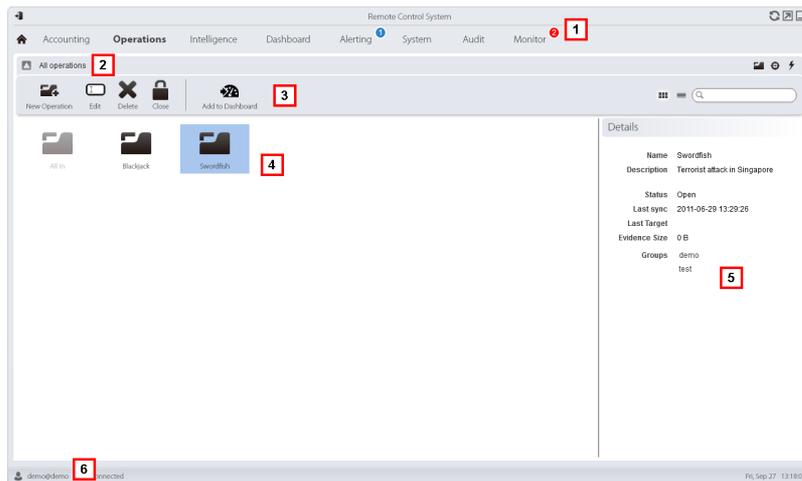
- ver y administrar los targets vinculados con una operation



NOTA: la función solo se activa si el usuario tiene autorización **Administración de operations**.

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación.
- 3 Barra de herramientas de la ventana.
- 4 Lista de operations creadas:
 -  Operation abierta. Si se establecieron targets y se instalaron agents correctamente, se recibirá la evidencia recopilada.
 -  Operation cerrada. Todos los targets están cerrados y los agents desinstalados. Aún se pueden ver todos los targets y la evidencia .
- 5 Datos de una operation seleccionada.
- 6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para ver una descripción de los datos en esta ventana consulte "[Datos de la operation](#)" En la página siguiente .

Para obtener más información sobre las operations consulte "[Qué debería saber acerca de las operations](#)" En la página precedente .

Ver los targets de la operation

Para ver los targets de la operation:

Paso Acción

- 1 Haga doble clic una operation: se abrirá la página de administración de targets.
Consulte "[Página de la operation](#)" abajo

Datos de la operation

A continuación se describen los datos de la operation seleccionada:

Datos	Descripción
Nombre	Nombre de la operation.
Descripción	Descripción del usuario
Contacto	Los campos descriptivos se utilizan para definir, por ejemplo, el nombre de una persona de contacto (juez, abogado, etc.).
Estado	Estado de la operation y comando de cierre: Abierta: la operation está abierta. Si se establecieron targets y se instalaron agents correctamente, RCS recibe la evidencia recopilada. Cerrada: la operation está cerrada y no podrá volver a abrirse. Los agents ya no enviarán más datos, pero todavía podrá consultar la evidencia que ya se recibió.
Grupos	Grupos que pueden ver la operation.

Página de la operation

Para ver una operation:

- En la sección **Operations**, haga doble clic en una operation

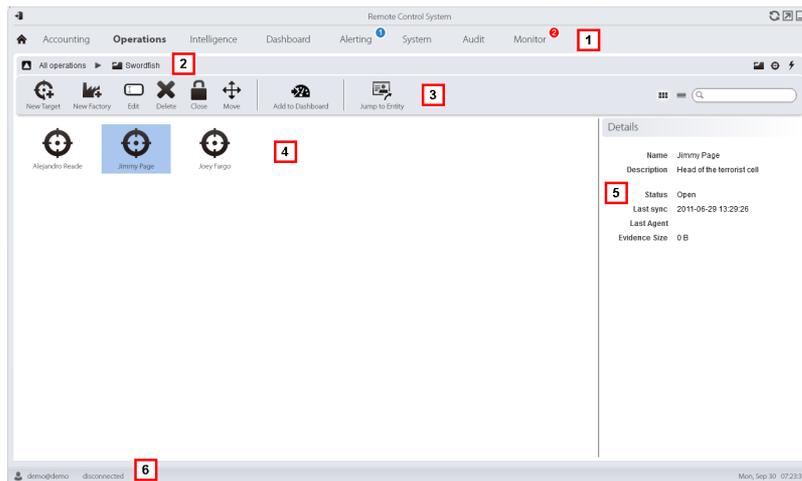
Propósito

Esta función le permite:

- administrar factories que, una vez compiladas, se convierten en agents que se instalarán en los dispositivos consulte "[Configuración avanzada de una factory o un agent](#)" En la página 62

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación.
- 3 Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono Función



Permite crear una factory.



NOTA: la función solo se activa si el usuario tiene autorización **Crear factories** . También se puede crear una factory a nivel target, **consulte "Página de la operation" En la página precedente**

- 4 Lista de targets:



target abierto



target cerrado

- 5 Datos de un target seleccionado.
- 6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para obtener más información sobre las operations consulte "[Qué debería saber acerca de las operations](#)" En la página 20 .

Para obtener más información sobre las factories consulte "[Qué debería saber acerca de las factories y los agents](#)" En la página 32 .

Para ver una descripción de los datos en esta ventana consulte "[Datos de la página de la operation](#)" abajo .

Para administrar rápidamente los datos de la operation consulte "[Asistentes en la página principal](#)" En la página 10 .

Crear una factory

Para crear una factory:

Paso Acción

- 1
 - Haga clic en **Nueva factory**: aparecerán los campos para ingresar datos.
 - Escriba el nombre y la descripción, y seleccione el tipo de dispositivo en **Tipo**.
- 2 Haga clic en **Guardar**: aparecerá la nueva factory con el nombre seleccionado en el área de trabajo principal.

Datos de la página de la operation

A continuación se describen los datos del target seleccionado:

Datos	Descripción
Nombre	Nombre del target.
Descripción	Descripción del usuario
Estado	Define el estado del target: <ul style="list-style-type: none">  Abierto. Si el técnico instala los agents correctamente, RCS recibirá la evidencia recopilada.  Cerrado. Cerrado, ya no se podrá volver a abrir.

Targets

Presentación

Introducción

Un target es una persona física a quien se va a monitorear. Se pueden utilizar varios agents, uno por cada dispositivo de propiedad del target.

Contenido

En esta sección se incluyen los siguientes temas:

Página del target	27
Datos de la página del target	30
Qué debería saber acerca de las factories y los agents	32
Compilación de una factory	34

Página del target

Para abrir un target

- En la sección **Operations**, haga doble clic en una operation y en un target

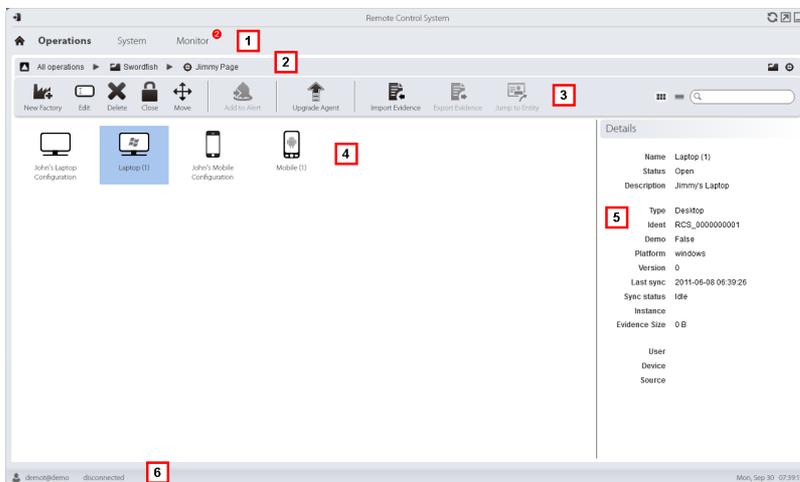
Propósito

Esta función le permite:

- administrar factories que, al compilarse, se convierten en agents que se instalan en el dispositivo del target.
- abrir una factory para una configuración básica (consulte "[Configuración básica de una factory o un agent](#)" En la página 52) o configuración avanzada (consulte "[Configuración avanzada de una factory o un agent](#)" En la página 62
- importar evidencia del target
- abrir un agent instalado
- actualizar el software del agent

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.

Área Descripción

- 2 Barra de navegación.
- 3 Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:



NOTA: el botón  muestra los elementos en una lista con sus datos.

Ícono Función



Permite crear una factory.



NOTA: la función solo estará activada si el usuario tiene autorización **Crear factories** .
También es posible crear una factory en el nivel de operation.consulte "[Página de la operation](#)" En la página 22 .



Permite editar una factory o agent.



Eliminar una factory o agent



Cierra un agent o factory.



Cambia la factory o agent a un nuevo target.



Actualiza el software de todos los agents a la última versión recibida del servicio técnico de HackingTeam



PRECAUCIÓN: la actualización no modificará la configuración que se transmitirá al agent en la siguiente sincronización.



IMPORTANTE: para Android, para actualizar el agent deben obtenerse privilegios raíz.Consulte "[Qué debería saber acerca de Android](#)" En la página 158 .



Importa la evidencia del target recopilada físicamente en el dispositivo.



NOTA: la función solo se activa si el usuario tiene autorización **Importar evidencia** .

Área Descripción

- 4 Íconos/lista de factories creadas y agents instalados.



: agent en modo de demostración.



: agent scout esperando verificación.



: agent soldier instalado.



: agent elite instalado.

- 5 Datos de la factory o agent seleccionado.
- 6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para ver una descripción de los datos en esta ventana consulte "[Datos de la página del target](#)" En la página opuesta .

Para obtener más información sobre los targets consulte "[Qué debería saber acerca de las factories y los agents](#)" En la página 32

Para administrar rápidamente los datos del target, consulte "[Asistentes en la página principal](#)" En la página 10 .

Crear una factory

Para crear una factory:

Paso Acción

- 1
 - Haga clic en **Nueva factory**: aparecerán los campos para ingresar datos.
 - Escriba el nombre y la descripción, y seleccione el tipo de dispositivo en **Tipo**.
- 2 Haga clic en **Guardar**: aparecerá la nueva factory con el nombre seleccionado en el área de trabajo principal.

Cerrar una factory o agent

Para cerrar una factory o agent:

Paso Acción

- 1 Seleccione una factory o agent y haga clic en **Cerrar**.
- 2 Confirme el cierre.



PRECAUCIÓN: *el cierre de un agent es irreversible. Este se desinstalará en la siguiente sincronización. Al cerrar una factory, se vuelve inaccesible. Los agents activos permanecen accesibles, mientras que todos los agents que no hayan sido sincronizados al menos una vez antes del cierre de la factory se desinstalarán.*

Eliminar una factory o agent

Para eliminar una factory o agent:

Paso Acción

- 1 Seleccione una factory o agent y haga clic en **Eliminar**.
Confirme la acción: se eliminarán los registros, las opciones de configuración y la evidencia.



PRECAUCIÓN: *esta operation es irreversible.*

Importar evidencia del target

Para importar evidencia:

Paso Acción

- 1 Haga clic en **Importar evidencia**: se abrirá la ventana de importación.
Haga clic en **Seleccionar carpeta** y seleccione la carpeta donde se encuentra el archivo offline.ini.
- 2 Haga clic en **Importar**: la evidencia se guardará en la base de datos y estará disponible para que el analista la vea.

Datos de la página del target

Para ver los datos de la página:

- En la sección **Operations**, haga doble clic en una operation, luego en un target y luego haga clic en **Vista de íconos** o **Vista en tablas**

Los elementos de la página se pueden ver como íconos o como una tabla.

Vista de íconos

Los íconos se describen a continuación:

Datos Descripción



Factory de tipo escritorio en estado Abierto.



Ejemplo de agent scout instalado en un dispositivo de escritorio de Windows, en estado abierto.



Ejemplo de agent soldier instalado en un dispositivo de escritorio con Windows, en estado abierto.



Ejemplo de agent elite instalado en un dispositivo de escritorio con Windows, en estado abierto.



NOTA: los íconos de color gris claro corresponden a factories y agents cerrados. Este es el ícono de un agent móvil para Android en estado cerrado: .



NOTA: los íconos de color gris claro corresponden a agents cerrados. Este es el ícono de un agent móvil para Android en estado cerrado: .

Vista en tabla

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Nombre	Nombre de la factory o agent.
Descripción	Descripción de la factory o agent
Estado	<p>Abierto: una factory abierta se puede compilar para crear agents. Es posible instalar un agent abierto, que se ejecuta y recopila evidencia.</p> <p>Cerrado: una factory o agent cerrado no se puede volver a abrir. Los datos en RCS se podrán consultar más adelante.</p>
Tipo	De tipo escritorio o móvil.
Nivel	(solo para los agents) Nivel del agent: scout, soldier, elite.
Plataforma	(solo para los agents) Sistema operativo en la que se instala el agent.
Versión	(solo para los agents) Versión del agent. Se crea una nueva versión cada vez que se crea una nueva configuración.

Datos	Descripción
Última sincronización	(solo para los agents) Fecha y hora de la última sincronización del agent.
Ident	(solo para los agents) Identificación unívoca de un agent.
Instancia	(solo para los agents) Identificación unívoca del dispositivo donde está instalado el agent.

Qué debería saber acerca de las factories y los agents

Métodos de infección

Un dispositivo puede ser infectado de las siguientes maneras:

- **infección física:** el dispositivo es infectado mediante la ejecución de un archivo transmitido por medio de memorias USB, CD o documentos. La evidencia se puede recopilar físicamente o a través de Internet, en el momento en el que el dispositivo se conecta.
- **infección remota:** el dispositivo es infectado mediante la ejecución de un archivo transferido a través de una conexión a Internet, o que puede estar disponible en un recurso web. La evidencia se puede recopilar físicamente o a través de Internet, en el momento en el que el dispositivo se conecta. La infección remota puede mejorarse a través de un Network Injector.

Componentes de la estrategia de infección

Componentes necesarios para una infección correcta:

- **Factory:** modelo del agent.
- **Vectores de instalación:** canales de infección.
- **Agent:** el software que se debe instalar en el dispositivo de target.
- **Target y operation:** se definen cuando el administrador del sistema abre investigaciones. Consulte el Manual del administrador del sistema.
- **Evidencia:** los tipos de registros a recopilar

Factories

La *factory* es un modelo que se usa para crear los agents que se instalarán. El ícono varía de acuerdo con el tipo de dispositivo en el que se instalará el agent:

-  : factory para un agent de escritorio
-  : factory para un agent móvil

En la factory se debe establecer lo siguiente:

- los *datos* que se obtendrán (configuración básica) o los *módulos* que se activarán dinámicamente (configuración avanzada)
- *vectores de instalación* (p. ej.: CD, Exploit, Network Injector)



Sugerencia: se pueden guardar las opciones de configuración como plantilla para cargarlas la próxima vez que cree un agent similar.



Sugerencia: una factory se puede usar para crear varios agents; por ejemplo, para instalarla mediante diferentes vectores de instalación (p. ej.: dos computadoras con diferentes sistemas operativos).

Cómo crear factories

Las factories son plantillas que se pueden crear en dos niveles jerárquicos diferentes de operation-target-agent:

- *en el nivel operation*: la factory, después de la instalación y la primera sincronización, crea automáticamente un agent y un target para cada dispositivo
- *en el nivel target*: la factory, después de la instalación y la primera sincronización, crea automáticamente un agent para ese target

El modo *nivel de operation* asegura que la evidencia recopilada se asigne por separado. De hecho, crea tantos agents como dispositivos existentes. Luego, si dos o más dispositivos pertenecen al mismo target, el agent se puede mover hacia el target correcto.

El modo *nivel de target*, si se usa correctamente, puede crear una factory que sirve para crear varios agents.

Vectores de instalación

Los vectores de instalación se seleccionan cuando se compila y define el método de instalación, física o remota, para un agent. Al realizarse la compilación, los vectores de instalación disponibles pueden variar según el sistema operativo del dispositivo.

Se pueden usar varios vectores de instalación para el mismo agent.



NOTA: las reglas de inyección se usan para la inyección de conexiones HTTP. Consulte "[Administración de los Network Injector](#)" En la página 70

Agents

Un *agent* es el resultado de la compilación de una factory con uno o más vectores de instalación. Un agent está listo para ser instalado en un dispositivo.

En la configuración básica se define el tipo de datos a recopilar, mientras que la configuración avanzada le permite activar o desactivar módulos de una manera dinámica e independiente.

Para ver los tipos de módulos disponibles en las configuraciones básica y avanzada consulte "[Lista de módulos](#)" En la página 143

Para obtener más información sobre los agents consulte "[Qué debería saber acerca de los agents](#)" En la página 38 .

Módulos de obtención de datos

Los módulos activan algunas actividades en el dispositivo del target; principalmente la obtención de datos. Se activan y establecen en la configuración básica (solo en algunos casos) o en la configuración avanzada.

Los tipos de módulos disponibles también dependen del tipo de dispositivo.

Para ver una lista completa consulte "[Lista de módulos](#)" En la página 143 .

Compilación de una factory

Para compilar una factory:

- En la sección **Operations**, haga doble clic en una operation, luego en un target, en una factory y por último haga clic en **Crear**
- En la sección **Operations**, haga doble clic en una operation, luego en un target, en una factory y por último haga clic en **Config. avanzada , Crear**

Propósito

Esta función le permite crear uno o más agents (reales o para probarlos en modo de demostración) dependiendo de los vectores de instalación elegidos y de las plataformas elegidas.



NOTA: para ver una descripción detallada de cada vector de instalación consulte "[Lista de vectores de instalación](#)" En la página 157



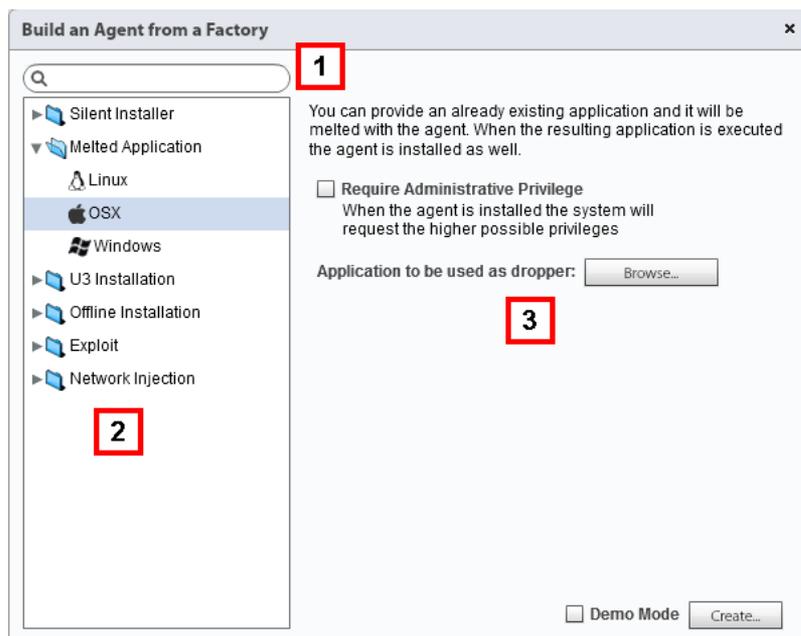
NOTA: la función solo se activa si el usuario tiene autorización **Creación de vectores de infección** .

Próximos pasos

La creación implica la instalación subsecuente en el dispositivo de un target.

Cómo se ve la función

Así es como se muestra la página para el agent de escritorio:



Área Descripción

- 1 Cuadro de búsqueda del vector de instalación y de la plataforma.
- 2 Vista del árbol de vectores y plataformas.
- 3 Área de configuración de las opciones de compilación para el vector elegido.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para obtener más información sobre las factories consulte "[Qué debería saber acerca de las factories y los agents](#)" En la página 32 .

Para ver una descripción detallada de cada vector de instalación consulte "[Lista de vectores de instalación](#)" En la página 157

Crear un agent

Para crear un agent:

Paso Acción

- 1 Seleccione uno o más vectores de instalación y establezca las opciones.

Paso Acción

- 2 Haga clic en **Crear**: se creará y descargará un archivo ZIP o ISO en la carpeta RCS Download, que está listo para ser instalado en el dispositivo.

Creación de un agent que se probará en el modo de demostración



IMPORTANTE: utilice esta opción solamente para realizar pruebas en dispositivos internos. Los agents en modo de demostración no son invisibles y la instalación de RCS no quedará oculta.

Para crear un agent para propósitos de prueba:

Paso Acción

- 1 Seleccione uno o más vectores de instalación y establezca las opciones.
- 2 Seleccione el cuadro de verificación **Modo de demostración**.
- 3 Haga clic en **Crear**; el agent instalado en el dispositivo mostrará su presencia con señales de audio y mensajes en pantalla.

Agents

Presentación

Introducción

Los agents obtienen datos del dispositivo en el que están instalados y los envían a los Collectors de RCS. Su configuración y software pueden actualizarse y transferir archivos que el target no notó.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de los agents	38
Página del agent	41
Datos del registro de configuración de un agent	43
Datos de registro de los eventos de un agent	44
Datos del registro de sincronización de un agent	44
Página de comandos	45
Transferencia de archivos hacia y desde el target	46

Qué debería saber acerca de los agents

Introducción

El agent puede quedar expuesto y ser identificado si se instala en entornos con antivirus o que son administrados por técnicos expertos.

Para evitar que esto ocurra, se incluyeron tres niveles diferentes de agents:

- scout
- soldier
- elite

El *agent scout* es un reemplazo del agent enviado al comienzo de la fase de instalación para analizar el nivel de seguridad del dispositivo del target.

El *agent soldier* y el *agent elite* son agents reales. El *agent soldier* se instala en entornos que no son completamente seguros y por lo tanto permiten recopilar algunos tipos de evidencia. El *agent elite* se instala en entornos seguros y puede recopilar todos los tipos de evidencia disponible.

Proceso de instalación de agents

<i>Fase</i>	<i>Descripción</i>
-------------	--------------------

- 1 El técnico instala el agent scout en el dispositivo del target.
- 2 El agent scout recopila evidencia del dispositivo para verificar el nivel de seguridad.
- 3 El técnico actualiza el agent:

<i>Si el entorno es...</i>	<i>Entonces...</i>
----------------------------	--------------------

seguro	el sistema instala el agent elite.
no completamente seguro	el sistema instala el agent soldier.
inseguro	el agent no puede ser actualizado.

Íconos de agents

El ícono del agent proporciona la siguiente información:

- nivel (scout, soldier, elite)
- tipo de dispositivo (de escritorio o móvil)
- sistema operativo donde está instalado

A continuación se muestran los íconos de los tres niveles de agents, por ejemplo, para un dispositivo de escritorio con Windows:

- : scout
- : soldier
- : elite

Agent scout

Una vez instalado, el agent scout aparece en la página del target después de la primera sincronización.

El agent scout obtiene evidencia:

- de tipo **Screenshot**: sirve para identificar al dispositivo del target
- de tipo **Device**: permite saber si el entorno que se va a infectar es tranquilo o si existen aplicaciones que podrían comprometer la integridad del agent.



IMPORTANTE: la evidencia de tipo Screenshot solo se recopila si el módulo está activado en la configuración. Si es necesario, recuerde activarlo antes de enviar el agent.

Agent soldier

El agent soldier le permite recopilar evidencia definida por medio de los módulos de configuración básica, excepto para los módulos **Call** y **Accessed file**.



IMPORTANTE: la configuración avanzada no está activada para los agents soldier.



Sugerencia: una vez que se instale el agent soldier, verifique la configuración definida en la fase inicial para asegurarse de que cumple con las necesidades de la investigación y las características del agent.

Agent elite

El agent elite le permite recopilar todos los tipos de evidencia por medio de la configuración básica y la avanzada

Sincronización de agents

Un agent se sincronizará solo si:

- la sincronización está activada en la configuración básica
- una acción de tipo **Synchronize** se agregó a la configuración avanzada.

Agents en línea y sin conexión

Un agent se comporta de manera diferente de acuerdo con la disponibilidad de una conexión a Internet:

Si la conexión a Internet...

no está disponible si el agent tiene módulos activados, comienza a registrar datos en el dispositivo.

está disponible si el agent efectuó la primera sincronización, es posible:

- cambiar la configuración, por ejemplo, a medida que las solicitudes de registro se vuelvan más específicas para ese dispositivo. Si se cambia la configuración de un agent, la configuración de la factory no cambiará
- actualizar el software.
- transferir archivos hacia y desde el dispositivo.
- analizar la evidencia enviada.



Sugerencia: comience con la creación de un agent y active solo la sincronización y el módulo del dispositivo. Posteriormente, una vez instalado, y después de recibir la primera sincronización, active gradualmente otros módulos, de acuerdo con la capacidad del dispositivo y el tipo de evidencia que desea recopilar.

Desactive temporalmente un agent

Las actividades del agent pueden suspenderse temporalmente sin desinstalar el agent. Para ello simplemente desactive todos los módulos y deje solo la sincronización activa.

Prueba de un agent

Para probar la configuración antes del uso de la producción, cree un agent en modo de demostración (consulte "[Compilación de una factory](#)" En la página 34).

El agent se crea en modo *demostración*, se comporta de acuerdo con la configuración especificada, con la única diferencia de que señala su presencia en el dispositivo (con audio, LED y mensajes en pantalla). Ese señalamiento permite la identificación fácil de un dispositivo infectado que se usa para prueba.



NOTA: en caso de que no se reciba evidencia de un agent en modo de demostración, esto puede ocurrir debido a un error en la configuración del servidor o a que no es posible conectarse a la dirección del Collector establecido (p. ej.: debido a problemas de configuración de la red).

Configuración de agents

Es posible cambiar la configuración de los agents (básica o avanzada) varias veces. Al guardar, se crea una copia de la configuración que posteriormente se guarda en el registro de configuración.

En la siguiente sincronización, el agent recibirá la nueva configuración (**Hora de envío**) y comunicará la instalación correcta (**Activado**). A partir de ese momento, cualquier cambio solo podrá realizarse guardando una nueva configuración.



NOTA: si los valores **Hora de envío** y **Activado** no tienen ningún valor asignado, aún se podrá hacer cambios en la configuración actual.

Para ver una descripción del registro de configuración de los agents consulte "[Datos del registro de configuración de un agent](#)" En la página 43 .

Página del agent

Para administrar los
agents
:

- En la sección **Operations**, haga doble clic en una operation, luego en un target y luego en un agent

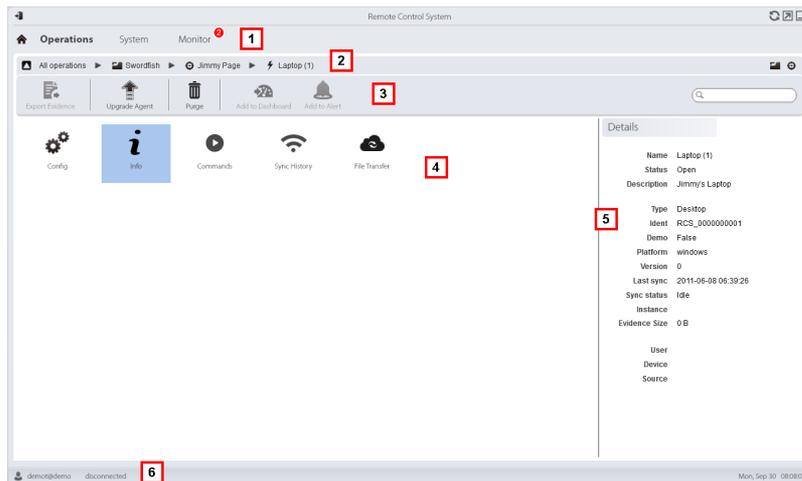
Propósito

Esta función le permite:

- verificar el registro de configuración de los agents y ver los detalles de cada configuración.
- transferir archivos hacia y desde el dispositivo del target
- importar y exportar la evidencia de un agent
- reemplazar el agent scout por un agent real (elite o soldier) y actualizar el software del agent
- mostrar los comandos ejecutados por el agent
- mostrar el historial de sincronización del agent

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación.
- 3 Barra de herramientas de la ventana.
A continuación se muestra la descripción de cada elemento:

Ícono Descripción



Envía el agent real (elite o soldier) al agent scout o actualiza el software del agent con la última versión que recibió de HackingTeam.



PRECAUCIÓN: la actualización no modificará la configuración que se transmitirá al agent en la siguiente sincronización.



IMPORTANTE: para Android, para actualizar el agent deben obtenerse privilegios raíz. Consulte "[Qué debería saber acerca de Android](#)" En la página 158 .



Elimina la evidencia en el dispositivo que aún no se transmitió a RCS.
Parámetros:

- **Fecha:** elimina la evidencia guardada antes de la fecha especificada.
- **Dimensión:** elimina la evidencia con un tamaño mayor al especificado.

Área Descripción

- 4 Posibles acciones en el agent. A continuación se muestra la descripción de cada elemento:

Ícono Descripción

-  Muestra el registro de configuración del agent, lo cual permite editar y guardar la configuración existente como una configuración nueva. Consulte "[Datos del registro de configuración de un agent](#)" abajo .
 -  Muestra el registro de eventos del agent (información). Consulte "[Datos de registro de los eventos de un agent](#)" En la página siguiente
 -  Muestra los resultados de los comandos ejecutados en el dispositivo mediante las acciones **Execute**. Consulte "[Página de comandos](#)" En la página 45 .
 -  Muestra el registro de sincronización del agent. Consulte "[Datos del registro de sincronización de un agent](#)" En la página siguiente .
 -  Abre la función para cargar o descargar archivos desde el dispositivo del target. Consulte "[Transferencia de archivos hacia y desde el target](#)" En la página 46
- 5 Detalles del agent.
- 6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz Consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para obtener más información sobre los agents consulte "[Qué debería saber acerca de los agents](#)" En la página 38 .

Datos del registro de configuración de un agent

A continuación se muestra la descripción de cada elemento:

Campo	Descripción
Descripción	Descripción de la configuración hecha por el usuario.
Usuario	Nombre del usuario que creó la configuración.
Guardada	Fecha en que se guardó la configuración.

<i>Campo</i>	<i>Descripción</i>
Hora de envío	Fecha en que se envió la configuración por medio de una sincronización.  ADVERTENCIA: si este valor es nulo, el agent aún no recibió la configuración.
Activado	Fecha de instalación de la nueva configuración en el agent.

Datos de registro de los eventos de un agent

A continuación se muestra la descripción de cada elemento:

<i>Campo</i>	<i>Descripción</i>
Obtención	Fecha y hora del evento obtenido en el dispositivo. Puede filtrarse. Últimas 24 horas es el valor predeterminado.
Recepción	Fecha y hora del evento registrado en RCS. Puede filtrarse. Últimas 24 horas es el valor predeterminado.
Contenido	Información de estado enviada por el agent.

Datos del registro de sincronización de un agent

A continuación se muestra la descripción de cada elemento:

<i>Campo</i>	<i>Descripción</i>
Fin de sincronización	Fecha y hora en que terminó la sincronización. Puede filtrarse. Últimas 24 horas es el valor predeterminado.
Inicio de sincronización	Fecha y hora en que se inició la sincronización.
IP	Dirección IP usada para la sincronización.
Evidencia	Número de piezas de evidencia que se transfirieron realmente en esa sincronización de la cantidad total de piezas de evidencia que se deben transferir.
Tamaño	El tamaño total de la evidencia transferida.
Velocidad	Velocidad de transferencia.
Expiró	Indica que la sincronización expiró.

Página de comandos

Para administrar los resultados de los comandos:

- En la sección **Operations**, haga doble clic en una operation, luego en un target, en un agent y en **Comandos**

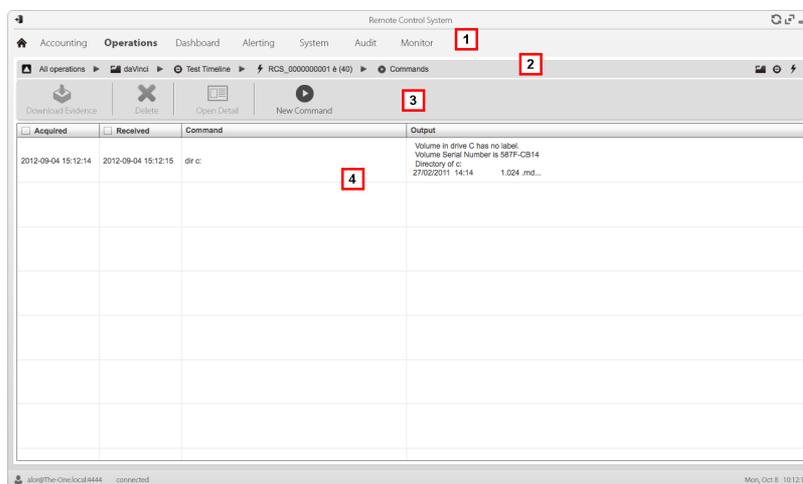
Propósito

Esta función le permite:

- verificar los resultados de los comandos ejecutados con la acción **Execute** establecida en el agent
- verificar los resultados del archivo ejecutable que se abre durante la transferencia de archivos hacia o desde el agent
- ejecutar uno o más comandos en un agent

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación.

Área Descripción

- 3 Barra de herramientas de la ventana.
A continuación se muestra la descripción de cada elemento:

Ícono Descripción



Permite exportar el comando seleccionado a un archivo .txt.



Muestra los detalles de los comandos seleccionados.



Abre una ventana para ingresar una o más cadenas de comandos. Todos los comandos se envían al agente en la siguiente sincronización y los resultados se muestran la siguiente vez que se reciben datos.



NOTA: la función solo se activa si el usuario tiene autorización **Ejecutar comandos en un agente**.

- 5 Lista de comandos basada en los filtros establecidos.
6 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Transferencia de archivos hacia y desde el target

Para transferir archivos hacia y desde el agente:

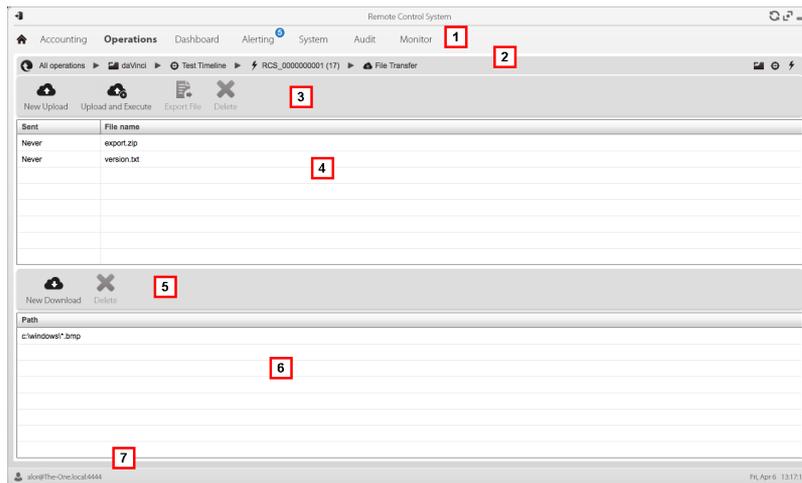
- En la sección **Operations**, haga doble clic en una operation, luego en un target, en un agent y en **Transferencia de archivos**

Propósito

Permite cargar y descargar archivos del dispositivo donde se instaló el agente.

Cómo se ve la función

Así es como se ve la función de transferencia de archivos hacia y desde el target:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación de la operation.

Área Descripción

- 3** Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono Descripción



Permite cargar un archivo al dispositivo, en la carpeta donde se instaló el agent. Cada carga exitosa se registra con la fecha y la hora, y el nombre de archivo.



NOTA: la función solo se activa si el usuario tiene autorización **Cargar archivo para agent**.



Permite cargar un archivo ejecutable en la carpeta del dispositivo donde se instaló el agent y ejecutarlo (usando **Execute**). Los resultados de la ejecución aparecen en la página **Comandos**. Consulte "[Página de comandos](#)" En la página 45 .

Cada carga exitosa se registra con la fecha y la hora, y el nombre de archivo.



IMPORTANTE: esta función puede inhibirse si el usuario no tiene los permisos correspondientes o no está permitida según la licencia de usuario.



Permite exportar el registro de cargas.



Elimina la carga seleccionada. Se guardarán los resultados del comando eliminado.

- 4** Registro de carga, con barra de herramientas.

- 5** Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono Descripción



Permite descargar un archivo desde un dispositivo. Se debe indicar el nombre del archivo y la ruta. Cada descarga exitosa se registra con el nombre del archivo completo con la ruta.

El archivo se guarda en la carpeta RCS Download en el escritorio.



Elimina el archivo seleccionado de la carpeta RCS Download.

- 6** Registro de descarga, con barra de herramientas.

- 7** Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para ver una descripción de los datos de los agents consulte "[Página del agent](#)" En la página 41 .

Factory y agent: configuración básica

Presentación

Introducción

La configuración básica le permite agregar módulos de obtención de datos y de ejecución de comandos simples que no requieren una configuración compleja.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de la configuración básica	51
Configuración básica de una factory o un agent	52
Datos de la configuración básica	55

Qué debería saber acerca de la configuración básica

Configuración básica

La configuración básica de una factory o un agent le permite activar y establecer rápidamente los valores para la obtención de evidencia.

La configuración básica no incluye la obtención de algunos tipos de evidencia ni las opciones detalladas de los métodos de obtención.

Configuración básica predeterminada:

- Obtención de información del sistema cuando el dispositivo está apagado (no se puede desactivar)
- Un módulo para la ejecución de la sincronización entre el agent y RCS cada cierto intervalo de tiempo.

Para ver la lista de tipos de módulos disponibles en la configuración básica consulte "[Datos de la configuración básica](#)" En la página 55 .



PRECAUCIÓN: cuando vuelva a la configuración básica desde la avanzada, se perderá la configuración avanzada y se restaurará la configuración básica predeterminada.

Exportar e importar las opciones de configuración

Es posible exportar o importar las opciones de configuración básica o avanzada para utilizarlas en otros sistemas RCS.

Las opciones de configuración básica o avanzada se exportan a un archivo .json, que se puede transferir a otro sistema e importar cuando se crea un agent.

Guardar la configuración como una plantilla

Las opciones de configuración básica o avanzada se guardan como una plantilla para que otros usuarios del mismo sistema RCS puedan volver a utilizarla.

Las opciones de configuración básica o avanzada se guardan como plantilla en la base de datos, junto con una descripción y el nombre del usuario. Al crear otro target, otro usuario puede cargarla y usarla como la configuración de ese agent.



IMPORTANTE: las plantillas de configuración básica y avanzada se guardan por separado en la base de datos. Las plantillas de configuración básica aparecen de este modo al crear un agent con una configuración básica, y lo mismo ocurre con las plantillas de configuración avanzada.

Configuración básica de una factory o un agent

Para configurar las opciones de las factories y los agents:

- En la sección **Operations**, haga doble clic en una operation, luego en un target y en una factory
- En la sección **Operations**, haga doble clic en una operation, luego en un target y en un agent

Propósito

Esta función le permite:

- configurar una factory o un agent para indicar si se requiere una sincronización en línea y definir los datos que se obtendrán
- abrir la función de compilación de una factory (*consulte "[Compilación de una factory](#)" En la página 34* .
- abrir la función de configuración avanzada (*consulte "[Configuración avanzada de una factory o un agent](#)" En la página 62*)



NOTA: la función solo se activa si el usuario tiene autorización **Configuración de agents**.

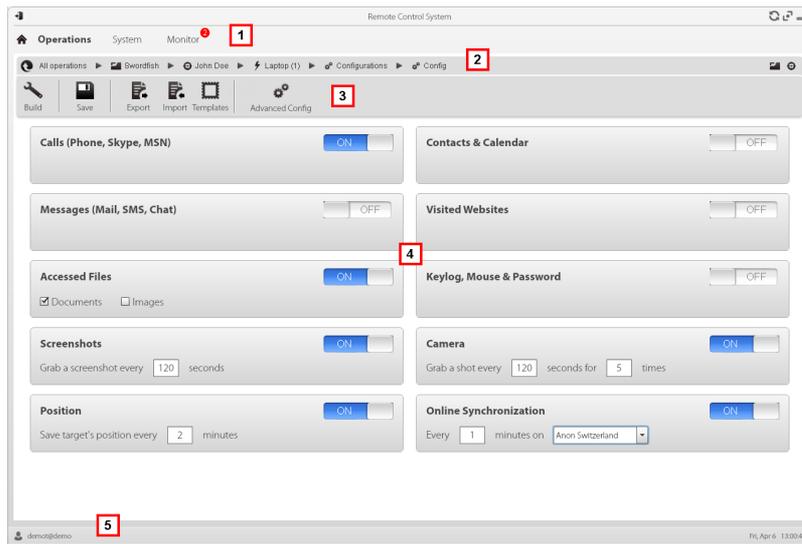
Próximos pasos

Después de establecer la configuración de una factory, se debe compilar para poder obtener un agent.

Después de cambiar la configuración del agent, simplemente guárdela. Si el agent está en línea, la nueva configuración se aplicará en la siguiente sincronización. De lo contrario, se requiere una instalación física.

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación.

Área Descripción

- 3 Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono Descripción

- | Ícono | Descripción |
|---|---|
|  | Compila la configuración en uno o más agents que se instalarán en base a los vectores de instalación seleccionados. Consulte " Compilación de una factory " En la página 34 |
|  | Guardar la configuración: la configuración del agent se registra y se envía al agent en la siguiente sincronización. Consulte " Datos del registro de configuración de un agent " En la página 43 |
|  | Exporta la configuración a un archivo .json. |
|  | Importa la configuración desde un archivo .json. |
|  | Permite cargar la plantilla de configuración básica o guardar la configuración actual como plantilla. Consulte " Qué debería saber acerca de la configuración básica " En la página 51 . |
|  | Abre la ventana de configuración avanzada. Consulte " Configuración avanzada de una factory o un agent " En la página 62 . |
|  | PRECAUCIÓN: cuando vuelva a la configuración básica desde la avanzada, se perderá la configuración avanzada y se restaurará la configuración básica. |

- 4 Lista de tipos de evidencia disponibles y estado de activación relacionado.



NOTA: la lista de módulos varía de acuerdo con el tipo de dispositivo.

- 5 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz Consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para obtener más información acerca de la configuración básica, consulte "[Qué debería saber acerca de la configuración básica](#)" En la página 51 .

Para ver una descripción de los datos en esta ventana consulte "[Datos de la configuración básica](#)" En la página siguiente .

Para ver una lista de los módulos disponibles en las dos configuraciones consulte "[Lista de módulos](#)" En la página 143

Configurar una factory o un agent

Para activar o desactivar la recopilación de evidencia:

Paso Acción

- 1
 - Haga clic en **OFF** para la evidencia a obtener: el botón cambia a **ON** y las opciones de configuración, cuando están disponibles, pueden establecerse.
- 2
 - En **Sincronización el línea** deje **ON** si el dispositivo del target puede acceder a Internet. Esto le permite establecer opciones gradualmente. Deje **OFF** si el dispositivo del target no puede acceder a Internet o si desea obtener evidencia del target de forma manual.
 - Haga clic en **Guardar** para guardar la configuración actual.

- 3 Continuar de modo diferente:

*Si está con-
figurando...*

Entonces...

una factory

haga clic en **Crear** para compilarla y obtener agents para las diferentes plataformas. Consulte "[Compilación de una factory](#)" En la página 34 .

un agent

las opciones de configuración de un agent se actualizan automáticamente en la siguiente sincronización.

Datos de la configuración básica

A continuación se muestran los tipos de evidencia que pueden activarse en la configuración básica de una factory o un agent.

<i>Grabación</i>	<i>Descripción</i>
Calls	Graba llamadas.  NOTA: no está disponible para los agents de nivel soldier.
Messages	Registra mensajes.

Grabación	Descripción
Accessed files	<p>(solo en computadoras de escritorio) Registra los documentos o imágenes que abrió el target. Documentos, imágenes: tipos de archivo.</p> <p> NOTA: no está disponible para los agents de nivel soldier.</p>
Screenshots	<p>Registra las ventanas abiertas en la pantalla del target. Imagen cada: intervalo de captura de imagen.</p>
Position	<p>Registra la posición geográfica del target. Guardar la posición del target cada: intervalo de obtención de la posición.</p>
Contacts & Calendar	<p>Registra los contactos.</p>
Visited websites	<p>Registra las direcciones URL de los sitios web visitados.</p>
Keylog	<p>(solo dispositivos móviles) Registra las teclas presionadas.</p>
Keylog, Mouse & Password	<p>(solo computadoras de escritorio) Registra las teclas presionadas, las contraseñas guardadas en el sistema y los clics hechos con el mouse.</p>
Camera	<p>Graba imágenes de la cámara web. Capturar imagen cada: intervalo de obtención de imagen. por...veces: repeticiones de la obtención.</p>
Online Synchronization	<p>Activado de forma predeterminada. Si está activado, el agent se comunica con el servidor para enviar datos y recibe nuevas configuraciones, actualizaciones, etc. Cada: intervalo de sincronización minutos en: nombre o dirección IP del Anonymizer o del Collector. El nombre o la dirección IP se pueden ingresar manualmente.</p>

Factory y agent: configuración avanzada

Presentación

Introducción

La configuración avanzada le permite ajustar los parámetros de configuración avanzada. Además de activar la recopilación de evidencia, los eventos pueden estar vinculados a las acciones, para activar reacciones específicas del agent y cambiar ciertas condiciones en el dispositivo (p. ej., se inicia el protector de pantalla). Las acciones pueden iniciar o detener los módulos y activar o desactivar otros eventos. Asimismo, todas las opciones de los eventos, acciones y módulos pueden establecerse de forma individual.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de la configuración avanzada	58
Configuración avanzada de una factory o un agent	62
Datos globales del agent	66

Qué debería saber acerca de la configuración avanzada

Configuración avanzada

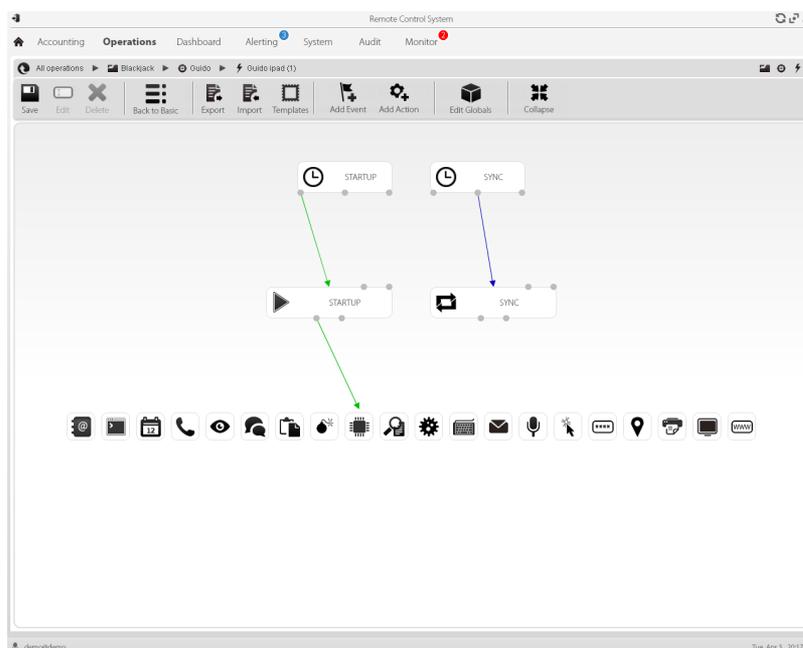
La configuración avanzada de una factory/agent le permite crear secuencias de activación complejas utilizando una sola interfaz gráfica.

El propósito de la secuencia es iniciar/detener la recopilación de evidencia y/o ejecutar una acción cuando ocurre un evento.

La configuración avanzada siempre incluye dos secuencias básicas:

- En cada sincronización (evento en ciclo repetitivo), se obtiene información del dispositivo (acción Iniciar módulo + módulo Dispositivo)
- Al final del intervalo de sincronización (el evento temporizador-ciclo repetitivo), se ejecuta la sincronización entre el agent y RCS (acción Synchronize)

A continuación se muestra una imagen que ilustra las dos secuencias básicas recomendadas para la obtención remota de datos:



NOTA: estas dos secuencias básicas se establecen de forma predeterminada y se recomiendan para el funcionamiento mínimo del agent.

Componentes de configuración avanzada

Los componentes de configuración avanzada son:

- los *eventos* que activan una acción (p. ej.: se recibe una llamada en el dispositivo)
- las *acciones* que se ejecutan cuando ocurre un evento (p. ej.: se comienza a grabar la llamada)
- las *subacciones* que se ejecutan cuando ocurre un evento (p. ej.: se envían mensajes SMS ocultos con la posición del dispositivo)
- los *módulos* que, al activarse por una acción, comienzan a recopilar la evidencia deseada o activan otras acciones en el dispositivo (p. ej.: grabación del audio de una llamada)
- las *secuencias* que se usan para indicar un grupo de eventos, acciones, subacciones y módulos.



NOTA: algunas opciones de eventos, acciones y módulos solo están disponibles en la configuración avanzada.

Lectura de secuencias

Se pueden leer secuencias complejas de esta forma:

- Cuando el dispositivo se conecta a la fuente de energía (evento)...
- ...envía un SMS (subacción) y...
- ...comienza a registrar la posición (acción que activa un módulo) y...
- ...desactiva el evento que ocurre cuando se cambia la tarjeta SIM (acción que desactiva un evento)
- ...y así sucesivamente

Las posibles combinaciones de eventos, acciones, subacciones y módulos son infinitas. A continuación se detalla una explicación de las reglas de diseño correctas.

Eventos

Los eventos son monitoreados por el agent y pueden iniciar, repetir o terminar una acción.



NOTA: un evento no puede iniciar un módulo directamente.

Por ejemplo, un evento **Window** (ventana abierta en el dispositivo) puede activar una acción. La acción entonces iniciará o detendrá un módulo.

Hay varios tipos de eventos disponibles. Para ver una lista completa consulte "[Lista de eventos](#)" En la página 134.

La relación entre un evento y una o más acciones se representa por medio de un conector:

<i>Relación entre eventos y acciones</i>	<i>Descripción</i>	<i>Conector</i>
Iniciar	Inicia una acción cuando ocurre un evento.	

<i>Relación entre eventos y acciones</i>	<i>Descripción</i>	<i>Conector</i>
Repetir	Repite una acción. Se puede especificar el intervalo y el número de repeticiones.	
Terminar	Inicia una acción cuando el evento termina.	



NOTA: un evento puede manejar hasta tres acciones distintas simultáneamente. La acción **Iniciar** se activa cuando ocurre un evento en el dispositivo (p. ej.: el evento **Standby** activa **Iniciar** cuando el dispositivo ingresa en modo de espera). La acción **Repetir** se activa en el intervalo establecido para toda la duración del evento. La acción **Detener** se activa cuando un evento termina (p. ej.: el evento **StandBy** activa **Terminar** cuando el dispositivo sale del modo de espera).

Acciones

Las acciones se activan cuando ocurre un evento. Pueden:

- iniciar o detener un módulo
- activar o desactivar un evento
- ejecutar una subacción

Por ejemplo, una acción (vacía) puede desactivar el evento **Proceso** (iniciar un proceso del sistema) que lo activó y activar el módulo **Position** (registrar la posición GPS). En caso de ser necesario, la acción también puede ejecutar una subacción **SMS** (enviar un mensaje a un número de teléfono especificado).

Existen varias *subacciones* disponibles que se pueden combinar sin restricciones (p. ej.: ejecutar un comando + crear un mensaje de alerta). Para ver una lista completa *consulte "Lista de subacciones" En la página 127*

Relaciones entre las acciones y los módulos

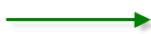
Una acción puede influir en un módulo de diferentes formas. La relación entre una acción y uno o más módulos se representa por medio de un conector:

<i>Relaciones entre las acciones y los módulos</i>	<i>Descripción</i>	<i>Conector</i>
Iniciar módulos	Inicia un módulo.	
Detener módulos	Detiene un módulo.	

Una acción puede iniciar o detener varios módulos simultáneamente.

Relaciones entre las acciones y los eventos

La relación entre una acción y uno o más eventos se representa por medio de un conector:

<i>Relación entre las acciones y los eventos</i>	<i>Descripción</i>	<i>Conector</i>
Activar eventos	Activa un evento.	
Desactivar eventos	Desactiva un evento.	



NOTA: una acción puede activar o desactivar varios eventos simultáneamente.

Módulos

Cada módulo activa la recopilación de una evidencia específica de un dispositivo del target. Una acción puede iniciarlos o detenerlos y producen evidencia.

Por ejemplo, una acción activada por un evento **Call** (se hizo o se recibió una llamada) puede iniciar un módulo **Position** (registra la posición GPS).

Existen varios módulos disponibles que pueden iniciarse y detenerse (p. ej.: iniciar módulo de posición + detener módulo de imagen de pantalla). Para ver una lista completa consulte "[Lista de módulos](#)" En la página 143 .

Exportar e importar las opciones de configuración

Es posible exportar o importar las opciones de configuración básica o avanzada para utilizarlas en otros sistemas RCS.

Las opciones de configuración básica o avanzada se exportan a un archivo .json, que se puede transferir a otro sistema e importar cuando se crea un agent.

Guardar la configuración como una plantilla

Las opciones de configuración básica o avanzada se guardan como una plantilla para que otros usuarios del mismo sistema RCS puedan volver a utilizarla.

Las opciones de configuración básica o avanzada se guardan como plantilla en la base de datos, junto con una descripción y el nombre del usuario. Al crear otro target, otro usuario puede cargarla y usarla como la configuración de ese agent.



IMPORTANTE: las plantillas de configuración básica y avanzada se guardan por separado en la base de datos. Las plantillas de configuración básica aparecen de este modo al crear un agent con una configuración básica, y lo mismo ocurre con las plantillas de configuración avanzada.

Configuración avanzada de una factory o un agent

Para abrir la configuración avanzada:

- En la sección **Operations**, haga doble clic en una operation, luego en un target, en una factory y por último haga clic en **Config. avanzada**
- En la sección **Operations**, haga doble clic en una operation, en un target, en un agent y haga clic en **Config. avanzada**

Propósito

Esta función le permite:

- crear secuencias de activación de módulos activados por eventos que ocurren en el dispositivo del target. Cada secuencia puede estar compuesta de una o más subacciones.
- Establecer las opciones generales de configuración de una factory o un agent.



NOTA: la función solo se activa si el usuario tiene autorización **Configuración de agents** .



NOTA: la configuración avanzada no está disponible para los agents de nivel soldier.



PRECAUCIÓN: cuando vuelva a la configuración básica desde la avanzada, se perderá la configuración avanzada y se restaurará la configuración básica predeterminada.

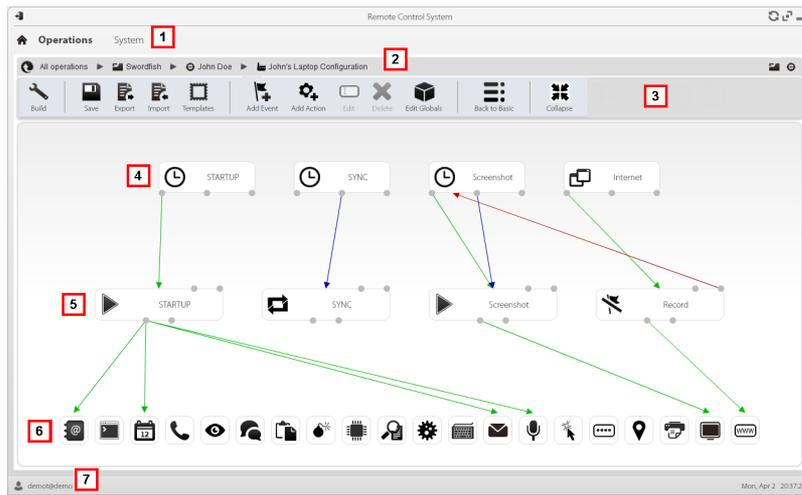
Próximos pasos

Para una factory, después de completar su configuración, compile para que el agent se instale. Consulte "[Compilación de una factory](#)" En la página 34

Para un agent, después de completar su configuración, simplemente guarde la nueva configuración. En la siguiente sincronización, la nueva configuración se enviará al agent.

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Barra de navegación.

Área Descripción

- 3 Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono Descripción

 Compila la configuración en uno o más agents, en base a los vectores de instalación seleccionados. Consulte "[Compilación de una factory](#)" En la página 34

 Guarda la configuración actual.

 Exporta la configuración a un archivo .json.

 Importa la configuración desde un archivo .json.

 Permite cargar la plantilla de configuración avanzada o guarda la configuración actual como plantilla.
Consulte "[Qué debería saber acerca de la configuración avanzada](#)" En la página 58 .

 Permite agregar un evento.

 Permite agregar una acción.

 Permite edita el evento o la acción seleccionada.

 Elimina el evento, acción o conexión lógica.

 Edita los datos globales del agent consulte "[Datos globales del agent](#)" En la página 66 .

 **PRECAUCIÓN:** cuando regresa a la configuración básica se pierden todos los datos.

 Contrae o expande los widgets de las acciones o eventos para para poder ver mejor la configuración actual.



- 4 Área de eventos. Los eventos **STARTUP** y **SYNC** son predeterminados.
- 5 Área de acciones. Las acciones **STARTUP** y **SYNC** son predeterminadas.

Área Descripción

- 6 Área de módulos. Los módulos cambian en base al dispositivo de escritorio o móvil.
- 7 Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para obtener más información acerca de la configuración avanzada, consulte "[Qué debería saber acerca de la configuración avanzada](#)" En la página 58 .

Creación de una secuencia de activación simple

Para crear una secuencia simple o recopilar evidencia cuando ocurre un evento:

Paso Acción

- 1 Crear un evento:
 - Haga clic en **Agregar evento**: se abrirá la ventana de selección y configuración del evento.
 - En **Tipo**, seleccione el tipo de evento y establezca las opciones. Consulte "[Lista de eventos](#)" En la página 134
 - Haga clic en **Guardar**: el nuevo evento se agregará al área de trabajo
- 2 Crear una acción:
 - Haga clic en **Agregar acción**: la acción vacía se agregará al área de trabajo
- 3 Vincule el evento a la acción, luego vincule la acción al módulo deseado:
 - Haga clic en el punto de conexión **Iniciar** del evento, luego arrastre la flecha a la acción
 - Haga clic en el punto de conexión **Iniciar módulos**, luego arrastre la flecha al tipo de datos que desea obtener. Consulte "[Lista de módulos](#)" En la página 143 .
- 4 Haga clic en **Guardar**: la configuración está lista para ser compilada (si es una factory) o transmitida al dispositivo en la siguiente sincronización (si es un agent).

Crear una secuencia de activación compleja

Para crear una secuencia compleja, o bien, cuando ocurre un evento, para comenzar a recopilar evidencia, ejecutar una subacción y activar o desactivar un evento:

Paso Acción

- 1 Crear un evento:
 - Haga clic en **Agregar evento**: se abrirá la ventana de selección y configuración del evento.
 - En **Tipo**, seleccione el tipo de evento y establezca las opciones. *Consulte "[Lista de eventos](#)" En la página 134*
 - Haga clic en **Guardar**: el nuevo evento se agregará al área de trabajo
- 2 Crear una acción y definir las subacciones:
 - Haga clic en **Agregar acción**: la acción vacía se agregará al área de trabajo
 - Haga doble clic en la acción, agregue la subacción en **Subacción** y configure las opciones. *Consulte "[Lista de subacciones](#)" En la página 127 .*
- 3 Conectar el evento a la acción:
 - Haga clic en uno de los puntos de conexión **Iniciar, Repetir, Terminar** del evento, luego arrastre la flecha a la acción
- 4 Conectar la acción al módulo:
 - Haga clic en los puntos de conexión **Iniciar módulos , Detener módulos** de la acción, luego arrastre la flecha al módulo que desea iniciar o detener. *Consulte "[Lista de módulos](#)" En la página 143 .*



Sugerencia: Arrastre varias flechas si se deben activar varios módulos.

Para una acción que requiere un evento para activarse o desactivarse:

- Haga clic en los puntos de conexión **Activar eventos o Desactivar eventos** en la acción, luego arrastre la flecha a los eventos que desea activar o desactivar.
- 5 Haga clic en **Guardar**: la configuración está lista para ser compilada (si es una factory) o transmitida al dispositivo en la siguiente sincronización (si es un agent).

Datos globales del agent

A continuación se muestran los datos globales del agent:

<i>Campo</i>	<i>Descripción</i>
Mínimo espacio en el disco	Espacio libre mínimo en el disco del dispositivo.

Campo	Descripción
Tamaño máximo de las evidencias	<p>Espacio máximo ocupado por la evidencia en el dispositivo del target, hasta la siguiente sincronización. De manera predeterminada: 1 GB.</p> <p>Cuando se alcanza ese límite, el agent deja de grabar y espera la siguiente sincronización. Si no ocurre ninguna sincronización, no se obtiene más evidencia.</p>
Eliminación segura de un agent	<p>Si está activado, elimina los archivos generados por el agent. En caso de un análisis forense, no quedará ningún rastro del agent.</p> <p> NOTA: este método demora más en completarse que una eliminación normal de archivos.</p>
Eliminación de un controlador	<p>Elimina el controlador al desinstalar.</p>
Mostrar	<p> <i>Llamada al servicio: solo se utiliza cuando el servicio de soporte técnico de HackingTeam lo solicita.</i></p>
Máscara	<p> <i>Llamada al servicio: solo se utiliza cuando el servicio de soporte técnico de HackingTeam lo solicita.</i></p>

El Network Injector

Presentación

Introducción

El Network Injector le permite interceptar las conexiones HTTP del target e inyectar a un agent en el dispositivo.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca del Network Injector y sus reglas	69
Administración de los Network Injector	70
Datos de la regla de inyección	73
Verifique el estado del Network Injector	79
Qué debería saber acerca de Appliance Control Center	79
Qué debería saber acerca de Tactical Control Center	82
Qué debería saber acerca de la identificación de contraseñas de redes Wi-Fi	86
Qué debería saber acerca del desbloqueo de las contraseñas del sistema operativo	88
Qué debería saber acerca del acceso remoto al Control Center	89
Comandos de Tactical Control Center y Appliance Control Center	91
Appliance Control Center	92
Datos de Appliance Control Center	99
Tactical Control Center	100
Datos del Tactical Control Center	117
Otras aplicaciones instaladas en Network Injectors	119

Qué debería saber acerca del Network Injector y sus reglas

Introducción

Network Injector monitorea todas las conexiones HTTP y, siguiendo las reglas de inyección, identifica las conexiones del target e inyecta el agent en las conexiones, vinculándolo a los recursos que el target está descargando de Internet.

Tipos de Network Injectors

Existen dos tipos de Network Injector:

- Appliance: servidor de red para instalaciones en un segmento interno al conmutador en un proveedor de servicios de Internet.
- Tactical: computadora portátil para instalaciones tácticas en redes Wi-Fi o LAN, y para desbloquear la contraseña del sistema operativo para infecciones físicas (ej.: a través de Silent Installer)

Ambos Network Injectors le permiten identificar automáticamente los dispositivos del target e infectarlos de acuerdo con las reglas establecidas a través del software de control (Appliance Control Center o Tactical Control Center). Tactical Network Injectors también permite la identificación manual. Consulte "[Qué debería saber acerca de Appliance Control Center](#)" En la página 79 , "[Qué debería saber acerca de Tactical Control Center](#)" En la página 82

Tipos de recursos que pueden ser infectados

Los recursos que RCS puede infectar son archivos de cualquier tipo.



NOTA: Network Injector no puede monitorear conexiones FTP o HTTPS.

Cómo crear una regla

Para crear una regla:

1. defina la forma de identificar las conexiones del target. Por ejemplo, comparando la dirección IP o MAC del target. O deje que el operador de Tactical Network Injector seleccione el dispositivo.
2. defina la forma de infectar al target. Por ejemplo, reemplazando un archivo que el target está descargando desde Internet o infectando un sitio web que el target usualmente visita.

Reglas de identificación automática o manual

Si se conoce alguna información de los dispositivos del target, se pueden crear varias reglas, adaptarlas a los diferentes hábitos del target, luego activar las reglas más eficientes de acuerdo con las situaciones que surjan durante un momento particular de la investigación.

Si no se conoce ninguna información sobre los dispositivos del target, use el Tactical Network Injector, el cual les permitirá a los operadores observar el target, identificar el dispositivo usado e infectarlo.

TACTICAL debe ser el valor en el campo **Patrón** de la regla de inyección para este tipo de control manual.

Qué sucede cuando una regla está activada/desactivada

RCS se comunica regularmente con el Network Injector para enviarle las reglas y obtener registros. Todas las reglas activadas en RCS Console se envían automáticamente a los Network Injectors. Las reglas desactivada se guardarán, pero no se enviarán ni estarán disponible en la siguiente sincronización.

Seleccione una de las reglas disponibles para activar una inyección específica en un Network Injector.

Inicio de la infección

Después de que Network Injector recibe las reglas de infección, está listo para iniciar un ataque.

Durante la fase de análisis de paquetes, verifica si alguno de los dispositivos en la red cumple con las reglas de identificación. En ese caso, envía al agent al dispositivo identificado y lo infecta.

Administración de los Network Injector

Para administrar los Network Injectors:

- Sección System , Network Injectors

Propósito

Cuando RCS está en funcionamiento, esta función le permite crear reglas de inyección y enviarlas al Network Injector.



NOTA: la función está activada solo si el usuario tiene autorización **Administración de redes de Network Injector** .

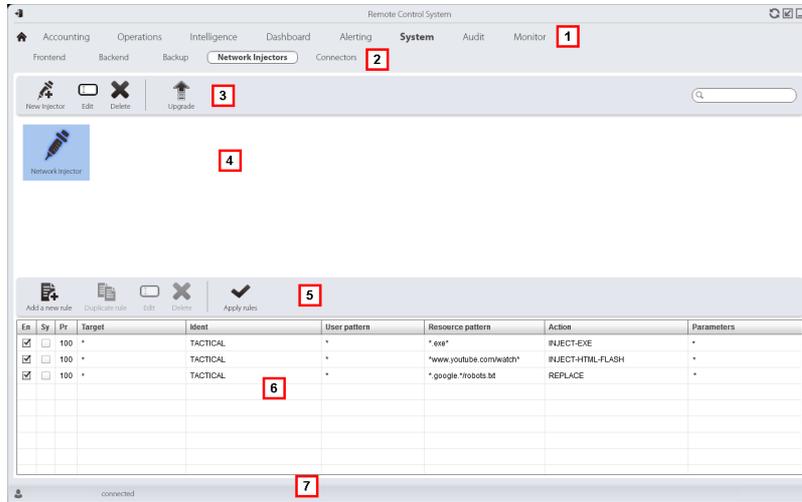
Qué puede hacer

Con esta función usted puede:

- crear una regla de inyección de un agent en un target
- enviar las reglas al Network Injector

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Menú de RCS.
- 2 Menú **System**.
- 3 Barra de herramientas del Network Injector.
- 4 Lista de Network Injectors.

Área Descripción

- 5 Barra de herramientas de inyección.
A continuación se muestra la descripción de cada elemento:

Acción Descripción



Agrega una regla nueva.



Copia la regla de conexión.



Abre la ventana con los datos de la regla.



Elimina la regla de conexión.



Envía reglas al Network Injector seleccionado. Appliance actualiza automáticamente la siguiente sincronización siempre que haya un proceso de infección activo. Mientras que con Tactical es el operador quien decide si las reglas deben actualizarse o no.

- 6 Lista de reglas del Network Injector seleccionado
7 Barra de estado de RCS. .

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para ver una descripción de los datos de las reglas de inyección consulte "[Datos de la regla de inyección](#)" En la página siguiente .

Para obtener más información en las reglas de inyección consulte "[Qué debería saber acerca del Network Injector y sus reglas](#)" En la página 69 .

Agregar una nueva regla de inyección

Para agregar una nueva regla:

Paso Acción

- 1 Seleccione el Network Injector para la nueva regla: se mostrarán los comandos de reglas y la tabla.

Paso Acción

- 2
 - Haga clic en **Nueva regla**: aparecerán los campos para ingresar datos.
 - Ingrese los datos solicitados. Si la regla está activada, se puede enviar al Network Injector. Consulte "[Datos de la regla de inyección](#)" abajo .
 - Haga clic en **Guardar**: aparecerá la nueva regla en el área de trabajo principal.

Enviar las reglas al Network Injector

Para enviar las reglas al Network Injector:

Paso Acción

- 1 Active la regla que se enviará al Network Injector. Para eso seleccione el cuadro de verificación **En** en la tabla.
- 2 Haga clic en **Aplicar reglas**: RCS recibe la solicitud para enviar las reglas al Network Injector seleccionado. La barra de progreso en el área de descarga muestra el progreso de la operación.



NOTA: Network Injector solo recibe las reglas actualizadas cuando se sincroniza con RCS server. Consulte "[Verifique el estado del Network Injector](#)" En la página 79 .

Datos de la regla de inyección

A continuación se describen los datos que definen las regla de infección disponibles:

Datos	Descripción
Activado	Si está seleccionado, la regla será enviada al Network Injector. Si no está seleccionado, la regla se guardará pero no será enviada.
Desactivar al sincronizar	Si está seleccionado, la regla se desactiva después de la primera sincronización del agent definido en la regla. Si no está seleccionado, el Network Injector continúa aplicando la regla, aun después de la primera sincronización.

<i>Datos</i>	<i>Descripción</i>
Probabilidad	<p>Probabilidad (en porcentaje) de aplicar la regla después del primer recurso infectado.</p> <p>0 %: después de infectar el primer recurso, el Network Injector ya no aplicará esta regla.</p> <p>100 %: después de infectar el primer recurso, el Network Injector siempre aplicará esta regla.</p> <p> Sugerencia: si se selecciona un valor mayor a 50 %, le recomendamos usar la opción Desactivar al sincronizar.</p>
Target	Nombre del target que se va a infectar.

<i>Datos</i>	<i>Descripción</i>
--------------	--------------------

Ident	Método de identificación de la conexión HTTP del target.
--------------	--



NOTA: Network Injector no puede monitorear conexiones FTP o HTTPS.

A continuación se describe cada método:

<i>Datos</i>	<i>Descripción</i>
STATIC-IP	IP estática asignada al target.
STATIC-RANGE	Rango de direcciones IP asignadas al target.
STATIC-MAC	Dirección MAC estática del target, tanto Ethernet como Wi-Fi.
DHCP	Dirección MAC de la interfaz de red del target.
RADIUS-LOGIN	Nombre de usuario RADIUS. User-Name (RADIUS 802.1x).
RADIUS-CALLID	Identificador de llamadas RADIUS. Calling-Station-Id (RADIUS 802.1x).
RADIUS-SESSID	Identificador de sesión RADIUS. Acct-Session-Id (RADIUS 802.1x).
RADIUS-TECHKEY	Clave RADIUS. NAS-IP-Address: Acct-Session-Id (RADIUS 802.1x).
STRING-CLIENT	Cadena de texto a identificar en el tráfico de datos desde el target.
STRING-SERVER	Cadena de texto a identificar en el tráfico de datos hacia el target.
TACTICAL	EL target no es identificado automáticamente pero puede ser identificado por el operador en Tactical Network Injector. Solo cuando el operador identifica el dispositivo, el campo Ident se personaliza con los datos recibidos de este.

<i>Datos</i>	<i>Descripción</i>																								
Patrón	Forma de identificación del tráfico del target. El formato depende del tipo de Ident seleccionado.																								
	<table border="1"> <thead> <tr> <th><i>Método</i></th> <th><i>Formato</i></th> </tr> </thead> <tbody> <tr> <td>DHCP</td> <td>Dirección correspondiente (p. ej.: "195.162.21.2").</td> </tr> <tr> <td>STATIC-IP</td> <td></td> </tr> <tr> <td>STATIC-MAC</td> <td></td> </tr> <tr> <td>STATIC-RANGE</td> <td>Rango de direcciones separado por '-' (p. ej.: "195.162.21.2-195.162.21.5").</td> </tr> <tr> <td>STRING-CLIENT</td> <td>Cadena de texto (p. ej.: "John@gmail.com").</td> </tr> <tr> <td>STRING-SERVER</td> <td></td> </tr> <tr> <td>RADIUS-CALLID</td> <td>ID o parte del ID.</td> </tr> <tr> <td>RADIUS-LOGIN</td> <td>Nombre o parte del nombre de usuario.</td> </tr> <tr> <td>RADIUS-SESSID</td> <td>ID o parte del ID.</td> </tr> <tr> <td>RADIUS-TECHKEY</td> <td>Clave o parte de la clave (p. ej.: "*.10.*").</td> </tr> <tr> <td>TACTICAL</td> <td>No es posible establecer un valor. El valor correcto será establecido por el operador en el campo.</td> </tr> </tbody> </table>	<i>Método</i>	<i>Formato</i>	DHCP	Dirección correspondiente (p. ej.: "195.162.21.2").	STATIC-IP		STATIC-MAC		STATIC-RANGE	Rango de direcciones separado por '-' (p. ej.: "195.162.21.2-195.162.21.5").	STRING-CLIENT	Cadena de texto (p. ej.: "John@gmail.com").	STRING-SERVER		RADIUS-CALLID	ID o parte del ID.	RADIUS-LOGIN	Nombre o parte del nombre de usuario.	RADIUS-SESSID	ID o parte del ID.	RADIUS-TECHKEY	Clave o parte de la clave (p. ej.: "*.10.*").	TACTICAL	No es posible establecer un valor. El valor correcto será establecido por el operador en el campo.
<i>Método</i>	<i>Formato</i>																								
DHCP	Dirección correspondiente (p. ej.: "195.162.21.2").																								
STATIC-IP																									
STATIC-MAC																									
STATIC-RANGE	Rango de direcciones separado por '-' (p. ej.: "195.162.21.2-195.162.21.5").																								
STRING-CLIENT	Cadena de texto (p. ej.: "John@gmail.com").																								
STRING-SERVER																									
RADIUS-CALLID	ID o parte del ID.																								
RADIUS-LOGIN	Nombre o parte del nombre de usuario.																								
RADIUS-SESSID	ID o parte del ID.																								
RADIUS-TECHKEY	Clave o parte de la clave (p. ej.: "*.10.*").																								
TACTICAL	No es posible establecer un valor. El valor correcto será establecido por el operador en el campo.																								

<i>Datos</i>	<i>Descripción</i>										
Acción	Método de infección que se aplicará al recurso indicado en Patrón de recursos :										
	<table border="1"> <thead> <tr> <th><i>Método</i></th> <th><i>Función</i></th> </tr> </thead> <tbody> <tr> <td>INJECT-EXE</td> <td>Infecta el archivo EXE descargado en tiempo real. El agent se instala cuando el target ejecuta el archivo EXE.</td> </tr> <tr> <td>INJECT-HTML-FILE</td> <td> <p>Le permite agregar el código HTML proporcionado en el archivo de la página web visitada.</p>  <p><i>Para ver más detalles, póngase en contacto con los técnicos de HackingTeam.</i></p> </td> </tr> <tr> <td>INJECT-HTML-FLASH</td> <td>Bloquea los videos de YouTube y le solicita al usuario que instale una actualización falsa de Flash para verlos. El agent se instala cuando el target instala la actualización.</td> </tr> <tr> <td>REPLACE</td> <td> <p>Reemplaza el recurso establecido en Patrón de recursos con el archivo proporcionado.</p>  <p>Sugerencia: este tipo de acción es muy efectiva cuando se usa en combinación con los documentos generados por Exploit.</p> </td> </tr> </tbody> </table>	<i>Método</i>	<i>Función</i>	INJECT-EXE	Infecta el archivo EXE descargado en tiempo real. El agent se instala cuando el target ejecuta el archivo EXE.	INJECT-HTML-FILE	<p>Le permite agregar el código HTML proporcionado en el archivo de la página web visitada.</p>  <p><i>Para ver más detalles, póngase en contacto con los técnicos de HackingTeam.</i></p>	INJECT-HTML-FLASH	Bloquea los videos de YouTube y le solicita al usuario que instale una actualización falsa de Flash para verlos. El agent se instala cuando el target instala la actualización.	REPLACE	<p>Reemplaza el recurso establecido en Patrón de recursos con el archivo proporcionado.</p>  <p>Sugerencia: este tipo de acción es muy efectiva cuando se usa en combinación con los documentos generados por Exploit.</p>
<i>Método</i>	<i>Función</i>										
INJECT-EXE	Infecta el archivo EXE descargado en tiempo real. El agent se instala cuando el target ejecuta el archivo EXE.										
INJECT-HTML-FILE	<p>Le permite agregar el código HTML proporcionado en el archivo de la página web visitada.</p>  <p><i>Para ver más detalles, póngase en contacto con los técnicos de HackingTeam.</i></p>										
INJECT-HTML-FLASH	Bloquea los videos de YouTube y le solicita al usuario que instale una actualización falsa de Flash para verlos. El agent se instala cuando el target instala la actualización.										
REPLACE	<p>Reemplaza el recurso establecido en Patrón de recursos con el archivo proporcionado.</p>  <p>Sugerencia: este tipo de acción es muy efectiva cuando se usa en combinación con los documentos generados por Exploit.</p>										

<i>Datos</i>	<i>Descripción</i>										
Patrón de recursos	Método de identificación de los recursos que serán inyectados, aplicado a la dirección URL del recurso web. El formato depende del tipo de Acción seleccionado.										
	<table border="1"> <thead> <tr> <th><i>Tipo de acción</i></th> <th><i>Contenido del patrón de recursos</i></th> </tr> </thead> <tbody> <tr> <td>INJECT-EXE</td> <td> <p>Dirección URL del archivo ejecutable a infectar. Use comodines para aumentar la cantidad de direcciones URL que coinciden. Ejemplos de posibles formatos: *[nombreExe]*.exe www.mozilla.org/firefox/download/firefoxsetup.exe</p> <p> NOTA: cuando se especifica la ruta completa, tenga cuidado con los mirrors usados por los sitios web para descargar archivos (p. ej.: "firefox.exe?mirror=it").</p> <p> Sugerencia: ingrese *.exe* para infectar todos los archivos ejecutables, independientemente de la dirección URL.</p> <p> IMPORTANTE: por ejemplo, si se ingresa *exe* sin el separador de extensión de archivo '.', todas las páginas que contengan accidentalmente las letras "exe" serán infectadas.</p> </td> </tr> <tr> <td>INJECT-HTML-FILE</td> <td> <p>Dirección URL del sitio web a infectar. Ejemplos de posibles formatos: www.oracle.com/ www.oracle.com/index.html</p> <p> NOTA: la dirección del sitio debe incluir el carácter final '/' si no se especifica HTML o una página dinámica (p. ej.: "www.oracle.com/").</p> <p> NOTA: no es posible infectar una página redireccionada. Verifique en el navegador la ruta correcta antes de indicarlo en la regla.</p> </td> </tr> <tr> <td>INJECT-HTML-FLASH</td> <td>Preconfigurado para YouTube y de solo lectura para el usuario.</td> </tr> <tr> <td>REPLACE</td> <td>URL del recurso a reemplazar.</td> </tr> </tbody> </table>	<i>Tipo de acción</i>	<i>Contenido del patrón de recursos</i>	INJECT-EXE	<p>Dirección URL del archivo ejecutable a infectar. Use comodines para aumentar la cantidad de direcciones URL que coinciden. Ejemplos de posibles formatos: *[nombreExe]*.exe www.mozilla.org/firefox/download/firefoxsetup.exe</p> <p> NOTA: cuando se especifica la ruta completa, tenga cuidado con los mirrors usados por los sitios web para descargar archivos (p. ej.: "firefox.exe?mirror=it").</p> <p> Sugerencia: ingrese *.exe* para infectar todos los archivos ejecutables, independientemente de la dirección URL.</p> <p> IMPORTANTE: por ejemplo, si se ingresa *exe* sin el separador de extensión de archivo '.', todas las páginas que contengan accidentalmente las letras "exe" serán infectadas.</p>	INJECT-HTML-FILE	<p>Dirección URL del sitio web a infectar. Ejemplos de posibles formatos: www.oracle.com/ www.oracle.com/index.html</p> <p> NOTA: la dirección del sitio debe incluir el carácter final '/' si no se especifica HTML o una página dinámica (p. ej.: "www.oracle.com/").</p> <p> NOTA: no es posible infectar una página redireccionada. Verifique en el navegador la ruta correcta antes de indicarlo en la regla.</p>	INJECT-HTML-FLASH	Preconfigurado para YouTube y de solo lectura para el usuario.	REPLACE	URL del recurso a reemplazar.
<i>Tipo de acción</i>	<i>Contenido del patrón de recursos</i>										
INJECT-EXE	<p>Dirección URL del archivo ejecutable a infectar. Use comodines para aumentar la cantidad de direcciones URL que coinciden. Ejemplos de posibles formatos: *[nombreExe]*.exe www.mozilla.org/firefox/download/firefoxsetup.exe</p> <p> NOTA: cuando se especifica la ruta completa, tenga cuidado con los mirrors usados por los sitios web para descargar archivos (p. ej.: "firefox.exe?mirror=it").</p> <p> Sugerencia: ingrese *.exe* para infectar todos los archivos ejecutables, independientemente de la dirección URL.</p> <p> IMPORTANTE: por ejemplo, si se ingresa *exe* sin el separador de extensión de archivo '.', todas las páginas que contengan accidentalmente las letras "exe" serán infectadas.</p>										
INJECT-HTML-FILE	<p>Dirección URL del sitio web a infectar. Ejemplos de posibles formatos: www.oracle.com/ www.oracle.com/index.html</p> <p> NOTA: la dirección del sitio debe incluir el carácter final '/' si no se especifica HTML o una página dinámica (p. ej.: "www.oracle.com/").</p> <p> NOTA: no es posible infectar una página redireccionada. Verifique en el navegador la ruta correcta antes de indicarlo en la regla.</p>										
INJECT-HTML-FLASH	Preconfigurado para YouTube y de solo lectura para el usuario.										
REPLACE	URL del recurso a reemplazar.										

<i>Datos</i>	<i>Descripción</i>
Factory	Para todas las acciones, a excepción de REPLACE . Agent que se inyectará en el recurso web seleccionado.
File	Solo para la acción REPLACE . Archivo que será reemplazado con el que se indique en Patrón de recursos .

Verifique el estado del Network Injector

Introducción

Network Injector se sincroniza con RCS Server para descargar las versiones actualizadas del software de control, así como las reglas de identificación y de inyección, para enviarlas a los registros.

Es posible monitorear el estado de Network Injector desde RCS Console.

Específicamente:

- en la sección **Monitor**: para identificar cuándo Network Injector se sincroniza y cuándo está disponible para la transferencia de datos.

Identificar cuándo se sincroniza Network Injector

A continuación se describe el procedimiento:

Paso Acción

- 1 En la sección **Monitor**, seleccione la fila correspondiente al objeto Network Injector que desea analizar. Verifique la columna **Estado**: si está marcada en verde, el Network Injector está sincronizado.

Esta situación ocurre cuando en el software Control Center (Appliance o Tactical):

- se hizo clic en **Config.**, el operador colocó nuevas reglas o actualizaciones de forma manual;
- se hizo clic en **Iniciar** o hay una infección en curso.



IMPORTANTE: RCS solo puede enviar las reglas y actualizaciones aplicadas cuando Network Injector está sincronizado.

Qué debería saber acerca de Appliance Control Center

Introducción

Appliance Control Center es una aplicación instalada en Network Injector Appliance.

Puede infectar a dispositivos en una red por cable gracias a las reglas de identificación e inyección para RCS.

Funciones de Appliance Control Center.

Con Appliance Control Center usted puede:

- Activar la sincronización con RCS para recibir las reglas actualizadas de identificación e inyección y enviar registros.
- Actualizar el Appliance Control Center con la última versión, enviada a través de la RCS Console.
- Identificar automáticamente los dispositivos conectados utilizando las reglas, e infectarlos.
- Configura el acceso remoto a las aplicaciones.

Sincronización con el RCS Server

Appliance Control Center se sincroniza con RCS para recibir las reglas de infección actualizadas, para verificar si hay una nueva versión de Appliance Control Center disponible y para enviar registros.

La sincronización puede ocurrir de dos maneras:

- manualmente, la primera vez que recibe las reglas de inyección.
- automáticamente con una infección en curso.

Durante la sincronización, RCS se comunica con Network Injector Appliance en intervalos de tiempo establecidos (aproximadamente 30 segundos).

En Appliance Control Center, es posible decidir cuándo activar la sincronización mediante la función **Network Injector**.

Actualización de las reglas de infección

Si el tráfico generado por el target no se puede infectar con las reglas actuales, requiere la asistencia del operador en la RCS Console para generar nuevas reglas y actualizar el Network Injector. En la siguiente sincronización, Appliance Control Center recibe las nuevas reglas que pueden verse y activar para la inyección.

Uso de las interfaces de red

Hay dos interfaces de red diferentes disponibles durante un ataque, una para el análisis y otra para la inyección. Se deben usar dos interfaces separadas para generar continuidad, especialmente para el análisis de paquetes.

Las interfaces de análisis de paquetes pueden ser de alta o baja velocidad.

Dirección IP de la interfaz de inyección

Si el servidor y el target de Appliance no pertenecen a la misma subred (direcciones IP con diferentes prefijos de enrutamiento), la interfaz de inyección debe ser una dirección pública, de lo contrario el target nunca podrá verla y la inyección fallará.

En una fase inicial puede usar la dirección actual en la interfaz con Appliance Control Center (con una **IP pública**="auto"), espere un mensaje que indique que la dirección es privada y, en ese caso, establezca una dirección pública para redirigir la dirección privada (**IP pública** = "xxx.xxx.xxx.xxx").

En análisis, por otro lado, se puede ejecutar a través de una interfaz de red con una dirección IP privada.

Infección mediante identificación automática

A continuación se describen los pasos necesarios para infectar dispositivos identificados mediante reglas de RCS. El ataque solo se puede realizar en redes con cable:

<i>Fase</i>	<i>Descripción</i>	<i>Dónde</i>
1	Prepare las reglas de identificación y de inyección para los targets conocidos que se van a atacar. Enviar las reglas al Network Injector	<i>RCS Console, System, Network Injector</i>
2	Realice una sincronización con RCS para recibir las reglas actualizadas y activar las reglas que se usarán para la inyección.	<i>Network Injector Appliance, Network Injector</i>
3	El sistema analiza los paquetes del tráfico e identifica los dispositivos del target gracias a las reglas de identificación y los infecta gracias a las reglas de inyección.	<i>Network Injector Appliance, Network Injector</i>

Infección mediante identificación automática

Este modo de trabajo es ideal para las situaciones en que se conoce alguna información del dispositivo del target (p. ej.: la dirección IP, MAC o RADIUS).

En este caso, las reglas de inyección de RCS incluyen todos los datos requeridos para identificar automáticamente los dispositivos del target. Solo se activan todas las reglas necesarias en ese momento para cada inyección.

Al iniciar la identificación automática con la función **Network Injector**, se muestran los dispositivos del target que se infectan inmediatamente mediante las reglas de inyección.

Acceso remoto a Appliance Control Center

También es posible acceder a Appliance Control Center de forma remota. Para obtener más información, consulte "[Qué debería saber acerca del acceso remoto al Control Center](#)" En la página 89.

Qué debería saber acerca de Tactical Control Center

Introducción

Tactical Control Center es una aplicación instalada en la computadora portátil, llamada Tactical Network Injector.

Puede infectar a dispositivos en una red por cable o Wi-Fi gracias a las reglas de identificación e inyección para RCS. La identificación del dispositivo puede ser automática o manual. En el segundo caso, el operador reconoce el dispositivo infectado y ejecuta el comando de aplicación de la regla de inyección para ese dispositivo.



El método de identificación deberá acordarse con el centro operativo.

Funcionamiento del Tactical Control Center

Con Tactical Control Center usted puede:

- Activar la sincronización con RCS para recibir las reglas actualizadas de identificación e inyección y enviar registros.
- Actualizar el Tactical Control Center, lo cual es fundamental para actualizar los agents en los dispositivos.
- Identificar automáticamente dispositivos en redes por cable o Wi-Fi, e infectarlas de acuerdo con las reglas de inyección e identificación de RCS.
- Identificar manualmente dispositivos en redes por cable o Wi-Fi, e infectarlas a través de las reglas de inyección de RCS (identificación por parte del operador).
- Conectarse a una red Wi-Fi para obtener la contraseña.
- Emular un Punto de acceso a una red Wi-Fi usada normalmente por el target.
- Desbloquear la contraseña del sistema operativo de la computadora del target.
- Configurar el acceso remoto a las aplicaciones.



NOTA: la red de inyección puede ser externa, o una red Wi-Fi simulada por el Tactical Control Center.

Sincronización con el RCS Server

Tactical Control Center se sincroniza con RCS para recibir las reglas de infección actualizadas, para verificar si hay una nueva versión de Tactical Control Center disponible y para enviar registros.

La sincronización puede ocurrir de dos maneras:

- manualmente, la primera vez que recibe las reglas de inyección.
- automáticamente con una infección en curso.

Durante la sincronización, RCS se comunica con Tactical Network Injector en intervalos de tiempo establecidos (aproximadamente 30 segundos).

En Tactical Control Center, es posible decidir cuándo activar la sincronización mediante la función **Network Injector**.

Actualización de las reglas de infección

Si el tráfico generado por el target no se puede infectar con las reglas actuales, requiere la asistencia del operador en la RCS Console para generar nuevas reglas y actualizar el Network Injector. En la siguiente sincronización, Tactical Control Center recibe las nuevas reglas que pueden verse y activar para la inyección.

Uso de las interfaces de red

Hay dos interfaces de red diferentes disponibles durante un ataque, una para el análisis y otra para la inyección. Se deben usar dos interfaces separadas para generar continuidad, especialmente para el análisis de paquetes.

Solo se utiliza la interfaz de análisis de paquetes cuando se emula un Punto de acceso y se obtienen contraseñas de red.

Las interfaces de análisis de paquetes pueden ser internas o externas: las externas se deben usar para el análisis de paquetes porque la velocidad de transmisión es mayor.

Infección mediante identificación automática

A continuación se describen los pasos necesarios para infectar dispositivos identificados mediante reglas de RCS. El ataque se puede ejecutar en redes por cable o Wi-Fi:

<i>Fase</i>	<i>Descripción</i>	<i>Dónde</i>
1	Prepare las reglas de identificación y de inyección para los targets conocidos que se van a atacar. Envíe las reglas al Tactical Network Injector.	<i>RCS Console, System, Network Injectors</i>
2	Realice una sincronización con RCS para recibir las reglas actualizadas y activar las reglas que se usarán para la inyección.	<i>Tactical Network Injector, Network Injector</i>
3	Si los dispositivos del target están conectados a la red Wi-Fi protegida, obtenga la contraseña.	<i>Tactical Network Injector, Wireless Intruder</i>
4	El sistema analiza los paquetes del tráfico e identifica los dispositivos del target gracias a las reglas de identificación y los infecta gracias a las reglas de inyección.	<i>Tactical Network Injector, Network Injector</i>
5	En caso de ser necesario, fuerce la reautenticación de los dispositivos no identificados por las reglas.	

Infección mediante identificación manual

A continuación se describen los pasos necesarios para infectar los dispositivos identificados de forma manual. La meta del operador es identificar los dispositivos del target.

El ataque se puede ejecutar en redes por cable o Wi-Fi:

<i>Fase</i>	<i>Descripción</i>	<i>Dónde</i>
1	Prepare las reglas de identificación que incluyen la identificación manual y las reglas de inyección para todos los dispositivos del target que serán atacados. Envíe las reglas al Tactical Network Injector.	<i>RCS Console, System, Network Injectors</i>
2	Realice una sincronización con RCS para recibir las reglas actualizadas y activar las reglas que se usarán para la inyección.	<i>Tactical Network Injector, Network Injector</i>
3	Si los dispositivos del target están conectados a la red Wi-Fi protegida, obtenga la contraseña.	<i>Tactical Network Injector, Wireless Intruder</i>
4	Si los dispositivos del target pueden conectarse a una red Wi-Fi abierta, intente emular un punto de acceso conocido por el target.	<i>Tactical Network Injector, Fake Access Point</i>
5	El sistema procesa todos los dispositivos conectados a la interfaz de red seleccionada. Use los filtros para buscar los dispositivos del target o para consultar el historial web para cada dispositivo.	<i>Tactical Network Injector, Network Injector</i>
6	Seleccione los dispositivos e inféctelos.	

Obtención de la contraseña de una red Wi-Fi protegida

Si el dispositivo del target está conectado a una red Wi-Fi protegida, se debe obtener la contraseña de acceso para iniciar sesión.

La función **Wireless Intruder** le permite conectarse a una red Wi-Fi y descifrar la contraseña. Para las redes protegidas WPA y WPA2, se puede cargar un diccionario adicional además del diccionario estándar. Se muestra la contraseña y el operador puede copiarla para usarla con la función de análisis e inyección (función **Network Injector**).

Forzar la autenticación de los dispositivos desconocidos

Puede ocurrir que no pueda conectarse a algunos dispositivos en una red Wi-Fi protegida con contraseña. Estos tipos de dispositivos aparecerán en la lista como desconocidos.

En este caso, se puede forzar la autenticación: el dispositivo se desconectará de la red, se volverá a conectar y se podrá identificar.

Infección mediante identificación automática

Este modo de trabajo es ideal para las situaciones en que se conoce alguna información del dispositivo del target (p. ej.: la dirección IP).

En este caso, las reglas de inyección de RCS incluyen todos los datos requeridos para identificar automáticamente los dispositivos del target. Solo se activan todas las reglas necesarias en ese momento para cada inyección.

Al iniciar la identificación automática con la función **Network Injector**, se muestran los dispositivos del target que se infectan inmediatamente mediante las reglas de inyección.

Infección mediante identificación manual

La identificación manual se puede indicar en las reglas de identificación de RCS. Este procedimiento normalmente se ejecuta cuando no hay información en el dispositivo a infectar, y se lo debe identificar en el campo.

En este caso, hay una serie de funciones disponibles para el operador que permiten seleccionar dispositivos conectados a la red:

- se pueden establecer filtros para el tráfico interceptado: solo se infectarán los dispositivos que cumplan con estos criterios.
- se puede verificar el historial de cada dispositivo para decidir cuáles se deberían infectar.

Una vez que se identifican los dispositivos del target, simplemente selecciónelos para iniciar la infección; las reglas de identificación están "personalizadas" con los datos del dispositivo para permitir la aplicación de las reglas de inyección.



- **NOTA:** los dispositivos que ya se hayan infectado mediante la identificación automática, se pueden infectar manualmente.

Establecer filtros en el tráfico interceptado

Al identificar targets manualmente, puede que algunos targets no se puedan identificar entre aquellos que estén conectados a la red. En este caso, use la función **Network Injector** para establecer los filtros para el tráfico interceptado.

El Tactical Control Center brinda los tipos de filtros:

- expresiones regulares
- Network BPF (Filtro de paquetes Bekerley)

Filtro con expresiones regulares

Las expresiones regulares son filtros amplios. Por ejemplo, si nuestro target está visitando una página de Facebook y hablando de windsurf, simplemente ingrese "facebook" o "windsurf".

El Tactical Network Injector interceptará todos los datos de tráfico y buscará las palabras enteras.

Para obtener más información sobre todas las expresiones regulares admitidas, consulte https://en.wikipedia.org/wiki/Regular_expression.

Filtro de red BPF (Berkeley Packet Filter)

Se usa para filtrar dispositivos usando la sintaxis BPF. Esta sintaxis incluye palabras clave acompañadas por calificadores:

- *calificadores de tipo* (p. ej.: **host**, **net**, **port**), indican el tipo de objeto buscado
- *calificadores de dirección* (p. ej.: **src**, **dst**) indican la dirección de los datos buscados
- *calificadores de protocolo* (p. ej.: **ether**, **wlan**, **ip**) indican el protocolo usado por el objeto buscado

Por ejemplo, si nuestro target está en la página de Facebook, ingrese "**host facebook.com**"

Para ver más detalles sobre los calificadores de sintaxis, consulte

<http://wiki.wireshark.org/CaptureFilters>.

Identificar el target analizando el historial

Otra manera de filtrar y reducir la lista de posibles targets es analizar el tráfico web del dispositivo para identificarlo como un target.

Emulación de un Punto de acceso conocido por el target

En ciertos escenarios, los dispositivos del target son atraídos para interceptar sus datos, identificarlos e infectarlos.

Para hacer esto, el Tactical Network Injector emula un Punto de acceso conocido para el dispositivo del target.

De esta manera, si el dispositivo está habilitado para conectarse automáticamente a las redes Wi-Fi disponibles, se conectará automáticamente al Punto de acceso emulado por el Tactical Network Injector en el momento en que ingresa en el área de Wi-Fi.

Desbloquear la contraseña del sistema operativo

Es posible desbloquear la contraseña de un sistema operativo. Para obtener más información, consulte "[Qué debería saber acerca del desbloqueo de las contraseñas del sistema operativo](#)" En la página 88.

Acceso remoto a Tactical Control Center

También es posible acceder a Tactical Control Center de forma remota. Para obtener más información, consulte "[Qué debería saber acerca del acceso remoto al Control Center](#)" En la página 89.

Qué debería saber acerca de la identificación de contraseñas de redes Wi-Fi

Introducción

Tactical Control Center incluye tres tipos de ataques para identificar las contraseñas de redes Wi-Fi (**Wireless Intruder**):

- Ataque de diccionario para WPA/WPA2
- Ataque de fuerza bruta para WEP
- Ataque de fuerza bruta de PIN para WPS

Ataque de diccionario para WPA/WPA2

Para realizar este ataque, el sistema identifica los *handshakes* entre el cliente y el punto de acceso e intenta descubrir la contraseña usando un diccionario de palabras comunes.

El *handshake* se guarda en la carpeta/opt/td-config/run/besside/wpa.cap. De ser necesario, puede copiar el *handshake* e intentar atacar con otra máquina más potente.

Una vez que el sistema identifica el *handshake*, el ataque puede continuar sin tener que permanecer cerca de la red Wi-Fi.

El ataque puede tomar mucho tiempo, es proporcional al tamaño del diccionario. El ataque falla si la contraseña no se encuentra en el diccionario de palabras comunes.

Ataque de fuerza bruta para WEP

Para realizar este ataque, el sistema hace una inyección simulando ser uno de los clientes conectados a la red y recopila datos para forzar la contraseña codificada. Cuando menos un cliente debe estar conectado a la red.

El ataque se tarda entre 10 y 15 minutos y la computadora portátil debe permanecer en el rango de cobertura de la red Wi-Fi en todo momento.

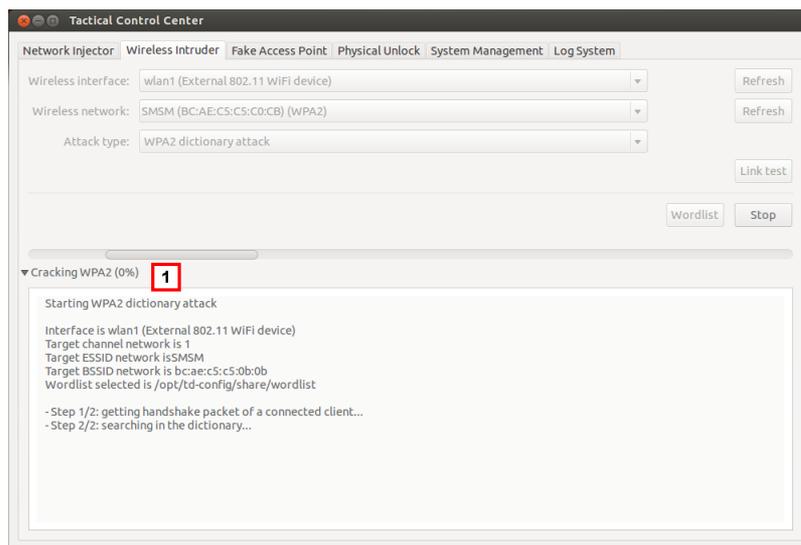
Ataque de fuerza bruta de PIN para WPS

Para realizar este ataque, el sistema intenta todas las combinaciones posibles para recuperar los puntos de acceso a través de un protocolo Wi-Fi Protected Setup.

El ataque puede tomar mucho tiempo y la computadora portátil debe permanecer en el rango de cobertura de la red Wi-Fi en todo momento.

Progreso del ataque

Es posible ver el porcentaje de progreso del ataque [1] (WPA/WPA2 y WPS) o los vectores de inicio capturados (WEP) en la pestaña **Tactical Control Center Wireless Intruder**.



Qué debería saber acerca del desbloqueo de las contraseñas del sistema operativo

Introducción

A través de una conexión FireWire o Thunderbolt con la computadora del target, el Tactical Network Injector puede acceder a la memoria RAM de la computadora del target y desbloquear la contraseña del sistema operativo. De este modo se puede atacar a la computadora, por ejemplo, con infecciones físicas (ej.: a través de Silent Installer).



NOTA: esta operation solo involucra a la RAM de la computadora del target: si la computadora se apaga o reinicia, no quedará ningún rastro de la operation.

La pestaña **Desbloqueo físico** del Tactical Control Center le permite ejecutar la operation de bloqueo y desbloqueo de contraseña.

Requisitos del Tactical Network Injector

Se deben usar los accesorios específicos de acuerdo con el tipo de conexión (FireWire o Thunderbolt):

- Adaptador ExpressCard/34
- cable

Requisitos de la computadora del target

La operation solo puede completarse con éxito si la computadora del target cumple con los siguientes requisitos:

- 4 GB de RAM como máximo
- Puerto de conexión FireWire o Thunderbolt (integrado o con adaptador)

Proceso estándar

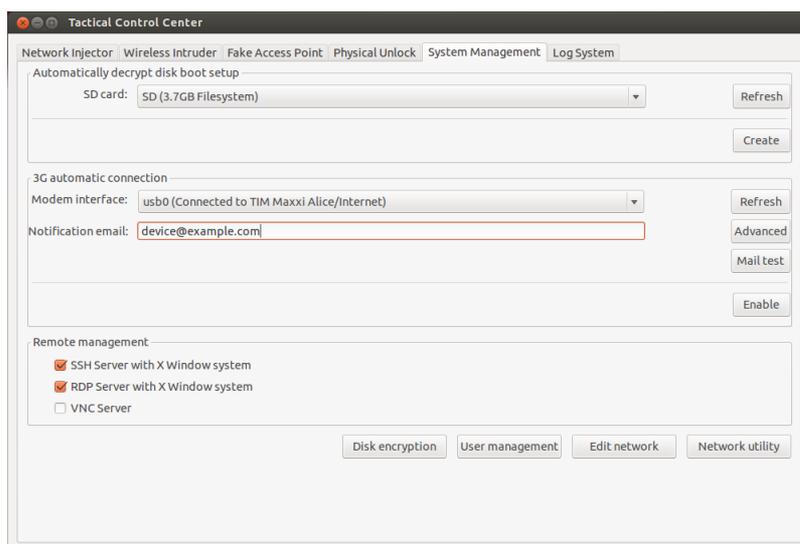
Fase Descripción

- 1 El operador:
 - conecta físicamente el Tactical Network Injector a la computadora del target a través de una conexión FireWire o Thunderbolt
 - ejecuta el procedimiento de desbloqueo de contraseñas del sistema operativo a través de la pestaña **Desbloqueo físico** del Tactical Control Center .
- 2 Tactical Network Injector
 - lee la memoria RAM (*volcado de memoria*) de la computadora
 - identifica la parte de la memoria dedicada a la contraseña del sistema operativo
 - usa esta información para desbloquear el sistema operativo y comunica el resultado al operador
- 3 El operador:
 - accede a la computadora del target con una contraseña en blanco (solo debe presionar Entrar en la página de inicio de sesión) o cualquier contraseña que tenga al menos 8 caracteres.
 - ejecuta operations en la computadora del target, por ejemplo, infecciones físicas (ej.: a través de Silent Installer)
 - en caso de ser necesario, inicia la función de bloqueo de contraseñas del sistema operativo a través de la pestaña **Desbloqueo físico** del Tactical Control Center.

Qué debería saber acerca del acceso remoto al Control Center

Introducción

Puede acceder a Tactical Control Center y Appliance Control Center desde un dispositivo remoto. La pestaña **Administración del sistema** de las aplicaciones le permite configurar esta opción. Por ejemplo, así es como se ve la pestaña Tactical Control Center.



Específicamente, se requiere lo siguiente para realizar un acceso remoto:

- Contraseña de disco codificado (solo para Tactical Control Center)
- Módem 3G para la conexión
- Dirección IP del dispositivo
- Protocolo de red

Contraseña del disco (solo para Tactical Control Center)

La computadora portátil del Tactical Network Injector tiene un disco codificado y se requiere la contraseña del disco cada vez que se enciende. Para evitar el ingreso manual de la contraseña, puede guardarla en una memoria SD y dejarla insertada (preferiblemente en la ranura SD de la computadora portátil).



NOTA: la contraseña no es la contraseña del sistema. De esta manera, la tarjeta SD no contiene información que puedan usar terceros para acceder al sistema operativo.

Para cambiar la contraseña, simplemente genere una nueva.

Módem 3G para la conexión

El módem 3G en **Interfaz de módem** se usa para conectar el dispositivo a una red.

Si se desconecta o reinicia el sistema con el módem activado, la conexión se restablece automáticamente.



Sugerencia: para tener una mayor seguridad, use el módem 3G integrado a la computadora portátil en lugar de un módem externo.

Dirección IP del dispositivo

Si se establece, se envía un correo electrónico a la dirección indicada en el **correo electrónico de notificación** con la dirección IP del dispositivo cada vez que se conecta.

Si la dirección IP es dinámica, espere hasta que se envíe un correo electrónico con la dirección que se utilizará para la conexión.

Si la dirección IP es estática, puede establecer que se envíe el correo electrónico para informarle cuando el dispositivo esté conectado.

Correo electrónico con modo de envío a dirección IP

Para enviar el correo electrónico, puede usar la configuración automática que utiliza el servidor de correo electrónico del dispositivo, o especificar manualmente un servidor de correo electrónico.

Si se usa la configuración automática, la dirección de correo electrónico del remitente será `root@hostname.local`, donde `hostname` es el host del dispositivo. En ese caso, se usará el especificado.

Para verificar si las comunicaciones se establecen correctamente, envíe un correo electrónico de prueba.

Protocolo de red

Las comunicaciones se realizan a través de un protocolo de red especificado en la sección **Administración remota**.

Otras funciones útiles

Puede abrir directamente algunos de los paneles del sistema operativo de la pestaña **Administración del sistema** por medio de las siguientes claves:

- **Cifrado de disco:** permite cambiar la contraseña del disco (solo Tactical Control Center)
- **Administración de usuarios:** permite editar a los usuarios y grupos de usuarios
- **Editar red:** permite editar la configuración de la red
- **Herramienta de red:** permite ejecutar un diagnóstico de red

Comandos de Tactical Control Center y Appliance Control Center

Introducción

Existen algunos comandos de terminal disponibles para administrar las aplicaciones de Tactical Control Center y Appliance Control Center.



NOTA: Para ejecutar estos comandos se requieren privilegios de administrador.

Comandos

A continuación se describen los comandos disponibles para Tactical Control Center y Appliance Control Center:

Comandos de Tactical Control Center	Comandos de Appliance Control Center	Función
tactical	appliance	Inicia la aplicación.
tactical -d o bien tactical --desync	appliance -d o bien appliance --desync	Desconecta el sistema de RCS Server actualmente sincronizado.
tactical -l o bien tactical --log	appliance -l o bien appliance --log	Muestra los registros de los procesos de infección actuales.  NOTA: la ventana de la aplicación debe estar abierta.
tactical -s o bien tactical --show-logs	appliance -s o bien appliance --show-logs	Muestra todos los archivos de registro guardados en el sistema de archivos.
tactical -r o bien tactical --report	appliance -r o bien appliance --report	Crea un informe del sistema y lo guarda en la carpeta Home del usuario.
tactical -v o bien Tactical --version	appliance -v o bien appliance --version	Muestra la versión de la aplicación.
tactical -h o bien tactical --help	appliance -h o bien appliance --help	Muestra los comandos disponible.

Appliance Control Center

Propósito

Appliance Control Center le permite:

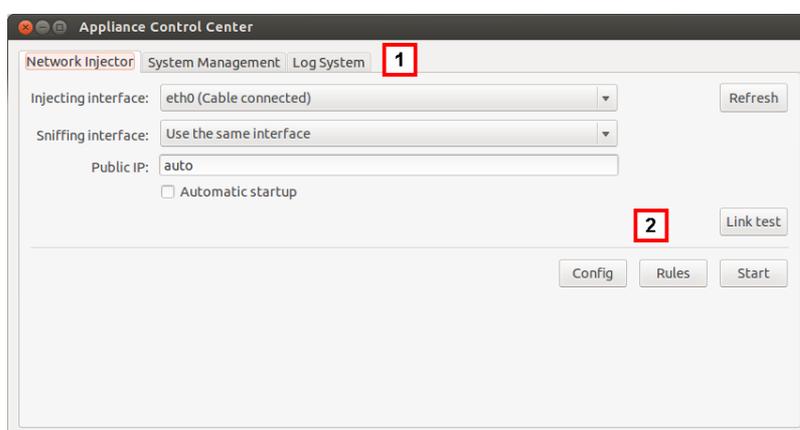
- administrar las inyecciones de Network Injector Appliance
- sincronizar Network Injector Appliance con RCS Server para recibir actualizaciones y enviar registros
- configurar el acceso remoto a las aplicaciones

Solicitud de contraseña

Cuando Appliance Control Center se abre, se debe ingresar una contraseña, la misma que se usa en la computadora portátil en la que se está ejecutando.

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Pestañas de acceso a las aplicaciones particulares. A continuación se muestra la descripción de cada elemento:

<i>Función</i>	<i>Descripción</i>
Network Injector	Administra el análisis de paquetes y la infección del dispositivo del target, sincroniza las reglas de RCS y actualiza los dispositivos de Appliance.
Administración del sistema	Configura el acceso remoto a las aplicaciones.
Sistema de registros	Visualización de registros.

- 2 Área con claves específicas para la pestaña.

Para obtener más información

Para obtener más información acerca de Appliance Control Center consulte "[Qué debería saber acerca de Appliance Control Center](#)" En la página 79 .

Para ver una descripción de los datos de Appliance Control Center consulte "[Datos de Appliance Control Center](#)" En la página 99

Activar la sincronización con RCS Server para recibir nuevas reglas

A continuación se muestra el procedimiento sobre cómo activar la sincronización con RCS Server para recibir las actualizaciones de las reglas:



NOTA: si la inyección está en curso, Network Injector ya está sincronizado con RCS Server y por lo tanto las reglas se cargan automáticamente. Ir al paso 4. Consulte "[Verifique el estado del Network Injector](#)" En la página 79

Pasos

Resultado

1. En la pestaña **Network Injector**, haga clic en **Config.**: la sincronización está activada.
2. Durante la sincronización, RCS consulta al Network Injector cada 30 segundos. Las reglas de inyección enviadas serán recibidas al finalizar el primer intervalo.



IMPORTANTE: solo se recibirán actualizaciones si se envían desde RCS Console. Consulte "[Administración de los Network Injector](#)" En la página 70

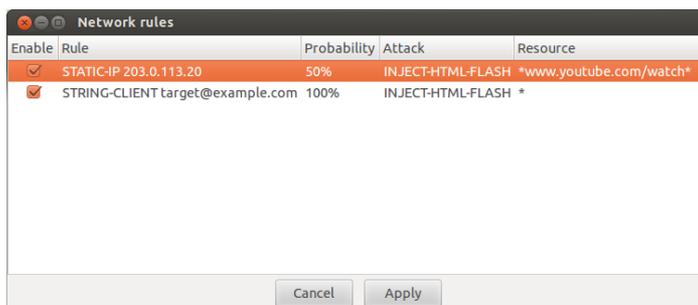
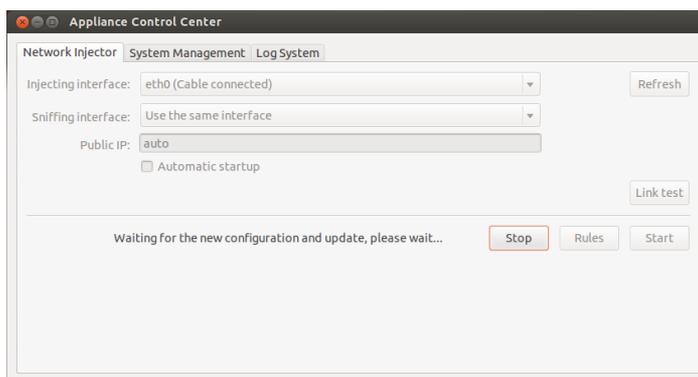


IMPORTANTE: realice una sincronización normal para garantizar el control constante de las actualizaciones de espacio.

3. Para detener la sincronización, haga clic en **Detener**.
4. Para ver las reglas recibidas de RCS Console, haga clic en **Reglas**: se mostrarán todas las reglas para Network Injector



IMPORTANTE: asegúrese de que la sincronización de las reglas se realice con éxito después de solicitar la actualización a RCS Console.



Hacer una prueba a la red

A continuación se muestra el procedimiento para hacer pruebas a la red para detectar análisis de

paquetes y/o inyección:

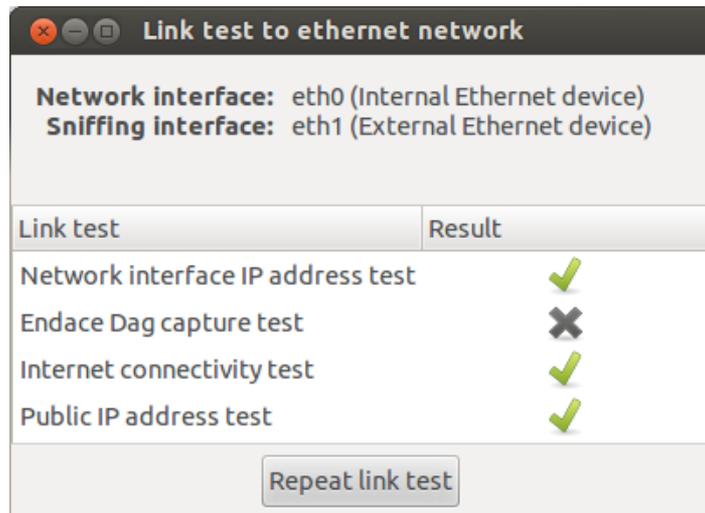
Pasos

1. En la pestaña **Network Injector**, seleccione la interfaz de la red.
2. Haga clic en **Prueba de enlace**: aparecerá una ventana donde se muestran los resultados.
3. Si la prueba falla, revise la configuración de la red deseada y repita la prueba.



IMPORTANTE: si la prueba falla el ataque no se podrá realizar con éxito.

Resultado



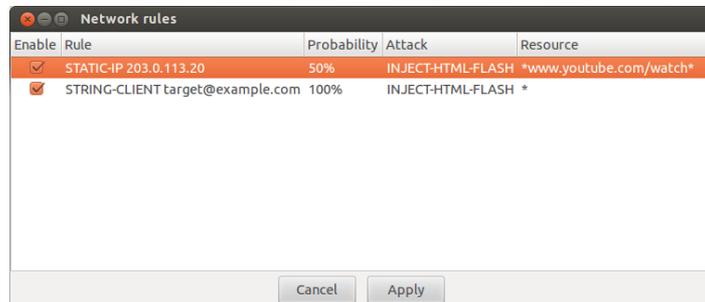
Infectar targets por medio de la identificación automática

Para comenzar la identificación automática y la infección:

Pasos

1. En la pestaña **Network Injector**, haga clic en **Reglas**: se mostrarán todas las reglas disponibles para Network Injector.
2. Solo se activarán las reglas que se usarán para la infección si se marca el campo **Activar** correspondiente.
3. Para confirmar, haga clic en **Aplicar**.

Resultado



Pasos

4. Seleccione la interfaz de red para la inyección en la lista desplegable **Interfaz de infección**.
5. En la lista desplegable **Interfaz de análisis de paquetes**, seleccione otra interfaz de red que se utilizará para el análisis de paquetes o la misma interfaz usada para la inyección.



Sugerencia: use dos interfaces diferentes para garantizar una mejor identificación del dispositivo.



NOTA: Las interfaces Endace (DAG), es decir, las interfaces de análisis de paquetes, se muestran en **Interfaz de análisis de paquetes**.

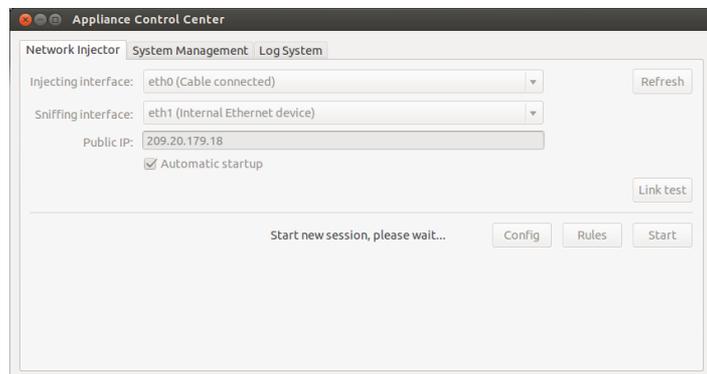
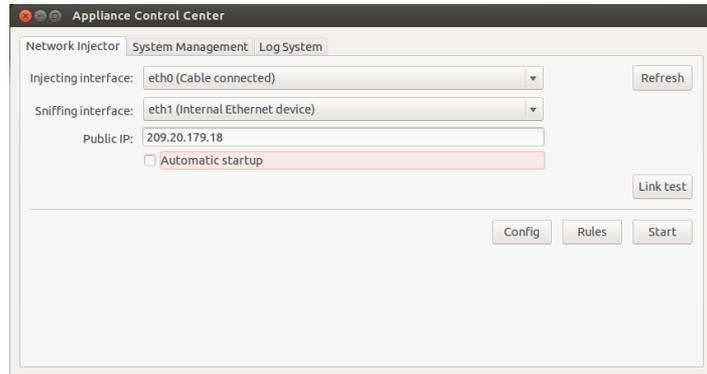
6. Haga clic en **Configuración automática** para reiniciar automáticamente la infección sin intervención humana, incluso después del reinicio o desconexión de Appliance Network Injector.
7. Haga clic en **Iniciar**.



IMPORTANTE: Appliance Control Center le permite configurar, iniciar una infección y cerrar Appliance Control Center dejando la infección activa. La próxima vez que se abra con la infección activa, aparecerá el botón Detener en lugar del botón Iniciar . Esto le permite configurar una nueva inyección y ejecutarla.



NOTA: para activar/desactivar las reglas cuando la infección está en curso, haga clic en **Reglas**.

Resultado

Pasos

Resultado

8. Para detener la infección, haga clic en **Detener**. O cierre la ventana para dejar la infección activa.



Sugerencia: cierre la ventana para permitir que el sistema ejecute automáticamente las actualizaciones de Appliance Control Center.

Configurar el acceso remoto a las aplicaciones

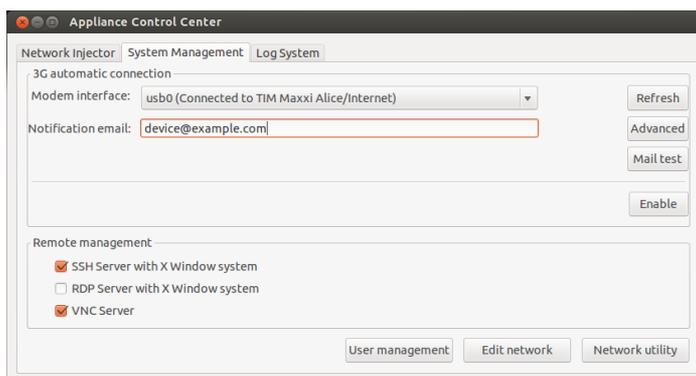
Para acceder a Appliance Control Center de forma remota:

Pasos**Resultado**

1. Conecte el módem al dispositivo.
2. En la pestaña **Administración del sistema** haga clic en **Volver a cargar**: el sistema reconocerá el módem y lo mostrará en la **Interfaz del módem**.
3. Si hay varios módems instalados, seleccione el módem deseado en la lista desplegable **Interfaz de módem**.
4. Para activar el envío de correos electrónicos con la dirección IP del dispositivo en cada conexión, siga estos pasos:
 - a. En **Correo electrónico de notificación** ingrese la dirección a la cual enviar el correo.
 - b. Haga clic en **Prueba de correo** para enviar un correo electrónico de prueba
 - c. Si no recibe el correo, haga clic en **Avanzada** para establecer manualmente el servidor de correos: aparecerá la ventana **Configuración avanzada de correo electrónico**.
 - d. Ingrese los datos indicados y haga clic en **Guardar**.
 - e. Haga clic en **Prueba de correo** para enviar un correo electrónico de prueba con el servidor configurado.
5. Para activar la conexión automática con el módem seleccionado, haga clic en **Activar**
6. Seleccione el protocolo de red que se usará para el acceso remoto.



NOTA: es posible abrir directamente algunas ventanas útiles del sistema operativo por medio de los botones que se encuentran en la parte inferior de la pantalla. Consulte "[Qué debería saber acerca del acceso remoto al Control Center](#)" En la página 89 .

**Ver los detalles de una infección**

Para ver los registros de la sesión actual, seleccione la pestaña **Sistema de registros**.

Para ver todos los archivos del registro, haga clic en la pestaña **Mostrar registros** en la pestaña **Sistema de registros**.



NOTA: todos los archivos de registro se guardan en el sistema de archivos en /var/log/td-config.

Datos de Appliance Control Center

Datos de la pestaña Network Injector

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Interfaz de inyección	Lista de interfaces de red conectadas. Seleccione la interfaz de inyección conectada a la red a la que está conectado el dispositivo que se invadirá.
Interfaz de análisis de paquetes	Al igual que una interfaz de inyección u otra interfaz de red se usa solo para analizar paquetes.  NOTA: Si el sistema incluye una tarjeta Endace DAG para conexiones Gigabit, la tarjeta será detectada y aparecerá en esta lista.
IP pública	Permite especificar una dirección IP pública que se puede mapear a la dirección IP privada de la interfaz de inyección. Si se ingresa el valor "auto", el sistema utiliza la dirección IP predeterminada en la interfaz de inyección y envía un mensaje indicando que es una dirección IP privada.
Configuración automática	La infección se reinicia automáticamente sin intervención humana, incluso después del reinicio o desconexión de Appliance Network Injector.  IMPORTANTE: Si esta opción no está seleccionada, la infección no se iniciará automáticamente.

Datos de la pestaña Administración del sistema

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Interfaz del módem	Módem 3G para la conexión del dispositivo.
Correo electrónico de notificación	Dirección de correo electrónico a la cual se envía la IP del dispositivo cada vez que se conecta a la red.  IMPORTANTE: campo obligatorio para las direcciones IP dinámicas.
Administración remota	Protocolo de red para el acceso remoto.

Tactical Control Center

Propósito

Tactical Control Center le permite:

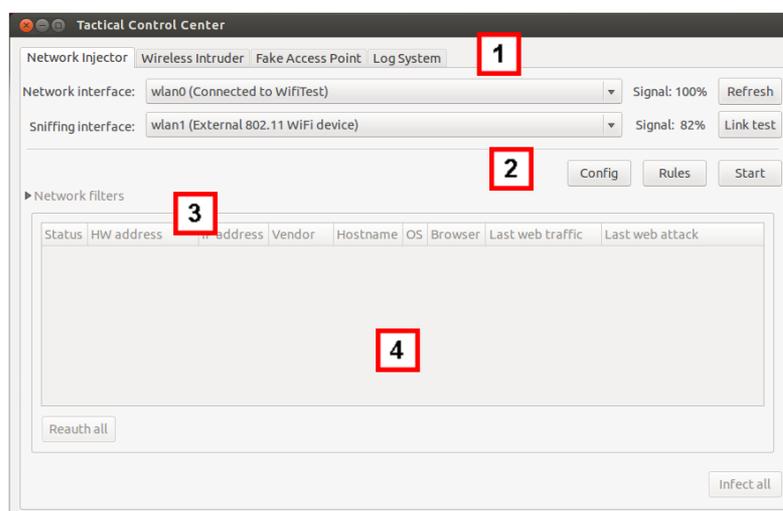
- administrar las inyecciones del Tactical Network Injector
- sincronizar Network Injector Appliance con RCS Server para recibir actualizaciones y enviar registros
- desbloquear la contraseña del sistema operativo de la computadora del target
- configurar el acceso remoto a las aplicaciones

Solicitud de contraseña

Cuando Tactical Control Center se abre, se debe ingresar una contraseña, la misma que se usa en la computadora portátil en la que se está ejecutando.

Cómo se ve la función

Así es como se ve la página:



Área Descripción

- 1 Pestañas de acceso a las aplicaciones particulares. A continuación se muestra la descripción de cada elemento:

Función	Descripción
Network Injector	Administra el análisis y la infección del dispositivo del target, sincroniza las reglas de RCS, actualiza los dispositivos Tactical y muestra las reglas actuales del Tactical Network Injector.
Wireless Intruder	Ingresa a una red Wi-Fi protegida, identificando la contraseña.
Fake Access Point	Emula un punto de acceso.
Desbloqueo físico	Desbloquea una contraseña del sistema operativo.
Administración del sistema	Configura el acceso remoto a las aplicaciones.
Sistema de registros	Visualización de registros.

- 2 Área con claves específicas para la pestaña.
 3 Filtros para filtrar el tráfico de Internet en los dispositivos.
 4 Área con la lista de dispositivos.

Para obtener más información

Para ver una descripción de Tactical Control Center consulte "[Datos del Tactical Control Center](#)" En la página 117 .

Para obtener más información acerca de Tactical Control Center consulte "[Qué debería saber acerca de Tactical Control Center](#)" En la página 82 .

Activar la sincronización con RCS Server para recibir nuevas reglas



NOTA: si la inyección está en curso, Network Injector ya está sincronizado con RCS Server y por lo tanto las reglas se cargan automáticamente. Ir al paso 4. Consulte "[Verifique el estado del Network Injector](#)" En la página 79

A continuación se muestra el procedimiento sobre cómo activar la sincronización con RCS para recibir las actualizaciones de las reglas:

Pasos

1. En la pestaña **Network Injector**, haga clic en **Config.**: la sincronización está activada.
2. Durante la sincronización, RCS consulta al Network Injector cada 30 segundos. Las reglas de inyección enviadas serán recibidas al finalizar el siguiente intervalo.



IMPORTANTE: solo se recibirán actualizaciones si se envían desde RCS Console. Consulte *"Administración de los Network Injector"* En la página 70

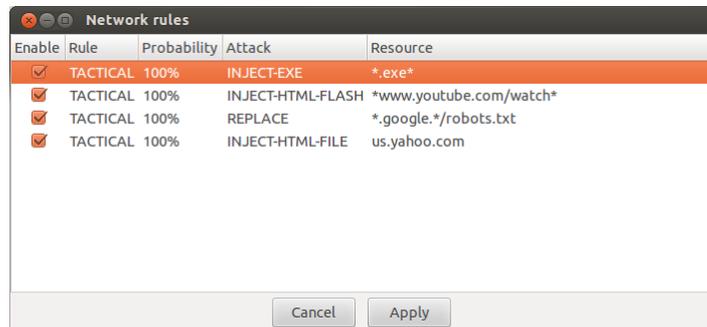
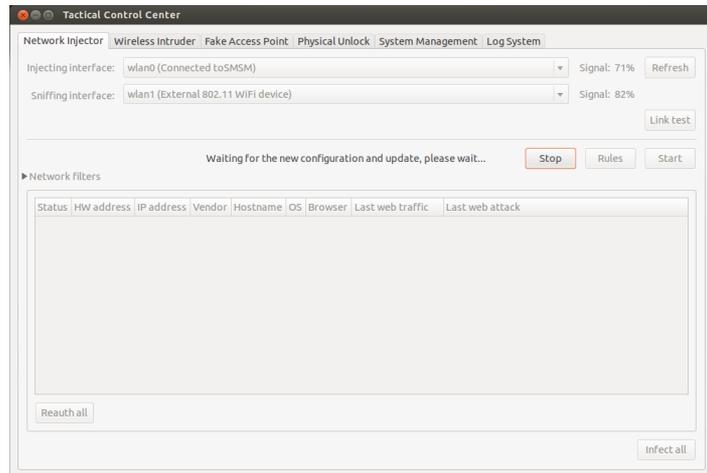


IMPORTANTE: realice una sincronización normal para garantizar el control constante de las actualizaciones de espacio .

3. Para detener la sincronización, haga clic en **Detener.**
4. Para ver las reglas recibidas de RCS Console, haga clic en **Reglas:** se mostrarán todas las reglas para Network Injector



IMPORTANTE: asegúrese de que la sincronización de las reglas se realice con éxito después de solicitar la actualización a RCS Console.

Resultado**Hacer una prueba a la red**

A continuación se muestra el procedimiento para hacer pruebas a la red para detectar análisis de paquetes y/o inyección:

Pasos

1. En la pestaña **Network Injector** o **Wireless Intruder** o **Fake Access Point**, seleccione la interfaz de red.
2. Haga clic en **Prueba de enlace**: aparecerá una ventana donde se muestran los resultados.
3. Si la prueba falla, muévase a una mejor posición donde la señal sea más potente y repita la prueba.



IMPORTANTE: si la prueba falla el ataque no se podrá realizar con éxito.

Resultado

✕
Link test to wireless network
☐

Injecting interface: wlan0 (Internal 802.11 WiFi device)
Sniffing interface: wlan1 (External 802.11 WiFi device)
Wireless channel: 1
Wireless ESSID: SMSM
Wireless BSSID: BC:AE:C5:C5:B0:0B

Link test	Result
Injecting interface quality signal	✓
Sniffing interface quality signal	✓
Injection test to wireless network	✓
Connectivity test to wireless network	✓
Unique AP ESSID name test	✗
Injecting interface IP address test	✓
Internet connectivity test	✓

Obtener una contraseña de red Wi-Fi protegida

A continuación se muestra cómo obtener una contraseña de red Wi-Fi protegida:

Pasos

1. En la pestaña **Wireless Intruder**, seleccione la interfaz de red Wi-Fi en **Interfaz inalámbrica**
2. En **Red ESSID**, seleccione la red cuya contraseña debe identificarse.



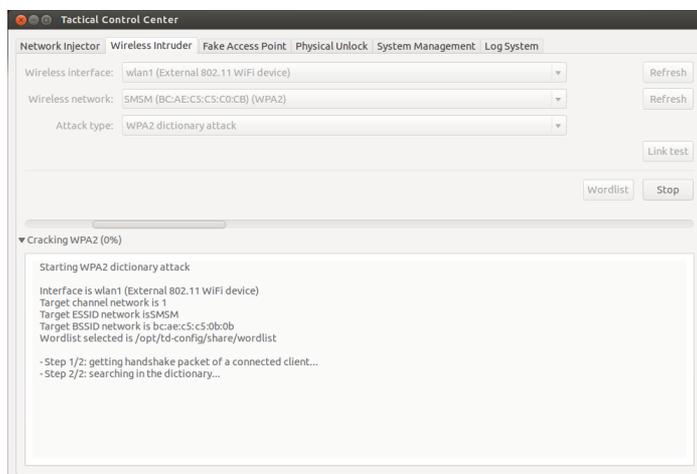
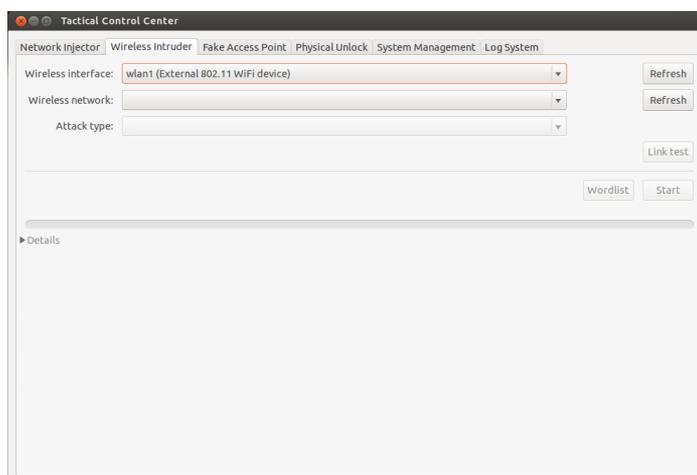
NOTA: administre las conexiones/desconexiones de la interfaz de red desde el sistema operativo y haga clic en **Volver a cargar**.

3. Seleccione el tipo de ataque en **Tipo de ataque**.
4. Si es necesario, haga clic en **Lista de palabras** para cargar un diccionario adicional para atacar las redes protegidas por WPA o WPA 2



IMPORTANTE: el diccionario adicional se debe cargar en cada ataque.

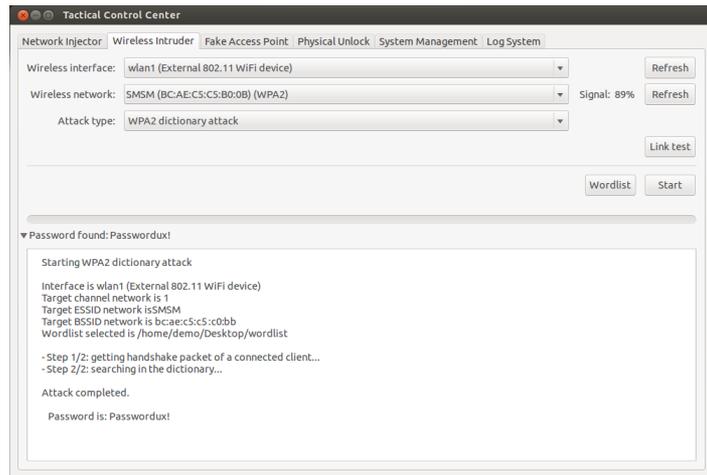
5. Haga clic en **Iniciar**: el sistema lanza varios ataques para encontrar la contraseña de acceso.
6. Haga clic en **Detener** para detener el ataque.

Resultado

Pasos

- Si el ataque se realiza con éxito, aparecerá la contraseña sobre el indicador de estado.

Resultado



- Con el **Administrador de red** del sistema operativo, use la contraseña para conectarse a la red Wi-Fi. El sistema guarda la contraseña y ya no necesita ingresarse.
- Abra la sección **Network Injector** para iniciar la identificación y la infección.

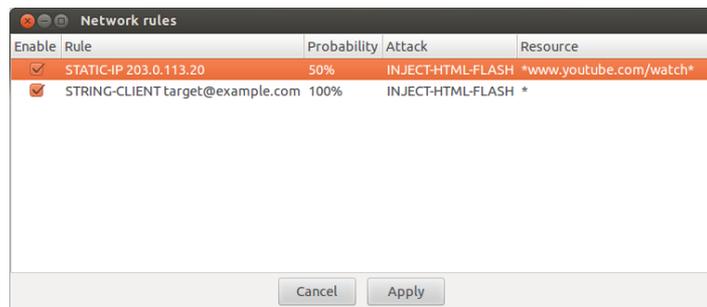
Infectar targets por medio de la identificación automática

Para comenzar la identificación automática y la infección:

Pasos

- En la pestaña **Network Injector**, haga clic en **Reglas**: se mostrarán todas las reglas disponibles para Network Injector.
- Solo se activarán las reglas que se usarán para la infección si se marca el campo **Activar** correspondiente.
- Para confirmar, haga clic en **Aplicar**.

Resultado



Pasos**Resultado**

- En la pestaña **Network Injector**, seleccione la interfaz de red para la inyección en la lista desplegable **Interfaz de infección**.
- En la lista desplegable **Interfaz de análisis de paquetes**, seleccione otra interfaz de red que se utilizará para el análisis de paquetes o la misma interfaz usada para la inyección.



NOTA: administre las conexiones/desconexiones de la interfaz de red desde el sistema operativo y haga clic en **Volver a cargar**.

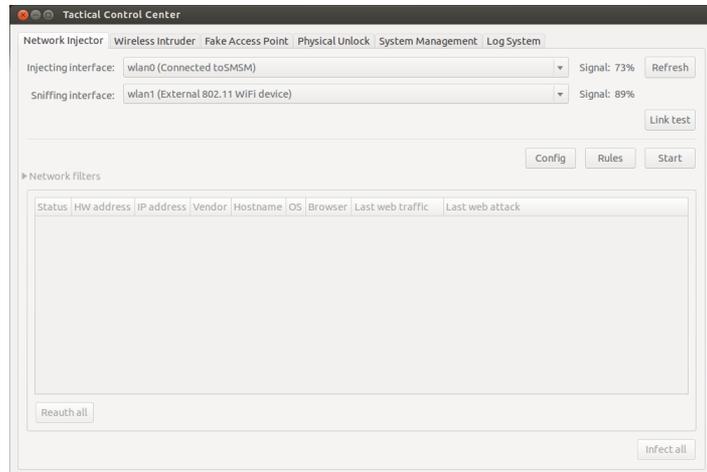


Sugerencia: use dos interfaces diferentes para garantizar una mejor identificación del dispositivo.

- Revise la potencia de la señal y, si es necesario, realice la prueba de la red (botón **Prueba de enlace**).



NOTA: la potencia de la señal debe ser cuando menos 70 %. Si se usa la misma interfaz de red para la inyección y el análisis de paquetes dará como resultado un único valor.



Pasos**Resultado**

7. Haga clic en **Iniciar** : se iniciará el proceso de análisis de paquetes de la red y se mostrarán todos los dispositivos identificados como targets. La columna **Estado** muestra el estado de identificación.



ADVERTENCIA: verifique el estado de identificación. Consulte "Datos del Tactical Control Center" En la página 117 .

8. Los dispositivos del target comienzan a infectarse. El inicio de la infección se registra.

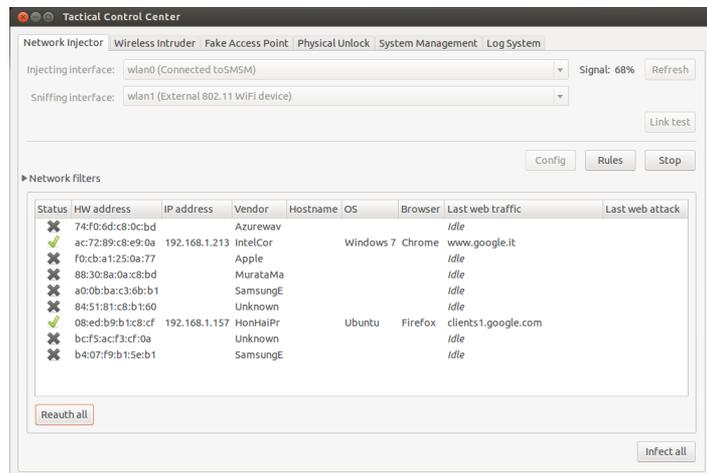


NOTA: para activar/desactivar las reglas cuando la infección está en curso, haga clic en **Reglas**.



NOTA: los dispositivos que no son del target no aparecerán en la lista y por lo tanto serán excluidos de la infección automática.

9. Para detener la infección, haga clic en **Detener**.

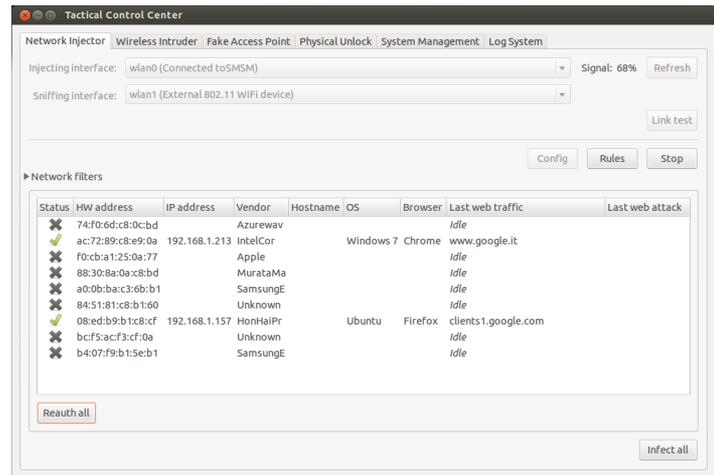
**Forzar la autenticación de los dispositivos desconocidos**

Para forzar la autenticación de los dispositivos desconocidos:

Pasos**Resultado**

Pasos

1. En la pestaña **Network Injector**, seleccione los dispositivos de la lista (estado )

Resultado

2. Haga clic en **Reaut. seleccionado**: los dispositivos serán forzados a volver a autenticarse.



Sugerencia: en ciertos casos, todos los dispositivos deberán autenticarse. Para hacerlo, haga clic en **Reaut. todo**.



NOTA: la clave **Reaut. seleccionado** se muestra si se seleccionan dispositivos, y **Reaut. todo** si no se selecciona ningún dispositivo.

3. Si la reautenticación se realiza con éxito, se iniciará la identificación automática: el

estado del dispositivo será  y podrá ser infectado a partir de ahora.

Infectar targets por medio de la identificación manual

Para infectar manualmente los dispositivos de la red:

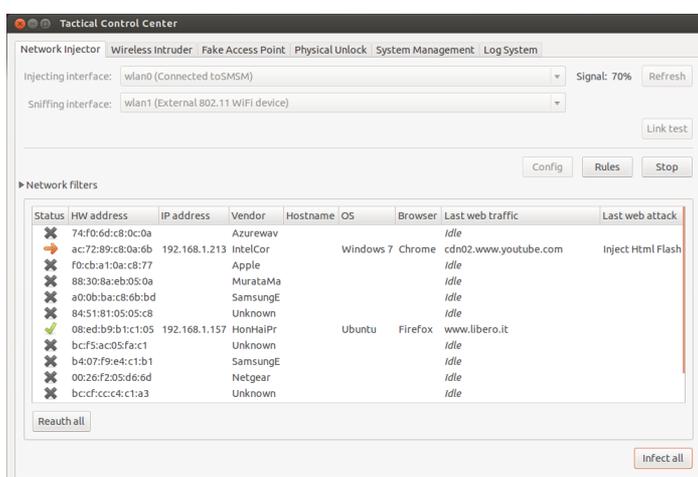
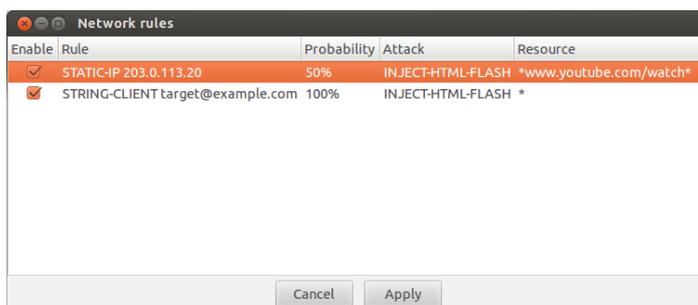
Pasos

1. En la pestaña **Network Injector**, haga clic en **Reglas**: se mostrarán todas las reglas disponibles para Network Injector.
2. Solo se activarán las reglas que se usarán para la infección si se marca el campo **Activar** correspondiente.
3. Para confirmar, haga clic en **Aplicar**.
4. En **Network Injector**, seleccione uno o más dispositivos a infectar e identifíquelos usando los datos que se muestran.



Sugerencia: si hay muchos dispositivos en la lista, filtre la selección. Consulte "[Establecer filtros en el tráfico interceptado](#)" En la página opuesta .

Resultado



<i>Pasos</i>	<i>Resultado</i>
5. Haga clic en Infectar seleccionado : se "personalizarán" y aplicarán todas las reglas de infección con los datos del dispositivo. Los ataques a los dispositivos se mostrarán en los registros.	
 IMPORTANTE: esta operación requiere una regla especial creada en RCS Console.	
 Sugerencia: para infectar a todos los dispositivos conectados, incluso aquellos que no sean el target o aún no estén conectados a uno, haga clic en Infectar todo .	
 NOTA: la clave Infectar seleccionado se muestra si se seleccionan dispositivos, e Infectar todo si no se selecciona ningún dispositivo.	
Resultado: si la infección se inició con éxito, el estado del dispositivo es  .	

Establecer filtros en el tráfico interceptado

Para seleccionar los dispositivos del target con los filtros en el tráfico de datos:

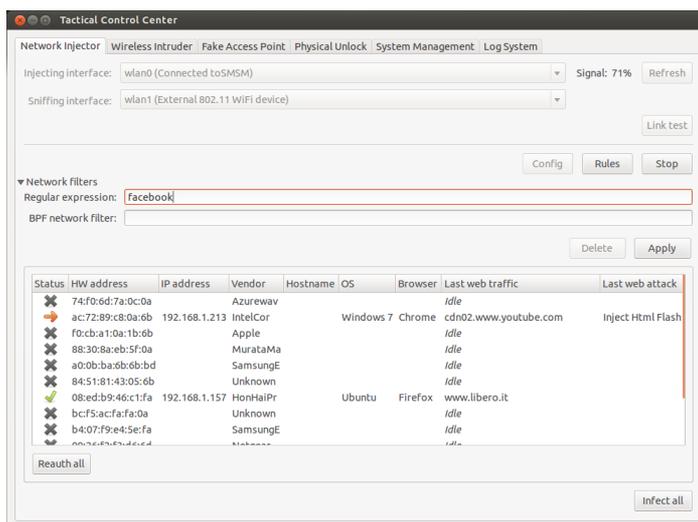
<i>Pasos</i>	<i>Resultado</i>
--------------	------------------

Pasos

1. En la pestaña **Network Injector**, haga clic en **Filtros de la red**.
2. Para realizar una búsqueda más amplia, ingrese una expresión regular en el cuadro de texto **Expresión regular**.
3. O, para redefinir la búsqueda, ingrese una expresión BPF en el cuadro de texto **Filtro de red BPF**.

Resultado: el sistema solo muestra los dispositivos filtrados en la lista.

Resultado



4. Infecte manualmente los dispositivos según lo que se describe en el procedimiento consulte "[Infecar targets por medio de la identificación manual](#)" En la página 108 .

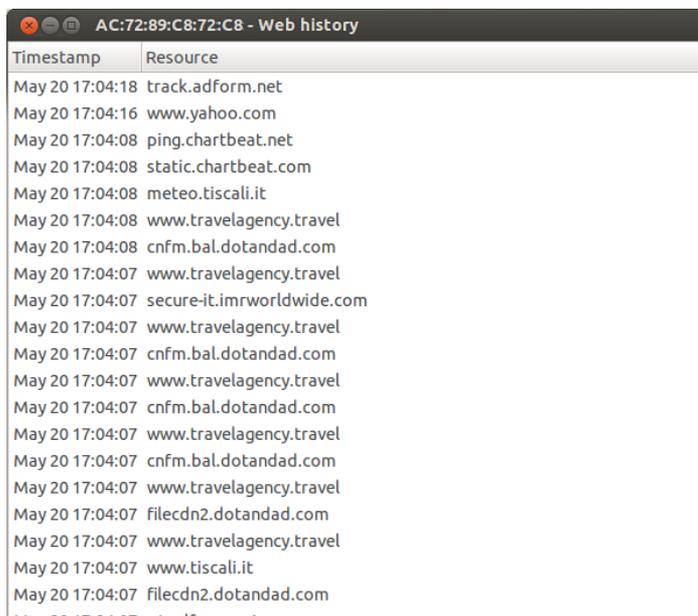
Identificar el target analizando el historial web

Para identificar un target:

Pasos

1. En la pestaña **Network Injector**, haga doble clic en el dispositivo a verificar: se abrirá una ventana con el historial de sitios web visitados por el navegador.

Resultado



Pasos**Resultado**

2. Si el dispositivo es del target, cierre el historial y realice el procedimiento **"Infectar targets por medio de la identificación manual"** En la página 108 .

Limpiar dispositivos infectados por error

Para eliminar la infección de los dispositivos, cierre el agent en RCS Console.

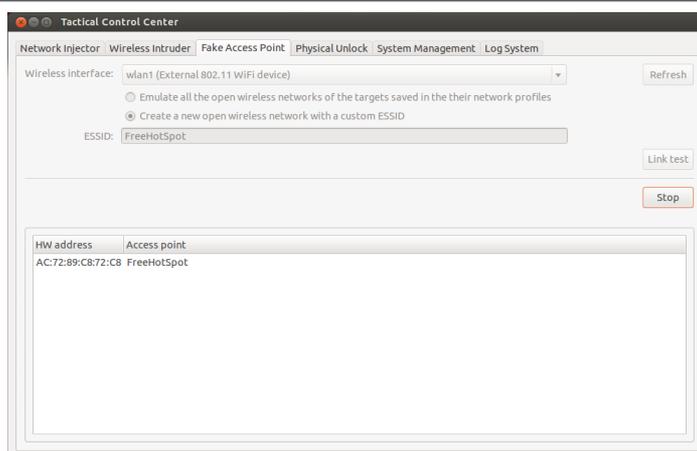
Emulación de un Punto de acceso conocido por el target

IMPORTANTE: antes de emular un Punto de acceso, detenga cualquier ataque en curso en la pestaña Network Injector.

Para transformar un Tactical Network Injector en un Punto de acceso conocido por los targets:

Pasos**Resultado**

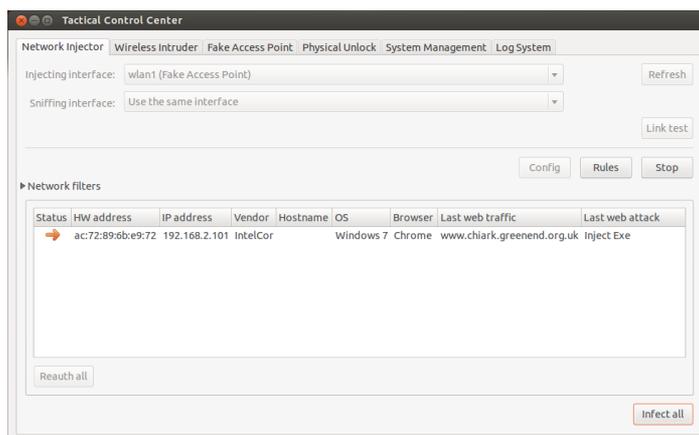
1. En la pestaña **Fake Access Point**, seleccione la interfaz de red a la cual escuchar, en la lista desplegable de la **Interfaz de red**.



2. Seleccione el tipo de emulación de Punto de acceso
3. Haga clic en **Iniciar**: Tactical Network Injector recuperará y mostrará los nombres de las redes Wi-Fi a las que suelen estar conectados los dispositivos.
4. Tactical Network Injector establecerá comunicaciones con los dispositivos simples, emulando el punto de acceso para cada red.

Pasos

5. En **Network Injector**, seleccione la misma interfaz de red que se muestra como punto de acceso en el menú desplegable de la **interfaz de Inyección**
6. Haga clic en **Iniciar**: se mostrarán los dispositivos conectados

Resultado

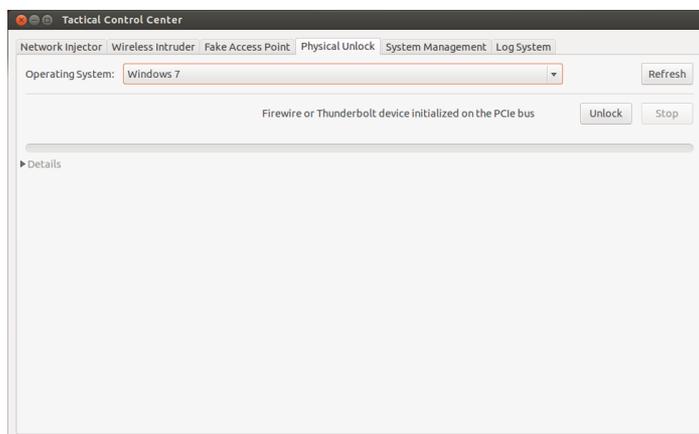
7. Infecte manualmente los dispositivos según lo que se describe en el procedimiento consulte "[Infectar targets por medio de la identificación manual](#)" En la página 108 .

Desbloquear una contraseña del sistema operativo.

Para desbloquear una contraseña del sistema operativo:

Pasos

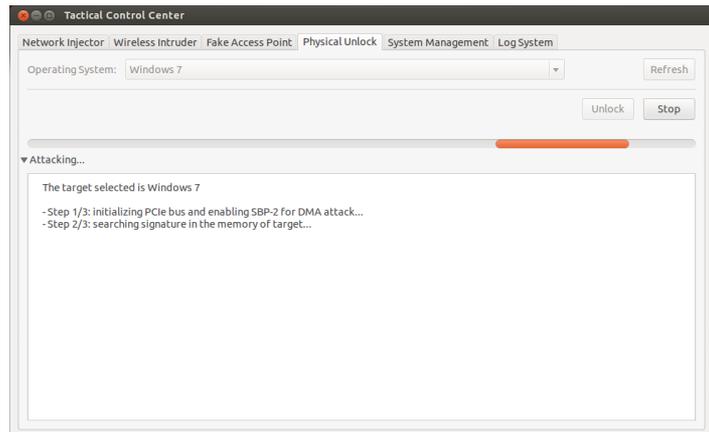
1. Conecte el Tactical Network Injector a la computadora del target a través de una conexión FireWire o Thunderbolt. Use el puerto ExpressCard/34 del lado de Tactical Network Injector.
2. En la pestaña **Desbloqueo físico**, haga clic en **Volver a cargar**: el sistema reconocerá el sistema operativo de la computadora y lo mostrará en **Sistema operativo**.
3. En la lista desplegable **Sistema operativo**, seleccione la versión del sistema operativo.

Resultado

Pasos

- Haga clic en **Desbloquear**: el sistema intentará desbloquear la contraseña y mostrará el progreso de la operation. Cuando termine se mostrará el resultado de la operation.

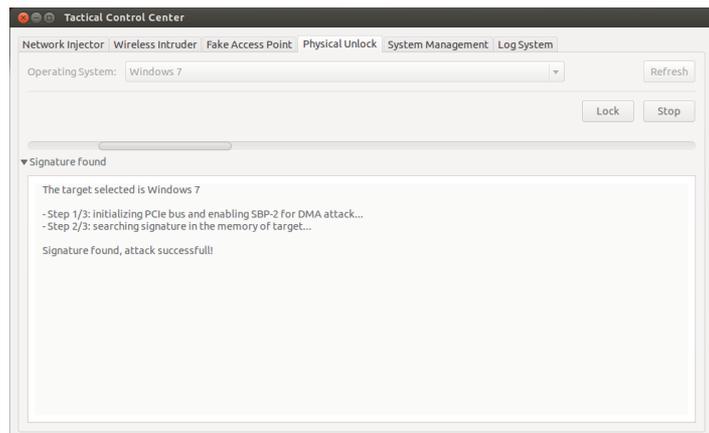
Resultado



- Para bloquear el sistema operativo, haga clic en **Bloquear**: se restaurará la contraseña y la computadora volverá a la condición anterior al procedimiento de desbloqueo.



NOTA: la clave **Bloquear** solo aparece si el procedimiento de desbloqueo se completó correctamente.



Configurar el acceso remoto a las aplicaciones

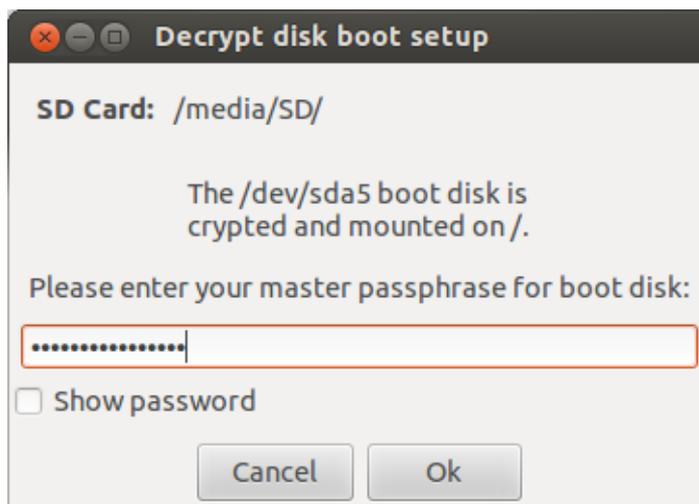
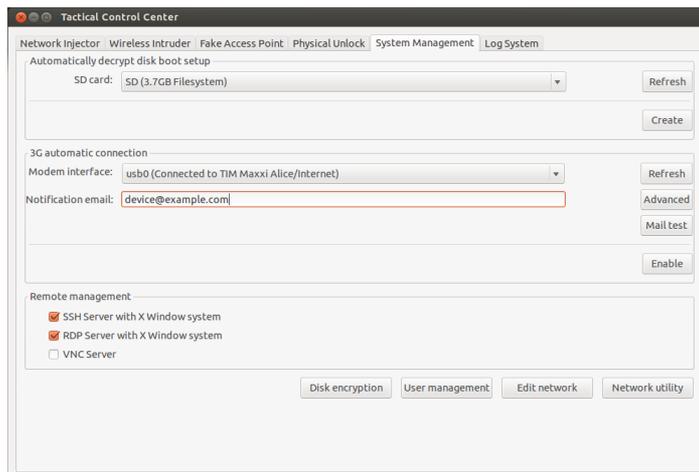
Para acceder a Tactical Control Center de forma remota:

Pasos

1. Inserte una tarjeta SD en la ranura de la computadora portátil.
2. En la pestaña **Administración del sistema** haga clic en **Volver a cargar**: el sistema reconocerá la tarjeta SD y la mostrará en **Tarjeta SD**.
3. Si se instalan varias tarjetas SD, seleccione la tarjeta requerida en el menú desplegable de **tarjetas SD** y haga clic en **Crear**.

4. Ingrese la contraseña de administrador del sistema y haga clic en **Aceptar**: el sistema generará una nueva contraseña y la guardará en la tarjeta SD.

Resultado



Pasos**Resultado**

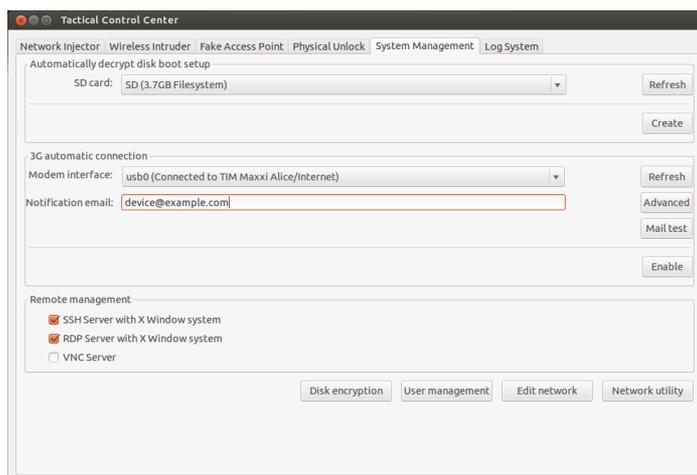
5. Conecte el módem al dispositivo.
6. En la pestaña **Administración del sistema** haga clic en **Volver a cargar**: el sistema reconocerá el módem y lo mostrará en la **Interfaz del módem**.
7. Si hay varios módems instalados, seleccione el módem deseado en la lista desplegable **Interfaz de módem**.
8. Para activar el envío de correos electrónicos con la dirección IP del dispositivo en cada conexión, siga estos pasos:
 - a. En **Correo electrónico de notificación** ingrese la dirección a la cual enviar el correo.
 - b. Haga clic en **Prueba de correo** para enviar un correo electrónico de prueba
 - c. Si no recibe el correo, haga clic en **Avanzada** para establecer manualmente el servidor de correos: aparecerá la ventana **Configuración avanzada de correo electrónico**.
 - d. Ingrese los datos indicados y haga clic en **Guardar**.
 - e. Haga clic en **Prueba de correo** para enviar un correo electrónico de prueba con el servidor configurado.
9. Para activar la conexión automática con el módem seleccionado, haga clic en **Activar**



NOTA: el módem activado en esta pestaña aparecerá en la pestaña **Network Injector**, en la lista desplegable **Interfaz de inyección** y se usará para infectar a los agents.



NOTA: es posible abrir directamente algunas ventanas útiles del sistema operativo por medio de los botones que se encuentran en la parte inferior de la pantalla. Consulte "[Qué debería saber acerca del acceso remoto al Control Center](#)" En la página 89 .



Apagar el Tactical Network Injector

No hay previsto ningún procedimiento particular. Solo apague normalmente la computadora.

Ver los detalles de una infección

Para ver los registros de la sesión actual, seleccione la pestaña **Sistema de registros**.

Para ver todos los archivos del registro, haga clic en la pestaña **Mostrar registros** en la pestaña **Sistema de registros**.



NOTA: todos los archivos de registro se guardan en el sistema de archivos en /var/log/td-config .

Datos del Tactical Control Center

Datos de la pestaña Network Injector

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Interfaz de inyección	Lista de interfaces de red conectadas. Seleccione la interfaz de inyección conectada a la red a la que está conectado el dispositivo que se invadirá. Al simular un punto de acceso, también se muestra la interfaz usada en la pestaña Fake Access Point . También se muestra el módem 3G configurado y activado para el acceso remoto en la pestaña Administración del sistema .
Interfaz de análisis de paquetes	Al igual que una interfaz de inyección u otra interfaz de red se usa solo para analizar paquetes.
Expresión regular	Expresión usada para filtrar los dispositivos conectados a la red. Se aplica a todos los datos transmitidos y recibidos por el dispositivo a través de la red, de cualquier tipo. <i>Consulte "Qué debería saber acerca de Tactical Control Center" En la página 82</i> .
Filtro de red BPF	Se usa para filtrar dispositivos usando la sintaxis BPF (Berkeley Packet Filter). Esta sintaxis incluye palabras clave acompañadas por calificadores: <i>Consulte "Qué debería saber acerca de Tactical Control Center" En la página 82</i> .

Datos encontrados del dispositivo

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Estado	<p>Estado de los dispositivos conectados a la red:</p> <p> : dispositivo desconocido. No puede infectarse por problemas relacionados con la autenticación. Fuerce la autenticación.</p> <p> : dispositivo en proceso de identificación.</p> <p> : dispositivo identificado y que puede ser infectado.</p> <p> : dispositivo infectado.</p>
Dirección MAC	Dirección de hardware de la tarjeta de red del dispositivo.
Dirección IP	Dirección IP de la red del dispositivo.
Proveedor	Marca de la tarjeta de red (bastante confiable).
Hostname	Nombre del dispositivo.
OS	Sistema operativo del dispositivo.
Navegador	Navegador web usado por el dispositivo.
Tráfico web más reciente	<p>Últimos sitios visitados por el dispositivo detectados y analizados en los últimos cinco minutos.</p> <p> NOTA: si el dispositivo no genera tráfico web al finalizar los cinco minutos, aparecerá el mensaje Idle. Esto generalmente ocurre cuando nadie está utilizando el dispositivo.</p>
Último ataque web	Último tipo de ataque y resultados. Para ver detalles adicionales, consulte la pestaña Sistema de registros .

Datos de la pestaña Wireless Intruder

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Interfaz inalámbrica	Lista de interfaces de red no conectadas. Seleccione la interfaz a conectar a la red Wi-Fi protegida a la que se quiere acceder.
Red ESSID	Nombre de la red local a la cual acceder.

<i>Datos</i>	<i>Descripción</i>
Tipo de ataque	Tipos de identificación de contraseña disponibles. Ataque de diccionario para WPA/WPA2 Ataque de fuerza bruta para WEP Ataque de fuerza bruta de PIN para WPS <i>Consulte "Qué debería saber acerca de la identificación de contraseñas de redes Wi-Fi" En la página 86 .</i>

Datos de la pestaña Fake Access Point

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Interfaz inalámbrica	Lista de interfaces de red no conectadas. Seleccione la interfaz que se mostrará como red Wi-Fi.
ESSID	Nombre de la red ESSID que se pretende crear.
Dirección MAC	Dirección de hardware de la tarjeta de red del dispositivo.
Punto de acceso	Nombre del Punto de acceso esperado por el dispositivo.

Datos de la pestaña Administración del sistema

A continuación se describen los datos:

<i>Datos</i>	<i>Descripción</i>
Tarjeta SD	Tarjeta de memoria para administrar la contraseña codificada del disco.
Interfaz del módem	Módem 3G para la conexión del dispositivo.
Correo electrónico de notificación	Dirección de correo electrónico a la cual se envía la IP del dispositivo cada vez que se conecta a la red.
	 IMPORTANTE: campo obligatorio para las direcciones IP dinámicas.

Administración remota Protocolo de red para el acceso remoto.

Otras aplicaciones instaladas en Network Injectors

Introducción

Los Network Injectors vienen instalados con algunas aplicaciones útiles de terceros.

Aplicaciones

A continuación se encuentran las aplicaciones instaladas en Tactical Network Injector y Network Injector Appliance:



NOTA: para ver las instrucciones de las aplicaciones, consulte los documentos entregados por los fabricantes de las aplicaciones.

<i>Nombre de la aplicación</i>	<i>Descripción</i>
Disniff	Paquete de herramientas que permite interceptar el tráfico de la red
hping3	Generador de tráfico en la red
Kismet	Herramienta de monitoreo para las redes Wireless 802.11b
Macchanger	Herramienta para cambiar la dirección MAC de la interfaz de red
Nbtscan	Detector de red que permite encontrar la información de los nombres NetBIOS
Netdiscover	Escáner de dirección de red activa/pasiva por medio de consultas ARP
Ngrep	grep de tráfico de red
Nmap	Mapeador de red
P0f	Herramienta Passive OS fingerprinting
Sslsniff	Herramienta de ataque Man-in-the-middle para tráfico de red SSL/TLS
Sslstrip	Herramienta de ataque Man-in-the-middle y hijacking para tráfico de red SSL/TLS
Tcpdump	Analizador de tráfico de red desde el intérprete de comandos
Wireshark	Analizador del tráfico de red
Xprobe	Herramienta de identificador de OS remoto

Monitoreo del sistema

Presentación

Introducción

El monitoreo del sistema garantiza el control constante del estado de los componentes y el uso de la licencia.

Contenido

En esta sección se incluyen los siguientes temas:

Monitoreo del sistema (monitor)	122
Datos de monitoreo del sistema (Monitor)	123

Monitoreo del sistema (monitor)

Para monitorear el sistema:

- Sección Monitor

Propósito

Esta función le permite:

- monitorear el estado del sistema en términos de hardware y software
- monitorear las licencias usadas en comparación con las que se compraron



Llamada al servicio: póngase en contacto con su gerente de cuenta de HackingTeam si necesita más licencias.

Cómo se ve la función

Así es como se ve la página:

Type	Name	Address	Last contact	Status	CPU Proc	CPU Host	Disk Free
📡	Satellite	127.0.0.1	2014-05-30 11:57:21	✓	70%	15%	20%
👤	Master	127.0.0.1	2014-05-30 11:57:21	✓	70%	15%	20%
💡	Intelligence	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
💰	Money	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
👁️	Or	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
👤	Anonymizer	172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
👤	Anonymizer	172.20.20.2	2014-05-30 11:57:21	✓	90%	70%	70%
👤	Anonymizer	172.20.20.3	2014-05-30 11:57:21	✓	90%	70%	70%
👤	Anonymizer	172.20.20.4	2014-05-30 11:57:21	✓	90%	70%	70%
👤	Anonymizer	172.20.20.5	2014-05-30 11:57:21	✓	90%	70%	70%

Área Descripción

- 1 Menú de RCS.

Monitor ¹: indica la cantidad actual de alarmas del sistema que se activaron.

- 2 Barra de herramientas de la ventana.

Área Descripción

- 3** Lista de componentes de RCS y su estado:
-  Alarma (genera y envía un correo electrónico al grupo de alerting)
 -  Advertencia
 -  Componente en funcionamiento
- 4** Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz consulte "[Elementos y acciones comunes de la interfaz](#)" En la página 12 .

Para ver una descripción de los datos en esta ventana consulte "[Datos de monitoreo del sistema \(Monitor\)](#)" abajo .

Datos de monitoreo del sistema (Monitor)

Datos del monitoreo de los componentes del sistema

A continuación se muestran los datos de monitoreo del sistema:

<i>Datos</i>	<i>Descripción</i>
Tipo	Tipo y nombre de los componentes monitoreados.
Nombre	A continuación se muestran algunos ejemplos: <ul style="list-style-type: none">  Anonymizer  Carrier  Collector  Database  Network Controller
Dirección	Dirección IP del componente.

<i>Datos</i>	<i>Descripción</i>
Último contacto	Fecha y hora de la última sincronización.
Estado	Estado del componente en la última sincronización:  Alarma: el componente no está funcionando, póngase en contacto con el grupo de alerting para repararlo de inmediato.  Advertencia: el componente indica una situación de riesgo, póngase en contacto con el administrador del sistema para que realice las revisiones necesarias.  Componente en funcionamiento.
Proceso de CPU	% de uso de CPU por parte del proceso particular.
Host de CPU	% de uso de CPU por parte del servidor.
Espacio libre en el disco	% de espacio libre en el disco.

Datos de monitoreo de la licencia

A continuación se describen los datos de monitoreo de la licencia: para las licencias restringidas, el formato es "x/y", donde "x" es la cantidad de licencias que el sistema utiliza actualmente e "y" es la cantidad máxima de licencias.



PRECAUCIÓN: *si todas las licencias están en uso, cualquier agent nuevo quedará en una cola de espera hasta que se libere una licencia o se compren más licencias.*

<i>Datos</i>	<i>Descripción</i>
Tipo de licencia	Tipo de licencia actualmente en uso para los agents. reusable: una licencia de agent puede volver a utilizarse después de que se desinstala. oneshot: la licencia de un agent solo es válida para una instalación.  NOTA: la licencia solo puede actualizarse si el usuario tiene autorización Modificación de licencias.
Usuarios	Cantidad de usuarios actualmente en uso por parte del sistema y cantidad máxima admitida.

Datos	Descripción
Agent	Cantidad de agents actualmente utilizados por el sistema y cantidad máxima admitida.
De escritorio Móvil	Cantidad de agents de escritorio y móviles actualmente utilizados por el sistema y cantidades máximas admitidas, respectivamente.
Servidores distribuidos	Cantidad de bases de datos actualmente utilizadas por el sistema y cantidad máxima admitida.
Collectors	Cantidad de Collectors actualmente utilizados por el sistema y cantidad máxima admitida.
Anonymizers	Cantidad de Anonymizers actualmente utilizados por el sistema y cantidad máxima admitida.

Anexo: acciones

Presentación

Introducción

Un agent es un grupo complejo de eventos, acciones, módulos y vectores de instalación. A continuación se muestra una lista de acciones simples con una descripción detallada de las opciones de configuración.

Contenido

En esta sección se incluyen los siguientes temas:

Lista de subacciones	127
Acción Destroy	127
Acción Execute	128
Acción Log	129
Acción SMS	129
Acción Synchronize	130
Acción Uninstall	131

Lista de subacciones

Descripción de los datos de las subacciones

A continuación se describen las subacciones:

<i>Datos</i>	<i>Descripción</i>
Nombre	Nombre arbitrario asignado a una acción
Subacciones	Lista de tipos de subacciones

Descripción de tipos de subacciones



NOTA: algunas subacciones pueden perderse debido a que no son compatibles con ciertos sistemas operativos.

A continuación se describen los tipos de subacciones disponibles:

<i>Acción</i>	<i>Dispositivo</i>	<i>Descripción</i>
Destroy	de escritorio, móvil	Hace que el dispositivo del target quede inservible.
Execute	de escritorio, móvil	Ejecuta un comando arbitrario en la máquina del target.
Log	de escritorio, móvil	Crea un mensaje personalizado.
SMS (mensaje de texto)	móvil	Envía un SMS oculto desde el dispositivo del target.
Synchronize	de escritorio, móvil	Ejecuta una sincronización con el Collector.
Desinstalación	de escritorio, móvil	Elimina el agent del dispositivo.



Acción Destroy

Propósito

La acción **Destroy** hace que el dispositivo del target quede inservible de forma temporal o permanente.

Parámetros

Nombre	Descripción
Permanente	El dispositivo queda inservible permanentemente.
	 ADVERTENCIA: es posible que el dispositivo necesite reparación.



Acción Execute

Propósito

La acción **Execute** ejecuta un comando arbitrario en el dispositivo del target. Si es necesario, se puede especificar la configuración del comando y las variables del entorno. El programa se ejecutará con los permisos del usuario que esté conectado al sistema en el momento de la ejecución.

Cualquier resultado del comando se puede ver en la página **Comandos**. Consulte "[Página de comandos](#)" En la página 45 .



ADVERTENCIA: aunque todos los comandos se ejecuten por medio del sistema de ocultamiento del agent para ser invisibles, cualquier cambio en el sistema de archivos (p. ej.: un archivo creado en el escritorio) será visible para el usuario. Preste atención.



ADVERTENCIA: se deben evitar programas que requieran la interacción del usuario o que abran interfaces gráficas.



Sugerencia: utilice aplicaciones iniciadas por una línea de comandos o un archivo en lotes, ya que el agent oculta sus procesos (y la ventana de línea de comandos correspondiente).

Referencia a la carpeta del agent

A la cadena de comandos se le puede agregar la variable \$dir\$ del entorno virtual que hace referencia a la carpeta de instalación del agent (oculta).

Datos importantes

<i>Campo</i>	<i>Descripción</i>
--------------	--------------------

Comando	Comando a ejecutar.
----------------	---------------------



Sugerencia: utilice una ruta absoluta.

Acción Log

Propósito

La acción **Log** crea un mensaje personalizado.



NOTA: los mensajes y registros personalizados que provienen de un agent se muestran en la sección **Info**. Consulte "[Página del agent](#)" En la página 41

Parámetros

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Texto	Texto del mensaje que aparece en la sección Info .
--------------	---

Acción SMS

Propósito

La acción **SMS** envía un SMS (mensaje de texto) oculto desde el dispositivo del target con la posición del dispositivo y los datos de la tarjeta SIM.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Número	El número de teléfono al que se envía el mensaje.
---------------	---

Position	Agrega al mensaje la celda GPS o la posición GSM del target.
-----------------	--

SIM	Agrega al mensaje la información de la tarjeta SIM del teléfono.
------------	--

Texto	Texto del mensaje.
--------------	--------------------

Acción Synchronize

Propósito

La acción **Synchronize**, sincroniza el agent y el RCS Server.

El proceso de sincronización está dividido en los siguientes pasos:

Paso Descripción

- 1 Autenticación recíproca del agent/RCS Server.
- 2 Sincronización temporal del agent/RCS Server.
- 3 Eliminación del agent en caso de cierre de la actividad relacionada.
- 4 Actualización de la configuración del agent.
- 5 Carga de todos los archivos en la cola "cargar".
- 6 Descarga de todos los archivos en la cola "descargar".
- 7 Descarga de toda la evidencia recopilada por el agent, con eliminación simultánea segura.
- 8 Eliminación segura en el agent de toda la evidencia descargada.

Configuración de escritorio

<i>Nombre</i>	<i>Descripción</i>
Host	Nombre del Anonymizer o Collector a conectar para la sincronización. Seleccione el nombre del servidor o ingrese el FQDN (nombre DNS) o dirección IP en el cuadro combinado.
Banda	Ancho de banda máximo que se puede usar durante la sincronización.
Retraso mínimo	Retraso mínimo en segundos entre el envío de una evidencia enviada y otra.
Retraso máximo	Retraso máximo en segundos entre el envío de una evidencia enviada y otra.
Cuando se completa correctamente, se detiene	Si está activado, la cadena de subacciones se interrumpe cuando la sincronización se completa correctamente. Las subacciones que permanecen en cola no se ejecutan.

Configuración móvil

<i>Nombre</i>	<i>Descripción</i>
Host	Nombre o dirección IP del Anonymizer o Collector al cual conectarse para la sincronización. Seleccione el nombre del servidor o ingrese el FQDN (nombre DNS) o dirección IP en el cuadro combinado.
Cuando se completa correctamente, se detiene	Si está activado, la cadena de subacciones se interrumpe cuando la sincronización se completa correctamente. Las subacciones que permanecen en cola no se ejecutan.
Tipo	<p>Internet: sincronización a través de una conexión a Internet.</p> <ul style="list-style-type: none"> • Forzar Wi-Fi: sincronización a través de una red Wi-Fi. Fuerza una conexión de datos Wi-Fi con cualquier red Wi-Fi abierta o presente, disponible antes del inicio de la sincronización. • Forzar Celda: sincronización a través de una red GPRS/UMTS/3G. Fuerza una conexión de datos GPRS/UMTS/3G con el operador de telefonía móvil antes de iniciar la sincronización. <p>APN: especifica las credenciales de acceso a un APN que el teléfono puede usar para recopilar datos. Esto es útil ya que evita cobrar al target por el tráfico generado por el agent.</p>

Criterio de selección del tipo de conexión (Windows Phone)

Para Windows Phone, el sistema define internamente el tipo de conexión a utilizar de acuerdo con los parámetros establecidos.

Si el dispositivo está configurado para conectarse por Wi-Fi y 3G/4G y hay una conexión Wi-Fi configurada, el sistema utilizará la red 3G/4G cuando la pantalla del dispositivo esté apagada y no se esté cargando o, en caso contrario, usará la red Wi-Fi.

Acción Uninstall

Propósito

La acción **Uninstall** elimina el agent del sistema del target. Se eliminarán todos los archivos.



NOTA: en un BlackBerry, la eliminación del agent requiere de un reinicio automático.



NOTA: si el dispositivo no tiene privilegios raíz en Android, el usuario debe autorizar la desinstalación. Para obtener más información sobre cómo saber si cuenta con privilegios raíz, consulte "[Qué debería saber acerca de Android](#)" En la página 158 .



NOTA: en Windows Phone, la eliminación del agent implica borrar todos los archivos generados por el agent, pero los íconos de la aplicación permanecerán en la lista de programas.

Anexo: eventos

Presentación

Introducción

Un agent es un grupo complejo de eventos, acciones, módulos y vectores de instalación. A continuación se muestra una lista de eventos simples con una descripción detallada de las opciones de configuración.

Contenido

En esta sección se incluyen los siguientes temas:

Lista de eventos	134
Evento AC	135
Evento Battery	135
Evento Call	136
Evento Connection	136
Evento Idle	137
Evento Position	137
Evento Process	137
Evento Quota	138
Evento Screensaver	138
Evento SimChange	139
Evento SMS	139
Evento Standby	139
Evento Timer	140
Evento Window	140
Evento WinEvent	140

Lista de eventos

Descripción de los datos de los eventos

Los eventos se describen a continuación:

<i>Datos</i>	<i>Descripción</i>
Activado	Activa o desactiva un evento.
Nombre	Nombre asignado al evento.
Tipo	Lista de tipos de eventos. Consulte la tabla que se muestra a continuación.

Descripción de los tipos de eventos



NOTA: algunos eventos pueden perderse debido a que no son compatibles con ciertos sistemas operativos.

Los tipos de eventos se describen a continuación:

<i>Evento</i>	<i>Dispositivo</i>	<i>Activa una acción cuando...</i>
AC	móvil	el teléfono celular se está cargando.
Battery	móvil	el nivel de carga de la batería está dentro del rango especificado.
Call	móvil	hay una llamada entrante o saliente.
Connection	de escritorio, móvil	el agent encuentra una conexión de red activa.
Idle	de escritorio	el usuario no interactúa con la computadora por un período de tiempo determinado.
Position	móvil	el dispositivo entra o sale de una posición determinada.
Process	de escritorio, móvil	se inicia una aplicación o se abre una ventana en el dispositivo.
Quota	de escritorio	el espacio que la evidencia ocupa en el disco del dispositivo excede el límite establecido.
Screensaver	de escritorio	el protector de pantalla se abre en el dispositivo del target.
SimChange	móvil	se cambia la tarjeta SIM.
SMS (mensaje de texto)	móvil	el dispositivo recibe un mensaje de texto del número indicado.

<i>Evento</i>	<i>Dispositivo</i>	<i>Activa una acción cuando...</i>
Standby	móvil	El dispositivo está en modo de espera.
Timer	de escritorio, móvil	transcurre un intervalo de tiempo especificado.
Window	de escritorio	se abre una ventana.
WinEvent	de escritorio	el sistema operativo registra un evento de Windows.

Evento AC

Propósito

El evento **AC** activa una acción cuando el teléfono celular se está cargando.

Evento Battery

Propósito

El evento **Battery** activa una acción cuando el nivel de carga de la batería está dentro del rango especificado.



Sugerencia: para reducir el impacto en el uso de la batería, es mejor asociar el evento **Battery**, establecido entre 0%-30%, a las acciones **Iniciar** y **Detener crisis**. De esta manera, si el nivel de carga de la batería desciende por debajo del valor establecido, se suspenderán las actividades del agent que consuman más energía.



ADVERTENCIA: ¡el módulo Crisis se puede configurar para anular la sincronización!

Parámetros

<i>Nombre</i>	<i>Descripción</i>
Min	Porcentaje mínimo de carga de la batería. Un porcentaje superior a este límite activará un evento.
Max	Porcentaje máximo de carga de la batería. Un porcentaje inferior a este límite activará un evento.

Evento Call

Propósito

El evento **Call** activa una acción cuando hay una llamada entrante o saliente.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Número	número de teléfono de quien llama o de quien recibe la llamada (o parte de este).
---------------	---



Sugerencia: déjelo en blanco para que se active con cualquier número.

Evento Connection

Propósito

El evento **Connection** activa una acción cuando el agent encuentra una red de conexión activa.

Para un dispositivo de escritorio, escriba la dirección de destino de la conexión.

Para un dispositivo móvil, el evento activa una acción en el momento en que el dispositivo obtiene una dirección IP válida en cualquier interfaz de red (p. ej.: Wi-Fi, ActiveSync, GPRS/3G+), y cancela la acción cuando finalizan todas las conexiones.

Configuración de escritorio

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Dirección IP	Dirección IP de destino para la conexión
---------------------	--



Escriba 0.0.0.0 para indicar cualquier dirección.



NOTA: no se tienen en cuenta las conexiones con direcciones locales en la misma subred del target.

Máscara de red	Máscara de red aplicada a la dirección IP.
-----------------------	--

Puerto	Puerto usado para identificar a la conexión.
---------------	--

ZZ Evento Idle

Propósito

El evento **Idle** activa una acción cuando el usuario no interactúa con la computadora por un período de tiempo determinado.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Hora	Segundos de inactividad. El evento se activa cuando finaliza este intervalo de tiempo.
-------------	--

Evento Position

Propósito

El evento **Position** activa una acción cuando el target entra o sale de una determinada posición. La posición puede estar definida por coordenadas GPS y un rango o por el ID de una celda GSM.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Tipo	Tipo de posición a utilizar.
-------------	------------------------------

GPS

- **Latitud, Longitud:** coordenadas
- **Distancia:** rango a partir de las coordenadas.

Celda GSM (todos los sistemas operativos, excepto Windows Phone)

- **País, Red, Área, ID:** datos de la celda GSM. Ingrese '*' para ignorar un campo. Por ejemplo, si se completa el campo **País** y los otros tres campos se completan con '*', el evento se activará en el momento en que el dispositivo entre o salga del país especificado.



Evento Process

Propósito

El evento **Process** activa una acción cuando se inicia una aplicación o se abre una ventana en el dispositivo.

Parámetros

Nombre *Descripción*

Tipo	<p>Nombre del proceso: el evento activa una acción cuando se inicia el proceso especificado.</p> <p>Título de la ventana: el evento activa una acción cuando se mantiene la atención en una ventana determinada.</p>
Cadena	<p>Nombre o parte del nombre del programa o del título de la ventana.</p> <p> Sugerencia: use caracteres especiales al especificar un programa (p. ej.: "*Calculadora*")</p>
Enfoque	<p>(solo para dispositivos de escritorio) Al seleccionarlo, el evento activa una acción solo cuando el proceso o ventana se encuentran en primer plano.</p>

Evento Quota

Propósito

El evento **Quota** activa una acción cuando el espacio del disco del dispositivo que se utiliza para almacenar la evidencia recopilada excede el límite establecido.

Cuando el espacio del disco se encuentra por debajo del límite, la acción será cancelada en la siguiente sincronización.

Parámetros

Nombre *Descripción*

Quota	Espacio en el disco que se usará para almacenar la evidencia recopilada.
--------------	--

Evento Screensaver

Propósito

El evento **Screensaver** activa una acción cuando se enciende el protector de pantalla en el dispositivo del target.

Evento SimChange

Propósito

El evento **SimChange** activa una acción cuando se cambia la tarjeta SIM.

Evento SMS

Propósito

El evento **SMS** activa una acción cuando se recibe un mensaje de texto específico de cierto número. El mensaje no se mostrará entre los mensajes recibidos del teléfono.



ADVERTENCIA: los mensajes entrantes solo se eliminan en BlackBerry OS 5.x.



NOTA: el mensaje recibido no se mostrará en el dispositivo del target.

Parámetros

Nombre *Descripción*

Número Número de teléfono del remitente del SMS. Cualquier SMS de este número permanecerá oculto.

Texto Parte del texto del mensaje que debe coincidir.



IMPORTANTE: la cadena no distingue entre mayúsculas y minúsculas.



Evento Standby

El evento **Standby** activa una acción cuando el dispositivo entra en modo de reposo.

Evento Timer

Propósito

El **evento Timer** activa una acción en los intervalos indicados.

Cuando el evento ocurre, se ejecuta la acción asociada a la acción **Iniciar**.

Durante el período que transcurre entre el inicio y la parada del evento, la acción **Repetir** se repite en el intervalo especificado por el conector asociado.

Cuando el evento termina, se ejecuta la acción **Detener**.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
---------------	--------------------

Tipo	Tipo de intervalo:
-------------	--------------------

- **Ciclo:** activa una acción y la repite de forma indefinida en cada intervalo, según lo que se especifique en la acción **Repetir**.
- **Diario:** activa una acción diaria a las horas especificadas en **Desde** y **Hasta**
- **Fecha:** activa una acción en el período indicado en **Desde** y **Hasta**



NOTA: seleccione **Siempre** para una acción continua.

- **Después de la instalación:** activa una acción después de cierta cantidad de días (**Días**) a partir de la instalación del agent.

Evento Window

Propósito

El evento **Ventana** activa una acción cuando se abre una ventana.

Evento WinEvent

Propósito

El evento **WinEvent** activa una acción cuando el sistema operativo registra un evento Windows.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
ID del evento	ID del evento Windows.
Origen	Origen del evento Windows (p. ej.: sistema, aplicación)

Anexo: módulos

Presentación

Introducción

Un agent es un grupo complejo de eventos, acciones, módulos y vectores de instalación. A continuación se muestra una lista de módulos simples con una descripción detallada de las opciones de configuración.

Contenido

En esta sección se incluyen los siguientes temas:

Lista de módulos	143
Módulo Addressbook	145
Módulo Application	145
Módulo Calendar	145
Módulo Call	145
Módulo Camera	146
Módulo Chat	146
Módulo Clipboard	147
Módulo Conference	147
Módulo Crisis	147
Módulo Device	149
Módulo File	149
Módulo Keylog	150
Módulo Livemic	150
Módulo Messages	151
Módulo Mic	152
Módulo Money	153
Módulo Mouse	153
Módulo Password	154
Módulo Position	154
Módulo Screenshot	154
Módulo URL	155

Lista de módulos



NOTA: algunos módulos pueden perderse debido a que no son compatibles con ciertos sistemas operativos.

A continuación se describen los módulos de registro:

Módulo	Configuración	Dispositivo	Registro...
Accessed files	básica	de escritorio	documentos o imágenes que abrió el target.
Addressbook	avanzada	de escritorio, móvil	contactos.
Application	avanzada	de escritorio, móvil	aplicaciones usadas.
Calendar	avanzada	de escritorio, móvil	calendario.
Call	avanzada	de escritorio, móvil	llamadas (p. ej.: GSM y VoIP).
Calls	básica	de escritorio, móvil	llamadas (p. ej.: teléfono, Skype, MSN).
Camera	básica, avanzada	de escritorio, móvil	Imágenes de la cámara web.
Chat	avanzada	de escritorio, móvil	chat (p. ej.: Skype, BlackBerry Messenger).
Clipboard	avanzada	de escritorio, móvil	información copiada en el portapapeles.
Contacts and Calendar	básica	de escritorio, móvil	contactos y calendario.
Dispositivo	avanzada	de escritorio, móvil	información del sistema.
File	avanzada	de escritorio	archivos abiertos por el target.
Keylog	avanzada	de escritorio, móvil	teclas presionadas en el teclado.
Keylog, Mouse and Password	básica	de escritorio	teclas presionadas en el teclado, clics del mouse y contraseñas guardadas.
Messages	avanzada	de escritorio, móvil	correos electrónicos, SMS, MMS.

Módulo	Configuración	Dispositivo	Registro...
Messages	básica	de escritorio, móvil	correos electrónicos, SMS y chat.
Mic	avanzada	de escritorio, móvil	audio de un micrófono.
Money	avanzada	de escritorio	información sobre el monedero digital de criptomonedas (p. ej.: Bitcoin).
Mouse	avanzada	de escritorio	clics del mouse.
Contraseña	avanzada	de escritorio, móvil	contraseñas guardadas.
Position	básica, avanzada	de escritorio, móvil	posición geográfica del target.
Screenshots	básica, avanzada	de escritorio, móvil	ventanas abiertas en la pantalla del target.
URL	avanzada	de escritorio, móvil	direcciones URL visitadas.
Visited websites	básica	de escritorio, móvil	direcciones URL visitadas.

A continuación se describen otros tipos de módulos:

Módulo	Configuración	Dispositivo	Acción
Conference	avanzada	móvil	Crea una conferencia entre 3 personas.
Crisis	avanzada	de escritorio, móvil	Reconoce situaciones de crisis (p. ej.: un analizador de paquetes ejecutándose). Puede desactivar temporalmente las sincronizaciones y todos los comandos.
Infección	avanzada	de escritorio	Eliminado a partir de la versión 8.4 de RCS.
Livemic	avanzada	móvil	Escucha las conversaciones en tiempo real.
Online Synchronization	básica	de escritorio, móvil	Sincroniza el agent con RCS para permitir recibir evidencia y restablecer el agent.

Módulo Addressbook

Propósito

El módulo **Addressbook** registra toda la información encontrada en la agenda del dispositivo. La versión de escritorio del dispositivo importa los contactos de Outlook, Skype y otras fuentes.

Módulo Application

Propósito

El módulo **Application** registra el nombre y la información de los procesos abiertos y cerrados del dispositivo del target.

La evidencia mostrará todas las aplicaciones usadas por el target en orden cronológico.

Módulo Calendar

Propósito

El módulo **Calendar** registra toda la información encontrada en el calendario del dispositivo del target. La versión de escritorio importa el calendario de Outlook y otras fuentes.

Módulo Call

Propósito

El módulo **Call** captura archivos de audio e información (hora de inicio, duración, persona que llamó y números a los que se llamó) para todas las llamadas que el target hizo o recibió.

En un dispositivo de escritorio, el módulo **Call** intercepta todas las conversaciones de voz en las aplicaciones compatibles.

En un dispositivo móvil, el módulo **Call** intercepta todas las llamadas (GSM y VoIP).

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Activar grabación de llamadas	(solo dispositivos móviles) Activa la grabación de llamadas. Si está desactivado, no se grabará el audio de las llamadas.
Tamaño del búfer	Tamaño del búfer de obtención usado para los sectores de audio.
Calidad	Calidad de audio (1=máxima compresión, 10=mejor calidad).

Módulo Camera

Propósito

El módulo **Camera** captura una imagen de la cámara integrada.



ADVERTENCIA: la captura de una imagen en una computadora de escritorio causa que el LED de la cámara destelle.

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Calidad	Calidad de la imagen (baja, media, alta).

Módulo Chat

Propósito

El módulo **Chat** registra todas las sesiones de chat del target. Cada mensaje se captura como una pieza única de evidencia.



IMPORTANTE: para Android, se requieren privilegios raíz para capturar chat. Consulte "[Qué debería saber acerca de Android](#)" En la página 158 .



IMPORTANTE: para que este módulo se inicie cuando el dispositivo se reinicia en BlackBerry, el teléfono debe estar en espera por varios minutos (luz de fondo apagada).

Módulo Clipboard

Propósito

El módulo **Clipboard** guarda el contenido del portapapeles en formato de texto.

Módulo Conference

Propósito

El módulo **Conference** llama al número indicado por medio de la creación de una conferencia cuando el target hace una llamada. El número del receptor puede escuchar la conversación en tiempo real.



IMPORTANTE: el funcionamiento del módulo depende de las características del operador telefónico. El target podría enterarse de que está en conferencia si el operador telefónico agrega una señal acústica mientras espera que inicie la llamada.

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Número	número de teléfono del receptor

Módulo Crisis

Comportamiento en dispositivos de escritorio

El módulo **Crisis** se activa (automáticamente o mediante una acción específica) y reconoce situaciones peligrosas en la máquina que pueden delatar la presencia del agent en el dispositivo (p. ej.: analizador de paquetes ejecutándose). Puede desactivar temporalmente las sincronizaciones y todos los comandos.

Este módulo aumenta su capacidad de permanecer oculto frente al software de protección.



NOTA: **Crisis** se puede activar de forma predeterminada en el dispositivo de escritorio para que el agent pueda detectar automáticamente situaciones peligrosas, y actuar en consecuencia (p. ej.: actuar sigilosamente).

Comportamiento en dispositivos móviles

El módulo **Crisis** se utiliza para suspender actividades que requieran un mayor uso de la energía de la batería. Según su configuración, este módulo puede desactivar temporalmente algunas funciones.

En un dispositivo móvil, el módulo **Crisis** debe iniciarse explícitamente con una acción específica (p. ej.: el agent se inicia cuando el nivel de la batería es demasiado bajo) y se detiene cuando finaliza la acción anormal.



NOTA: este módulo no crea evidencia.

Datos importantes de los dispositivos de escritorio

En dispositivos de escritorio, la configuración predeterminada no debe cambiarse a menos que lo sugiera el equipo de servicio técnico de RCS.

<i>Campo</i>	<i>Descripción</i>
Inhibir red	Inhíbe la sincronización mientras hay procesos potencialmente peligrosos.
Inhibidores (de red)	Lista de procesos que evitarán la sincronización mientras se ejecutan.
Inhibir hooking	Inhíbe el hooking de un programa mientras un proceso potencialmente peligroso está funcionando.
Inhibidores (hooking)	Lista de procesos que evitarán el hooking mientras se ejecutan.
Process	Proceso a agregar a la lista.

Datos importantes de los dispositivos móviles

En la versión para dispositivos móviles, se pueden especificar las funciones a agregar:

<i>Campo</i>	<i>Descripción</i>
Micrófono	si está seleccionado, impide la grabación de audio por micrófono
Calls	si está seleccionado, impide la grabación de audio de llamadas
Camera	si está seleccionado, impide la toma de fotos por la cámara
Position	si está seleccionado, impide el uso de GPS
Sincronización	si está seleccionado, impide la sincronización



Advertencia: ¡operaciones muy arriesgadas! ¡Antes de impedir la sincronización, póngase en contacto con el servicio técnico de HackingTeam! Puede perder permanentemente a su agent.

Módulo Device

Propósito

El módulo **Device** registra información del sistema (p. ej.: tipo de procesador, memoria en uso, sistema operativo instalado, privilegios raíz). Puede ser útil para monitorear el uso de la memoria del disco y recuperar la lista de aplicaciones instaladas.



NOTA: para Android, si el dispositivo tiene privilegios raíz, el tipo de evidencia **Device** lo indica como **root:yes**.

Datos importantes de los dispositivos móviles

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Recupera la lista de aplicaciones	Además de la información del sistema, registra la lista de aplicaciones instaladas.

Módulo File

Propósito

El módulo **File** registra todos los archivos abiertos en la computadora del target. También se puede capturar el archivo cuando se abre.

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Inclusiones del filtro	Lista de extensiones de archivo que se registrarán. Opcionalmente puede especificar el proceso para registrar el archivo solo cuando se esté ejecutando o cuando ese proceso lo abra.
Exclusiones del filtro	Lista de extensiones que no se registrarán. Opcionalmente puede especificar el proceso para ignorar el archivo solo cuando se esté ejecutando o cuando ese proceso lo abra.

<i>Campo</i>	<i>Descripción</i>
Máscara	<p>Cadena para filtrar el proceso y el archivo que se van a registrar o a ignorar.</p> <p>Sintaxis <i>Proceso</i> <i>Filtro</i></p> <p>Ejemplo de funciones que se usan para registrar "skype.exe *.*" "word.exe *John*.doc"</p> <p>Ejemplo de funciones que se usan para ignorar "skype.exe *.dat"</p>
Registra la ruta y el método de acceso	Registra el tipo de ruta del archivo y acceso (p. ej.: lectura, escritura)
Capturar contenido del archivo	Si está activado, el archivo se copia y se descarga en el primer acceso.
Tamaño máximo/mínimo	Máximo y mínimo tamaño admitido para el archivo a descargar.
Más reciente que	Fecha mínima de creación del archivo a descargar.

Módulo Keylog

Propósito

El módulo **Keylog** registra todas las teclas presionadas en el dispositivo del target.



NOTA: es compatible con todos los caracteres Unicode a través de IME.

Módulo Livemic

Propósito

El módulo **Livemic** le permite escuchar una conversación en curso en tiempo real.



PRECAUCIÓN: este módulo se proporciona "tal cual está" y su uso puede ser peligroso. Cada dispositivo funciona de manera diferente. Recomendamos que realice pruebas antes de usarlo en el campo.

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Número	Cantidad de teléfonos usados para escuchar. Debe incluir el código internacional del país, p. ej.: "+341234567890".
	ADVERTENCIA: no oculta el ID del dispositivo que llama, y desactiva el micrófono al escuchar la conversación.

Módulo Messages

Propósito

El módulo **Messages** registra todos los mensajes recibidos y enviados por el target. Este módulo registra:

- correo electrónico
- SMS (solo para dispositivos móviles)
- MMS (solo para dispositivos móviles)



IMPORTANTE: para Android se requieren privilegios raíz. Consulte "[Qué debería saber acerca de Android](#)" En la página 158 .

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Activado	Activa el registro.
Desde	Registra los mensajes a partir de la fecha indicada.
Hasta	Registra los mensajes hasta la fecha indicada.
Tamaño máximo	Tamaño máximo del mensaje a registrar.

Módulo Mic

Propósito

El módulo **Mic** graba el audio del ambiente a través del micrófono del dispositivo.



IMPORTANTE: no encienda el micrófono para grabar llamadas de datos (p. ej.: Skype, Viber) sin haber probado completamente el modelo del teléfono con la misma versión de sistema operativo. Puede desactivar el audio del cliente y hacer que la aplicación no pueda utilizarse.



IMPORTANTE: con algunos sistemas operativos el módulo no se activa durante llamadas.



NOTA: para Windows Phone, en algunos modelos de dispositivos, el inicio y el final de la grabación pueden estar acompañados de una señal de audio.

Datos importantes de los dispositivos de escritorio

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Silencio entre voces	<p>Cantidad máxima de segundos de silencio admitidos en la grabación. Después del período establecido, el agent deja de grabar y se reinicia cuando se vuelven a recibir sonidos.</p> <p> ADVERTENCIA: si el valor es muy bajo, la grabación excluirá todos los silencios y la conversación fluirá sin pausas. Si el valor es muy alto, la grabación incluirá todos los silencios y la conversación será demasiado larga.</p>
Reconocimiento de voz	<p> NOTA: no es compatible con iOS, BlackBerry, Android y Symbian, Windows Phone.</p> <p>Valor para identificar la voz humana y excluir el ruido de fondo de la grabación.</p> <p> ADVERTENCIA: 0.2-0.28 es el intervalo sugerido para identificar la voz humana. Los valores más altos se adaptan mejor a las voces femeninas pero pueden incidir en la grabación del ruido de fondo.</p>

<i>Campo</i>	<i>Descripción</i>
Autosense	Si está activado, el agent intentará cambiar la configuración del mezclador de audio (micrófono encendido/apagado, selección de línea y volumen) para optimizar la calidad de grabación de audio, permitiendo volúmenes más bajos o menos interrupciones en la grabación.

Módulo Money

Propósito

El módulo **Money** registra información en el monedero digital de criptodivisas del target (p. ej.: Bitcoin). Específicamente, registra:

- la dirección o direcciones del target
- la lista de transacciones completas
- la agenda del target con las direcciones de las transacciones
- el saldo

Módulo Mouse

Propósito

El módulo **Mouse** captura la imagen de una pequeña área de la pantalla alrededor del puntero del mouse, con cada clic.

Ayuda a burlar teclados virtuales que se usan para evitar el registro de teclas presionadas. Consulte "[Módulo Keylog](#)" En la página 150 .

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Ancho	dimensiones de la imagen capturada
Alto	

Módulo Password

Propósito

El módulo **Password** registra todas las contraseñas guardadas en las cuenta del usuario. Se recopilan las contraseñas guardadas del navegador, los mensajes instantáneos y los clientes de web-mail.

Módulo Position

Propósito

El módulo **Position** registra la posición del dispositivo por medio del sistema GPS, la celda GSM o la información de Wi-Fi.

Datos importantes de los dispositivos móviles

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
--------------	--------------------

GPS	Encuentra la posición con información del GPS.
------------	--

Celda	Encuentra la posición con información de la celda GSM o CDMA.
--------------	---

Wi-Fi	Encuentra la posición con el BSSID de una estación Wi-Fi.
--------------	---



NOTA: para Windows Phone, el sistema establece internamente la forma más eficiente de encontrar la posición del dispositivo en un momento determinado, independientemente de los parámetros establecidos.

Módulo Screenshot

Propósito

El módulo **Screenshot** captura una imagen de pantalla del dispositivo del target.



IMPORTANTE: para Android, se requieren privilegios raíz para tomar capturas de pantalla. Consulte "[Qué debería saber acerca de Android](#)" En la página 158 .

Datos importantes

A continuación se describen los datos:

<i>Campo</i>	<i>Descripción</i>
Calidad	Calidad final de la imagen capturada. Baja: peor calidad de imagen, máxima compresión Alta: mejor calidad de imagen, mínima compresión  Sugerencia: deje el valor predeterminado.
Solo la ventana en primer plano	(solo para dispositivos de escritorio) Captura una imagen instantánea de la ventana que está en primer plano.

Módulo URL

Propósito

El módulo **URL** registra el nombre de los sitios web visitados por el navegador del target.



IMPORTANTE: para que este módulo se inicie cuando el dispositivo se reinicia en BlackBerry, el teléfono debe estar en espera por varios minutos (luz de fondo apagada).

Apéndice: vectores de instalación

Presentación

Introducción

Un agent es un grupo complejo de eventos, acciones, módulos y vectores de instalación. A continuación se muestra una lista de vectores de instalación simples con una descripción detallada de las opciones de configuración.

Contenido

En esta sección se incluyen los siguientes temas:

Lista de vectores de instalación	157
Qué debería saber acerca de Android	158
Obtención de un certificado Code Signing	159
Vector Exploit	159
Vector Installation Package	160
Preparación de Installation Package para Windows Phone	164
Vector Local Installation	169
Vector Melted Application	170
Vector Network Injection	171
Vector Offline Installation	172
Vector de instalación persistente	172
Vector QR Code/Web Link	175
Vector Silent Installer	176
Vector U3 Installation	177
Vector WAP Push Message	177

Lista de vectores de instalación

A continuación se muestra una lista de vectores con los tipos de dispositivos y sistemas operativos compatibles:

Vector de instalación	Dispositivo	Sistema operativo	Descripción
Exploit	De escritorio	OS X, Windows	Agrega el agent a cualquier documento (el formato del documento puede depender de los exploits disponibles).
	Móvil	iOS	
Installation Package	Móvil	Android, BlackBerry, iOS, Symbian, Windows Phone, WinMobile	Crea un instalador automático con el agent.
Local Installation	Móvil	BlackBerry, iOS, WinMobile	Instala el agent en el dispositivo del target, por USB o a través de una tarjeta de memoria SD/MMC.
Melted Application	De escritorio	Linux, OS X, Windows	Agrega el agent a cualquier archivo ejecutable.
	Móvil	Android, Symbian, WinMobile	
Network Injection	De escritorio	Linux, OS X, Windows	Enlace a la página de creación de reglas de inyección. <i>Consulte "Administración de los Network Injector" En la página 70 .</i>
	Móvil	-	
Offline Installation	De escritorio	Multiplataforma	Crea un archivo ISO para la generación de un CD/DVD/USB de arranque que se utilizará en la computadora que está apagada o hibernando

Vector de instalación	Dispositivo	Sistema operativo	Descripción
Instalación persistente	De escritorio	Windows	Introduce el agent al firmware de la computadora del target.
QR Code/Web Link	Móvil	Multiplataforma, Android, BlackBerry, Symbian, WinMobile	Genera un código QR para sitios web o reportes, que instalará el agent si el target lo fotografía.
Silent Installer	De escritorio	Linux, OS X, Windows	Crea un archivo ejecutable vacío que, cuando se ejecuta en el dispositivo del target, instala el agent.
Instalación U3	De escritorio	Windows	Crea un paquete que se instalará por medio de una llave U3. La llave U3 que instala automáticamente el agent en el dispositivo del target al insertarlo.
Wap Push Message	Móvil	Multiplataforma, Android, BlackBerry, Symbian, WinMobile	Envía un mensaje WAP que instalará el agent si el target acepta el mensaje.

Qué debería saber acerca de Android

Privilegios raíz

El sistema operativo Android requiere privilegios raíz para ejecutar algunas aplicaciones en sus dispositivos.

El agent de un dispositivo Android requiere privilegios raíz para:

- capturar chat, consulte "[Módulo Chat](#)" En la página 146
- capturar correos electrónicos, consulte "[Módulo Messages](#)" En la página 151
- tomar capturas de pantalla, consulte "[Módulo Screenshot](#)" En la página 154
- mantenerse actualizado, consulte "[Página del agent](#)" En la página 41 , "[Página del target](#)" En la página 27

Obtener privilegios raíz

Los privilegios raíz se pueden obtener automáticamente sin ninguna interacción en el dispositivo. De todas formas, la obtención automática no está garantizada en todos los casos. En caso de que la obtención automática falle y la opción **Interacción necesaria del usuario** haya sido seleccionada durante la recopilación del agent, el agent requerirá que el usuario obtenga manualmente los privilegios del dispositivo si así lo permite el sistema operativo.

Verificar los privilegios raíz

Para verificar los privilegios raíz en el dispositivo del target, active el módulo **Device**.

El estado de raíz se indica en el tipo de evidencia **Device** ; si se obtuvieron privilegios raíz, se mostrará **root:yes**.

Obtención de un certificado Code Signing

Introducción

Para poder usar las funciones de firma del código disponibles durante la compilación del vector, es necesario obtener un certificado Code Signing emitido por una autoridad de certificación reconocida.

La mayoría de las autoridades de certificación ofrecen certificados Code Signing, incluidas:

- Verisign (<http://www.verisign.com>)
- Thawte (<http://www.thawte.com>)
- GoDaddy (<http://www.godaddy.com>)

Instalación de un certificado Code Signing

En el sistema backend que se encuentra en la carpeta C:\RCS\DB\bin, ingrese el siguiente comando:

```
> rcs-db-config --sign-cert ArchivoDelCertificado --sign-pass  
ContaseñaDelCertificado
```

Resultado: el certificado se instalará en el sistema y se podrá utilizar la función de firma del código.

Vector Exploit

Propósito

La compilación crea un instalador que, al abrirlo en el dispositivo del target, explota la vulnerabilidad de un programa específico. Se puede experimentar diversos comportamientos, dependiendo del Exploit específico (p. ej. el programa que se está ejecutando aborta).

Instalación de dispositivos de escritorio

Se crea el instalador y el paquete de los archivos de herramientas se guardan automáticamente en la carpeta C:\RCS\Collector\public. Estos archivos pueden utilizarse para diversos tipos de ataques (p. ej.: a través de un enlace a un sitio web).

Instalación de dispositivos móviles

Se debe copiar el instalador en el dispositivo y ejecutar install.sh desde la carpeta copiada.



IMPORTANTE: se debe desbloquear el dispositivo.

El paquete de archivos de herramientas se copia automáticamente a la carpeta C:\RCS\Collector\public. Estos archivos pueden utilizarse para diversos tipos de ataques (p. ej.: a través de un enlace a un sitio web).

Ejemplo de comandos para copiar el instalador en un dispositivo con iOS

```
mymac>scp -r ./RCS_IPHONE root@myiphone.local.net:/tmp
mymac>ssh root@myiphone.local.net
myiphone>cd /tmp/RCS_IPHONE
myiphone>sh install.sh
```

Eliminar los archivos que ya no están en uso

Los paquetes guardados en la carpeta C:\RCS\Collector\public se pueden eliminar utilizando la función **Administrador de archivos**, en la sección **System, Frontend** .

Parámetros

<i>Nombre</i>	<i>Descripción</i>
Tipo de archivo	Tipo de archivo a infectar (p. ej.: .PDF).
Seleccionar un Exploit	Nombre completo de la aplicación usada por el target para abrir el archivo (p. ej.: Adobe Acrobat Reader 10).
URL	Parámetros que identifican al archivo a infectar.
Documento	URL: conexión a un Anonymizer donde se guardó el instalador.
...	Documento: para seleccionar el archivo a infectar.

Vector Installation Package

Propósito

La compilación crea un archivo ejecutable que instala el agent en modo silencioso. Es posible cargar el archivo ejecutable en el dispositivo a través de cualquiera de estos métodos:

- descarga desde URL
- enlace por SMS, MMS o correo electrónico
- directamente desde la computadora por cable USB
- (solo para Windows Mobile) copia directa en tarjeta SD
- (solo para Windows Phone) archivo adjunto por correo electrónico

Notas para los sistemas operativos Android (preparación del vector)

La compilación genera dos vectores APK (Android Application Package File):

- *ApplicationName.v2.apk*: vector para Android 2.x
- *ApplicationName.default.apk*: vector para Android 3.x y 4.x

Notas para los sistemas operativos Android (instalación)

A continuación se describe el procedimiento de instalación:

Paso Acción

- 1 Active la opción **Orígenes desconocidos** en las opciones de configuración del dispositivo (usualmente en **Configuración, Aplicaciones**). Después de la instalación es posible desactivar esta opción.



NOTA: si no se activa esta opción, durante la instalación aparecerá una solicitud de autorización para instalar una aplicación que no es de Android Market.

- 2 Si el vector contiene los módulos Screenshot, Chat y Messages, es necesario obtener los privilegios raíz del dispositivo. Consulte "[Qué debería saber acerca de Android](#)" En la página 158
- 3 Ejecute el vector APK apropiado en el dispositivo.
- 4 Durante la instalación del vector APK, acepte los permisos solicitados por el agent.
- 5 Para Android 3.x y 4.x, haga clic en **Abrir** para iniciar el vector, de lo contrario el vector no se instalará.



IMPORTANTE: el vector APK predeterminado para Android 3.x y 4.x aparecerá como una aplicación normal llamada DeviceInfo, que muestra la información del dispositivo.

- 6 Durante la ejecución del vector, si está activada la opción **Solicitar privilegios de administrador**, podría aparecer una solicitud para obtener privilegios raíz.

Notas para los sistemas operativos Windows Phone (preparación del vector)

La compilación de una factory con el vector Installation Package para el sistema operativo Windows Phone crea el archivo .zip *NombreDeFactory_winphone_silent.zip* en la carpeta RCS Download que contiene dos archivos:

- *NombreDeLaAplicación.xap*: paquete con las aplicaciones que se instalarán en el dispositivo del target
- *NombreDeLaAplicación.aetx*: certificado de la empresa que instalará la aplicación



IMPORTANTE: para que la compilación se realice correctamente, siga el procedimiento para cargar los archivos necesarios en RCS. Consulte "[Preparación de Installation Package para Windows Phone](#)" En la página 164

Notas para los sistemas operativos Windows Phone (instalación)

La aplicación MyPhoneInfo, que se utiliza para instalar el agent, se incluye en el paquete con las aplicaciones .xap. Para la instalación no es necesario desbloquear el teléfono.

Los archivos .xap y .aetx se pueden enviar al dispositivo del target:

- como archivos adjuntos en un correo electrónico;
- como enlaces por correo electrónico, SMS o en una página web

Para la instalación por Internet, el servicio Web debe soportar los tipos MIME para los archivos .xap y .aetx; las siguientes instrucciones deben estar en los archivos *mime.types*:

- `application/x-silverlight-app xap`
- `application/x-aetx aetx`

Realice el siguiente procedimiento para ambos modos:

Paso Acción

- 1 Abra el archivo *NombreDeLaAplicación.aetx*.



IMPORTANTE: este es el certificado que debe abrirse siempre primero.

- 2 Para responder las preguntas que se muestran haga clic en **Agregar**.
- 3 Abra el archivo *NombreDeLaAplicación.xap*.
- 4 Responda las preguntas que se muestran haciendo clic en **Instalar**: la aplicación MyPhoneInfo se instalará en el teléfono.
- 5 Desde la lista de aplicaciones, abra la aplicación MyPhoneInfo cuando menos una vez.

Paso Acción

- 6 Cierre MyPhoneInfo: el agent está listo.



IMPORTANTE: si sale de la aplicación sin cerrarla, la aplicación, y por lo tanto el agent, quedarán suspendidos. El agent solo se inicia cuando la aplicación está cerrada o el teléfono se vuelve a encender.

El agent se comunica con RCS Server siempre y cuando la aplicación MyPhoneInfo esté instalada en el dispositivo y el dispositivo esté encendido. Si no hay ninguna conexión de datos móvil disponible, el agent solo podrá comunicarse con RCS Server cuando el usuario utilice el teléfono o cuando el teléfono esté conectado a una computadora o a un cargador.



NOTA: cuando el dispositivo está encendido, el agent se tarda 30 minutos en restablecer la comunicación con RCS Server. Los 30 minutos están garantizados si existen conexiones de datos y Wi-Fi en el dispositivo. De lo contrario, podría demorar más.

Notas para los sistemas operativos Windows Mobile

Es posible especificar un instalador CAB existente al cual se añadirá el agent.

Si no se especifica el CAB, el sistema utilizará un CAB predeterminado que no instala nada.

Notas para los sistemas operativos BlackBerry

Para permitir que el agent se descargue en un BlackBerry, extraiga el archivo zip creado en un servidor web al que el dispositivo tenga acceso.



NOTA: el servidor web debe soportar los tipos MIME para los archivos .jad y .cod, .text/vnd.sun.j2me.app-descriptor y application/vnd.rim.cod. respectivamente. La carpeta Public del Collector ejecuta esta función de forma automática.

Una vez que el instalador se ejecuta en el dispositivo, acepte los permisos solicitados por el agent.

Notas para los sistemas operativos Symbian



IMPORTANTE: para Symbian es necesario obtener el certificado.

Parámetros de Android, WinMobile, Windows Phone

<i>Nombre</i>	<i>Descripción</i>
Nombre de la aplicación	Nombre de la aplicación (visible para el target)

<i>Nombre</i>	<i>Descripción</i>
Solicitud de interacción del usuario	(solo para Android) Si la obtención automática no funciona, esta opción activa la solicitud del usuario para obtener privilegios raíz del dispositivo de forma manual.
	 ADVERTENCIA: la solicitud se mostrará en el dispositivo del target.

Parámetros para BlackBerry

<i>Nombre</i>	<i>Descripción</i>
Nombre de la aplicación	Nombre del instalador (visible para el target)
Nombre Descripción	(solo para BlackBerry) Datos de la aplicación usados para "ocultar" el agent.
Proveedor	
Versión	

Parámetros para Symbian

<i>Nombre</i>	<i>Descripción</i>
Nombre de la aplicación	Nombre de la aplicación (visible para el target)
Certificado vinculado a IMEI	Certificado del dispositivo.
Llave vinculada al certificado	Llave del certificado.
Edición S60	Versión del sistema operativo.
Configuración de Symbian	Parámetros: <ul style="list-style-type: none"> • UID 1-6: lista de los UID asociados con el certificado • Llave: archivo de la llave

Preparación de Installation Package para Windows Phone

Introducción

Para los dispositivos con Windows Phone, el agent se instala en el dispositivo del target a través de la aplicación Windows Phone. Para completar con éxito la instalación del agent, los siguientes archivos deben estar en RCS Server:

- un archivo .pfx para firmar el paquete de instalación .xap de Windows Phone
- un archivo .aetx como certificado para la aplicación de Windows Phone

Secuencia recomendada

Para generar los archivos .pfx y .aetx complete los siguientes pasos y cárguelos en RCS Server:

Pas- Acción

o

-
- 1 Obtenga un código de ID de Symantec que se utiliza para comprar el certificado necesario para distribuir la aplicación Windows Phone.
 - 2 Obtenga el certificado de Symantec necesario para distribuir las aplicaciones de Windows.
 - 3 Instale el certificado de Symantec necesario para distribuir las aplicaciones de Windows.
 - 4 Genere los archivos .pfx y .aetx
 - 5 Cargue los archivos .pfx y .aetx en RCS Server

Cómo leer estas instrucciones



NOTA: los enlaces a las páginas web en los procedimientos funcionaban perfectamente cuando se escribió este manual. Si el enlace no funciona, encuentre la página web correcta.

En caso de que hubiera discrepancias entre lo que se indica en el manual y las instrucciones recibidas directamente de las organizaciones involucradas, siga las instrucciones de las organizaciones.

Obtener un código ID de Symantec

Para obtenerlo, prosiga de la siguiente manera:

Paso Acción

-
- 1 Registre una cuenta de Microsoft en <https://signup.live.com/signup.aspx?lic=1>.
 - 2 Registre una cuenta en Windows Phone Dev Center e inicie sesión con su cuenta de Microsoft en <https://dev.windowsphone.com/en-us/join/>

Paso Acción

- 3
 - Haga clic en **Unirse ahora**: aparecerá la página de registro de la cuenta de Windows Phone Dev Center.
 - Seleccione **Empresa** como **Tipo de cuenta**.
 - Haga clic en **Siguiente**.
 - En la sección **Account Info**, ingrese sus datos y contactos.
 - En la sección **Publisher Info**, ingrese el nombre que se mostrará como distribuidor de la aplicación durante la instalación como el **Nombre del editor**.



ADVERTENCIA: el usuario que instale el paquete .xap y el certificado .aetx en este teléfono verá este nombre.

- En la sección **Approver Info**, ingrese los datos y la información de contacto del gerente de la empresa que puede autorizar la solicitud de registro.
- Siga las instrucciones en pantalla para completar el registro.



IMPORTANTE: proporcione una dirección de correo electrónico y un número de teléfono; se usarán para validar el registro y enviar el ID del editor.

- 4 Después del registro, recibirá un correo electrónico de Symantec, el socio de Microsoft que se encarga de validar a las empresas registradas en el Centro de desarrollo de Windows Phone, para validar el registro. También puede haber otras comunicaciones por teléfono.



IMPORTANTE: solicite a la persona encargada de autorizar que responda el correo electrónico de Symantec a la brevedad.

- 5 Después de la validación, recibirá un correo electrónico con los datos de la cuenta:
 - Publisher ID
 - Publisher Name



NOTA: para obtener más información, visite [http://msdn.microsoft.com/library/windowsphone/help/jj206719\(v=vs.105\).aspx](http://msdn.microsoft.com/library/windowsphone/help/jj206719(v=vs.105).aspx)

Obtener un certificado de Symantec

Para distribuir las aplicaciones de Windows Phone se requiere el certificado Enterprise Mobile Code Signing.

Para obtenerlo, prosiga de la siguiente manera:

Paso Acción

- 1 Puede comprar un certificado Enterprise Mobile Code Signing en <https://products.websecurity.symantec.com/orders/enrollment/microsoftCert.do>.
- 2
 - Ingrese el **ID del editor** que recibió y la dirección de correo electrónico indicada en la sección **Account Info** durante el registro en el Centro de desarrollo de Windows Phone.
 - Complete la compra siguiendo las instrucciones en pantalla.
- 3 Al finalizar, recibirá un par de correos electrónicos de Symantec que le indicarán:
 - la confirmación del pedido
 - la lista de funciones activadas de acuerdo con el pedido
 - el certificado y las instrucciones sobre cómo importarlo en su computadora



NOTA: para obtener más información, visite https://knowledge.verisign.com/support/code-signing-support/index?page=content&id=SO20770&actp=search&viewlocale=en_US

Instalación del certificado de Symantec

Para confirmar la instalación del certificado Enterprise Mobile Code Signing, primero instale lo siguiente:

- Enterprise Mobile Root
- Certificado Enterprise Mobile CA



IMPORTANTE: use siempre el mismo navegador para descargar los certificados. El procedimiento indicado se refiere al navegador Firefox.

Siga este procedimiento:

Paso Acción

- 1 Abra Firefox.
- 2 Copie la URL recibida en el correo electrónico y péguela en la barra de direcciones para instalar el certificado Microsoft Enterprise Mobile Root.
- 3 En la ventana de diálogo **Descargar certificado**, marque las tres casillas combinadas y haga clic en **Aceptar**.
- 4 Copie la dirección URL recibida en el correo electrónico y péguela en la barra de direcciones para instalar el certificado Microsoft Enterprise CA Root.

Paso Acción

- 4 En la ventana de diálogo **Descargar certificado**, marque las tres casillas combinadas y haga clic en **Aceptar**.
 -  **NOTA:** para verificar si se instalaron los certificados, seleccione el certificado en el menú de **Firefox, Opciones y Avanzadas**. Luego seleccione la pestaña **Certificados** y haga clic en **Mostrar certificados**: aparecerá la lista de nombres con los certificados instalados en **Autoridades**.
- 5 Instale el certificado Enterprise Mobile Code Signing desde el enlace que se encuentra en el correo electrónico recibido y haga clic en **Continuar**.

Genere los archivos .pfx y .aetx

Los archivos .pfx y .aetx necesarios para firmar y distribuir las aplicaciones de Windows Phone se pueden generar con el certificado Enterprise Mobile Code Signing.



IMPORTANTE: para el procedimiento se requiere Windows Phone Software Developer Kit 8.0, disponible en <http://www.microsoft.com/it-it/download/windows.aspx> esté instalado en la computadora. La herramienta AET Generator incluida en este paquete le permite crear el archivo .aetx.



IMPORTANTE: para ejecutar el procedimiento, utilice el mismo navegador que utilizó para instalar los certificados. El procedimiento indicado se refiere al navegador Firefox.

Siga este procedimiento:

Paso Acción

- 1 Abra Firefox.
- 2 En el menú **Firefox**, seleccione **Opciones**. A continuación, seleccione la pestaña **Avanzada**, y luego **Certificados**.
- 3 Haga clic en **Mostrar certificados**.
- 4
 - En la pestaña **Certificados personales**, seleccione el certificado *Nombre del editor* y haga clic en **Exportar**
 - Guarde el archivo con la extensión .p12
 - Ingrese la contraseña de exportación del certificado: "password"



IMPORTANTE: ingrese esa contraseña y no otra.

- 5 Cambie el nombre del archivo con la extensión .pfx

Paso Acción

- 6 Desde el intérprete de comandos de Windows, abra la carpeta donde está guardado el archivo .pfx y ejecute el siguiente comando:

```
"%ProgramFiles (x86)%\Microsoft SDKs\Windows  
Phone\v8.0\Tools\AETGenerator\AETGenerator.exe"  
NombreDelArchivo.pfx password
```

donde *NombreDelArchivo* es el nombre del archivo .pfx.

Resultado: se generarán tres archivos en la carpeta donde se encuentra el archivo .pfx:

- AET.aetx
- AET.aet
- AET.xml



NOTA: para obtener más información, visite <http://msdn.microsoft.com/en-us/library/windowsphone/develop/jj206943%28v=vs.105%29.aspx>

Cargue los archivos .pfx y .aetx en el servidor de base de datos de RCS

Siga este procedimiento:

Paso Acción

- 1 Copie los archivos al servidor de la base de datos de RCS
- 2 Desde el intérprete de comandos de Windows, ejecute el siguiente comando para usar el archivo .pfx para firmar las aplicaciones de Windows Phone:

```
rca-db-config --sign-pfx-winphone  
RutaDelArchivo\NombreDelArchivo.pfx
```

donde *RutaDelArchivo* es la ruta del archivo .pfx en RCS Server

- 3 Desde el intérprete de comandos de Windows, ejecute el siguiente comando para usar el archivo .aetx como certificado para las aplicaciones de Windows Phone:

```
rca-db-config --sign-aetx-winphone  
RutaDelArchivo\NombreDelArchivo.aetx
```

donde *RutaDelArchivo* es la ruta del archivo .aetx en RCS Server

Vector Local Installation

Propósito

La compilación instala el agent directamente en el dispositivo del target o crea una carpeta en la tarjeta SD para insertarla en el dispositivo.



IMPORTANTE: para completar con éxito la instalación en un dispositivo BlackBerry, la aplicación BlackBerry Desktop Software debe estar instalada en una computadora con Windows. La consola creará un archivo .zip con todos los archivos necesarios para infectar a un BlackBerry conectado. Copie el archivo zip en la computadora con Windows (en caso de ser necesario) luego descomprima el archivo .zip. Conecte el BlackBerry a la PC por cable USB, luego ejecute el archivo install.bat. Si el BlackBerry tiene protección por PIN, ingrese el PIN cuando se le solicite.



IMPORTANTE: para completar con éxito la instalación en un dispositivo iOS, la aplicación iTunes debe estar instalada en la computadora.

Vector Melted Application

Propósito

La compilación modifica un archivo ejecutable existente al insertar el agent en él.

Los componentes del agent están codificados para evitar el uso de ingeniería inversa.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
Aplicación que se usará como dropper	<p>Archivo ejecutable en el que se agrega el agent. El tipo de archivo difiere en base al sistema operativo:</p> <p>Dispositivos de escritorio</p> <ul style="list-style-type: none"> • OS X: archivo MacOs comprimido .app. Se debe comprimir la aplicación (una carpeta) con el comando de zip de la consola Terminal.app. •  IMPORTANTE: no use el elemento del menú Comprimir desde la aplicación Finder. • Windows: archivo EXE • Linux: archivo DEB <p>Dispositivos móviles</p> <ul style="list-style-type: none"> • Android: aplicación APK de terceros. •  IMPORTANTE: pruebe la aplicación final. De hecho, algunas aplicaciones ejecutan controles de seguridad adicionales de runtime. • Symbian: archivo .sixx • WinMobile: archivo .cab
Solicitud de interacción del usuario	<p>(solo para Android, WinMobile, OS X) Si la obtención automática no funciona, esta opción activa la solicitud del usuario para obtener privilegios raíz del dispositivo de forma manual.</p> <p> ADVERTENCIA: la solicitud se mostrará en el dispositivo del target.</p>

Vector Network Injection

Propósito

La página abre la función Network Injector en la sección System.

Vector Offline Installation

Propósito

La compilación crea un archivo ISO de instalación automática que se grabará en un CD o en una memoria USB (solo para Windows).

Inserte el CD o la llave USB, luego encienda la computadora del target. Arranque desde el medio insertado y espere a que aparezca un menú. La infección puede hacerse de forma selectiva, eligiendo de una lista de todos los usuarios disponibles del sistema.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
CD/DVD de arranque	Crea un instalador automático ISO para CD o DVD.
Memoria USB de arranque	(solo para Windows) Crea un instalador automático para una llave USB.
Dump Mask	<p>Extrae automáticamente los documentos pertenecientes a cierto usuario. Los documentos pueden guardarse en un periférico USB para importarlos luego en la base de datos RCS.</p> <p>Existen tres opciones disponibles para la captura de documentos:</p> <ul style="list-style-type: none">• Documentos: documentos MS Office, PDF y archivos de texto• Imágenes: fotografías e imágenes• Personalizado: selecciona las extensiones de archivos que serán capturadas, separadas por el carácter pipe (" ").

Vector de instalación persistente

Propósito

El vector de **instalación persistente** introduce el agent al firmware de la computadora del target. Este tipo de infección tiene dos grandes ventajas:

- resiste el formateo y la sustitución del disco
- puede ejecutarse en una nueva computadora, aún antes de que se configuren los usuarios

Preparar el vector

Para compilar la factory con el vector de instalación persistente, cargue el archivo de actualización del firmware `isflash.bin` para infectar a la computadora.



IMPORTANTE: solo es posible infectar a las computadoras que contienen el archivo `isflash.bin`.



NOTA: este vector puede infectar a la mayoría de los productos de firmware creados por Insyde®, solo algunas versiones pueden resistir la infección.

Cómo obtener el archivo:

Paso Acción

- 1 Identifique el modelo exacto de la computadora portátil que se va a infectar.
- 2 Identifique y descargue el firmware correcto (BIOS) para ese modelo específico de computadora en el sitio web del fabricante.
- 3 Descomprima y ejecute el archivo `.exe`: aparecerá un mensaje de error.



PRECAUCIÓN: para evitar que la computadora se dañe, siga este procedimiento en un modelo de computadora diferente al de la computadora para la cual se descargó el firmware.

- 4 Con la ventana del mensaje de error abierta, ejecute `cd %temp%` desde el intérprete de comandos de Windows; se mostrarán los archivos temporales de la computadora.
- 5 En la carpeta temporal creada cuando el archivo del firmware `.exe` se inició, encuentre `isflash.bin` (usualmente es de 5, 9 o 17 MB).
- 6 Copie y pegue el archivo `isflash.bin` en otra carpeta.
- 7 Ahora puede cerrar la ventana con el mensaje de error.
- 8 En RCS Console, compile la factory por medio del vector de instalación persistente, cargue el archivo `isflash.bin` que obtuvo en los pasos anteriores.

Instalación del agent

Al compilar una factory con el vector de instalación persistente se crea un archivo `.zip` `NombreDeFactory_windows_persistent.zip` en la carpeta RCS Download



PRECAUCIÓN: para evitar daños irreparables a la computadora, use el firmware específico para la computadora que desea infectar.



NOTA: se necesitan dos personas para completar el procedimiento.

Cómo instalar el agent:

Paso Acción

- 1 Descomprima *NombreDeFactory_windows_persistent.zip*.
- 2 Copie todo el contenido del archivo .zip descomprimido en una llave con formateo FAT o FAT32.



IMPORTANTE: la llave solo debe contener el archivo *NombreDeFactory_windows_persistent.zip*

- 3 Apague la computadora del target, quítele la batería y desconecte el cable de electricidad.
- 4 Inserte la llave en el puerto USB.
- 5 Presione simultáneamente Fn + Esc + el botón de encendido y espere de 5 a 10 segundos.
- 6 Mantenga presionadas las teclas, conecte el cable de electricidad y espere de 5 a 10 segundos.
- 7 Suelte únicamente el botón de encendido y espere otros cinco segundos.
- 8 Suelte las teclas Fn y Esc: la computadora se iniciará sin que se encienda el monitor. Cuando la computadora se inicie, se encenderá el ventilador. Después de unos 10 minutos, la computadora se apagará o reiniciará.



IMPORTANTE: no interrumpa el procedimiento de arranque. La duración depende de la velocidad de la llave y el tamaño del firmware que se va a actualizar.



NOTA: si el procedimiento falla, inténtelo nuevamente insertando la llave en otro puerto USB.

Condiciones de activación de la infección

Si el agent se instaló correctamente, la infección solo estará activada la siguiente vez que se reinicie la computadora, si hay al menos un usuario en el sistema. La infección solo involucra a los usuarios existentes en el momento en que se activa la infección.

Si se instala en una computadora que no realizó correctamente el procedimiento de desconexión o hibernación, es necesario apagar y reiniciar la computadora para activar la infección.

Verificar la instalación

Debido a que una computadora del target no muestra signos de la instalación de un agent, debe usar la RCS Console para verificar la instalación antes de salir de la computadora del target.

Cómo verificar la instalación:

<i>Si...</i>	<i>Entonces...</i>
La computadora es nueva y no se configuró ningún usuario	<ol style="list-style-type: none"> 1. reinicie la computadora 2. instale Windows y cree al menos un usuario 3. reinicie la computadora 4. use la RCS Console para verificar que el agent sincroniza y envía la evidencia 5. reinicie la computadora
ya hay usuarios en la computadora	<ol style="list-style-type: none"> 1. reinicie la computadora 2. verifique que el agent se sincroniza con la RCS Console y envía la evidencia

Parámetros

<i>Nombre</i>	<i>Descripción</i>
UEFI del firmware	El archivo <code>isflash.bin</code> específico para la computadora portátil que se va a infectar, donde se instalará el agent.

Vector QR Code/Web Link

Propósito

La compilación crea un código QR que se agregará a cualquier sitio web o documento impreso. Tan pronto como el target captura el código QR, el agent se instala en el dispositivo.

Operations

Ni bien el target se conecta con el Anonymizer y solicita el instalador, el Collector descarga el instalador correcto para el sistema operativo del dispositivo del target en la carpeta `C:\RCS\Collector\public`.



NOTA: si el sistema operativo del target es desconocido, use la versión multiplataforma.

Eliminar los archivos que ya no están en uso

Los paquetes guardados en la carpeta `C:\RCS\Collector\public` se pueden eliminar utilizando la función **Administrador de archivos**, en la sección **System, Frontend**.

Parámetros

<i>Nombre</i>	<i>Descripción</i>
Nombre de la aplicación	Nombre del instalador (visible para el target)
URL	Conexión a un Anonymizer donde se guardó el instalador.
Solicitud de interacción del usuario	(solo para Android) Si la obtención automática no funciona, esta opción activa la solicitud del usuario para obtener privilegios raíz del dispositivo de forma manual.  ADVERTENCIA: la solicitud se mostrará en el dispositivo del target.
Aplicación que se usará como dropper	(solo para Android) Aplicaciones APK de terceros donde se agregará el agent.  IMPORTANTE: pruebe la aplicación final. De hecho, algunas aplicaciones ejecutan controles de seguridad adicionales de runtime.
Nombre	(solo para BlackBerry) Datos de la aplicación usados para "ocultar" el agent.
Descripción	
Proveedor	
Versión	
Certificado vinculado a IMEI	(solo para Symbian) Certificado del dispositivo.
Llave vinculada al certificado	(solo para Symbian) Llave del certificado.
Edición S60	(solo para Symbian) Versión del sistema operativo.

Vector Silent Installer

Propósito

La compilación crea un archivo ejecutable que instala el agent en modo silencioso. No hay ningún resultado visible en el dispositivo.

Vector U3 Installation

Propósito

La compilación crea un instalador automático ISO que se escribirá en una llave U3 (SanDisk) por medio del programa **U3 customizer** (es posible descargar el software de Internet).

Cuando la llave se inserta en el dispositivo, se abre un menú para la instalación del agent (no se detectará ningún disco USB automáticamente).

Vector WAP Push Message

Propósito

Crea un mensaje WAP-Push que invita al target a visitar un enlace.

Operations

Envía un mensaje WAP-Push que contiene texto o un enlace al instalador del agent. Si el mensaje es aceptado en el dispositivo del target, el agent será instalado.



IMPORTANTE: para Symbian es necesario obtener el certificado.



NOTA: si el sistema operativo del target es desconocido, use la versión multiplataforma. Esto crea instaladores para todas las plataformas compatibles y se guarda en la carpeta Public del Collector. Ni bien el target se conecta con el Anonymizer y solicita el instalador, el Collector descarga el instalador correcto para el sistema operativo del dispositivo del target.

Instalación

La compilación crea un instalador y guarda automáticamente el paquete de archivos en la carpeta C:\RCS\Collector\public .

Eliminar los archivos que ya no están en uso

Los paquetes guardados en la carpeta C:\RCS\Collector\public se pueden eliminar utilizando la función **Administrador de archivos**, en la sección **System, Frontend** .

Parámetros

<i>Nombre</i>	<i>Descripción</i>
Nombre de la aplicación	Nombre del instalador (visible para el target)
Número de teléfono	Número de teléfono del target, incluido el código de área internacional.
URL	Conexión a un Anonymizer donde se guardó el instalador. Si el paquete se guardó en otro sitio web, indique la dirección URL.
Tipo de servicio	Tipo de servicio solicitado: <ul style="list-style-type: none"> • Carga: el teléfono del target se redirecciona automáticamente al recurso indicado en la URL. En base a la configuración de seguridad del teléfono, se puede instalar automáticamente o se puede mostrar un mensaje para el usuario, en el que se le solicite proceder. • Indicación: se mostrará un mensaje en el que se le indique al usuario cómo proceder. • SMS: envía un enlace precedido por el texto especificado
Texto	(solo para Indicación y SMS) Prueba para el usuario target.
Solicitud de interacción del usuario	(solo para Android) Si la obtención automática no funciona, esta opción activa la solicitud del usuario para obtener privilegios raíz del dispositivo de forma manual. <div style="display: flex; align-items: center;">  <p>ADVERTENCIA: la solicitud se mostrará en el dispositivo del target.</p> </div>
Aplicación que se usará como dropper	(solo para Android) Aplicaciones APK de terceros donde se agregará el agent. <div style="display: flex; align-items: center;">  <p>• IMPORTANTE: pruebe la aplicación final, ya que algunas aplicaciones ejecutan controles de seguridad adicionales de runtime.</p> </div>
Nombre	(solo para BlackBerry) Datos de la aplicación usados para "ocultar" el agent.
Descripción	
Proveedor	
Versión	
Certificado vinculado a IMEI	(solo para Symbian) Certificado del dispositivo.

Nombre	Descripción
Llave vinculada al certificado	(solo para Symbian) Llave del certificado.
Edición S60	(solo para Symbian) Versión del sistema operativo.

]HackingTeam[

RCS 9.3 Guía del técnico
Guía del técnico 1.7 JUN-2014
© COPYRIGHT 2014
info@hackingteam.com

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
tel.: + 39 02 29 060 603
fax: + 39 02 63 118 946
www.hackingteam.com
e-mail: info@hackingteam.com
