

]HackingTeam[

RCS 8.4

The hacking suite for governmental interception

Manuale del tecnico



Proprietà delle informazioni

© COPYRIGHT 2013, HT S.r.l.

Tutti i diritti riservati in tutti i paesi.

Nessuna parte di questo manuale può essere tradotta in altra lingua e/o adattata e/o riprodotta in altra forma e/o mezzo meccanico, elettronico, per fotocopie, registrazioni o altro, senza una precedente autorizzazione scritta da parte di HackingTeam .

Tutte le società e i nomi di prodotti possono essere marchi legali o marchi registrati delle rispettive società la cui proprietà viene qui riconosciuta. In particolare Internet Explorer™ è un marchio registrato dalla Microsoft Corporation.

L'elaborazione del testo e delle immagini è stata vagliata con la massima cura, nonostante ciò HackingTeam si riserva il diritto di modificare e/o aggiornare le informazioni qui contenute per correggere errori tipografici e/o imprecisioni, senza preavviso o alcun impegno da parte della stessa.

Qualsiasi riferimento a nomi, dati, e indirizzi di altre società non facenti parte di HackingTeam è casuale e, salvo diversa indicazione, è riportato a titolo puramente esemplificativo, allo scopo di meglio chiarire l'utilizzo del prodotto.

NOTA: richieste di ulteriori copie di questo manuale o di informazioni tecniche sul prodotto, devono essere indirizzate 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

e-mail: info@hackingteam.com

Sommario

Glossario dei termini	xiii
Introduzione a questa Guida	1
Novità della guida	2
Documentazione fornita	3
Convenzioni tipografiche per le segnalazioni	4
Convenzioni tipografiche per la formattazione	4
Destinatari del prodotto e di questa guida	5
Dati di identificazione dell'autore del software	6
RCS (Remote Control System)	7
Differenze rispetto alle versioni precedenti	8
Glossario dei termini	8
Terminologia vettori di infection per desktop	8
Terminologia vettori di infection per mobile	8
RCS Console per il Tecnico	10
Avvio di RCS Console	11
Come si presenta la pagina di login	11
Accedere a RCS Console	11
Descrizione della homepage	12
Introduzione	12
Come si presenta	12
Descrizione dei wizard da homepage	13
Introduzione	13
Come si presenta	13
Investigation Wizard	14
Elementi e azioni comuni dell'interfaccia	15
Come si presenta RCS Console	15
Azioni sempre disponibili sull'interfaccia	17
Cambiare la lingua dell'interfaccia o la propria password	17
Convertire le date-ora di RCS Console al proprio fuso orario	18
Azioni sulle tabelle	18
Procedure del Tecnico	19
Introduzione	19
Procedure	19
Effettuare l'injection su connessioni HTTP	19
Infettare un computer non connesso a internet	20
Infettare un computer connesso a Internet	20
Mantenere aggiornato il software degli agent	21
I target	22

Cose da sapere sulle operation	23
Cos'è un'operation	23
Assegnare l'operation a un gruppo di utenti	23
Cosa avviene quando si crea una nuova operation	23
Cosa avviene quando si chiude un'operation	23
Pagina dell'operation	23
Scopo	23
Come si presenta la funzione	24
Per saperne di più	25
Creare una factory	26
Creare un target	26
Chiudere un target	26
Modificare i dati di un target	26
Eliminare un target	27
Cose da sapere sui target	27
Cos'è un target	27
Compiti dell'Amministratore	27
Cosa avviene quando si crea un target	28
Cosa avviene quando si chiude un target	28
Apertura e chiusura di un'operation	28
Pagina del target	28
Scopo	28
Come si presenta la funzione	29
Per saperne di più	31
Creare una factory	31
Chiudere una factory o un agent	31
Eliminare una factory o un agent	32
Importare le evidence del target	32
Esportare le evidence del target	32
Dati della pagina target	32
Visualizzazione a icone	33
Visualizzazione a tabella	33
Cose da sapere sulle Factory e sugli Agent	34
Modalità di infezione	34
Componenti della strategia di infezione	34
Le factory	35
Modalità di creazione delle factory	35
I vettori di installazione	35
Gli agent	36
I moduli per l'acquisizione dei dati	36

Compilazione di una factory	36
Scopo	36
Passi successivi	36
Come si presenta la funzione	36
Per saperne di più	37
Creare un agent	37
Creare un agent da collaudare in modalità demo	38
Gli agent	39
Cose da sapere sugli agent	40
Installazione di un agent	40
Acquisizione evidence per analisi ambiente installazione	40
Analisi ambiente di installazione	40
Aggiornamento dello scout agent	40
Sincronizzazione di un agent	41
Agent offline e online	41
Disabilitazione temporanea di un agent	41
Collaudo di un agent	41
Configurazione dell'agent	42
Pagina dell'agent	42
Scopo	42
Come si presenta la funzione	43
Per saperne di più	45
Dati dello storico configurazioni di un agent	45
Dati dello storico eventi di un agent	46
Dati dello storico sincronizzazioni dell'agent	46
Trasferimento file da/a il target	46
Scopo	46
Come si presenta la funzione	47
Per saperne di più	49
Pagina dei comandi	49
Scopo	49
Come si presenta la funzione	49
Per saperne di più	50
Factory e agent: configurazione base	51
Cose da sapere sulla configurazione base	52
Configurazione base	52
Esportazione e importazione di configurazioni	52
Salvataggio della configurazione come template	52
Configurazione base di una factory o di un agent	52
Scopo	53

Passi successivi	53
Come si presenta la funzione	53
Per saperne di più	54
Configurare una factory o un agent	55
Dati della configurazione base	55
Factory e agent: configurazione avanzata	57
Cose da sapere sulla configurazione avanzata	58
Configurazione avanzata	58
Componenti della configurazione avanzata	58
Lettura delle sequenze	59
Eventi	59
Azioni	60
Relazioni tra azioni e moduli	60
Relazioni tra azioni e eventi	60
Moduli	61
Esportazione e importazione di configurazioni	61
Salvataggio della configurazione come template	61
Configurazione avanzata di una factory o di un agent	61
Scopo	61
Passi successivi	62
Come si presenta la funzione	62
Per saperne di più	64
Creare una sequenza di attivazione semplice	64
Creare una sequenza di attivazione complessa	64
Dati globali dell'agent	65
Gestione dei frontend	67
Scopo della funzione	67
Come si presenta la funzione	67
Per saperne di più	68
I Network Injector	69
Cose da sapere su Network Injector e le sue regole	70
Introduzione	70
Tipi di risorse infettabili	70
Come creare una regola	70
Cosa succede quando si abilita/disabilita una regola	70
Regole identificazione automatica e da operatore	70
Avvio dell'infezione	70
Gestione dei Network Injector	71
Scopo	71
Cosa è possibile fare	71

Come si presenta la funzione	71
Per saperne di più	73
Aggiungere una nuova regola di injection e applicarla al target	73
Dati di un Network Injector	74
Dati delle regole di injection	74
Cose da sapere su Appliance Control Center	79
Introduzione	79
Sincronizzazione con RCS	79
Indirizzo IP dell'interfaccia di injection	80
Appliance Control Center	80
Scopo	80
Cosa è possibile fare	80
Richiesta della password	80
Come si presenta la funzione	80
Per saperne di più	81
Procedure	81
Abilitazione sincronizzazione con RCS	81
Infettare i target tramite identificazione automatica	82
Visualizzare i dettagli dell'infezione	83
Dati del Appliance Control Center	84
Dati scheda Network Injector	84
Cose da sapere su Tactical Control Center	84
Introduzione	84
Funzionamento del Tactical Control Center	84
Sincronizzazione con RCS	85
Aggiornamento delle regole di infezione	85
Utilizzo delle interfacce di rete	85
Processo di infezione tramite identificazione automatica	86
Processo di infezione tramite identificazione manuale	86
Abilitazione sincronizzazione con RCS	87
Acquisizione password di rete WiFi protetta	87
Infezione tramite identificazione automatica	87
Forzatura autenticazione dei dispositivi sconosciuti	87
Infezione tramite identificazione da operatore	88
Impostazione di filtri sul traffico intercettato	88
Filtro con espressioni regolari	88
Filtro BPF (Berkeley Packet Filter) di rete	88
Individuazione del target tramite analisi cronologia	89
Emulazione di un Access Point conosciuto dal target	89
Tactical Control Center	89

Scopo	89
Cosa è possibile fare	89
Richiesta della password	90
Come si presenta la funzione	90
Per saperne di più	91
Procedure	91
Abilitazione sincronizzazione con RCS	91
Avviare un test della rete	92
Acquisire la password di una rete WiFi protetta	93
Infettare i target tramite identificazione automatica	94
Impostare i filtri sul traffico intercettato	96
Forzare l'autenticazione dei dispositivi sconosciuti	97
Infettare i target tramite identificazione manuale	97
Pulire i dispositivi erroneamente infettati	98
Individuare un target analizzando la cronologia web	98
Emulare un Access Point conosciuto dal target	99
Spegnere il Tactical Network Injector	100
Visualizzare i dettagli dell'infezione	100
Dati del Tactical Control Center	101
Dati scheda Network Injector	101
Dati dei dispositivi rilevati	101
Dati scheda Wireless Intruder	102
Dati scheda Fake Access Point	102
Appendice: azioni	104
Elenco delle sotto-azioni	105
Descrizione dati sotto-azioni	105
Descrizione tipi di sotto-azioni	105
Azione Destroy	105
Scopo	105
Sistemi operativi	105
Parametri	106
Azione Execute	106
Scopo	106
Riferimento a cartella dell'agent	106
Sistemi operativi	106
Dati significativi	107
Azione Log	107
Scopo	107
Sistemi operativi	107
Parametri	107

Azione SMS	107
Scopo	107
Sistemi operativi	107
Parametri	108
Azione Synchronyze	108
Scopo	108
Sistemi operativi	108
Parametri desktop	109
Parametri mobile	109
Azione Uninstall	110
Scopo	110
Sistemi operativi	110
Parametri	110
Appendice: eventi	111
Elenco degli eventi	112
Descrizione dati eventi	112
Descrizione tipi eventi	112
Evento AC	113
Scopo	113
Sistemi operativi	113
Parametri	113
Evento Battery	113
Scopo	113
Sistemi operativi	113
Parametri	113
Evento Call	114
Scopo	114
Sistemi operativi	114
Parametri	114
Evento Connection	114
Scopo	114
Sistemi operativi	114
Parametri mobile	114
Parametri desktop	115
Evento Idle	115
Scopo	115
Sistemi operativi	115
Parametri	115
Evento Position	115
Scopo	115

Sistemi operativi	116
Parametri	116
Evento Process	116
Scopo	116
Sistemi operativi	116
Parametri	116
Evento Quota	117
Scopo	117
Sistemi operativi	117
Parametri	117
Evento Screensaver	117
Scopo	117
Sistemi operativi	117
Parametri	117
Evento SimChange	118
Scopo	118
Sistemi operativi	118
Parametri	118
Evento SMS	118
Scopo	118
Sistemi operativi	118
Parametri	118
Evento Standby	119
Sistemi operativi	119
Parametri	119
Evento Timer	119
Scopo	119
Sistemi operativi	119
Parametri	119
Evento Window	120
Scopo	120
Sistemi operativi	120
Parametri	120
Evento WinEvent	120
Scopo	120
Sistemi operativi	120
Parametri	120
Appendice: moduli	121
Elenco dei moduli	122
Modulo Addressbook	123

Scopo	123
Sistemi operativi	124
Dati significativi	124
Modulo Application	124
Scopo	124
Sistemi operativi	124
Dati significativi	124
Modulo Calendar	124
Scopo	124
Sistemi operativi	124
Dati significativi	125
Modulo Call	125
Scopo	125
Sistemi operativi	125
Dati significativi	125
Modulo Camera	125
Scopo	125
Sistemi operativi	126
Dati significativi	126
Modulo Chat	126
Scopo	126
Sistemi operativi	126
Dati significativi	126
Modulo Clipboard	127
Scopo	127
Sistemi operativi	127
Dati significativi	127
Modulo Conference	127
Scopo	127
Sistemi operativi	127
Dati significativi	127
Modulo Crisis	128
Comportamento su dispositivi desktop	128
Comportamento su dispositivi mobile	128
Sistemi operativi	128
Dati significativi desktop	128
Dati significativi mobile	129
Modulo Device	129
Scopo	129
Sistemi operativi	129

Dati significativi mobile	129
Modulo File	130
Scopo	130
Sistemi operativi	130
Dati significativi	130
Modulo Infection	131
Modulo Keylog	131
Scopo	131
Sistemi operativi	131
Dati significativi	131
Modulo Livemic	131
Scopo	131
Sistemi operativi	132
Dati significativi	132
Modulo Messages	132
Scopo	132
Sistemi operativi	132
Dati significativi	133
Modulo Mic	133
Scopo	133
Piattaforme	133
Dati significativi	133
Modulo Mouse	134
Scopo	134
Sistemi operativi	134
Dati significativi	134
Modulo Password	135
Scopo	135
Sistemi operativi	135
Dati significativi	135
Modulo Position	135
Scopo	135
Sistemi operativi	135
Dati significativi mobile	135
Modulo Screenshot	136
Scopo	136
Sistemi operativi	136
Dati significativi	136
Modulo Url	136
Scopo	136

Sistemi operativi	136
Dati significativi	137
Appendice: vettori di installazione	138
Ottenere un certificato per il Code Signing	139
Introduzione	139
Installazione del certificato Code Signing	139
Elenco dei vettori di installazione	139
Sistemi operativi supportati dagli agent	139
Vettore Exploit (desktop)	140
Scopo	140
Installazione	140
Eliminazione file non più utilizzati	141
Sistemi operativi	141
Parametri	141
Vettore Melted Application	141
Scopo	141
Sistemi operativi	141
Parametri	141
Vettore Network Injection	142
Scopo	142
Sistemi operativi	142
Parametri	142
Vettore Offline Installation	142
Scopo	142
Sistemi operativi	142
Parametri	143
Vettore Silent Installer	143
Scopo	143
Sistemi operativi	143
Parametri	143
Vettore U3 Installation	144
Scopo	144
Sistemi operativi	144
Parametri	144
Vettore Exploit (mobile)	145
Scopo	145
Installazione	145
Eliminazione file non più utilizzati	145
Esempio comandi per copiare installer nel dispositivo iOS	145
Sistemi operativi	145

Parametri	145
Vettore Installation Package	146
Scopo	146
Note per sistemi operativi Android (preparazione del vettore)	146
Note per sistemi operativi Android (installazione)	146
Note per sistemi operativi Windows Mobile	147
Note per sistemi operativi BlackBerry	147
Note per sistemi operativi Symbian	147
Sistemi operativi	147
Parametri Android, iOS, WinMobile	147
Parametri BlackBerry	148
Parametri Symbian	148
Vettore Local Installation	148
Scopo	148
Sistemi operativi	149
Parametri	149
Vettore QR Code/Web link	149
Scopo	149
Funzionamento	149
Eliminazione file non più utilizzati	149
Sistemi operativi	149
Parametri	149
Vettore WAP Push Message	150
Scopo	150
Funzionamento	150
Installazione	150
Eliminazione file non più utilizzati	150
Sistemi operativi	150
Parametri	151
Ottenere un certificato Symbian	151
Introduzione	151
Sequenza consigliata	151
Ottenere l'ID del Editore (voi)	152
Creare le chiavi Certificate Public e Private	152
Creare il Development Certificate	153

Glossario dei termini

Di seguito i termini utilizzati in questo manuale e loro definizione.

A

Accounting

Sezione della console dedicata alla gestione degli accessi a RCS.

Agente

Sonde software installate sui dispositivi sotto monitoraggio. Progettate per raccogliere prove e comunicarle al Collector.

Alerting

Sezione della console dedicata alle segnalazioni di nuove prove.

Amministratore

Colui che abilita l'accesso al sistema agli utenti, crea i gruppi di lavoro e definisce le indagini in essere, gli obiettivi e il tipo di dati da raccogliere.

Amministratore di sistema

Colui che installa i server e le console, si occupa degli aggiornamenti software e del ripristino dei dati in caso di malfunzionamento.

Analista

Persona incaricata dell'analisi dei dati raccolti durante le indagini.

Anonymizer

(opzionale) Protegge il server da attacchi esterni e consente l'anonimato durante le operazioni di indagine. Trasferisce i dati degli agent ai Collector.

Audit

Sezione della console che riporta tutte le azioni degli utenti e del sistema. Utilizzata per controllare abusi di RCS.

avvisi da evidence

Avvisi, normalmente email, inviati agli analisti per avvisarli che una nuova evidence corrisponde alle regole impostate.

B

back end

Ambiente destinato alla decodifica e salvataggio delle informazioni raccolte. In architettura distribuita include il Master Node e i database Shard.

BRAS

(Broadband Remote Access Server) instrada il traffico da/a DSLAM verso la rete dell'ISP e fornisce l'autenticazione per gli iscritti dell'ISP.

BSSID

(Basic Service Set IDentifier) Identificativo dell'Access Point e dei suoi client.

C

Collector

Riceve i dati inviati dagli agent, direttamente o tramite la catena di Anonymizer.

console

Computer su cui è installato RCS Console. Accede direttamente a RCS Server o al Master Node.

D

Dashboard

Sezione della console dedicata all'Analista. Usata per avere una rapida panoramica dello stato delle investigazioni, dei target e degli agent più importanti.

DSLAM

(Digital Subscriber Line Access Multiplexer) apparato di rete, spesso collocato negli scambi telefonici dell'operatore telefonico. Connette più interfacce DSL a un canale di comunicazione digitale ad alta velocità usando le tecniche di multiplexing.

E

entità

Insieme di informazioni di intelligence associate a un target.

ESSID

(Extended Service Set Identifier) Conosciuto anche come SSID, identifica la rete WiFi.

evidence

Dati delle prove raccolti. Il formato dipende dal tipo di evidence (es.: immagine).

F

factory

Un modello per la configurazione e la compilazione di agent.

front end

Ambiente destinato a comunicare con gli agent per raccogliere informazioni e impostare la loro configurazione. In architettura distribuita include il Collector e il Network Controller.

G

gruppo di alerting

Raggruppa gli utenti che devono ricevere notifiche via mail ogni volta che si genera un allarme di sistema (per esempio, il database ha superato il limite di spazio libero disponibile). Normalmente, questo gruppo è associato a nessuna operation.

M

Monitor

Sezione della console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

N

Network Controller

Componente che controlla lo stato dei Network Injector e degli Anonymizer, spedendo loro le nuove configurazioni o aggiornamenti software.

Network Injector

Componente hardware che controlla il traffico di rete del target e inietta un agent nelle risorse Web selezionate. Fornito in due versioni, Appliance o Tactical:

Appliance è per installazioni presso ISP, mentre Tactical è utilizzato sul campo.

Network Injector Appliance

Versione rack di Network Injector, per l'installazione presso l'ISP. Cfr.: Tactical Network Injector.

O

operation

Investigazione verso uno o più target, i cui dispositivi saranno i destinatari degli agent.

R

RCS

(Remote Control System) il prodotto oggetto di questo manuale.

RCS Console

Software dedicato all'interazione con RCS Server.

RCS Server

Una o più macchine, in base all'architettura di installazione, dove sono installati i componenti alla base di RCS: i database Shard, i Network Controller e Collector.

regole di alert

Regole che creano alert quando una nuova evidence viene salvata o quando l'agent sincronizza per la prima volta.

regole di injection

Impostazioni che definiscono come identificare traffico HTTP, quale risorsa da infettare e quale metodo usare per l'infezione.

S

sequenze di acquisizione

Insieme di eventi, azioni e moduli di acquisizione complessi che costituiscono la configurazione avanzata di un agent.

SSH

(Secure SHell) protocollo di rete per sessioni remote cifrate, servizi remoti o esecuzioni comandi.

System

Sezione della console dedicata alla gestione del sistema.

T

Tactical Network Injector

Versione portatile di Network Injector, per utilizzo tattico. Cfr.: Network Injector Appliance.

TAP

(Test Access Port) dispositivo hardware inserito in reti informatiche che permette il monitoraggio passivo del flusso dati in transito.

target

La persona fisica sotto investigazione.

Tecnico

Colui che su mandato dell'Amministratore crea e gestisce gli agent.

V

VPS

(Virtual Private Server) server remoto su cui installare l'Anonymizer. Normalmente disponibile a noleggio.

W

WPA

(WiFi Protected Access) Protezione per le reti WiFi.

WPA 2

(WiFi Protected Access) Protezione per le reti WiFi.

Introduzione a questa Guida

Presentazione

Obiettivi del manuale

Questo manuale guida il *Tecnico* a utilizzare RCS Console per:

- creare gli agent e installarli su un target definito dall'Amministratore
- creare le regole per l'injection di connessioni HTTP per i Network Injector

Di seguito sono presentate le informazioni necessarie alla consultazione del manuale.

Contenuti

Questa sezione include i seguenti argomenti:

Novità della guida	2
Documentazione fornita	3
Convenzioni tipografiche per le segnalazioni	4
Convenzioni tipografiche per la formattazione	4
Destinatari del prodotto e di questa guida	5
Dati di identificazione dell'autore del software	6

Novità della guida

Elenco note di rilascio e aggiornamenti di questa guida in linea.

<i>Data rilascio</i>	<i>Codice</i>	<i>Versione software</i>	<i>Descrizione</i>
8 Luglio 2013	Manuale del tecnico 1.4 LUG-2013	8.4	<p>Sul Tactical Control Center è stata aggiunta la possibilità di fare il test della connessione di rete, selezionare un dizionario aggiuntivo per attaccare una rete con protezione WPA o WPA 2 e visualizzare le regole installate. È ora sempre visibile la potenza del segnale di rete.</p> <p>Vedi "Cose da sapere su Tactical Control Center" a pagina84 .</p> <p>Sull'Appliance Control Center è possibile mappare un indirizzo IP pubblico sull'indirizzo IP privato preimpostato sull'interfaccia di rete e visualizzare le regole installate.</p> <p>Vedi "Cose da sapere su Appliance Control Center" a pagina79 .</p> <p>Rimossa la regola INJECT-HTML-JAVA e aggiunte le regole INJECT-HTML-FILE e INJECT-HTML-FLASH.</p> <p>Vedi "Dati delle regole di injection" a pagina74 .</p> <p>Eliminato il vettore Applet Web e deprecato il modulo Infection.</p> <p>Aggiunta nota all'azione Uninstall su Android.</p> <p>Vedi "Azione Uninstall" a pagina110 .</p> <p>Per Android il limite dei privilegi di root necessari per i moduli Chat, Messages e Screenshot si è esteso a tutte le versioni del sistema operativo.</p> <p>Vedi "Modulo Chat" a pagina126 , "Modulo Messages" a pagina132</p>
15 Marzo 2013	Manuale del tecnico 1.3 MAR-2013	8.3	<p>Modificato uso del Tactical Control Center. Vedi "Tactical Control Center" a pagina89 .</p> <p>Modificato uso del Appliance Control Center. Vedi "Appliance Control Center" a pagina80 .</p> <p>Aggiunta possibilità di creare una factory a livello di operation. Vedi "Pagina dell'operation" a pagina23 .</p> <p>Modificati i vettori Installation Package e Melted application vedi "Elenco dei vettori di installazione" a pagina139 vedi "Elenco dei vettori di installazione" a pagina139 vedi "Elenco dei vettori di installazione" a pagina139 .</p> <p>Aggiunta possibilità di disabilitare le evidenze screenshot nello scout agent. Vedi "Cose da sapere sugli agent" a pagina40 .</p> <p>Aggiunta gestione licenza per esclusione caricamento file e esecuzione comandi sul dispositivo del target. Vedi "Trasferimento file da/a il target" a pagina46 .</p>

Data rilascio	Codice	Versione software	Descrizione
15 Ottobre 2012	Manuale del tecnico 1.2 OTT- 2012	8.2	<p>Aggiunto salvataggio configurazioni base o avanzate come template. Vedi "Cose da sapere sulla configurazione base" a pagina52 e Vedi "Cose da sapere sulla configurazione avanzata" a pagina58 .</p> <p>Aggiunto wizard per creazione rapida di una investigazione. Vedi "Descrizione dei wizard da homepage" a pagina13</p> <p>Aggiunta gestione dello scout agent. Vedi "Cose da sapere sugli agent" a pagina40 .</p>
30 Giugno 2012	Manuale del tecnico 1.1 GIU 2012	8.1	<p>Aggiunte funzioni sull'agent vedi "Pagina dell'agent" a pagina42 .</p> <p>Aggiunto evento Idle vedi "Evento Idle" a pagina115 .</p> <p>Modificata installazione per i vettori Exploit, WAP push e QR Code. Modificati i vettori Offline Installation, Installation Package vedi "Elenco dei vettori di installazione" a pagina139 .</p> <p>Modificato processo per ottenere certificato per Symbian vedi "Ottenere un certificato Symbian" a pagina151 .</p> <p>Certificato Code Signing per vettori Melted Application e Silent Installer vedi "Ottenere un certificato per il Code Signing" a pagina139 .</p>
16 Aprile 2012	Manuale del tecnico 1.0 APR- 2012	8.0	Prima pubblicazione

Documentazione fornita

A corredo del software RCS sono forniti i seguenti manuali:

Manuale	Destinatari	Codice	Formato di distribuzione
Manuale dell'amministratore di sistema	Amministratore di sistema	<i>Manuale dell'amministratore di sistema</i> 1.3 MAR-2013	PDF
Manuale dell'amministratore	Amministratori	<i>Manuale dell'amministratore</i> 1.3 MAR-2013	PDF

<i>Manuale</i>	<i>Destinatari</i>	<i>Codice</i>	<i>Formato di distribuzione</i>
Manuale del tecnico (questo manuale)	Tecnici	<i>Manuale del tecnico 1.4 LUG-2013</i>	PDF
Manuale dell'analista	Analisti	<i>Manuale dell'analista 1.3 MAR-2013</i>	PDF

Convenzioni tipografiche per le segnalazioni

Di seguito le segnalazioni previste in questo documento (Microsoft Manual of Style):



AVVERTENZA: indica una situazione rischiosa che se non evitata, può causare danni fisici all'utente o alle attrezzature.



PRUDENZA: indica una situazione rischiosa che se non evitata, può causare la perdita di dati.



IMPORTANTE: offre indicazioni essenziali al completamento del compito. Mentre le note possono essere trascurate e non inficiano il completamento del compito, le indicazioni importanti non devono essere trascurate.



NOTA: informazioni neutre e positive che enfatizzano o aggiungono informazioni a dei punti nel testo principale. Fornisce informazioni che possono essere applicate solo in casi speciali.



Suggerimento: consiglia l'utente nell'applicare le tecniche e le procedure descritte nel testo ai loro bisogni specifici. Può suggerire un metodo alternativo e non è fondamentale alla comprensione del testo.



Richiede assistenza: l'operazione può essere portata a termine solo su indicazioni dell'assistenza tecnica.

Convenzioni tipografiche per la formattazione


Di seguito la legenda di alcune convenzioni tipografiche:

<i>Esempio</i>	<i>Stile</i>	<i>Descrizione</i>
Vedi " Dati degli utenti "	<i>corsivo</i>	indica il titolo di un capitolo, una sezione, una sottosezione, un paragrafo, una tabella o una figura di questo manuale, o di un'altra pubblicazione di riferimento.

Esempio	Stile	Descrizione
<ggmmaaaa>	<aaa>	indica un testo che dovrà essere specificato dall'utente secondo una certa sintassi. Nell'esempio <ggmmaaaa> è una data e può diventare "14072011".
Selezionare uno dei server elencati [2].	[x]	indica l'oggetto citato nel testo e che compare nell'immagine adiacente.
Fare clic su Add . Selezionare il menu File, Save data .	grassetto	indica una scritta sull'interfaccia operatore, sia di un elemento grafico (es.: tabella, scheda) sia di un pulsante a video.
Premere ENTER	MAIUSCOLO	indica il nome di tasti della tastiera.
Cfr.: Network Injector Appliance	-	suggerisce di confrontare la definizione di un termine in glossario o contenuto con altro termine o contenuto.

Destinatari del prodotto e di questa guida

Di seguito le figure professionali che interagiscono con RCS.

Destinatario	Attività	Competenze
Amministratore di sistema	Segue le indicazioni dell'assistenza HackingTeam fornite in fase contrattuale. Installa e aggiorna i server RCS, i Network Injector e le RCS Console. Programma e gestisce i backup. Ripristina i backup in caso di sostituzione dei server.  AVVERTENZA: l'amministratore di sistema deve avere tutte le competenze necessarie richieste. HackingTeam non si assume alcuna responsabilità di malfunzionamenti o danni alle attrezzature arrecati da una installazione non professionale.	<i>Tecnico di reti esperto</i>
Amministratore	Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze.	<i>Responsabile dell'indagine</i>
Tecnico	Crea gli agent e li configura. Configura le regole di un Network Injector.	<i>Tecnico specializzato in intercettazioni</i>
Analista	Analizza le evidence e le esporta.	<i>Operativo</i>

Dati di identificazione dell'autore 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

e-mail: info@hackingteam.com

RCS (Remote Control System)

Presentazione

Introduzione

RCS (Remote Control System) è una soluzione a supporto delle investigazioni che intercetta attivamente e passivamente dati e informazioni dai dispositivi dei bersagli di tali investigazioni. RCS infatti crea, configura e installa nell'assoluto anonimato degli agenti software che raccolgono dati e informazioni e inviano i risultati al database centrale per la decodifica e il salvataggio.

Contenuti

Questa sezione include i seguenti argomenti:

Differenze rispetto alle versioni precedenti	8
---	----------

Differenze rispetto alle versioni precedenti

Di seguito le differenze rispetto alla versione RCS 7.6.

Glossario dei termini

<i>RCS v. 7.6</i>	<i>RCS 8.0 e successive</i>
Attività	Operation
Agente	Module
Anonymizer chain	Anonymizing chain
Backdoor	Agente
Backdoor Class	Factory
Collection Node (ASP)	Collector
Injection Proxy Appliance (IPA)	Network Injector Appliance
Log Repository (RCSDB)	Master Node e Shard aggiuntivi
Mobile Collection Node (RSSM)	Collector
RCSAnon	Anonymizer

Terminologia vettori di infection per desktop

RCS v. 7.6 *RCS 8.0 e successive*

EXE	Melted application
CD	Offline Installation
USB	Offline Installation
EXPL	Exploit

Terminologia vettori di infection per mobile

RCS v. 7.6 *RCS 8.0 e successive*

SD	Local Installation
CAB	Installation Package
APP	Exploit

RCS v. 7.6 RCS 8.0 e successive

SIS	Installation Package, Symbian
COD	
APK	Installation Package WAP Push Message

RCS Console per il Tecnico

Presentazione

Ruolo del Tecnico

Il ruolo del Tecnico è:

- creare delle regole di injection per ogni Network Injector installato
- creare agent di infezione per i vari dispositivi del target
- mantenere aggiornato il software degli agent

Funzioni abilitate per il Tecnico

Per completare le attività che gli competono, il Tecnico ha accesso alle seguenti funzioni:

- **Operation**
- **System**

Contenuti

Questa sezione include i seguenti argomenti:

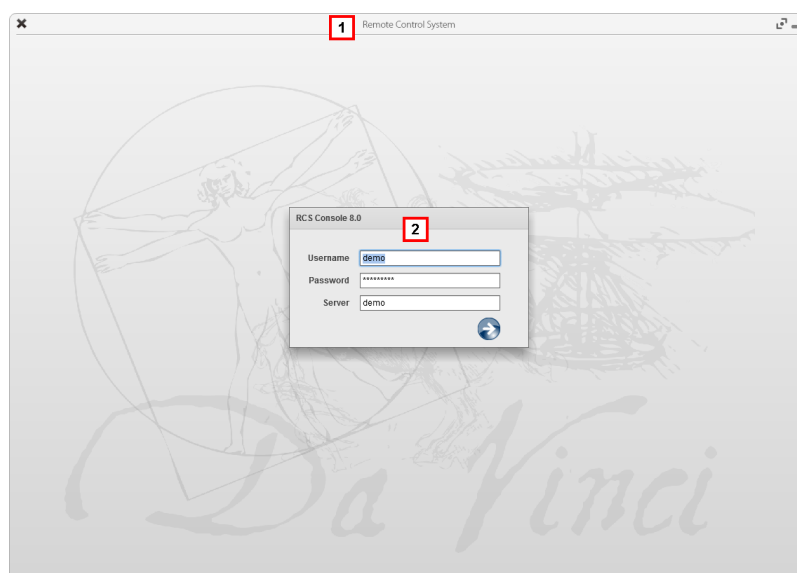
Avvio di RCS Console	11
Descrizione della homepage	12
Descrizione dei wizard da homepage	13
Elementi e azioni comuni dell'interfaccia	15
Procedure del Tecnico	19

Avvio di RCS Console

All'avvio, RCS Console chiede di inserire le proprie credenziali precedentemente impostate dall'Amministratore.

Come si presenta la pagina di login

Ecco come viene visualizzata la pagina di login:



Area Descrizione

- 1 Barra del titolo con pulsanti di comando:
 - ✕ Chiusura di RCS Console.
 - 🔍 Pulsante di ingrandimento della finestra.
 - ▬ Pulsante di riduzione a icona della finestra.
- 2 Finestra di dialogo per inserimento delle proprie credenziali.


Accedere a RCS Console

Per accedere alle funzioni di RCS Console:

Passo Azione


- 1 In **Username** e **Password** inserire le credenziali come assegnate dall'Amministratore.

Passo Azione

- 2 In **Server** inserire il nome della macchina o l'indirizzo del server cui ci si vuole collegare.
- 3 Fare clic su : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. Vedi "[Descrizione della homepage](#)" nel seguito .

Descrizione della homepage

Per visualizzare l'homepage:

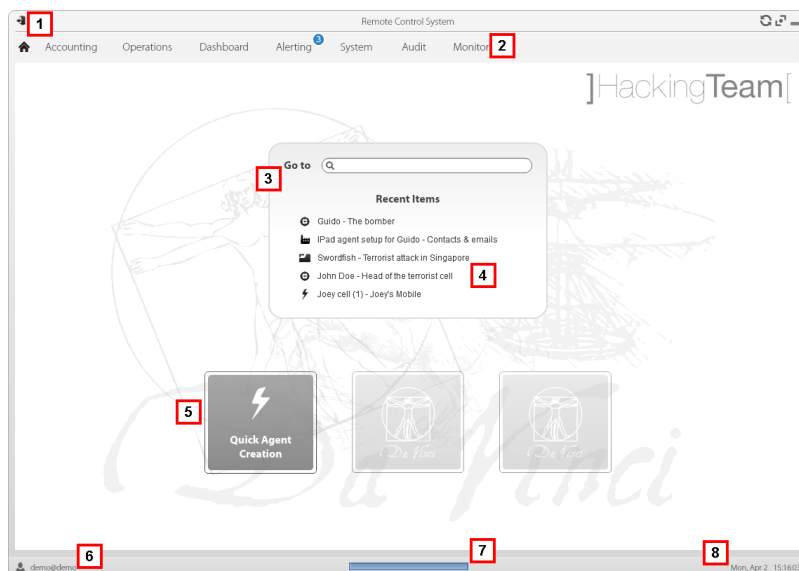
- fare clic su 

Introduzione

RCS Console presenta all'avvio questa homepage, unica per tutti gli utenti. I menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

Ecco come viene visualizzata l'homepage con già presente una cronologia degli argomenti recenti. Per il dettaglio degli elementi e le azioni comuni:

**Area Descrizione**


- 1 Barra del titolo con pulsanti di comando.

Area Descrizione

- 2 Menu di RCS con le funzioni abilitate per l'utente
- 3 Casella di ricerca per cercare tra i nomi di operation, target e agent, per nome o descrizione.
- 4 Collegamenti agli ultimi cinque elementi aperti (operation, target e agent).
- 5 Pulsanti per avvio dei Wizard.
- 6 Utente connesso con possibilità di cambiare la lingua e la password.
- 7 Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento.
- 8 Data e ora attuale con possibilità di cambio fuso orario.

Descrizione dei wizard da homepage

Per visualizzare
l'homepage:

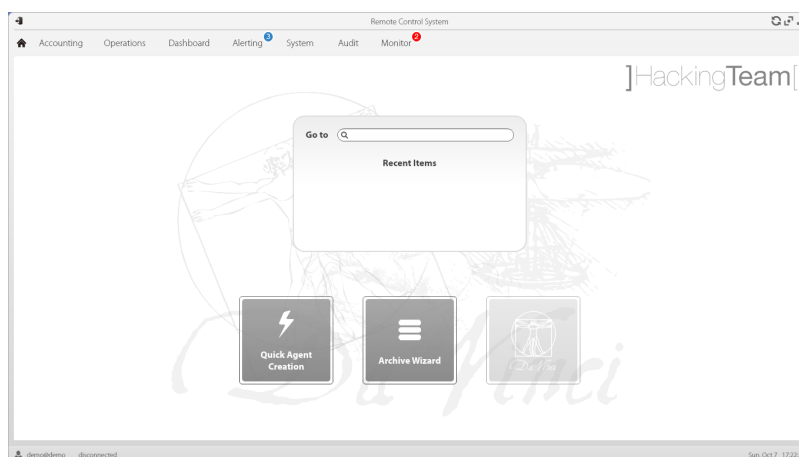
- fare clic su 

Introduzione

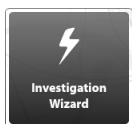
Per utenti con certi privilegi RCS Console presenta dei pulsanti che attivano dei wizard.

Come si presenta

Ecco come viene visualizzata l'homepage con i wizard abilitati:



Pulsante	Funzione
-----------------	-----------------



Aprire il wizard per la creazione rapida di un agent.



NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Tecnico.



Aprire il wizard per l'archiviazione rapida dei dati di operation e target.



NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Amministratore di sistema.



Pulsante non utilizzato.

Investigation Wizard

Questo wizard crea un agent rapidamente. Il wizard chiede il nome (es.: "SmartSpy") e il tipo di agent che si vuole creare (desktop o mobile) e in sequenza crea:

1. una operation "SmartSpy"
2. un target "SmartSpy"
3. una factory "SmartSpy"
4. un gruppo di utenti "SmartSpy" di cui l'utente attuale è il solo appartenente




e porta direttamente alla pagina della configurazione della factory. Vedi "[Configurazione base di una factory o di un agent](#)" a pagina 52

A questa operation, target o gruppo di utenti è possibile aggiungere altri elementi semplicemente agendo nelle pagine di dettaglio.

I dati sono archiviati in backup e possono essere ripristinati in qualsiasi momento.

Di seguito la spiegazione delle diverse opzioni:

Opzione	Descrizione
Archive all data into a backup	Salva tutti i dati dell'operation o del target scelto in un file di backup di tipo full. Il backup compare nell'elenco dei backup programmati e può essere ripristinato in qualsiasi momento.

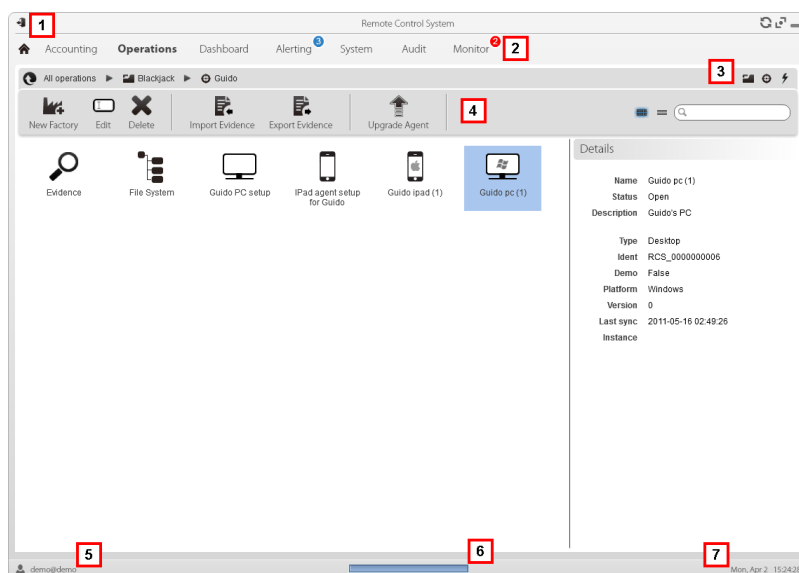
Opzione	Descrizione
Remove all data from the live system	<p>Elimina dal database tutte le evidenze dell'operation o del target selezionato. L'operation o il target restano aperti e funzionanti. Solo il database viene ridotto di dimensione.</p> <p> PRUDENZA: se combinate questa opzione con il backup istantaneo date un nome particolare al backup in modo che sia evidente che le evidenze corrispondenti sono stati eliminate dal sistema.</p>
Mark the item as closed	<p>Chiude l'operation o il target selezionato.</p> <p> PRUDENZA: l'operation o il target vengono chiusi senza possibilità di essere riaperti. Gli agent non inviano più i dati, ma è possibile consultare le evidenze già ricevute.</p>
Delete the item from the system	<p>Elimina tutti i dati dell'operation o del target selezionato. Vengono eliminati dai database i dati dell'operation, dei target, degli agent e tutte le evidenze.</p> <p> PRUDENZA: eliminare un'operation/target è un'azione irreversibile e causa la perdita dei dati associati a quella operation/target.</p>

Elementi e azioni comuni dell'interfaccia

Ogni pagina del programma utilizza elementi comuni e permette azioni simili tra loro. Per facilitare la consultazione di questo manuale, sono stati descritti in questo capitolo elementi e azioni comuni ad alcune le funzioni.

Come si presenta RCS Console

Ecco come viene visualizzata una pagina tipica di RCS Console. In questo esempio mostriamo la pagina di un target:



Area Descrizione

- 1 Barra del titolo con pulsanti di comando:
 - 👤 Logout da RCS.
 - 🔄 Pulsante di aggiornamento della pagina.
 - 🔍 Pulsante di ingrandimento della finestra.
 - ▬ Pulsante di riduzione a icona della finestra.
- 2
 - 🏠 Pulsante per tornare alla homepage
 - Menu di RCS con le funzioni abilitate per l'utente
- 3 Barra di navigazione per l'operation. Di seguito la descrizione:

Icona Descrizione


- 🏠 Torna al livello superiore.
- 📁 Mostra la pagina dell'operation.
- 🎯 Mostra la pagina del target.
- 🏭 Mostra la pagina della factory.
- ⚡ Mostra la pagina dell'agent.


Area Descrizione

- 4 Pulsanti per visualizzare tutti gli elementi indipendentemente dalla loro appartenenza. Di seguito la descrizione:

Icona Descrizione

 Mostra tutte le operation.

 Mostra tutti i target.

 Mostra tutti gli agent.

- 5 Barre con i pulsanti della finestra.

- 6 Pulsanti e casella di ricerca:

Oggetto**Descrizione**

Casella di ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite.



Visualizza gli elementi in una tabella.



Visualizza gli elementi come icone.

- 7 Utente connesso con possibilità di cambiare la lingua e la password.
- 8 Area download con possibilità durante un'esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS Download.
- barra superiore: percentuale generazione sul server.
 - barra inferiore: percentuale download dal server su RCS Console.
- 9 Data e ora attuale con possibilità di cambio fuso orario.

Azioni sempre disponibili sull'interfaccia**Cambiare la lingua dell'interfaccia o la propria password**

Per cambiare la lingua dell'interfaccia o la propria password:

Passo Azione

- 1 Fare clic su **[6]** compare una finestra di dialogo con i dati dell'utente.
- 2 Cambiare lingua o password e fare clic su ***** per confermare e uscire.

Convertire le date-ora di RCS Console al proprio fuso orario

Per convertire tutte le date-ora al proprio fuso orario:

Passo Azione

- 1 Fare clic su **[8]** compare una finestra di dialogo con la data-ora attuale:
 - Ora UTC:** data-ora di Greenwich (GMT)
 - Ora Locale:** data-ora dove è installato il server RCS
 - Ora Console:** data-ora della console da cui si sta lavorando e che può essere convertita.
- 2 Cambiare il fuso orario e fare clic su ***** per confermare e uscire: tutte le date-ora visualizzate sono convertite come richiesto.

Azioni sulle tabelle

RCS Console mostra diversi dati in forma di tabella. Le tabelle permettono di:

- ordinare i dati per colonna in ordine crescente/decrescente
- filtrare i dati per ogni colonna

Azione

Descrizione

Ordinare per colonna

Fare clic sull'intestazione per ottenere l'ordine per quella colonna, crescente o decrescente.

Event	Path
SYNC	Swordfish
INSTANCE	Swordfish > J
EVIDENCE	*

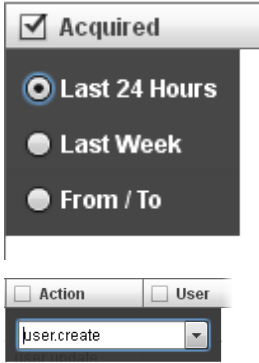
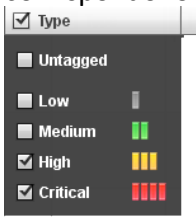
Filtrare un testo

Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.

<input checked="" type="checkbox"/> Info
boss

L'esempio mostrerà elementi con descrizioni tipo:

- "myboss"
- "bossanova"

Azione	Descrizione
Filtrare in base a un'opzione	<p>Selezionare un'opzione: compaiono gli elementi che corrispondono all'opzione scelta.</p> 
Filtrare in base a più opzioni	<p>Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte.</p> 
Cambiare la dimensione delle colonne	<p>Selezionare il bordo della colonna e trascinarlo.</p>

Procedure del Tecnico

Introduzione


Il Tecnico deve occuparsi delle regole di infezione per il recupero di informazioni importanti. Di seguito la descrizione di alcune procedure tipiche con il rimando ai capitoli importanti. Si tratta solo di semplici indicazioni. È fondamentale la competenza e la capacità di sfruttare la flessibilità di RCS per adattarlo alle esigenze dell'indagine.

Procedure

Effettuare l'injection su connessioni HTTP

Per effettuare l'injection su connessioni HTTP è necessario utilizzare Network Injector:

Passo Azione

- 1** Nella sezione **System, Network Injector** creare le regole di identificazione e injection per Network Injector Appliance e Tactical Network Injector.
Vedi "[Gestione dei Network Injector](#)" a pagina71
 **NOTA:** non è richiesta l'installazione di alcun agent.
- 2** Nel caso di utilizzo del Network Injector Appliance, il sistema applica le regole di identificazione sul traffico dati. Una volta trovati i dispositivi target li infetta con le regole di injection.
Oppure nel caso di utilizzo del Tactical Network Injector si potrà operare sia con identificazione e infezione automatica sia tramite operatore.
Vedi "[Tactical Control Center](#)" a pagina89 .

Infettare un computer non connesso a internet

Per infettare un computer non connesso a Internet.

Passo Azione

- 1** Creare una factory disabilitando la sincronizzazione a livello di operation, vedi "[Pagina dell'operation](#)" a pagina23 .
Oppure creare una factory a livello di target, sempre senza sincronizzazione, vedi "[Pagina del target](#)" a pagina28
- 2** Compilare la factory selezionando il vettore di installazione adatto alla piattaforma del dispositivo e al metodo di installazione, quindi creare l'agent.
Vedi "[Compilazione di una factory](#)" a pagina36 .
- 3** Installare l'agent presso il dispositivo del target nelle modalità scelte.
Vedi "[Elenco dei vettori di installazione](#)" a pagina139 .
- 4** Dopo il tempo necessario recuperare le evidence prodotte sul dispositivo del target.
- 5** Importare le evidence dell'agent e analizzarle.
Vedi "[Pagina dell'agent](#)" a pagina42 .

Infettare un computer connesso a Internet

Per infettare un computer connesso a Internet.



Suggerimento: questi passaggi sono fondamentali quando non si conoscono sin dall'inizio le attività del target da registrare, oppure si vuole evitare di registrare una quantità eccessiva di dati.

Passo Azione

- 1 Creare una factory: il sistema abilita automaticamente la sincronizzazione.
Vedi "[Pagina dell'operation](#)" a pagina23
- 2 Compilare la factory selezionando il vettore di installazione adatto alla piattaforma del dispositivo e al metodo di installazione, quindi creare l'agent.
Vedi "[Compilazione di una factory](#)" a pagina36 .
- 3 Installare l'agent presso il dispositivo del target nelle modalità scelte.
Vedi "[Elenco dei vettori di installazione](#)" a pagina139 .
- 4 Alla prima sincronizzazione l'agent compare nella pagina del target.
Vedi "[Pagina del target](#)" a pagina28
- 5 Riconfigurare l'agent utilizzando la configurazione base o avanzata. Alla successiva sincronizzazione l'agent applica la nuova configurazione.
Vedi "[Configurazione base di una factory o di un agent](#)" a pagina52
Vedi "[Configurazione avanzata di una factory o di un agent](#)" a pagina61 .

Mantenere aggiornato il software degli agent

Ciclicamente HackigTeam aggiorna il suo software. Per aggiornare agent già installati:

Passo Azione

- 1
 - Nella sezione **Operations, Target** aggiornare gli agent. Vedi "[Pagina del target](#)" a pagina28oppure
 - Nella sezione **Operations, Target** entrare in un agent e aggiornarlo. Vedi "[Pagina dell'agent](#)" a pagina42 .

I target

Presentazione

Introduzione

Un target è una persona fisica da sottoporre a monitoraggio. Possono essere utilizzati più agent, uno per ogni dispositivo posseduto dal target.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulle operation	23
Pagina dell'operation	23
Cose da sapere sui target	27
Pagina del target	28
Dati della pagina target	32
Cose da sapere sulle Factory e sugli Agent	34
Compilazione di una factory	36

Cose da sapere sulle operation

Cos'è un'operation

L'operation rappresenta l'indagine da eseguire. Un'operation contiene uno o più target, ovvero le persone fisiche da intercettare. Il Tecnico assegna al target uno o più agent di tipo *desktop* o *mobile*. Così l'agent può essere installato su un computer o su un dispositivo mobile.

Assegnare l'operation a un gruppo di utenti

Per garantire il massimo della riservatezza dei dati si suggerisce di associare un'operation solo agli utenti di RCS incaricati dell'indagine. Utenti non associati all'operation non vedranno alcun dato dell'operation e delle evidenze raccolte. Per questo motivo è necessario che chi crea un'operation faccia parte di almeno uno dei gruppi associati ad essa al momento della creazione.

Cosa avviene quando si crea una nuova operation

Quando un'operation viene creata è già dichiarata aperta, quindi è possibile creare i target dell'operation e chiedere al Tecnico la generazione e l'installazione degli agent. Ad operation aperta gli agent iniziano a raccogliere i dati e a inviarli a RCS.

Cosa avviene quando si chiude un'operation

L'operation deve essere chiusa alla chiusura effettiva dell'indagine, quando si è sicuri che tutti gli agent hanno già trasmesso tutte le evidenze raccolte al Backend.

La chiusura provoca automaticamente la chiusura dei target e la chiusura degli agent. Quando un agent viene chiuso, alla prima sincronizzazione viene disinstallato lasciando così pulito il dispositivo.

Un'operation chiusa non può più essere riaperta. Solo i dati dell'operation e le evidenze raccolte restano nel database.



PRUDENZA: in caso di sincronizzazioni non frequenti, per esempio ogni quattro giorni, attendere l'ultima sincronizzazione pianificata prima di chiudere l'operation.

Pagina dell'operation

Per entrare in una operation:

- sezione **Operation**, doppio-clic su una operation

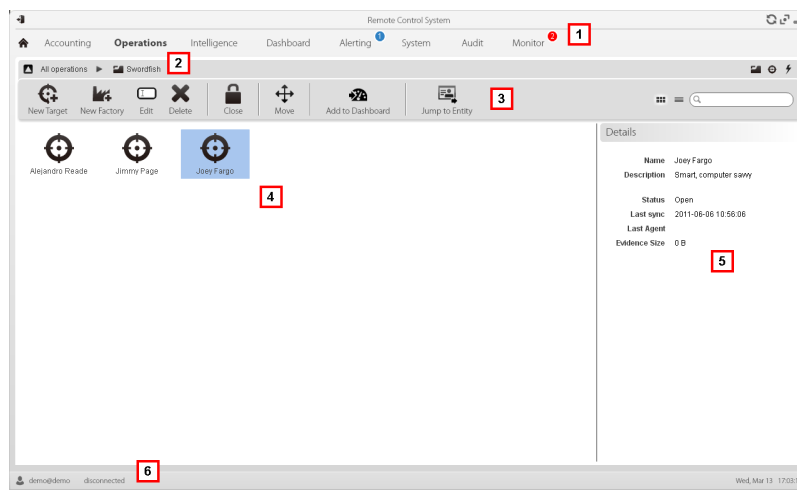
Scopo

Questa funzione permette di:

- gestire le factory, che compilate, diventeranno agent da installare sui dispositivi *vedi "Configurazione avanzata di una factory o di un agent" a pagina 61*
- creare uno o più target da monitorare durante un'operation
- gestire l'attivazione/disattivazione di un target.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Barra di navigazione.

Area Descrizione

3 Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona Funzione



Aggiunge un target.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Target management**.



Crea una factory.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Factory creation**. È possibile creare una factory anche a livello di target, *vedi "Pagina dell'operation" a pagina23*.



Modifica il target selezionato.



Elimina il target selezionato.



Chiude il target.



Sposta il target in un'altra operation.



Aggiunge il target alla dashboard.

4 Elenco dei target:



target Aperto



target Chiuso

5 Dati del target selezionato.

6 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per saperne di più sulle factory vedi "[Cose da sapere sulle Factory e sugli Agent](#)" a pagina34 .
Per gestire rapidamente i dati di un'operation vedi "[Descrizione dei wizard da homepage](#)" a pagina13 .

Creare una factory

Per creare una factory:

Passo Azione

- 1
 - Fare clic su **New Factory**: compaiono i dati da compilare.
 - Inserire il nome e la descrizione e in **Type** selezionare il tipo di dispositivo.
- 2 Fare clic su **Save**: nell'area di lavoro principale compare la nuova factory con il nome scelto.

Creare un target

Per creare un nuovo target:

Passo Azione

- 1 Fare clic su **New Target**: compaiono i dati da compilare.
- 2 Compilare i dati richiesti e fare clic su **Save**: nell'area di lavoro principale compare il nuovo target in stato Aperto, ovvero pronto per essere utilizzato da un Tecnico.

Chiudere un target

Per chiudere un target e attivare la disinstallazione dei suoi agent:

Passo Azione

- 1 Selezionare un target, quindi fare clic su **Close**.
- 2 Confermare la chiusura: viene chiuso il target e viene automaticamente avviata la disinstallazione dei suoi agent. I dati restano disponibili sul database.



PRUDENZA: la chiusura del target è irreversibile, vedi "[Cose da sapere sui target](#)" alla pagina successiva

Modificare i dati di un target

Per modificare i dati di un target:

Passo Azione

- 1** Selezionare un target, quindi fare clic su **Edit**: compaiono i suoi dati.
- 2** Modificare i dati e fare clic su **Save**.

Eliminare un target

Per eliminare un target:

Passo Azione

- 1** Selezionare un target, quindi fare clic su **Delete**.
- 2** Confermare l'azione facendo clic su **OK**: vengono eliminati dai database i dati del target, dei suoi agent e tutte le evidenze.



PRUDENZA: eliminare un target è un'azione irreversibile e causa la perdita dei dati associati a quel target.

Cose da sapere sui target

Cos'è un target

Il target rappresenta la persona fisica da investigare. Il Tecnico assegna al target uno o più agent di tipo desktop o mobile. Così l'agent può essere installato su un computer o su un dispositivo mobile.

Compiti dell'Amministratore

Il ruolo dell'Amministratore nella gestione dei target è a un livello di organizzazione generale; è compito del Tecnico configurare e lavorare operativamente sui target secondo le disposizioni dell'Amministratore.

L'Amministratore ha il compito di:

- creare un nuovo target all'interno di un'operation
- dare disposizioni al Tecnico sulle tempistiche di attivazione e la tipologia delle prove da raccogliere attraverso gli agent di un determinato target, in base alle caratteristiche del mandato ricevuto dall'autorità giudiziaria
- verificare la corretta applicazione delle disposizioni attraverso il controllo dell'Audit
- chiudere un target

Cosa avviene quando si crea un target

Quando un target viene creato è già dichiarato *aperto*, quindi è possibile chiedere al Tecnico la generazione e l'installazione degli agent.

Cosa avviene quando si chiude un target

È possibile chiudere un target, per esempio alla chiusura effettiva dell'indagine su quel target.

La chiusura di un target chiude automaticamente i suoi agent. Quando un agent viene chiuso, alla prima sincronizzazione viene disinstallato lasciando così pulito il dispositivo.

Un target chiuso non può più essere riaperto. Solo i dati del target stesso e quelli già inviati dagli agent restano nel database.



PRUDENZA: quando si chiude un target, si disinstallano automaticamente tutti gli agent associati. Chiudere un target solo quando si è certi di avere tutti i dati che servono.



PRUDENZA: in caso di sincronizzazioni non frequenti, per esempio ogni quattro giorni, attendere l'ultima sincronizzazione pianificata prima di chiudere il target.



Suggerimento: chiudere un target solo quando si è sicuri che gli agent hanno già scaricato tutte le informazioni di cui si ha bisogno.

Apertura e chiusura di un'operation

Nel caso di chiusura di una operation, tutti i target associati sono irrevocabilmente chiusi, e tutti i loro agent disinstallati. Vedi "[Cose da sapere sulle operation](#)" a pagina23 .

Pagina del target

Per entrare in un target

- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target

Scopo

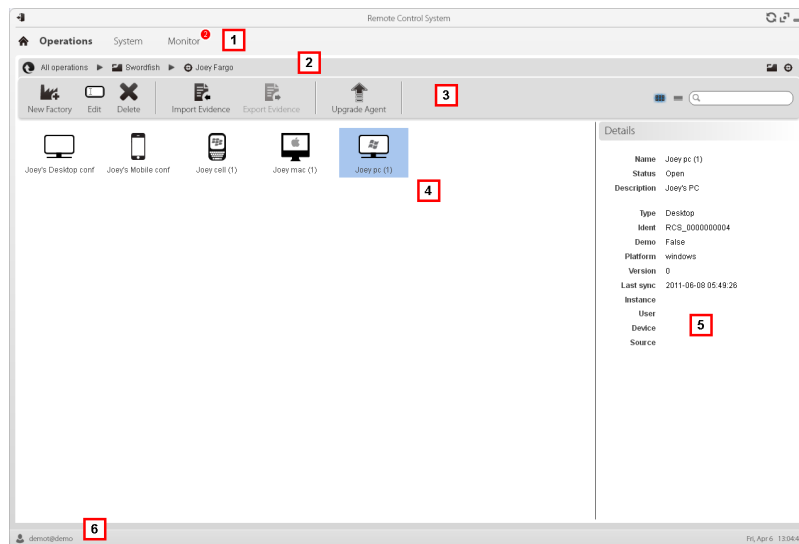
Questa funzione permette di:

- gestire le factory, che compilate, diventeranno agent da installare sul dispositivo del target.
- aprire una factory per la configurazione base (vedi "[Configurazione base di una factory o di un agent](#)" a pagina52) o per la configurazione avanzata (vedi "[Configurazione avanzata di una factory o di un agent](#)" a pagina61
- importare le evidence del target

- entrare in un agent installato
- aggiornare il software dell'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina:





Area Descrizione

- 1 Menu di RCS.
- 2 Barra di navigazione.

Area Descrizione

3 Barre con i pulsanti della finestra. Di seguito la descrizione:

 NOTA: il pulsante  visualizza gli elementi in elenco con i loro dati.

Icona Funzione



Crea una factory.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Factory creation**.
È possibile creare una factory anche a livello di operation, vedi "[Pagina dell'operation](#)" a pagina23 .



Modifica una factory o un agent.



Eliminare una factory o un agent.



Chiude l'agent o la factory.



Aggiunge l'agent alla dashboard.



Aggiunge l'agent agli alert: tutte le volte che avviene la sincronizzazione viene generato un alert.



Sposta la factory o l'agent in un altro target.



Importa le evidence del target raccolte fisicamente sul dispositivo.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Import evidence**.



Esporta le evidence del target in formato .tgz.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Evidence export** .



Aggiorna il software di tutti gli agent con l'ultima versione ricevuta dall'assistenza HackingTeam.



PRUDENZA: l'aggiornamento non aggiorna la configurazione che viene trasmessa agli agent alla successiva sincronizzazione.

Area Descrizione

4 Icone/elenco delle factory create e degli agent installati.



: agent in modalità demo.



: scout agent in attesa di verifica.

5 Dati della factory o dell'agent selezionato.

6 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per la descrizione dei dati presenti sulla finestra vedi "[Dati della pagina target](#)" nella pagina di fronte .

Per saperne di più sui target vedi "[Cose da sapere sulle Factory e sugli Agent](#)" a pagina34

Per gestire rapidamente i dati di un target vedi "[Descrizione dei wizard da homepage](#)" a pagina13 .

Creare una factory

Per creare una factory:

Passo Azione

- 1**
 - Fare clic su **New Factory**: compaiono i dati da compilare.
 - Inserire il nome e la descrizione e in **Type** selezionare il tipo di dispositivo.
- 2** Fare clic su **Save**: nell'area di lavoro principale compare la nuova factory con il nome scelto.

Chiudere una factory o un agent

Per chiudere una factory o un agent:

Passo Azione

- 1** Selezionare una factory o un agent e fare clic su **Close**.

Passo Azione

- 2 Confermare la chiusura.



PRUDENZA: chiudere un agent è un'azione irreversibile che ne provoca la sua disinstallazione alla prima sincronizzazione. Chiudere una factory, invece, non la rende più accessibile. Gli agent attivi resteranno comunque accessibili mentre tutti gli agent che non hanno effettuato almeno una sincronizzazione prima della chiusura della factory saranno disinstallati.

Eliminare una factory o un agent

Per eliminare una factory o un agent:

Passo Azione

- 1 Selezionare una factory o un agent, quindi fare clic su **Delete**.
Confermare l'azione: sono eliminati gli storici, le configurazioni, le evidence.



PRUDENZA: l'operazione è irreversibile.

Importare le evidence del target

Per importare le evidence:

Passo Azione

- 1 Fare clic su **Import Evidence**: si apre la finestra di importazione.
Fare clic su **Select Directory** e selezionare la cartella dove il file offline.ini è salvato
- 2 Fare clic su **Import**: le evidence sono salvate nel database e disponibili per la visualizzazione da parte degli Analisti.

Esportare le evidence del target

Per esportare le evidence :

Passo Azione

- 1 Fare clic su **Export Evidence**: si apre la finestra di esportazione.
- 2 Fare clic su **Ok**: le evidence sono salvate nella cartella specificata.

Dati della pagina target

Per visualizzare i dati della pagina:

- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, fare clic su **Icon view** o **Table view**

Gli elementi della pagina possono essere visualizzati a icone o a tabella.

Visualizzazione a icone

Di seguito la descrizione delle icone:

Dato *Descrizione*



Factory di tipo desktop e mobile in stato Aperto.



Agent di tipo desktop, in stato Aperto, per i sistemi operativi:

- OS X
- Windows



Agent di tipo mobile, in stato Aperto, per i sistemi operativi:

- Android,
- BlackBerry,
- iOS,
- Symbian
- Windows Mobile



NOTA: factory e agent in stato **CLOSED** hanno l'icona di colore grigio chiaro. Questa è l'icona di un agent mobile per Android in stato Chiuso:



NOTA: agent in stato **CLOSED** hanno l'icona di colore grigio chiaro. Questa è l'icona di un agent mobile per Android in stato Chiuso:



NOTA: lo scout agent mostra una bussola accanto all'icona del dispositivo. Questa è l'icona di uno scout agent desktop Windows

Visualizzazione a tabella

Di seguito la descrizione dei dati:

<i>Dato</i>	<i>Descrizione</i>
Nome	Nome della factory o dell'agent.
Descrizione	Descrizione della factory o dell'agent.
Status	Open: una factory aperta può essere compilata per creare più agent. Un agent aperto può essere installato, è funzionante e registra evidence. Closed: una factory o un agent chiusi non possono essere più aperti. I dati presenti in RCS sono ancora consultabili.
Type	Tipologia desktop o mobile.
Platform	(solo agent) Sistema operativo su cui l'agent si è installato.
Version	(solo agent) Versione dell'agent. A ogni nuova configurazione viene creata una nuova versione.
Last sync	(solo agent) Data e ora dell'ultima sincronizzazione dell'agent.
Ident	(solo agent) Identificativo univoco di un agent.
Instance	(solo agent) Identificativo univoco del dispositivo su cui l'agent è installato.

Cose da sapere sulle Factory e sugli Agent

Modalità di infezione

È possibile infettare un dispositivo tramite:

- **infezione fisica:** il dispositivo viene infettato tramite l'esecuzione di un file trasferito da memorie USB, CD o documenti. Le evidence possono essere raccolte fisicamente o via Internet non appena il dispositivo si connette.
- **infezione da remoto:** il dispositivo viene infettato dall'esecuzione di un file trasferito via connessione Internet o reso disponibile in una risorsa Web. Le evidence possono essere raccolte fisicamente o via Internet non appena il dispositivo si connette. L'infezione da remoto può essere potenziata tramite l'utilizzo di un Network Injector.



Componenti della strategia di infezione

I componenti richiesti per una corretta infezione sono:

- **Factory:** modello di un agent.
- **Vettori di installazione:** canali di infezione.
- **Agent:** il software da installare sul dispositivo del target.
- **Target e operation:** definiti in fase di apertura dell'indagine da chi ha il ruolo di Amministratore di sistema. Fare riferimento al Manuale dell'Amministratore di Sistema.
- **Evidence:** le registrazioni da raccogliere

Le factory

La *factory* è un modello da cui creare un agent da installare. L'icona che la rappresenta è diversa in base al tipo di dispositivo cui l'agent è destinato:

-  : factory per agent desktop
-  : factory per agent mobile

Nella factory devono essere configurati:

- i dati da acquisire (configurazione base) o moduli da attivare dinamicamente (configurazione avanzata)
- i *vettori di installazione* (es.: CD, exploit, Network Injector)



Suggerimento: è possibile salvare una configurazione come template per caricarla alla successiva creazione di un agent simile.



Suggerimento: una factory può essere usata per creare più agent, per esempio da installare tramite vettori di installazione diversi (es.: due computer con sistemi operativi diversi).

Modalità di creazione delle factory

Le factory sono dei modelli che possono essere creati a due livelli della gerarchia operation-target-agent:

- *a livello di operation*: la factory, dopo la sua installazione e prima sincronizzazione, crea automaticamente per ogni dispositivo un agent e un target
- *a livello di target*: la factory, dopo la sua installazione e prima sincronizzazione, crea automaticamente un agent per quel target

La modalità a *livello di operation* garantisce l'assegnazione separata delle evidenze raccolte. Infatti crea tanti agent quanti sono i dispositivi. Successivamente se due o più dispositivi appartengono allo stesso target, sarà possibile spostare l'agent nel target giusto.

La modalità a *livello di target*, se erroneamente usata, rischia di creare una factory che però viene utilizzata per la creazione di più agent.

I vettori di installazione

I vettori di installazione sono scelti durante la compilazione e definiscono la modalità di installazione, fisica o remota, di un agent. Durante la compilazione i vettori di installazione disponibili possono variare in base al sistema operativo del dispositivo.

È possibile utilizzare più vettori di installazione per uno stesso agent.



NOTA: per effettuare l'injection su connessioni HTTP vengono utilizzate le regole di injection. Vedi "[Gestione dei Network Injector](#)" a pagina 71

Gli agent

Un *agent* è il risultato della compilazione di una *factory* con uno o più vettori di installazione. Un agent è pronto per essere installato sul dispositivo.

La configurazione base definisce il tipo di dati da acquisire, mentre la configurazione avanzata consente di attivare o disattivare i moduli in maniera dinamica ed autonoma.

Per i tipi di moduli disponibili nella configurazione base e avanzata vedi "[Elenco dei moduli](#)" a pagina122

Per saperne di più sugli agent vedi "[Cose da sapere sugli agent](#)" a pagina40 .

I moduli per l'acquisizione dei dati

I moduli determinano alcune attività sul dispositivo del target, in massima parte acquisizione dati. Sono abilitati e configurati nella configurazione base (solo alcuni) o nella configurazione avanzata.

I tipi di moduli disponibili dipendono anche dal tipo di dispositivo.

Per l'elenco completo vedi "[Elenco dei moduli](#)" a pagina122 .

Compilazione di una factory

Per compilare una factory:

- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su una factory, fare clic su **Build**
- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su una factory, fare clic su **Advanced Config, Build**

Scopo

Questa funzione permette di creare uno o più agent (effettivi o da collaudare in modalità demo) in base ai vettori di installazione e alle piattaforme scelte.



NOTA: per la descrizione dettagliata di ogni vettore di installazione vedi "[Elenco dei vettori di installazione](#)" a pagina139



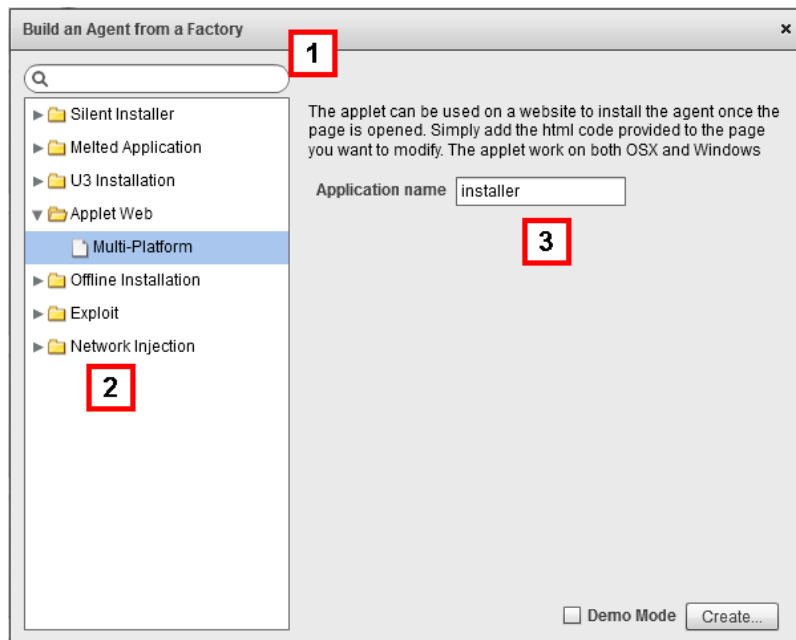
NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Installation vector creation**.

Passi successivi

La creazione di un agent implica la successiva installazione sul dispositivo del target.

Come si presenta la funzione

Ecco come viene visualizzata la pagina per un agent desktop:



Area Descrizione

- 1 Casella di ricerca dei vettori di installazione e piattaforme.
- 2 Visualizzazione ad albero dei vettori e delle piattaforme.
- 3 Area per l'inserimento dei parametri di compilazione dei vettori scelti.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per saperne di più sulle factory vedi "[Cose da sapere sulle Factory e sugli Agent](#)" a pagina34 .

Per la descrizione dettagliata di ogni vettore di installazione vedi "[Elenco dei vettori di installazione](#)" a pagina139

Creare un agent

Per creare un agent:

Passo Azione

- 1 Selezionare uno o più vettori di istallazione e impostare le opzioni richieste.

Passo Azione

- 2 Fare clic su **Create**: viene creato un file ZIP o ISO e scaricato nella cartella RCS Download, pronto per essere installato sul dispositivo.

Creare un agent da collaudare in modalità demo



IMPORTANTE: utilizzare questa opzione solo per collaudi effettuati su dispositivi interni. Gli agent in modalità demo non sono invisibili e la presenza di RCS non viene quindi nascosta.

Per creare un agent a scopo di collaudo:

Passo Azione

- 1 Selezionare uno o più vettori di installazione e impostare le opzioni richieste.
- 2 Selezionare la casella di controllo **Demo**.
- 3 Fare clic su **Create**; l'agent installato sul dispositivo mostrerà la sua presenza con messaggio sonori e video.

Gli agent

Presentazione

Introduzione

Gli agent acquisiscono dati dal dispositivo su cui sono installati e li inviano ai Collector di RCS. La loro configurazione e il loro software possono essere aggiornati e possono essere trasferiti file in modo assolutamente invisibile dal/al target.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sugli agent	40
Pagina dell'agent	42
Dati dello storico configurazioni di un agent	45
Dati dello storico eventi di un agent	46
Dati dello storico sincronizzazioni dell'agent	46
Trasferimento file da/a il target	46
Pagina dei comandi	49



Cose da sapere sugli agent

Installazione di un agent

L'agent può essere esposto e identificato se viene installato in ambienti con antivirus o in ambienti gestiti da personale tecnicamente esperto.

Per evitare che questo accada all'installazione viene in realtà inviato un suo sostituto, lo *scout agent*, che ha il solo compito di installarsi presso il dispositivo del target e verificarne l'ambiente.

Una volta installato, alla prima sincronizzazione lo scout agent compare nella pagina del target. L'icona che lo rappresenta, simile a quella dell'agent, indica la piattaforma su cui è installato. Per esempio:

-  : scout agent installato su un dispositivo Windows
-  : scout agent installato su dispositivo BlackBerry

Acquisizione evidence per analisi ambiente installazione

Dopo il completamento dell'installazione lo scout agent acquisisce evidence:

- di tipo **Screenshot** utili a identificare il dispositivo del target
- di tipo **Device** utili a capire se l'ambiente da infettare è tranquillo oppure se contiene applicazioni rischiose per l'integrità dell'agent.



IMPORTANTE: Le evidence di tipo screenshot vengono raccolte solo se il modulo è attivo nella configurazione. Se necessario, ricordarsi di abilitarlo prima di inviare l'agent.

Analisi ambiente di installazione



Dopo che lo scout agent ha acquisito le evidence, è necessario controllarle e decidere se l'ambiente di installazione è sicuro per l'agent vero e proprio.

Se l'ambiente è sicuro basta procedere con l'aggiornamento dell'agent: lo scout agent viene sostituito dal vero agent.

Se l'ambiente non è sicuro è necessario chiudere lo scout agent.

Aggiornamento dello scout agent

Con l'aggiornamento dello scout agent viene installato l'agent vero e proprio e nella pagina del target l'icona dello scout agent viene sostituita con quella dell'agent.

-  : agent installato su un dispositivo Windows
-  : agent installato su dispositivo BlackBerry

Sincronizzazione di un agent

Un agent si sincronizza solo se:

- la sincronizzazione è abilitata nella configurazione base.
- nella configurazione avanzata è stata aggiunta un'azione di tipo **Synchronize**.

Agent offline e online

L'agent si comporta diversamente in base alla disponibilità di una connessione a Internet:

**Se la
connessione
a Internet
è...**

non disponibile	se l'agent ha già dei moduli abilitati inizia a registrare i dati internamente al dispositivo.
disponibile	se l'agent ha effettuato la prima sincronizzazione è possibile: <ul style="list-style-type: none">• cambiare configurazione, per esempio man mano che le richieste di registrazioni si fanno più specifiche per quel dispositivo. La riconfigurazione dell'agent non modifica la configurazione della factory• aggiornare il suo software,• trasferire dei file da e verso il dispositivo,• analizzare le evidenze che sono state già inviate



Suggerimento: iniziare creando un agent e abilitando solo la sincronizzazione e il modulo del dispositivo. Quindi, una volta che l'agent è installato e alla ricezione della prima sincronizzazione, abilitare gradualmente gli altri moduli in base alle capacità del dispositivo e al tipo di evidenze che si vogliono raccogliere.

Disabilitazione temporanea di un agent

È possibile sospendere temporaneamente le attività di un agent senza disinstallarlo, semplicemente disabilitando tutti i moduli e lasciando attiva solo la sincronizzazione.

Collaudo di un agent

Per testare una configurazione prima di usarla, creare un agent in modalità Demo (vedi "[Compilazione di una factory](#)" a pagina 36).

L'agent viene creato in versione *demo* comportandosi in base alla configurazione impostata, con la sola differenza che segnala in modo evidente (con segnalazioni audio, led e messaggi a video) la sua presenza sul dispositivo. Le segnalazioni permettono di identificare facilmente il dispositivo infettato usato per il test.



NOTA: eventuali non ricezioni di evidence da un agent in modalità demo possono essere dovute a una errata configurazione del server, oppure all'impossibilità di raggiungere l'indirizzo del Collector impostato (es.: per problemi nella configurazione di rete).

Configurazione dell'agent

La configurazione di un agent (base o avanzata) può essere modificata più volte. A ogni salvataggio viene creata una copia della configurazione e viene salvata nello storico configurazioni.

Alla successiva sincronizzazione, l'agent riceverà la nuova configurazione (**Sent time**) e comunicherà l'avvenuta installazione (**Activated**). Da quel momento eventuali modifiche saranno possibili solo salvando una nuova versione della configurazione.



NOTA: Se **Sent time** e **Activated** non sono ancora valorizzati, è possibile ancora modificare la configurazione corrente.

Per la descrizione dello storico delle configurazioni degli agent vedi "[Dati dello storico configurazioni di un agent](#)" a pagina45 .

Pagina dell'agent

Per gestire
gli agent:

- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent

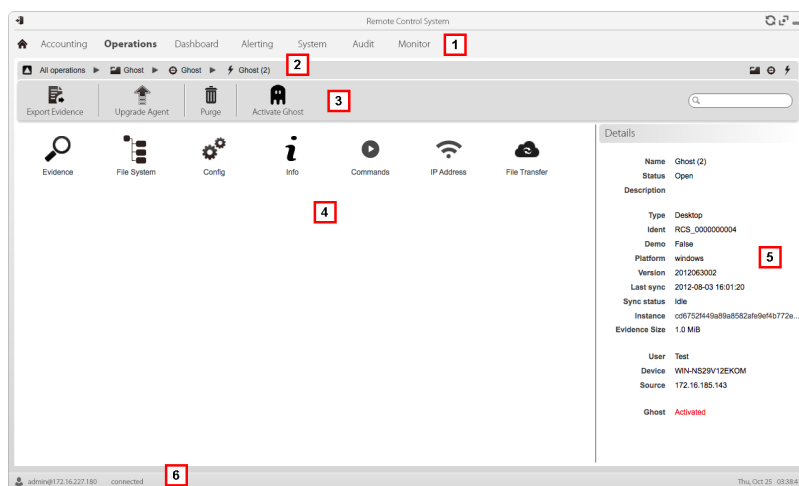
Scopo

Questa funzione permette di:

- verificare lo storico delle configurazioni dell'agent ed entrare nel dettaglio di ogni configurazione.
- trasferire file dal/al dispositivo del target
- importare/esportare le evidence dell'agent
- sostituire lo scout agent con il vero agent e aggiornare il software dell'agent
- visualizzare i comandi eseguiti dall'agent
- visualizzare gli indirizzi IP da cui l'agent ha contattato il Collector

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Barra di navigazione.

Area Descrizione

- 3** Barre con i pulsanti della finestra.
Di seguito la descrizione:

Icona Descrizione



Esporta le evidence dell'agent.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Evidence export**.



Invia allo scout agent l'agent vero e proprio, oppure aggiorna il software dell'agent con l'ultima versione ricevuta dall'assistenza HackingTeam.



PRUDENZA: l'aggiornamento non aggiorna la configurazione che viene trasmessa agli agent alla successiva sincronizzazione.



Elimina le evidence sul dispositivo non ancora trasferite a RCS.





Parametri:

- **Date before:** elimina le evidence registrate in data antecedente a quella impostata.
- **Size bigger than:** elimina le evidence con dimensione maggiore di quella impostata.

Area Descrizione

4 Azioni possibili sull'agent. Di seguito la descrizione:

Icona Descrizione

- 
 Mostra il risultato dei comandi lanciati sul dispositivo tramite azioni **Execute**.
- 
 Mostra lo storico sincronizzazioni dell'agent. Vedi "[Dati dello storico sincronizzazioni dell'agent](#)" alla pagina successiva .
- 
 Mostra lo storico delle configurazioni dell'agent, permettendo di modificare la configurazione attuale o una precedente e salvarla come nuova. Vedi "[Dati dello storico configurazioni di un agent](#)" nel seguito .
- 
 Apre la funzione per caricare o scaricare file dal dispositivo del target. Vedi "[Trasferimento file da/a il target](#)" alla pagina successiva

5 Dettagli dell'agent.

6 Barra di stato di RCS.

Per saperne di più


Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per saperne di più sugli agent vedi "[Cose da sapere sugli agent](#)" a pagina40 .

Dati dello storico configurazioni di un agent

Di seguito la descrizione:

Campo	Descrizione
Description	Descrizione libera della configurazione.
User	Nome utente che ha creato la configurazione.
Saved	Data salvataggio della configurazione.

<i>Campo</i>	<i>Descrizione</i>
Sent time	Data spedizione della configurazione tramite sincronizzazione.  AVVERTENZA: se questo valore è nullo, l'agent non ha ancora ricevuto la configurazione.
Activated	Data installazione nuova configurazione nell'agent.

Dati dello storico eventi di un agent

Di seguito la descrizione:

<i>Campo</i>	<i>Descrizione</i>
Acquired	Data-ora dell'evento acquisito sul dispositivo. È possibile filtrare. Last 24 hours è l'impostazione predefinita.
Received	Data-ora dell'evento registrato in RCS. È possibile filtrare. Last 24 hours è l'impostazione predefinita.
Content	Informazione di stato inviata dall'agent.

Dati dello storico sincronizzazioni dell'agent

Di seguito la descrizione:

<i>Campo</i>	<i>Descrizione</i>
Acquired	Data-ora della sincronizzazione. È possibile filtrare. Last 24 hours è l'impostazione predefinita.
IP	Indirizzo IP da cui è stata fatta la sincronizzazione.
Address	Luogo da cui si è stabilita la connessione.

Trasferimento file da/a il target

Per trasferire file da/a l'agent:

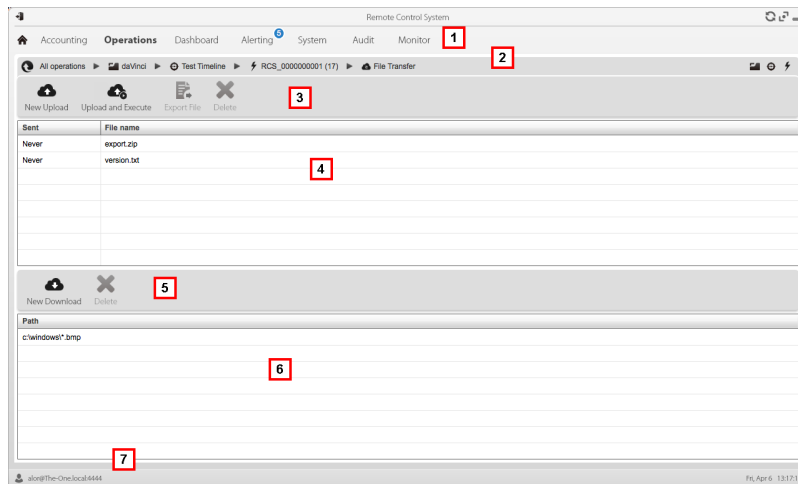
- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, doppio clic su **File Transfer**

Scopo

Caricare e scaricare file sul dispositivo dove è installato l'agent.

Come si presenta la funzione






Ecco come viene visualizzata la funzione di trasferimento file da/a il target:



Area Descrizione

- 1 Menu di RCS.
- 2 Barra di navigazione per l'operation. Di seguito la descrizione:

Icona Descrizione

-  Mostra l'elenco delle operation.
-  Mostra la pagina dell'operation.
-  Mostra la pagina del target.
-  Mostra la pagina della factory.
-  Mostra la pagina dell'agent.

Area Descrizione

- 3 Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona Descrizione



Carica un file nella cartella del dispositivo dove è installato l'agent. Ogni caricamento avvenuto viene registrato nello storico con data-ora e il nome del file.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Upload files to agent**.



Carica un file eseguibile nella cartella del dispositivo dove è installato l'agent e lo esegue (tramite comando **Execute**). Il risultato dell'esecuzione compare nella pagina **Commands**. Vedi "[Pagina dei comandi](#)" nella pagina di fronte .

Ogni caricamento avvenuto viene registrato nello storico con data-ora e il nome del file.



IMPORTANTE: questa funzione può essere inibita se l'utente è privo dei relativi permessi o se la licenza d'uso non la permette.



Esporta lo storico dei caricamenti.



Elimina il caricamento selezionato. Eventuali risultati del comando eliminato vengono mantenuti.

- 4 Storico dei caricamenti, con i pulsanti dei comandi.

- 5 Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona Descrizione



Scarica un file dal dispositivo. È necessario indicare il percorso incluso di nome file. Ogni scaricamento avvenuto viene registrato nello storico con il nome del file completo di percorso.

Il file viene salvato nella cartella RCS Download sul desktop.



Elimina dalla cartella RCS Download il file selezionato.

- 6 Storico degli scaricamenti, con i pulsanti dei comandi.

Area Descrizione

7 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per la descrizione dei dati degli agent vedi "[Pagina dell'agent](#)" a pagina42 .

Pagina dei comandi

Per gestire
i risultati dei
comandi:

- sezione **Operations**, doppio-clc su una operation, doppio-clc su un target, doppio-clc su un agent, doppio-clc su **Commands**

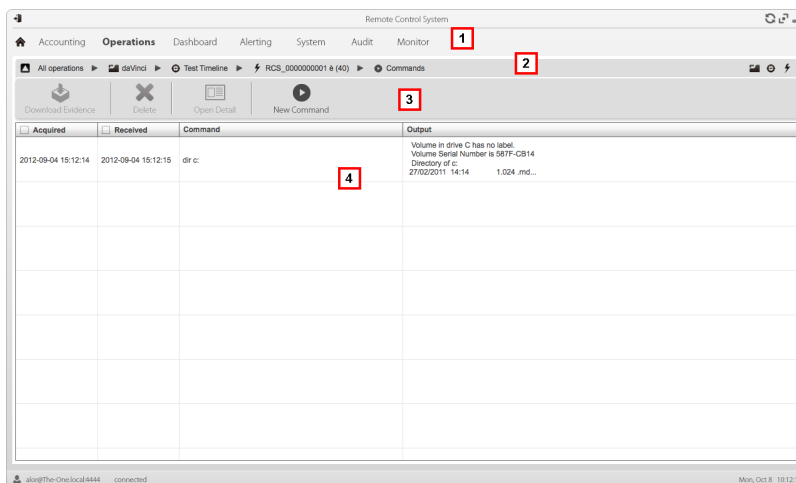
Scopo

Questa funzione permette di:

- verificare i risultati dei comandi eseguiti dall'azione **Execute** configurata sull'agent
- verificare i risultati del file eseguibile attivato durante il trasferimento di file da/a l'agent
- lanciare uno o più comandi estemporanei a un agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Barra di navigazione.
- 3 Barre con i pulsanti della finestra.
Di seguito la descrizione:

Icona Descrizione

Esporta in un file .txt il comando selezionato.



Elimina i comandi selezionati.



Mostra il dettaglio del comando selezionato.



Apri una finestra per l'inserimento di una o più stringhe di comando. Alla successiva sincronizzazione tutti i comandi vengono inviati all'agent e il risultato viene visualizzato alla successiva ricezione.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Command execution on agents**.

- 5 Elenco dei comandi in base ai filtri impostati.
- 6 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina 15 .

Factory e agent: configurazione base

Presentazione

Introduzione

La configurazione base permette di inserire moduli di acquisizione dati o di esecuzione comandi semplici, che non richiedono impostazioni complesse.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulla configurazione base	52
Configurazione base di una factory o di un agent	52
Dati della configurazione base	55

Cose da sapere sulla configurazione base

Configurazione base

La configurazione base di una factory/agent permette di abilitare e definire rapidamente l'acquisizione delle evidenze.

La configurazione base non prevede l'acquisizione di alcuni tipi di evidenze, né l'impostazione dettagliata delle modalità di acquisizione

Configurazione base di default:

- L'acquisizione delle informazioni di sistema all'accensione del dispositivo (non disabilitabile)
- Un modulo per l'esecuzione della sincronizzazione tra agent e RCS ad un certo intervallo.

Per l'elenco dei tipi di moduli presenti nella configurazione base vedi "[Dati della configurazione base](#)" a pagina 55.



PRUDENZA: se dalla configurazione avanzata si vuole tornare alla configurazione base, si perderanno tutte le impostazioni e si tornerà alla configurazione base di default.

Esportazione e importazione di configurazioni

L'esportazione/importazione di una configurazione base o avanzata serve a riutilizzare una configurazione su altri sistemi RCS.

La configurazione base o avanzata viene esportata in un file .json che può essere trasferito in un altro sistema e importato durante la creazione di un agent.

Salvataggio della configurazione come template

Il salvataggio come template di una configurazione base o avanzata serve a riutilizzare la configurazione da parte di utenti diversi dello stesso sistema RCS.

La configurazione base o avanzata viene salvata come template nel database, accompagnata da una descrizione e dal nome utente. Durante la creazione di un altro target può essere caricata da un altro utente e diventa quindi la configurazione di quell'agent.



IMPORTANTE: i template di configurazioni base e avanzate vengono salvati separatamente nel database. I template di configurazioni base compaiono quindi durante la creazione di un agent con configurazione base, i template di configurazioni advanced compaiono durante la creazione di un agent con configurazione avanzata.

Configurazione base di una factory o di un agent

Per configurare factory e agent:

- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su una factory
- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent

Scopo

Questa funzione permette di:

- configurare la factory/agent indicando se è richiesta la sincronizzazione online e quali dati si desidera acquisire
- aprire la funzione di compilazione della factory (vedi "[Compilazione di una factory](#)" a pagina 36).
- aprire la funzione di configurazione avanzata (vedi "[Configurazione avanzata di una factory o di un agent](#)" a pagina 61)



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Agent configuration**.

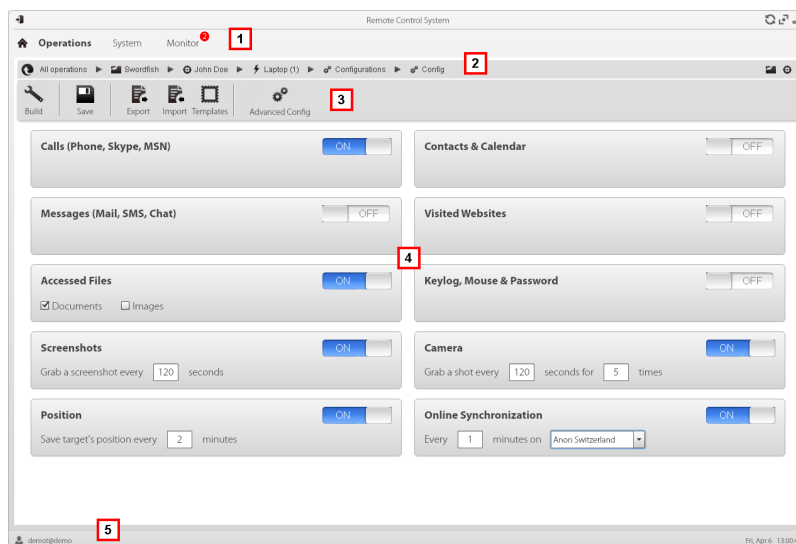
Passi successivi

Dopo aver configurato la factory è necessario compilarla per ottenere l'agent.

Dopo aver modificato la configurazione di un agent, è sufficiente salvarla. Se l'agent è online, alla successiva sincronizzazione sarà applicata la nuova configurazione. Altrimenti occorre procedere all'installazione fisica.

Come si presenta la funzione









Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Barra di navigazione.
- 3 Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona Descrizione

- | | |
|---|--|
|  | Compila la configurazione in uno o più agent da installare, in base ai vettori di installazione scelti. Vedi " Compilazione di una factory " a pagina36 |
|  | Salva la configurazione: la configurazione di un agent viene registrata nello storico e alla successiva sincronizzazione viene inviata all'agent.
Vedi " Dati dello storico configurazioni di un agent " a pagina45 |
|  | Esporta la configurazione in un file .json. |
|  | Importa la configurazione da un file .json. |
|  | Carica il template di una configurazione base o salva la configurazione attuale come template.
Vedi " Cose da sapere sulla configurazione base " a pagina52 . |
|  | Apri la finestra della configurazione avanzata. Vedi " Configurazione avanzata di una factory o di un agent " a pagina61 . |
|  | PRUDENZA: se dalla configurazione avanzata si vuole tornare alla configurazione base, si perderanno tutte le impostazioni e si tornerà alla configurazione base. |
- 4 Elenco dei tipi di acquisizione disponibili e relativo stato di attivazione.
 NOTA: l'elenco dei moduli varia in base al tipo di dispositivo.
 - 5 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per saperne di più sulla configurazione base vedi "[Cose da sapere sulla configurazione base](#)" a pagina52 .

Per la descrizione dei dati presenti sulla finestra vedi "[Dati della configurazione base](#)" nel seguito .
Per l'elenco dei moduli disponibili nelle due configurazioni vedi "[Elenco dei moduli](#)" a pagina122

Configurare una factory o un agent

Per attivare o disattivare la raccolta delle evidence:

Passo Azione

- 1 • Fare clic su **OFF** in corrispondenza dell'evidence da acquisire: il pulsante diventa **ON** e le opzioni di configurazione, dove disponibili, possono essere impostate.
- 2 • In **Online Synchronization** lasciare **ON** se il dispositivo target avrà accesso a Internet. Questo permette di impostare le opzioni gradualmente. Lasciare **OFF** se il dispositivo target non avrà accesso a Internet o se si desidera acquisire manualmente le evidence dal target.
 - Fare clic su **Salva** per salvare la configurazione corrente.
- 3 Proseguire in modo diverso:

<i>Se si sta configurando...</i>	<i>Allora...</i>
----------------------------------	------------------

una factory	fare clic su Build per compilarla e ottenere gli agent per diverse piattaforme. Vedi " Compilazione di una factory " a pagina36 .
--------------------	--

un agent	alla prossima sincronizzazione l'agent aggiorna automaticamente la propria configurazione.
-----------------	--

Dati della configurazione base

Di seguito i tipi di registrazioni attivabili nella configurazione base di una factory o di un agent.

<i>Registrazione</i>	<i>Descrizione</i>
Calls	Registra chiamate.
Messages	Registra messaggi.
Accessed files	(solo desktop) Registra documenti o immagini aperti dal target. Document, Images: tipi di file.
Screenshots	Registra la schermata attiva sul display del target. Grab a screenshot every: intervallo acquisizione immagine.

Registrazione	Descrizione
Position	Registra la posizione geografica del target. Save target position every: intervallo acquisizione posizione.
Contacts & Calendar	Registra i contatti e il calendario.
Visited websites	Registra l'indirizzo URL delle pagine web visitate.
Keylog	(solo mobile) Registra i tasti premuti sulla tastiera.
Keylog, Mouse & Password	(solo desktop) Registra i tasti premuti sulla tastiera, le password salvate sul sistema e i clic del mouse.
Camera	Registra le immagini della webcam. Grab a shot every: intervallo acquisizione immagine. for...times: ripetizioni dell'acquisizione.
Online Synchronization	Abilitata di default. Se abilitata, l'agent contatta il server per l'invio dei dati e la ricezione delle nuove configurazioni, aggiornamenti e così via. Every: intervallo di sincronizzazione minute on: nome o indirizzo IP dell'Anonymizer o del Collector. È possibile inserire manualmente il nome o indirizzo IP. La struttura delle catene è visibile nella sezione System , funzione Frontend . Vedi " Gestione dei frontend " a pagina67 . Se disabilitata indica che il dispositivo è sempre offline le evidenze saranno recuperate fisicamente e importate nel database. Vedi " Pagina del target " a pagina28

Factory e agent: configurazione avanzata

Presentazione

Introduzione

La configurazione avanzata permette di impostare opzioni avanzate di configurazione. Oltre ad abilitare la raccolta delle evidence, gli eventi possono essere collegati ad azioni, per attivare reazioni specifiche dell'agent e cambiare certe condizioni nel dispositivo (es.: avvio del salva schermo). Le azioni possono avviare o fermare moduli e abilitare o disabilitare altri eventi. Inoltre tutti gli eventi, azioni e le opzioni dei moduli possono essere impostati individualmente.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulla configurazione avanzata	58
Configurazione avanzata di una factory o di un agent	61
Dati globali dell'agent	65

Cose da sapere sulla configurazione avanzata

Configurazione avanzata

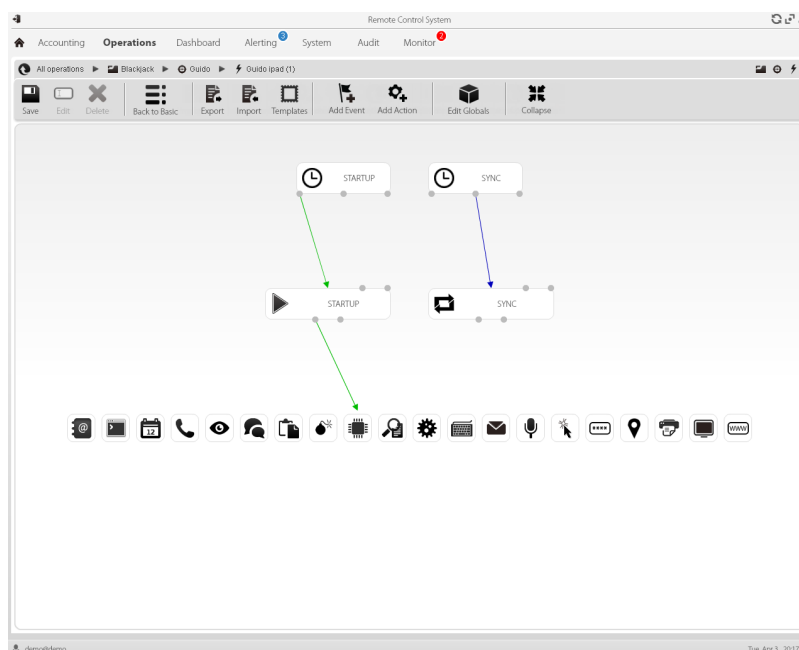
La configurazione avanzata di una factory/agent permette di creare delle sequenze complesse di attivazione tramite una semplice interfaccia grafica.

La sequenza avrà lo scopo di avviare/fermare le la raccolta delle evidence, e/o eseguire un'azione al verificarsi di un evento.

La configurazione avanzata include sempre due sequenze base:

- A ogni sincronizzazione (evento Loop) acquisisce le informazioni sul dispositivo (azione Start module + modulo Device)
- Allo scadere dell'intervallo di sincronizzazione (evento Timer-Loop) esegui la sincronizzazione tra agent e RCS (azione Synchronize)

Di seguito l'immagine che descrive le due sequenze base suggerite per l'acquisizione dati da remoto:



NOTA: queste due sequenze base sono impostate di default e sono suggerite per il minimo funzionamento dell'agent.

Componenti della configurazione avanzata

I componenti della configurazione avanzata sono:

- gli *eventi* che scatenano un'azione (es.: una chiamata ricevuta sul dispositivo)
- le *azioni* eseguite a fronte di un evento (es.: avvio della registrazione di una chiamata)
- le *sotto-azioni* eseguite a fronte di un evento (es.: invio di un SMS nascosto con la posizione del dispositivo)
- i *moduli* che a fronte dell'azione iniziano a raccogliere le prove desiderate o eseguono altre azioni sul dispositivo (es.: registrazione dell'audio della chiamata)
- le *sequenze*, ovvero l'insieme di eventi, azioni, sotto-azioni e moduli.



NOTA: alcuni eventi, azioni e moduli possono essere impostati solo nella configurazione avanzata.

Letture delle sequenze

Le sequenze complesse possono essere lette così:

- Alla connessione del dispositivo all'alimentazione (evento)...
- ...manda un SMS (sotto-azione) e...
- ...avvia la registrazione della posizione (azione verso modulo) e...
- ...disabilita l'evento scatenato al cambio della SIM (azione che disabilita un evento)
- ...e così via

Le possibili combinazioni tra eventi, azioni, sotto-azioni e moduli sono infinite. Di seguito la spiegazione dettagliata delle regole di progettazione corrette.

Eventi

Gli eventi vengono controllati dall'agent e possono avviare, ripetere o concludere un'azione.



NOTA: non è possibile avviare un modulo direttamente da un evento.

Per esempio un evento **Window** (apertura di una finestra sul dispositivo) può avviare un'azione. Sarà poi l'azione che avvierà/fermerà un modulo.

Sono disponibili diversi tipi di eventi. Per l'elenco completo *vedi "Elenco degli eventi" a pagina 112*.

La relazione tra un evento e una o più azioni è rappresentata da un connettore:

<i>Relazione tra evento e azione</i>	<i>Descrizione</i>	<i>Connettore</i>
Start	Avvia un'azione quando accade l'evento.	
Repeat	Ripete un'azione. È possibile specificare l'intervallo e il numero di ripetizioni.	
End	Avvia un'azione quando l'evento si conclude.	



NOTA: un evento può gestire fino a tre azioni distinte contemporaneamente. L'azione **Start** viene avviata quando l'evento accade sul dispositivo (es.: l'evento **Standby** scatena la **Start** quando il dispositivo entra in standby). L'azione **Repeat** viene scatenata all'intervallo definito per tutta la durata dell'evento. L'azione **Stop** viene avviata quando l'evento si conclude (es.: l'evento **StandBy** scatena la **End** quando il dispositivo esce dalla modalità di standby).

Azioni

Le azioni sono innescate dall'accadere di un evento. Possono:

- avviare o fermare un modulo
- abilitare e disabilitare un evento
- eseguire una sotto-azione

Per esempio un'azione (vuota) può disabilitare l'evento **Process** (avvio di un processo di sistema) che l'ha innescata e abilitare il modulo **Position** (registra posizione GPS). Se necessario l'azione può anche eseguire una sotto-azione **SMS** (invio messaggio a un numero telefonico specificato).

Sono disponibili diverse *sotto-azioni* che possono essere combinate tra loro senza limitazioni (es.: eseguire un comando + creare un messaggio di Alert). Per l'elenco completo vedi "[Elenco delle sotto-azioni](#)" a pagina 105

Relazioni tra azioni e moduli

Un'azione può agire su un modulo in modi diversi. La relazione tra un'azione e uno e più moduli è rappresentata da un connettore:

<i>Relazione tra azione e moduli</i>	<i>Descrizione</i>	<i>Connettore</i>
Start modules	Avvia un modulo.	
Stop modules	Ferma un modulo.	

Un'azione può avviare/fermare più moduli contemporaneamente.

Relazioni tra azioni e eventi

La relazione tra un'azione e uno e più eventi è rappresentata da un connettore:

<i>Relazione tra azione e eventi</i>	<i>Descrizione</i>	<i>Connettore</i>
Enable events	Abilita un evento.	
Disable events	Disabilita un evento.	



NOTA: un'azione può abilitare/disabilitare più eventi contemporaneamente.

Moduli

Ogni modulo abilita la raccolta di una specifica evidenza dal dispositivo del target. Possono essere avviati/fermati da un'azione e producono le evidenze.

Per esempio un modulo **Position** (registra posizione GPS) può essere avviato da un'azione innescata da un evento **Call** (è stata ricevuta/effettuata una chiamata).

Sono disponibili diversi moduli che possono essere avviati/fermati (es.: avvia modulo posizione + ferma modulo screenshot). Per l'elenco completo vedi "[Elenco dei moduli](#)" a pagina 122 .

Esportazione e importazione di configurazioni

L'esportazione/importazione di una configurazione base o avanzata serve a riutilizzare una configurazione su altri sistemi RCS.

La configurazione base o avanzata viene esportata in un file .json che può essere trasferito in un altro sistema e importato durante la creazione di un agent.

Salvataggio della configurazione come template

Il salvataggio come template di una configurazione base o avanzata serve a riutilizzare la configurazione da parte di utenti diversi dello stesso sistema RCS.

La configurazione base o avanzata viene salvata come template nel database, accompagnata da una descrizione e dal nome utente. Durante la creazione di un altro target può essere caricata da un altro utente e diventa quindi la configurazione di quell'agent.



IMPORTANTE: i template di configurazioni base e avanzate vengono salvati separatamente nel database. I template di configurazioni base compaiono quindi durante la creazione di un agent con configurazione base, i template di configurazioni advanced compaiono durante la creazione di un agent con configurazione avanzata.

Configurazione avanzata di una factory o di un agent

Per aprire la configurazione avanzata:

- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio clic sulla factory, fare clic su **Advanced config**
- sezione **Operations**, doppio-clic su una operation, doppio-clic su un target, doppio clic sull'agent, fare clic su **Advanced config**

Scopo

Questa funzione permette di:

- creare sequenze di attivazione dei moduli scatenate da eventi che si verificano sul dispositivo del target. Ogni sequenza può essere composta di una o più sotto-azioni.
- Impostare i parametri generali di una factory/agent.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Agent configuration**.



PRUDENZA: se dalla configurazione avanzata si vuole tornare alla configurazione base, si perderanno tutte le impostazioni e si tornerà alla configurazione base di default.

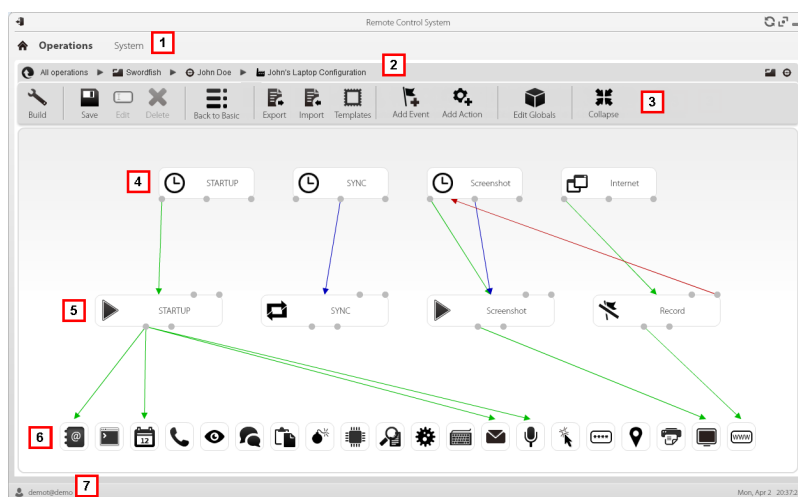
Passi successivi

Per una factory, terminare la sua configurazione e compilarla per ottenere l'agent da installare. Vedi "[Compilazione di una factory](#)" a pagina 36

Per un agent, terminare la sua configurazione e salvarla. Alla successiva sincronizzazione la nuova configurazione sarà inviata all'agent.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione


- 1 Menu di RCS.
- 2 Barra di navigazione.


Area Descrizione


3 Barre con i pulsanti della finestra. Di seguito la descrizione:


Icona Descrizione


 Compila la configurazione in uno o più agent, in base ai vettori di installazione scelti. Vedi "[Compilazione di una factory](#)" a pagina36


 Salva la configurazione corrente.


 Modifica l'evento o l'azione selezionati.


 Elimina l'evento, l'azione o la connessione logica selezionati.


 **PRUDENZA: torna alla configurazione di base perdendo tutte le impostazioni.**


 Esporta la configurazione in un file .json.


 Importa la configurazione da un file .json.

 Carica il template di una configurazione avanzata o salva la configurazione attuale come template.
Vedi "[Cose da sapere sulla configurazione avanzata](#)" a pagina58 .

 Inserisce un evento.

 Inserisce un'azione.

 Modifica i dati globali dell'agent vedi "[Dati globali dell'agent](#)" a pagina65 .

 Comprime o espande i widget degli eventi e delle azioni per permettere una migliore visione della configurazione corrente.



4 Area degli eventi. Gli eventi **STARTUP** e **SYNC** sono abilitati di default.

5 Area delle azioni. Le azioni **STARTUP** e **SYNC** sono abilitate di default.

6 Area dei moduli di registrazione. I moduli cambiano in base al dispositivo desktop o mobile.

7 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per saperne di più sulla configurazione avanzata vedi "[Cose da sapere sulla configurazione avanzata](#)" a pagina58 .

Creare una sequenza di attivazione semplice

Per creare una sequenza semplice, ovvero acquisire prove all'accadere di un evento:

Passo Azione

- 1 Creare un evento:
 - Fare clic su **Add Event**: compare la finestra di selezione e impostazione evento.
 - In **Type** selezionare il tipo di evento e impostarne le opzioni. Vedi "[Elenco degli eventi](#)" a pagina112
 - Fare clic su **Save**: il nuovo evento viene aggiunto all'area di lavoro

- 2 Creare un'azione:
 - Fare clic su **Add Action**: l'azione vuota viene aggiunta all'area di lavoro

- 3 Collegare l'evento all'azione, poi collegare l'azione al modulo desiderato:
 - Fare clic sul punto di connessione **Start** dell'evento e trascinare la freccia sull'azione
 - Fare clic sul punto di connessione **Start modules** dell'azione e trascinare la freccia sui tipi di dati che si vogliono acquisire. Vedi "[Elenco dei moduli](#)" a pagina122 .

- 4 Fare clic su **Salva**: la configurazione è pronta per essere compilata (se factory) o trasmessa al dispositivo alla prossima sincronizzazione (se agent).

Creare una sequenza di attivazione complessa

Per creare una sequenza complessa, ovvero all'accadere di un evento raccogliere le evidenze, eseguire una sotto-azione ed eventualmente abilitare/disabilitare un evento:

Passo Azione

- 1 Creare un evento:
 - Fare clic su **Add Event**: compare la finestra di selezione e impostazione evento.
 - In **Type** selezionare il tipo di evento e impostarne le opzioni. Vedi "[Elenco degli eventi](#)" a pagina112
 - Fare clic su **Save**: il nuovo evento viene aggiunto all'area di lavoro
- 2 Creare un'azione e definire le sotto-azioni:
 - Fare clic su **Add Action**: l'azione vuota viene aggiunta all'area di lavoro
 - Fare doppio clic sull'azione e in **Subaction** aggiungere le sotto-azioni desiderate e impostarne le opzioni. Vedi "[Elenco delle sotto-azioni](#)" a pagina105 .
- 3 Collegare l'evento all'azione:
 - Fare clic su uno dei punti di connessione **Start, Repeat, End** dell'evento e trascinare la freccia sull'azione
- 4 Collegare l'azione al modulo:
 - Fare clic sui punti di connessione **Start modules , Stop modules** dell'azione e trascinare la freccia sul modulo da avviare o fermare. Vedi "[Elenco dei moduli](#)" a pagina122 .



Suggerimento: Trascinare più frecce se più moduli devono essere abilitati.




Se si tratta di un'azione che richiede l'abilitazione/disabilitazione di un evento:

- Fare clic sul punto di connessione **Enable events o Disable events** dell'azione e trascinare la freccia sugli eventi da abilitare/disabilitare.
- 5 Fare clic su **Salva**: la configurazione è pronta per essere compilata (se factory) o trasmessa al dispositivo alla prossima sincronizzazione (se agent).

Dati globali dell'agent

I dati globali dell'agent sono descritti di seguito:

<i>Campo</i>	<i>Descrizione</i>
Minimum disk free	Quantità minima spazio disco libero sul dispositivo.

Campo	Descrizione
Maximum evidence size	<p>Quantità massima spazio occupato dalle evidenze sul dispositivo del target, fino alla successiva sincronizzazione. Il default è 1 GB.</p> <p>Al raggiungimento di questo limite, l'agent termina la registrazione in attesa della successiva sincronizzazione. Se la sincronizzazione non avviene, non vengono acquisite ulteriori evidenze.</p>
Wipe	<p>Se abilitato, cancella in modo sicuro i file generati dall'agent. Nessuna traccia dell'agent sarà rilevabile in caso di un'analisi forense.</p> <p> NOTA: questa modalità richiede un tempo maggiore rispetto alla normale eliminazione del file.</p>
Remove driver	<p>Rimuove il driver alla disinstallazione.</p>
No hide	<p> Richiede assistenza: utilizzare solo su richiesta dell'assistenza tecnica HackingTeam.</p>
Mask	<p> Richiede assistenza: utilizzare solo su richiesta dell'assistenza tecnica HackingTeam.</p>

Gestione dei frontend

Per gestire i frontend:

- sezione System, Frontend

Scopo della funzione

Durante il funzionamento di RCS, questa funzione permette di verificare lo stato di Anonymizer e Collector, modificare la configurazione degli Anonymizer e delle catene e aggiornare i VPS.

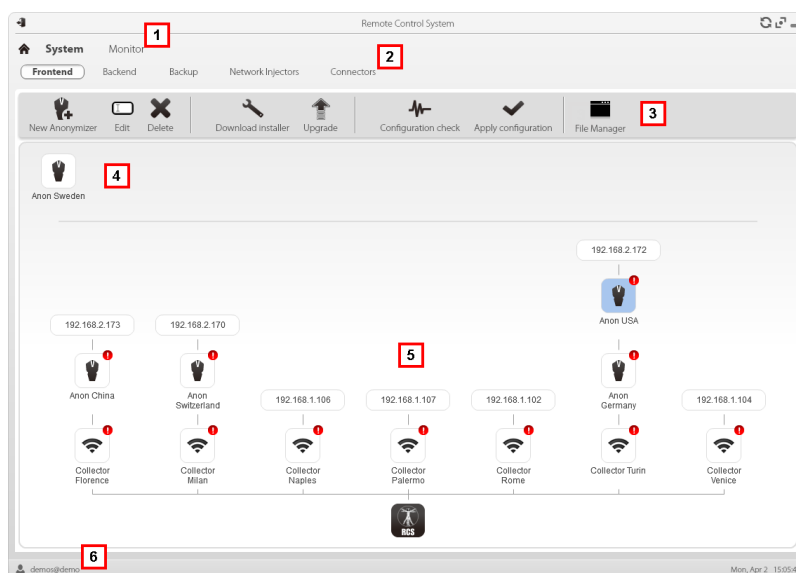
In fase di installazione, questa funzione permette di creare un nuovo "oggetto" Anonymizer che funziona da collegamento logico tra RCS Console e la singola componente software da installare su un VPS.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Frontend management**.

Come si presenta la funzione







Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Menu **System**.

Area Descrizione

- 3 Barre con i pulsanti della finestra.
- 4 Anonymizer configurati non ancora inclusi in una catena.
- 5 Catene di Anonymizer sul sistema con l'indirizzo IP dell'ultimo elemento.
Possibili stati:
 -  : Anonymizer non in catena.
 -  : Anonymizer in catena e funzionante.
 -  : Anonymizer non monitorato da Network Controller.
 -  : Anonymizer con malfunzionamenti.
 -  : Collector in funzione.
 -  : Collector non funzionante.
- 6 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

I Network Injector

Presentazione

Introduzione

Network Injector permette di intercettare le connessioni HTTP del target e fare injection di un agent sul dispositivo.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere su Network Injector e le sue regole	70
Gestione dei Network Injector	71
Dati delle regole di injection	74
Cose da sapere su Appliance Control Center	79
Appliance Control Center	80
Dati del Appliance Control Center	84
Cose da sapere su Tactical Control Center	84
Tactical Control Center	89
Dati del Tactical Control Center	101

Cose da sapere su Network Injector e le sue regole

Introduzione

Network Injector controlla tutte le connessioni HTTP e seguendo le regole di injection individua le connessioni del target e inserisce l'agent all'interno delle connessioni, agganciandolo a delle risorse che il target sta scaricando da internet.

Tipi di risorse infettabili

Le risorse infettabili da RCS sono file di qualsiasi tipo.



NOTA: Network Injector non è in grado di monitorare connessioni FTP o HTTPS.

Come creare una regola

Per creare la regola occorre:

1. definire il metodo per identificare le connessioni del target. Per esempio, confrontando l'indirizzo IP o MAC del target. Oppure lasciar selezionare il dispositivo all'operatore del Tactical Network Injector.
2. definire il metodo per infettare il target. Per esempio attraverso la sostituzione di un file che il target sta scaricando dalla rete oppure attraverso l'infezione di una pagina web che il target visita abitualmente.

Cosa succede quando si abilita/disabilita una regola

Abilitare una regola vuol dire renderla disponibile per il processo di infezione da parte di Network Injector. RCS regolarmente comunica con i Network Injector per trasmettere le regole e acquisire i log. Nel caso del Tactical Network Injector è l'operatore che deve abilitare tale sincronizzazione.

Una regola non abilitata non è applicabile, ovvero non può essere inviata ai Network Injector.

Regole identificazione automatica e da operatore

Se si conoscono già informazioni relative ai dispositivi target, è possibile creare numerose regole adattandole alle diverse abitudini del target, per poi abilitare la o le regole più efficaci a seconda dell'opportunità che si crea in un determinato momento dell'investigazione.

Se invece non si conosce nulla dei dispositivi target, occorre utilizzare il Tactical Network Injector che con la sua presenza sul campo permette agli operatori di osservare il target, identificare il dispositivo che sta usando e infettarlo.

Per questo tipo di gestione manuale è necessario specificare **TACTICAL** nel campo **User patterns** .

Avvio dell'infezione

Dopo che Network Injector ha ricevuto le regole di infezione è pronto per iniziare un attacco.

Nella fase di sniffing controlla se tra i dispositivi presenti in rete qualcuno soddisfa le regole di identificazione. In caso affermativo invia l'agent al dispositivo identificato e lo infetta.

Gestione dei Network Injector

Per gestire i Network
Injector:

- sezione System, Network Injector

Scopo

Durante il funzionamento di RCS, questa funzione permette di creare le regole di monitoring e di injection e inviarle al Network Injector.



NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Injector management**.

Cosa è possibile fare

Con questa funzione è possibile:

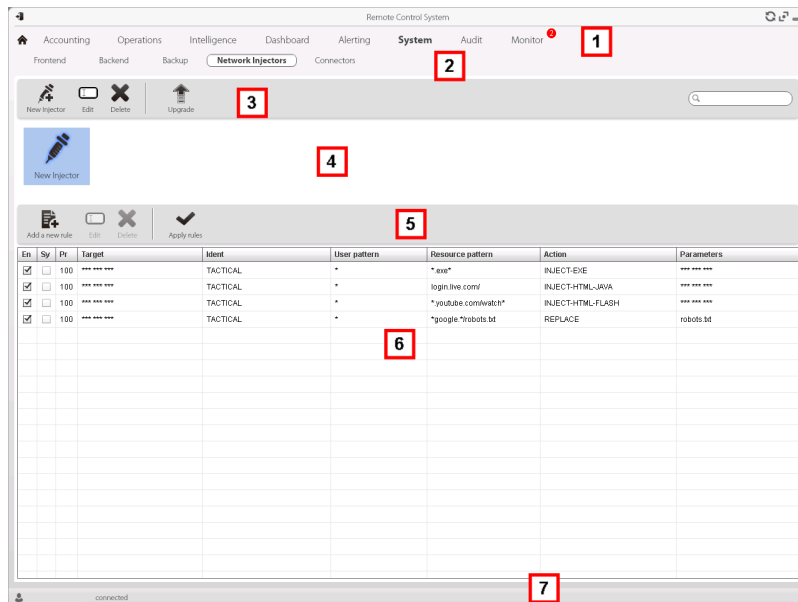
- creare una regola di injection di un agent su un target e applicare la regola sul Network Injector.



NOTA: per creare una regola di injection non è necessario installare un agent.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Menu di RCS.
- 2 Menu **System**.
- 3 Barra con i pulsanti dedicati ai Network Injector.
- 4 Elenco dei Network Injector.

Area Descrizione

- 5 Barra con i pulsanti dedicati alle regole di injection.



NOTA: le funzioni sono abilitate solo se si è in possesso dell'autorizzazione **Injector rules management**.

Di seguito la descrizione:

Azione Descrizione



Aggiunge una nuova regola.



Apri la finestra con i dati della regola.



Elimina la regola selezionata.



Aggiorna la configurazione del Network Injector selezionato. Se è presente una nuova versione del Tactical o Appliance Control Center, questa viene resa disponibile all'installazione. L'Appliance si aggiorna automaticamente alla successiva sincronizzazione, basta che ci sia un processo di infezione attivo. Mentre con il Tactical sarà l'operatore a scegliere se aggiornare l'applicativo.

- 6 Elenco delle regole del Network Injector selezionato.

En: selezionare per abilitare le regole da applicare.

- 7 Barra di stato di RCS. .

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "[Elementi e azioni comuni dell'interfaccia](#)" a pagina15 .

Per la descrizione dei dati delle regole di injection vedi "[Dati delle regole di injection](#)" alla pagina successiva .

Per saperne di più sulle regole di injection vedi "[Cose da sapere su Network Injector e le sue regole](#)" a pagina70 .

Aggiungere una nuova regola di injection e applicarla al target




Per aggiungere una nuova regola:

Passo Azione

- 1 Selezionare il Network Injector per il quale si desidera aggiungere la nuova regola.
- 2
 - Fare clic su **Add New Rule**: compaiono i dati da compilare.
 - Compilare i dati richiesti. Se la regola è abilitata è già possibile inviarla al Network Injector. Vedi "[Dati delle regole di injection](#)" nel seguito .
 - Fare clic su **Save**: nell'area di lavoro principale compare la nuova regola.
- 3 Abilitare le regole da attivare selezionando la casella di controllo **En** nella tabella.
- 4 Fare clic su **Apply rules**: RCS invia al Network Injector selezionato le regole. Un indicatore di stato mostra l'avanzamento dell'operazione.


Dati di un Network Injector

Di seguito la descrizione dei dati del Network Injector selezionato:

<i>Dato</i>	<i>Descrizione</i>
Name Description	Descrizioni libere.
Version	Versione software.
Address	Indirizzo IP dell'apparato.
Port	443.
Monitor via NC	Se abilitato, Network Controller acquisisce lo stato di Network Injector ogni 30 secondi. Se non abilitato, Network Injector continua le sue operazioni di sniffing e injection ma Network Controller non ne verifica lo stato. Usato quando non è possibile per qualsiasi ragione connettersi al Network Injector una volta installato presso l'ISP, o nel caso di utilizzo tattico.
Log	<p>Ultimi messaggi registrati nei log.</p> <p> NOTA: l'aggiornamento dei log del Tactical Network Injector dipendono dalla frequenza con cui l'operatore abilita la sincronizzazione.</p> <p> : aggiorna l'elenco.</p> <p> : elimina i log visualizzati.</p>

Dati delle regole di injection

Di seguito la descrizione dei dati che definiscono le regole di infezione disponibili:

Dato	Descrizione
Abilitato	Se selezionato, la regola sarà inviata al Network Injector. Se non selezionato, la regola viene salvata ma non inviata.
Disable on sync	Se selezionato, la regola viene disabilitata alla prima sincronizzazione dell'agent definito nella regola. Se non selezionato, Network Injector continua ad applicare la regola, anche dopo la prima sincronizzazione.
Probability	Probabilità (in percentuale) di applicazione delle regole dopo la prima risorsa infettata. 0%: dopo aver infettato la prima risorsa, Network Injector non applica più questa regola. 100%: dopo aver infettato la prima risorsa, Network Injector continua ad applicare questa regola.  Suggerimento: se si applica un valore superiore al 50%, si consiglia di utilizzare l'opzione Disable on sync .
Target	Nome del target da infettare.

<i>Dato</i>	<i>Descrizione</i>
-------------	--------------------

Ident	Metodo di identificazione delle connessioni HTTP del target.
--------------	--









NOTA: Network Injector non può monitorare connessioni FTP o HTTPS.







Di seguito la descrizione di ogni metodo:

<i>Dato</i>	<i>Descrizione</i>
-------------	--------------------

STATIC-IP	IP statico assegnato al target.
STATIC-RANGE	Range di indirizzi IP assegnati al target.
STATIC-MAC	Indirizzo MAC statico del target, sia Ethernet che WiFi.
DHCP	Indirizzo MAC dell'interfaccia di rete del target.
RADIUS-LOGIN	Nome utente RADIUS. User-Name (RADIUS 802.1x).
RADIUS-CALLID	Identificativo del chiamante RADIUS. Calling-Station-Id (RADIUS 802.1x).
RADIUS-SESSID	Identificativo sessione RADIUS. Acct-Session-Id (RADIUS 802.1x).
RADIUS-TECHKEY	Chiave RADIUS. NAS-IP-Address: Acct-Session-Id (RADIUS 802.1x).
STRING-CLIENT	Stringa di testo da individuare nel traffico dati proveniente dal target.
STRING-SERVER	Stringa di testo da individuare nel traffico dati destinato al target.
TACTICAL	Il target non viene identificato automaticamente, ma si demanda la sua identificazione all'intervento dell'operatore sul Tactical Network Injector. Quindi è solo quando l'operatore identifica il dispositivo, che il campo Ident viene "personalizzato" con i dati ricevuti dal dispositivo stesso.

<i>Dato</i>	<i>Descrizione</i>																								
User pattern	Metodo di identificazione del traffico del target. Il formato dipende dal tipo di Ident selezionato.																								
	<table border="1"> <thead> <tr> <th><i>Metodo</i></th> <th><i>Formattazione</i></th> </tr> </thead> <tbody> <tr> <td>DHCP</td> <td>Indirizzo corrispondente (es.: "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>Range di indirizzi separati da '-' (es.: "195.162.21.2-195.162.21.5").</td> </tr> <tr> <td>STRING-CLIENT</td> <td>Stringa di testo (es.: "John@gmail.com").</td> </tr> <tr> <td>STRING-SERVER</td> <td></td> </tr> <tr> <td>RADIUS-CALLID</td> <td>ID o parte dell'ID.</td> </tr> <tr> <td>RADIUS-LOGIN</td> <td>Nome o parte del nome dell'utente.</td> </tr> <tr> <td>RADIUS-SESSID</td> <td>ID o parte dell'ID.</td> </tr> <tr> <td>RADIUS-TECHKEY</td> <td>Chiave o parte della chiave (es.: "*.10.*").</td> </tr> <tr> <td>TACTICAL</td> <td>Non è possibile impostare un valore. Il valore corretto sarà definito dall'operatore sul campo.</td> </tr> </tbody> </table>	<i>Metodo</i>	<i>Formattazione</i>	DHCP	Indirizzo corrispondente (es.: "195.162.21.2").	STATIC-IP		STATIC-MAC		STATIC-RANGE	Range di indirizzi separati da '-' (es.: "195.162.21.2-195.162.21.5").	STRING-CLIENT	Stringa di testo (es.: "John@gmail.com").	STRING-SERVER		RADIUS-CALLID	ID o parte dell'ID.	RADIUS-LOGIN	Nome o parte del nome dell'utente.	RADIUS-SESSID	ID o parte dell'ID.	RADIUS-TECHKEY	Chiave o parte della chiave (es.: "*.10.*").	TACTICAL	Non è possibile impostare un valore. Il valore corretto sarà definito dall'operatore sul campo.
<i>Metodo</i>	<i>Formattazione</i>																								
DHCP	Indirizzo corrispondente (es.: "195.162.21.2").																								
STATIC-IP																									
STATIC-MAC																									
STATIC-RANGE	Range di indirizzi separati da '-' (es.: "195.162.21.2-195.162.21.5").																								
STRING-CLIENT	Stringa di testo (es.: "John@gmail.com").																								
STRING-SERVER																									
RADIUS-CALLID	ID o parte dell'ID.																								
RADIUS-LOGIN	Nome o parte del nome dell'utente.																								
RADIUS-SESSID	ID o parte dell'ID.																								
RADIUS-TECHKEY	Chiave o parte della chiave (es.: "*.10.*").																								
TACTICAL	Non è possibile impostare un valore. Il valore corretto sarà definito dall'operatore sul campo.																								

<i>Dato</i>	<i>Descrizione</i>
Resource pattern	<p>Metodo di identificazione della risorsa da infettare, applicato all'URL della risorsa Web. Il formato dipende dal tipo di Action selezionata.</p> <p> NOTA: lasciare vuoto se l'azione selezionata è INJECT-UPGRADE.</p>
Tipo azione	Contenuto di Pattern risorsa
INJECT-EXE	<p>URL del file eseguibile da infettare. Utilizzare le wildcard per aumentare il numero di URL corrispondenti.</p> <p>Esempi di formati possibili:</p> <pre>*<nomeExe>*.exe</pre> <pre>www.mozilla.org/firefox/download/firefoxsetup.exe</pre> <p> NOTA: quando si specifica un path completo, fare attenzione agli eventuali mirror utilizzati dai siti web per lo scaricamento dei file (es.: "firefox.exe?mirror=it").</p> <p> Suggerimento: digitare *.exe* per infettare tutti gli eseguibili, indipendentemente dalla URL.</p> <p> IMPORTANTE: se si digita per esempio: *exe*, senza il carattere '.' dell'estensione del file, saranno infettate tutte le pagine che contengono accidentalmente le lettere "exe".</p>
INJECT-HTML-FILE	<p>URL della pagina web da infettare.</p> <p>Esempi di formati possibili:</p> <pre>www.oracle.com/</pre> <pre>www.oracle.com/index.html</pre> <p> NOTA: se non si specifica una pagina HTML o dinamica, includere nell'indirizzo del sito il carattere '/' finale (es.: "www.oracle.com/").</p> <p> NOTA: non è possibile infettare una pagina di redirect. Verificare sul browser il path corretto del sito web prima di indicarlo nella regola.</p>
INJECT-HTML-FLASH	Preconfigurato per Youtube e non modificabile dall'utente.
INJECT-UPGRADE	Non utilizzato.
REPLACE	URL della risorsa da sostituire.

<i>Dato</i>	<i>Descrizione</i>												
Action	Metodo di infezione che verrà applicato sulla risorsa indicata in Resource pattern :												
	<table border="1"> <thead> <tr> <th><i>Metodo</i></th> <th><i>Funzione</i></th> </tr> </thead> <tbody> <tr> <td>INJECT-EXE</td> <td>Infetta in tempo reale il file EXE scaricato. L'installazione dell'agent avviene nel momento in cui il target esegue il file EXE.</td> </tr> <tr> <td>INJECT-HTML-FILE</td> <td>Permette di aggiungere il codice HTML fornito nel file all'interno della pagina web visitata.  Richiede assistenza: contattare i tecnici HackingTeam per ulteriori dettagli.</td> </tr> <tr> <td>INJECT-HTML-FLASH</td> <td>Blocca i video su youtube e richiede all'utente di installare un finto aggiornamento di Flash per visualizzarli. L'agent viene installato quando il target installa l'aggiornamento.</td> </tr> <tr> <td>INJECT-UPGRADE</td> <td>Notifica il Java Runtime Environment sul dispositivo che un aggiornamento è disponibile. L'agent si installa nel momento in cui il target esegue l'aggiornamento. Non fa riferimento a Resource pattern.</td> </tr> <tr> <td>REPLACE</td> <td>Sostituisce la risorsa definita in Resource pattern con il file fornito.  Suggestione: questo tipo di azione è molto efficace se usata in combinazione con i documenti generati da Exploit.</td> </tr> </tbody> </table>	<i>Metodo</i>	<i>Funzione</i>	INJECT-EXE	Infetta in tempo reale il file EXE scaricato. L'installazione dell'agent avviene nel momento in cui il target esegue il file EXE.	INJECT-HTML-FILE	Permette di aggiungere il codice HTML fornito nel file all'interno della pagina web visitata.  Richiede assistenza: contattare i tecnici HackingTeam per ulteriori dettagli.	INJECT-HTML-FLASH	Blocca i video su youtube e richiede all'utente di installare un finto aggiornamento di Flash per visualizzarli. L'agent viene installato quando il target installa l'aggiornamento.	INJECT-UPGRADE	Notifica il Java Runtime Environment sul dispositivo che un aggiornamento è disponibile. L'agent si installa nel momento in cui il target esegue l'aggiornamento. Non fa riferimento a Resource pattern .	REPLACE	Sostituisce la risorsa definita in Resource pattern con il file fornito.  Suggestione: questo tipo di azione è molto efficace se usata in combinazione con i documenti generati da Exploit.
<i>Metodo</i>	<i>Funzione</i>												
INJECT-EXE	Infetta in tempo reale il file EXE scaricato. L'installazione dell'agent avviene nel momento in cui il target esegue il file EXE.												
INJECT-HTML-FILE	Permette di aggiungere il codice HTML fornito nel file all'interno della pagina web visitata.  Richiede assistenza: contattare i tecnici HackingTeam per ulteriori dettagli.												
INJECT-HTML-FLASH	Blocca i video su youtube e richiede all'utente di installare un finto aggiornamento di Flash per visualizzarli. L'agent viene installato quando il target installa l'aggiornamento.												
INJECT-UPGRADE	Notifica il Java Runtime Environment sul dispositivo che un aggiornamento è disponibile. L'agent si installa nel momento in cui il target esegue l'aggiornamento. Non fa riferimento a Resource pattern .												
REPLACE	Sostituisce la risorsa definita in Resource pattern con il file fornito.  Suggestione: questo tipo di azione è molto efficace se usata in combinazione con i documenti generati da Exploit.												
Agente	Per tutte le azioni tranne le REPLACE . Agent da iniettare nella risorsa Web selezionata.												
File	Solo per Action REPLACE . File da sostituire a quello indicato in Pattern risorsa .												

Cose da sapere su Appliance Control Center

Introduzione

Appliance Control Center è un applicativo installato sul Network Injector Appliance.

Sincronizzazione con RCS

Appliance Control Center si sincronizza a RCS per ricevere le regole di infezione aggiornate e per controllare se è disponibile una nuova versione del Appliance Control Center.

La sincronizzazione può avvenire in due modi:

- manualmente la prima volta per ricevere le regole di injection.
- automaticamente, anche con un'infezione in corso, per esempio per scaricare nuove regole di infezione.

Indirizzo IP dell'interfaccia di injection

Affiché l'infezione abbia successo, l'interfaccia di injection deve avere un indirizzo pubblico, altrimenti il target non riuscirà mai a vederla.

Con Appliance Control Center è possibile in una prima fase utilizzare l'indirizzo preimpostato sull'interfaccia (con **Public IP** = "auto"), attendere un eventuale messaggio che segnala che quell'indirizzo è privato e in quel caso impostare un indirizzo pubblico per il reindirizzamento dell'indirizzo privato (**Public IP** = "xxx.xxx.xxx.xxx").

Lo sniffing invece, può essere fatto tramite un'interfaccia di rete con indirizzo IP privato.

Appliance Control Center

Scopo

Appliance Control Center permette di infettare i dispositivi:

- **automaticamente**, tramite l'applicazione di regole di identificazione basate su informazioni già conosciute dei dispositivi (es.: indirizzo IP)

Cosa è possibile fare

Con il Appliance Control Center è possibile:

- aggiornare il dispositivo Appliance con l'ultima versione fornita da RCS Console
- abilitare la sincronizzazione con la sede operativa per la ricezione delle regole di injection e l'invio dei log.
- applicare le regole di identificazione dei dispositivi e infettarli

Richiesta della password

All'avvio Appliance Control Center chiede la password di accesso, la stessa del portatile su cui si sta lavorando.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Schede per l'accesso alle singole applicazioni. Di seguito la descrizione:

Funzione	Descrizione
Network injector	Gestisce lo sniffing e l'infezione dei dispositivi del target, sincronizza le regole RCS e aggiorna i dispositivi Appliance.
Log System	Elenca i log in tempo reale.

- 2 Area con i pulsanti per ricaricare l'elenco dei dispositivi, avviare le connessioni alla rete, abilitare la sincronizzazione, abilitare il riavvio automatico dopo il boot e abilitare l'aggiornamento del Network Appliance.

Per saperne di più

Per saperne di più sul Appliance Control Center vedi "[Cose da sapere su Appliance Control Center](#)" a pagina 79.

Per la descrizione dei dati del Appliance Control Center vedi "[Dati del Appliance Control Center](#)" a pagina 84

Procedure

Abilitazione sincronizzazione con RCS

Di seguito la procedura per la prima sincronizzazione con RCS (senza infezioni in corso):

Passi

1. Nella scheda **Network Injector** fare clic sul pulsante **Config**: la sincronizzazione viene abilitata e allo scadere del prossimo intervallo saranno ricevute le regole di injection previste, eventuali aggiornamenti del software e saranno spediti i log.



IMPORTANTE: abilitare regolarmente la sincronizzazione per garantire un aggiornamento costante dalla sede operativa e il successo delle infezioni.

2. Per interrompere la sincronizzazione fare clic su **Stop**.
3. Per visualizzare le regole ricevute da RCS Console fare clic su **Rules**: compaiono tutte le regole per il Network Injector



IMPORTANTE: controllare l'effettiva sincronizzazione delle regole dopo aver chiesto a RCS Console un loro aggiornamento.

Risultato

Rule	Probability	Attack	Resource
STRING-CLIENT test@example.com	100%	INJECT-HTML-JAVA	*
STATIC-IP 203.0.113.20	50%	INJECT-HTML-JAVA	*.com*

Infettare i target tramite identificazione automatica

Per avviare l'identificazione e infezione automatica:

Passi

1. Nella scheda **Network Injector** selezionare nella casella di riepilogo **Network Interface** l'interfaccia di rete per l'injection.
2. Nella casella di riepilogo **Sniffing interface** selezionare una diversa interfaccia di rete da usare per lo sniffing oppure scegliere la stessa interfaccia usata per l'injection.



Suggerimento: usare due interfacce di rete diverse garantisce una migliore identificazione dei dispositivi.



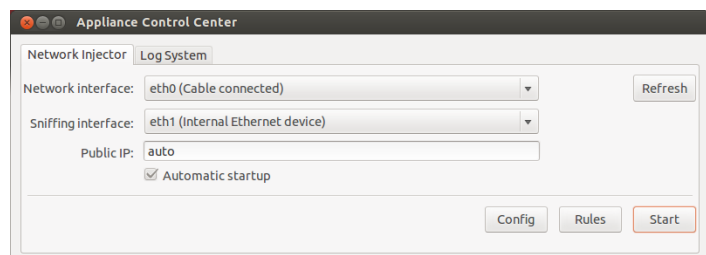
NOTA: le interfacce Endace (DAG), ovvero le interfacce di sniffing compaiono in **Sniffing Interface**.

3. Fare clic su **Automatic Startup** se si desidera che l'infezione riparta automaticamente senza alcun intervento umano anche in seguito di riavvii o spegnimento dell'Appliance Network Injector.
4. Fare clic su **Start**.



IMPORTANTE: Appliance Control Center permette di configurare, avviare l'infezione e chiudere lo stesso Appliance Control Center lasciando l'infezione in corso. Alla successiva riapertura con infezione in corso comparirà il pulsante **Stop** invece del pulsante **Start**. Questo permette di riconfigurare e far partire una nuova infezione.

5. Per fermare l'infezione fare clic su **Stop** oppure chiudere la finestra se si desidera lasciare attiva l'infezione.



Risultato**Visualizzare i dettagli dell'infezione**

Per visualizzare i dati registrati selezionare la scheda **Log System**.

Dati del Appliance Control Center

Dati scheda Network Injector

Di seguito la descrizione dei dati:

<i>Dato</i>	<i>Descrizione</i>
Network interface	Elenco delle interfacce di rete già connesse. Selezionare l'interfaccia di injection connessa alla rete dove è collegato il dispositivo da attaccare.
Sniffing interface	Come Network Interface oppure altra interfaccia di rete da utilizzare solo per lo sniffing.  NOTA: Se il sistema dispone di una scheda Endace DAG per connessioni Gigabit, la scheda sarà rilevata e visualizzata in questo elenco.
Public IP	Permette di specificare un indirizzo IP pubblico da mappare sull'indirizzo IP privato dell'interfaccia di injection. Se si inserisce "auto", il sistema utilizza l'indirizzo IP preconfigurato sull'interfaccia di injection e segnala con un messaggio se si tratta di un indirizzo IP privato.
Automatic Startup	Fa ripartire automaticamente l'infezione senza alcun intervento umano anche in seguito di riavvii o spegnimento dell'Appliance Network Injector.  IMPORTANTE: Se questa opzione non viene selezionata non ci sarà alcuna partenza automatica dell'infezione.

Cose da sapere su Tactical Control Center

Introduzione

Tactical Control Center è un applicativo installato su computer portatile, chiamato Tactical Network Injector.

Riesce a collegarsi a reti WiFi protette, infettare dispositivi grazie alle regole di identificazione e injection di RCS o infettare dispositivi identificati manualmente.

Le regole di identificazione e di infezione sono identiche a quelle usate per il Network Injector Appliance, con l'unica differenza che il Tactical Network Injector offre in più una regola di identificazione "manuale". È quindi l'operatore a riconoscere il dispositivo da infettare e dà il comando di applicare le regole di injection a quel dispositivo.

Funzionamento del Tactical Control Center

Con il Tactical Control Center è possibile:

- Abilitare la sincronizzazione con RCS per la ricezione delle regole di identificazione e di injection aggiornate.
- Scaricare l'aggiornamento di Tactical Control Center, fondamentale per aggiornare gli agent sui dispositivi.
- Infettare tramite identificazione automatica dei dispositivi presenti in una rete cablata o WiFi grazie alle regole di identificazione e injection di RCS.
- Infettare da operatore i dispositivi presenti in una rete cablata o WiFi tramite le regole di injection di RCS. L'identificazione è a carico dell'operatore.
- Connettersi a una rete WiFi protetta per ottenerne la password.
- Emulare un Access Point di una rete WiFi utilizzata normalmente dal target.



NOTA: la rete di injection può essere esterna oppure una rete WiFi aperta simulata dallo stesso Tactical Control Center.

Sincronizzazione con RCS

Tactical Control Center si sincronizza a RCS per ricevere le regole di infezione aggiornate e per controllare se è disponibile una nuova versione del Tactical Control Center.

La sincronizzazione può avvenire in due modi:

- manualmente la prima volta per ricevere le regole di injection.
- automaticamente, anche con un'infezione in corso, per esempio per scaricare nuove regole di infezione.

Aggiornamento delle regole di infezione

Se il traffico generato dal target non è infettabile con le regole attualmente presenti, è necessario richiedere l'intervento di un operatore sulla RCS Console per generare nuove regole e aggiornare il Network Injector. Alla successiva sincronizzazione Tactical Control Center riceve le nuove regole e sarà possibile visualizzarle.

Utilizzo delle interfacce di rete

In fase di attacco sono disponibili due diverse interfacce di rete, una per lo sniffing e una per l'injection. L'utilizzo di due interfacce separate è indicato per garantire una continuità soprattutto nello sniffing.

In fase di emulazione dell'Access Point e in fase di acquisizione della password di rete si lavora con la sola interfaccia di sniffing.

Le interfacce di sniffing possono essere interne o esterne: le interfacce esterne sono indicate per lo sniffing perché la velocità di trasmissione è migliore.

Processo di infezione tramite identificazione automatica

Di seguito i passaggi tipici per infettare dispositivi identificati automaticamente dalle regole di RCS. L'attacco può essere sferrato su reti cablate o WiFi:

Fase	Descrizione	Dove
1	Preparare le regole di identificazione e injection per i dispositivi target conosciuti che si vogliono attaccare. Inviare le regole al Tactical Network Injector.	<i>RCS Console, System, Network Injector</i>
2	Abilitare la sincronizzazione con RCS per ricevere le regole aggiornate.	<i>Tactical Network Injector, Network Injector</i>
3	Se i dispositivi target sono connessi a una rete WiFi protetta acquisirne la password.	<i>Tactical Network Injector, Wireless Intruder</i>
4	Il sistema fa lo sniffing del traffico, identifica i dispositivi target grazie alle regole di identificazione e li infetta grazie alle regole di injection.	<i>Tactical Network Injector, Network Injector</i>
5	Se necessario, forzare una riautenticazione di eventuali dispositivi che le regole non sono riuscite a individuare.	

Processo di infezione tramite identificazione manuale

Di seguito i passaggi tipici per infettare dispositivi identificati manualmente. L'obiettivo dell'operatore è individuare i dispositivi target.

L'attacco può essere sferrato su reti cablate o WiFi:

Fase	Descrizione	Dove
1	Preparare le regole di identificazione che prevedono l'intervento manuale e le regole di injection per tutti i tipi di dispositivi target che si vogliono attaccare. Inviare le regole al Tactical Network Injector.	<i>RCS Console, System, Network Injector</i>
2	Abilitare la sincronizzazione con RCS per ricevere le regole aggiornate.	<i>Tactical Network Injector, Network Injector</i>
3	Se i dispositivi target sono connessi a una rete WiFi protetta acquisirne la password.	<i>Tactical Network Injector, Wireless Intruder</i>

<i>Fase</i>	<i>Descrizione</i>	<i>Dove</i>
4	Se i dispositivi target possono connettersi a una rete WiFi aperta, provare a emulare un Access Point conosciuto dai target.	<i>Tactical Network Injector, Fake Access Point</i>
5	Il sistema propone tutti i dispositivi connessi all'interfaccia di rete selezionata. Utilizzare i filtri per cercare i dispositivi target oppure controllare la cronologia web di ogni dispositivo.	<i>Tactical Network Injector, Network Injector</i>
6	Selezionare i dispositivi e infettarli.	<i>Network Injector</i>

Abilitazione sincronizzazione con RCS

Il Tactical Control Center riceve da RCS la versione del software aggiornato, le regole di identificazione e di injection e contestualmente spedisce i propri log.

In questa comunicazione è RCS che a intervalli di tempo prestabiliti (circa 30 sec.) cerca di comunicare con il Tactical Network Injector. Dal Tactical Control Center, con la funzione **Network Injector** si può decidere quando abilitare la sincronizzazione e inviare l'aggiornamento del software.

Acquisizione password di rete WiFi protetta

Se il dispositivo target è collegato a una rete WiFi protetta occorre ottenerne la password di accesso per poter entrare.

La funzione **Wireless intruder** permette di collegarsi a una rete WiFi e fare il cracking della password. Per le reti con protezioni WPA e WPA 2, oltre al dizionario standard è possibile caricare un dizionario aggiuntivo. La password viene visualizzata e l'operatore la può copiare per utilizzarla con la funzione di sniffing e injection (funzione **Network Injector**).

Infezione tramite identificazione automatica

Questa modalità di lavoro si adatta a scenari dove si hanno già alcune informazioni sul dispositivo target (es.: indirizzo IP).

In questo caso le regole di injection provenienti da RCS contengono già tutti i dati necessari per identificare automaticamente i dispositivi target.

L'avvio dell'identificazione automatica da parte della funzione **Network Injector** mette mano a mano in evidenza i dispositivi target che vengono subito infettati dalle regole di injection.

Forzata autenticazione dei dispositivi sconosciuti

In una rete WiFi protetta con password, è probabile non riuscire ad agganciare qualche dispositivo. I dispositivi di questo tipo compariranno nell'elenco come sconosciuti.

In questo caso è possibile forzare una loro autenticazione: il dispositivo si disconnetterà dalla rete per riconnettersi e verrà identificato.

Infezione tramite identificazione da operatore

Nelle regole di identificazione provenienti da RCS è possibile indicare che l'identificazione sarà a cura dell'operatore. Questa prassi è frequente quando a priori non si hanno informazioni sul dispositivo da infettare e occorre identificarlo direttamente sul campo.

In questo caso l'operatore ha a disposizione una serie di funzioni per selezionare i dispositivi connessi alla rete:

- può impostare dei filtri sul traffico intercettato: solo i dispositivi che rispondono ai criteri vengono infettati.
- può controllare la cronologia di ogni dispositivo per determinare se è quello da infettare.

Una volta determinati i dispositivi target è sufficiente selezionarli e avviare l'infezione: le regole di identificazione vengono "personalizzate" con i dati dei dispositivi per permettere alle regole di injection di agire.



NOTA: è comunque possibile infettare manualmente dispositivi che sono già stati infettati tramite identificazione automatica.

Impostazione di filtri sul traffico intercettato

Nel caso di identificazione dei target tramite operatore, ci si potrebbe trovare in uno scenario con una rete con diversi dispositivi connessi dei quali però non si riesce a individuare il dispositivo target. In questo caso è possibile utilizzare la funzione **Network Injector** per impostare dei filtri sul traffico intercettato.

Tactical Control Center mette a disposizione due tipi di filtri:

- espressioni regolari
- BPF (Berkeley Packet Filter) di rete

Filtro con espressioni regolari

Le espressioni regolari sono un filtro ad ampio spettro. Per esempio se il nostro target sta consultando una pagina di Facebook e sta parlando di windsurf è sufficiente inserire la parola "facebook" oppure la parola "windsurf".

Tactical Network Injector intercetta tutto il traffico dati e cerca le parole inserite.

Per una descrizione dettagliata di tutte le espressioni regolari ammesse fare riferimento a https://en.wikipedia.org/wiki/Regular_expression.

Filtro BPF (Berkeley Packet Filter) di rete

Serve per filtrare con maggiore precisione i dispositivi utilizzando la sintassi BPF (Berkeley Packet Filter). Questa sintassi prevede l'inserimento di parole chiave accompagnate da qualificatori:

- *qualificatori di tipo* (es.: **host**, **net**, **port**), indicano il tipo dell'oggetto cercato
- *qualificatori di direzione* (es.: **src**, **dst**) indicano la direzione dei dati cercati

- *qualificatori di protocollo* (es.: **ether, wlan, ip**) indicano il protocollo usato dall'oggetto cercato

Per esempio se il nostro target sta consultando una pagina di Facebook potremmo inserire "**host facebook.com**"

Per conoscere nel dettaglio tutti i qualificatori della sintassi fare riferimento alla pagina <http://wiki.wireshark.org/CaptureFilters>.

Individuazione del target tramite analisi cronologia

Una ulteriore possibilità per filtrare e ridurre l'elenco dei possibili target, è analizzare il traffico web di ogni dispositivo per riconoscerlo come target.

Emulazione di un Access Point conosciuto dal target

In certi scenari è necessario attrarre i dispositivi target per poter intercettare i loro dati, identificarli e infettarli.

Per farlo Tactical Network Injector emula un Access Point già registrato sul dispositivo target

In questo modo, se il dispositivo è abilitato alla connessione automatica alle reti WiFi disponibili, non appena entra nell'area WiFi si connette automaticamente all'Access Point emulato dal Tactical Network Injector. .

Tactical Control Center

Scopo

Tactical Control Center permette di identificare e infettare i dispositivi:

- **automaticamente**, tramite l'applicazione di regole di identificazione basate su informazioni già conosciute dei dispositivi (es.: indirizzo IP)
- **manualmente**, tramite una serie di tentativi da parte dell'operatore di individuare il dispositivo del target e infettarlo.

La modalità di identificazione va concordata con la sede operativa.

Cosa è possibile fare

Con il Tactical Control Center è possibile:

- aggiornare il dispositivo Tactical con l'ultima versione fornita da RCS Console
- abilitare la sincronizzazione con la sede operativa per la ricezione delle regole di injection e l'invio dei log.
- ottenere la password da una rete WiFi per entrare
- emulare un Access Point per attrarre i dispositivi del target
- applicare le regole di identificazione dei dispositivi e infettarli

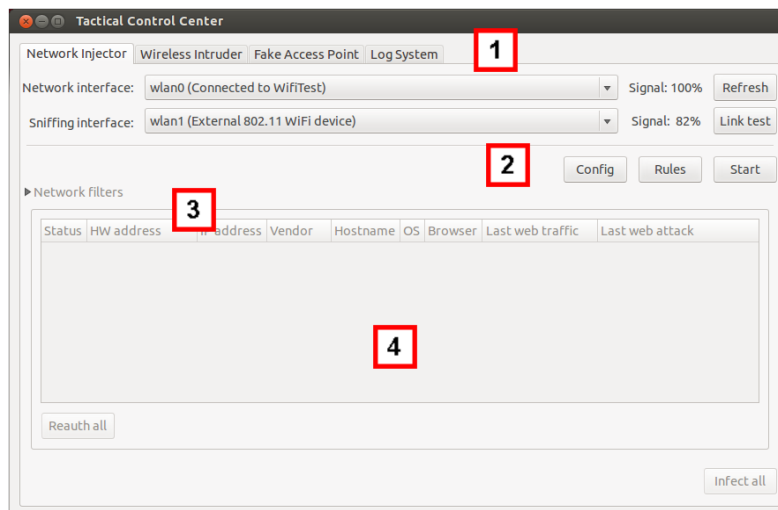
- forzare una nuova autenticazione nel caso di dispositivi non identificabili al primo tentativo
- selezionare i dispositivi sulla base di filtri o informazioni di cronologia

Richiesta della password

All'avvio Tactical Control Center chiede la password di accesso, la stessa del portatile su cui si sta lavorando.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area Descrizione

- 1 Schede per l'accesso alle singole applicazioni. Di seguito la descrizione:

Funzione	Descrizione
-----------------	--------------------

Network injector	Gestisce lo sniffing e l'infezione dei dispositivi del target, sincronizza le regole RCS, aggiorna i dispositivi Tactical e mostra le regole attualmente presenti sul Tactical Network Injector.
-------------------------	--

Wireless Intruder	Entra in una rete WiFi protetta tramite individuazione password.
--------------------------	--

Fake Access Point	Emula un Access Point.
--------------------------	------------------------

Log System	Elenca i log in tempo reale.
-------------------	------------------------------

- 2 Area con i pulsanti per ricaricare l'elenco dei dispositivi, avviare le connessioni alla rete, abilitare la sincronizzazione
- 3 Filtri per filtrare traffico in internet dei dispositivi.
- 4 Area con l'elenco dei dispositivi.

Per saperne di più

Per la descrizione dei dati del Tactical Control Center vedi "[Dati del Tactical Control Center](#)" a pagina101 .

Per saperne di più sul Tactical Control Center vedi "[Cose da sapere su Tactical Control Center](#)" a pagina84 .

Procedure

Abilitazione sincronizzazione con RCS

Di seguito la procedura per la prima sincronizzazione con RCS (senza infezioni in corso):

Passi

1. Nella scheda **Network Injector** fare clic sul pulsante **Config**: la sincronizzazione viene abilitata e allo scadere del prossimo intervallo saranno ricevute le regole di injection previste e spediti i log.



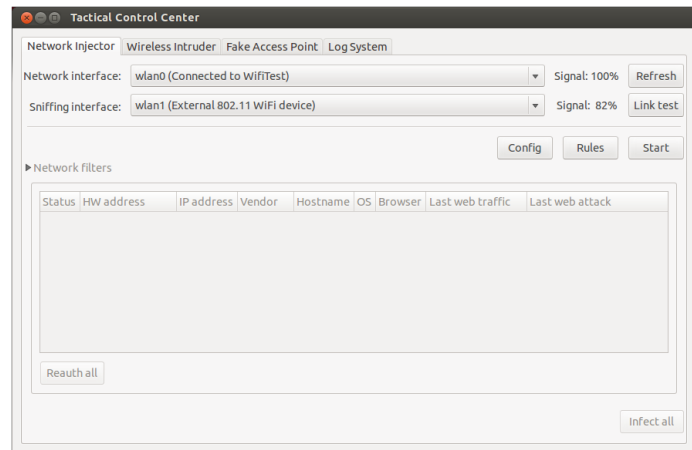
IMPORTANTE: abilitare regolarmente la sincronizzazione per garantire un aggiornamento costante dalla sede operativa e il successo delle infezioni.

2. Per interrompere la sincronizzazione fare clic su **Stop**.

3. Per visualizzare le regole ricevute da RCS Console fare clic su **Rules**: compaiono tutte le regole per il Network Injector



IMPORTANTE: controllare l'effettiva sincronizzazione delle regole dopo aver chiesto a RCS Console un loro aggiornamento.

Risultato

Rule	Probability	Attack	Resource
TACTICAL	100%	INJECT-HTML-FLASH	*.youtube.com/watch*
TACTICAL	100%	REPLACE	*google.*/robots.txt
TACTICAL	100%	INJECT-HTML-JAVA	login.live.com/
TACTICAL	100%	INJECT-EXE	*.exe*

Avviare un test della rete

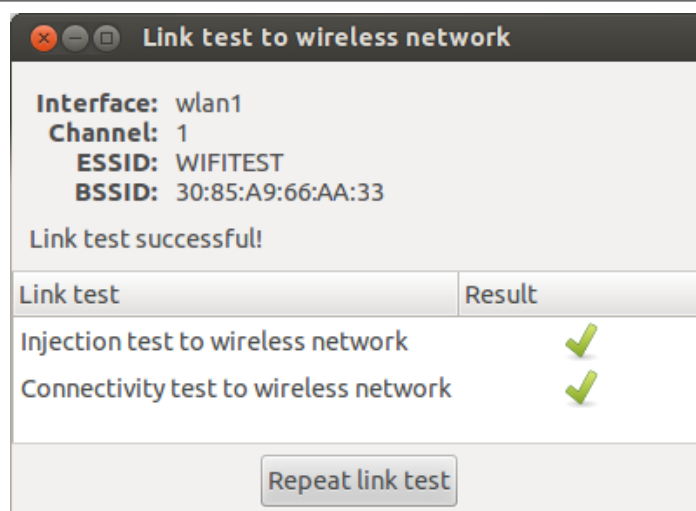
Di seguito la procedura per verificare la rete per lo sniffing e/o injection::

Passi

1. Nella scheda **Network Injector** o nella scheda **Wireless Intruder** selezionare l'interfaccia di rete.
2. Fare clic sul pulsante **Link test**: compare una finestra dove compariranno i risultati del test.
3. Se il test non ha successo, spostarsi in una posizione migliore dove il segnale è più forte e ripetere il test.



IMPORTANTE: l'attacco non può andare a buon fine se il test non ha successo.

Risultato**Acquisire la password di una rete WiFi protetta**

Di seguito la procedura per acquisire la password di una rete WiFi protetta:

Passi

1. Nella scheda **Wireless Intruder** selezionare in **Wireless interface** l'interfaccia di rete WiFi
2. Selezionare in **ESSID network** la rete di cui individuare la password.

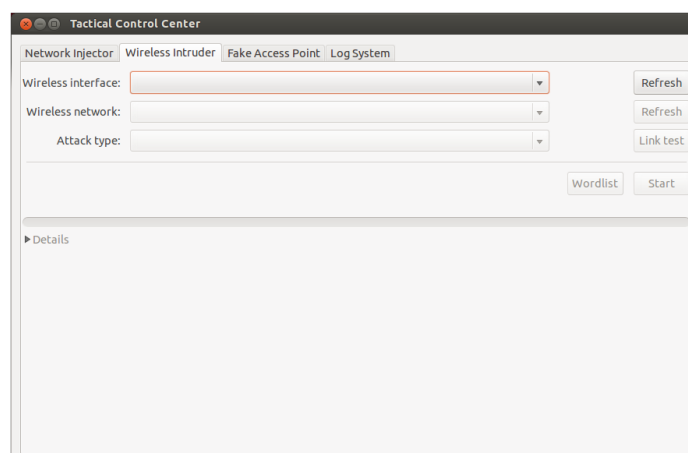


NOTA: gestire da sistema operativo eventuale connessione/disconnessione di interfacce di rete e premere il pulsante **Refresh**.

3. In **Attack type** scegliere il tipo di attacco.
4. Se necessario fare clic su **Wordlist** per caricare un dizionario aggiuntivo per attaccare reti con protezione WPA o WPA 2

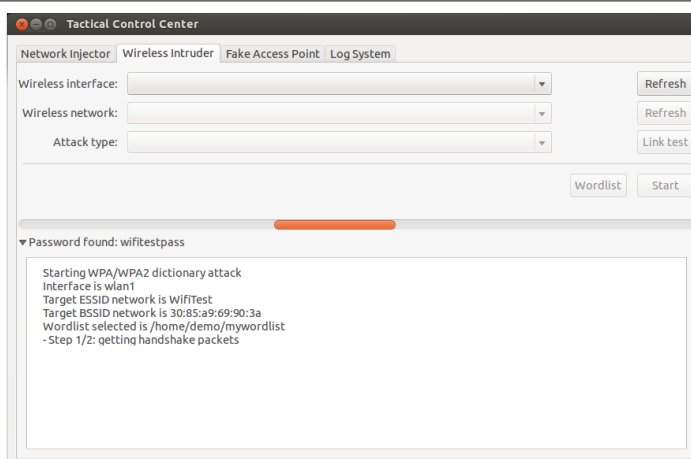


IMPORTANTE: il dizionario aggiuntivo deve essere caricato ad ogni attacco.

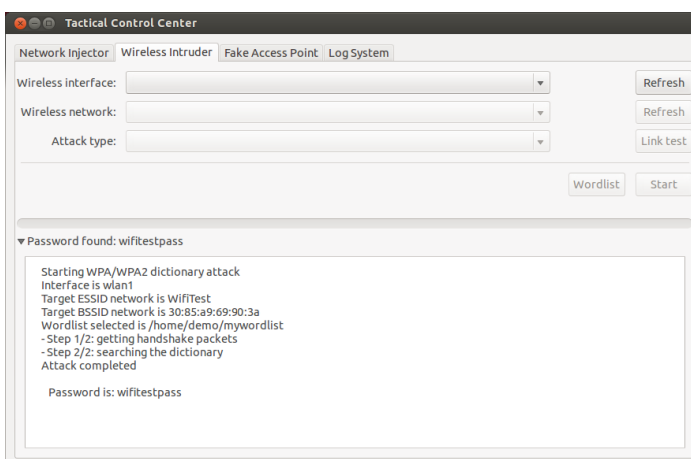
Risultato

Passi

5. Fare clic su **Start**: il sistema lancia diversi attacchi per rivelare la password di accesso.
6. Fare clic su **Stop** se serve fermare l'attacco.

Risultato

7. Se gli attacchi hanno avuto successo, sopra l'indicatore di stato compare la password.



8. Tramite il **Network Manager** del sistema operativo aprire la connessione verso la rete WiFi di cui si conosce la password. La password verrà memorizzata dal sistema e non sarà più necessario inserirla.
9. Aprire la sezione **Network Injector** per iniziare l'identificazione e l'infezione.

Infettare i target tramite identificazione automatica

Per avviare l'identificazione e infezione automatica:

Passi

1. Nella scheda **Network Injector** selezionare nella casella di riepilogo **Network Interface** l'interfaccia di rete per l'injection.
2. Nella casella di riepilogo **Sniffing interface** selezionare una diversa interfaccia di rete da usare per lo sniffing oppure scegliere la stessa interfaccia usata per l'injection.



NOTA: gestire da sistema operativo eventuale connessione/disconnessione di interfacce di rete e premere il pulsante **Refresh**.

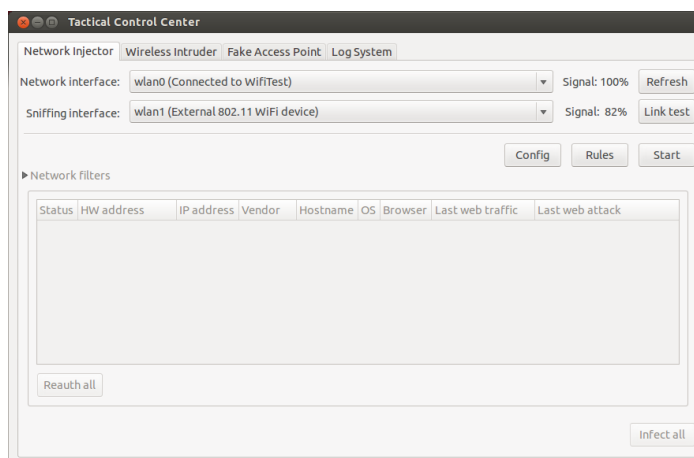
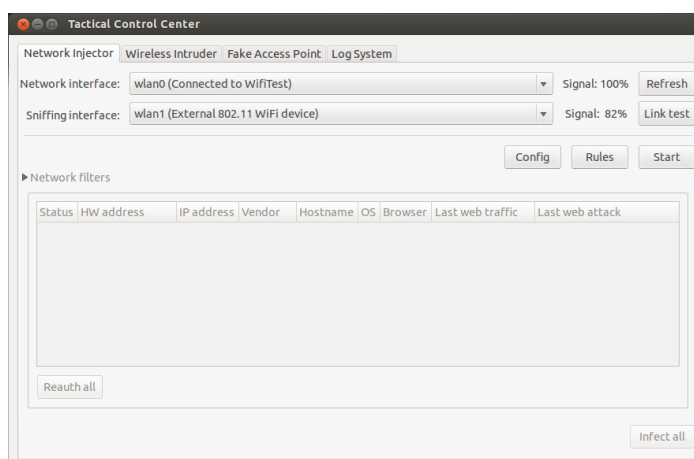


Suggerimento: usare due interfacce di rete diverse garantisce una migliore identificazione dei dispositivi.

3. Controllare la potenza del segnale e se necessario avviare il test della rete (pulsante **Link test**).



NOTA: la potenza del segnale deve essere almeno del 70%. Si avrà un unico valore se si usa la stessa interfaccia di rete per l'injection e per lo sniffing.

Risultato

Passi

- Fare clic su **Start**
- Si avvia il processo di sniffing della rete e compaiono tutti i dispositivi identificati come target. La colonna **Status** mostra lo stato dell'identificazione.



AVVERTENZA: controllare bene lo stato dell'identificazione. Vedi "[Dati del Tactical Control Center](#)" a pagina 101.

- I dispositivi target iniziano ad essere infettati. Nel log viene registrato l'inizio dell'infezione.



NOTA: i dispositivi non target non compaiono nell'elenco e sono quindi esclusi dall'infezione automatica.

- Per fermare l'infezione fare clic su **Stop**.

Risultato

Status	HW address	IP address	Vendor	Hostname	OS	Browser	Last web traffic	Last web attack
✘	ac:72:89:cc:85:77		IntelCor				idle	
✔	74:f0:6d:b7:0c:0d	192.168.1.143	Azurewav				idle	
✘	58:94:6b:b5:cb:d4		IntelCor				idle	
✔	08:ed:b9:75:c1:cf	192.168.1.154	HonHaiPr				idle	
✘	3c:74:37:4b:dd:fb		Rim				idle	
✘	60:21:c0:bd:44:7b		Unknown				idle	

Impostare i filtri sul traffico intercettato

Per selezionare i dispositivi target tramite filtri sul traffico dati:

Passi

- Nella scheda **Network Injector**, fare clic su **Network filters**.
- Per una ricerca ad ampio raggio digitare un'espressione regolare nella casella di testo **Regular expression**.
- Oppure, per una ricerca più raffinata digitare un'espressione BPF nella casella di testo **BPF Network Filter**.

Risultato: il sistema mostra nell'elenco solo i dispositivi filtrato.

Risultato

Status	HW address	IP address	Vendor	Hostname	OS	Browser	Last web traffic	Last web attack
✘	ac:72:89:cc:85:77		IntelCor				idle	
✔	74:f0:6d:b7:0c:0d	192.168.1.143	Azurewav	Target	Windows 7	Chrome	facebook.com	
✘	58:94:6b:b5:cb:d4		IntelCor				idle	
✔	08:ed:b9:75:c1:cf	192.168.1.154	HonHaiPr				idle	
✘	3c:74:37:4b:dd:fb		Rim				idle	
✘	60:21:c0:bd:44:7b		Unknown				idle	


Passi**Risultato**

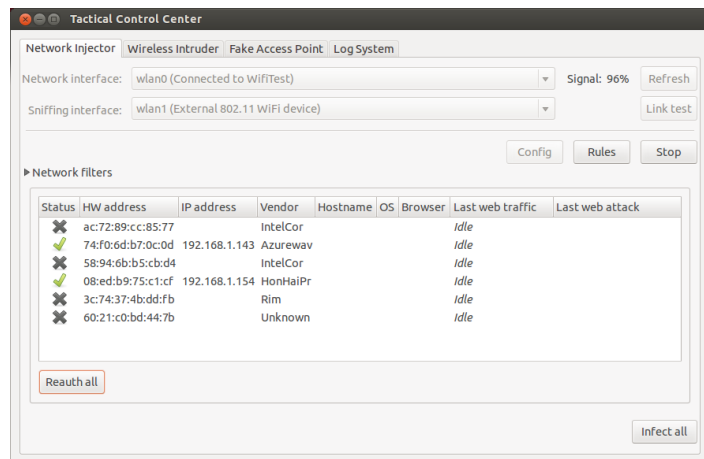
4. Procedere nell'infezione manuale come descritto dalla procedura *vedi "Infettare i target tramite identificazione manuale" nel seguito*.

Forzare l'autenticazione dei dispositivi sconosciuti

Per forzare un dispositivo sconosciuto ad autenticarsi:

Passi**Risultato**


1. Nella scheda **Network Injector**, nell'elenco dei dispositivi, selezionare quelli sconosciuti (stato )



2. Premere il pulsante **Reauth selected**: i dispositivi sono costretti a riautenticarsi.



Suggerimento: in certi casi può essere necessario chiedere la autenticazione di tutti i dispositivi presenti. Per farlo fare clic su **Reauth All**.

3. Se la riautenticazione ha successo, viene avviata l'identificazione automatica: lo stato dei dispositivi sarà  e da adesso in poi sarà possibile infettarli.

Infettare i target tramite identificazione manuale

Per infettare manualmente i dispositivi in rete:

Passi**Risultato**

1. In **Network Injector** nell'elenco dei dispositivi selezionare uno o più dispositivi da infettare identificandoli tramite i dati esposti.



Suggerimento: se i dispositivi nell'elenco sono tanti, usare i filtri di selezione. Vedi "[Impostare i filtri sul traffico intercettato](#)" a pagina 96 .


2. Fare clic sul pulsante **Infect selected**: tutte le regole di injection vengono "personalizzate" con i dati del dispositivo e applicate. Nei log sarà visibile l'attacco verso i dispositivi.



IMPORTANTE: questa operazione prevede la presenza in RCS di una regola speciale.



Suggerimento: in certi casi può essere necessario infettare tutti i dispositivi connessi, anche quelli non target o non ancora connessi. Per farlo fare clic su **Infect All**.

Risultato: se l'infezione è stata avviata con successo, lo stato dei dispositivi è  .

Pulire i dispositivi erroneamente infettati

Per rimuovere l'infezione dai dispositivi è necessario agire su RCS Console, tramite la chiusura dell'agent.

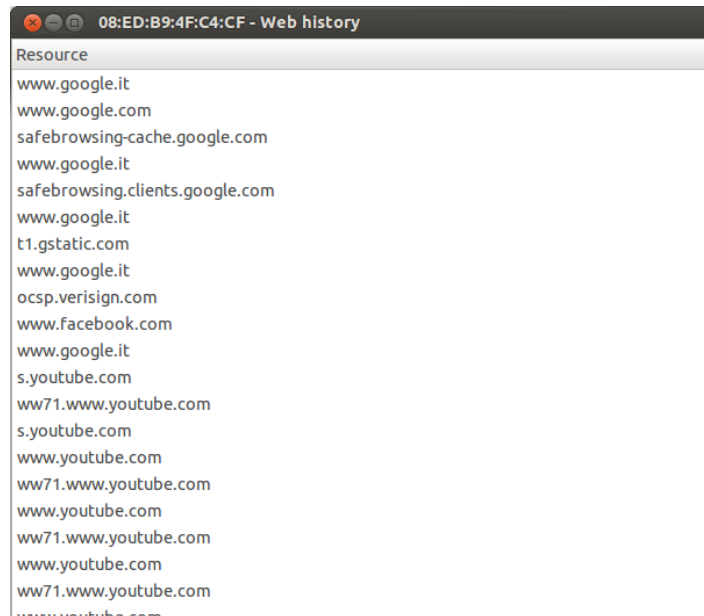
Individuare un target analizzando la cronologia web

Per individuare un target:

Passi

1. Nella scheda **Network Injector** fare doppio clic sul dispositivo da controllare: si apre una finestra con la cronologia dei siti web visitati dal browser.

Risultato



2. Se il dispositivo è quello target, chiudere la cronologia e procedere con la procedura **"[Infettare i target tramite identificazione manuale](#)"** a pagina97.

Emulare un Access Point conosciuto dal target

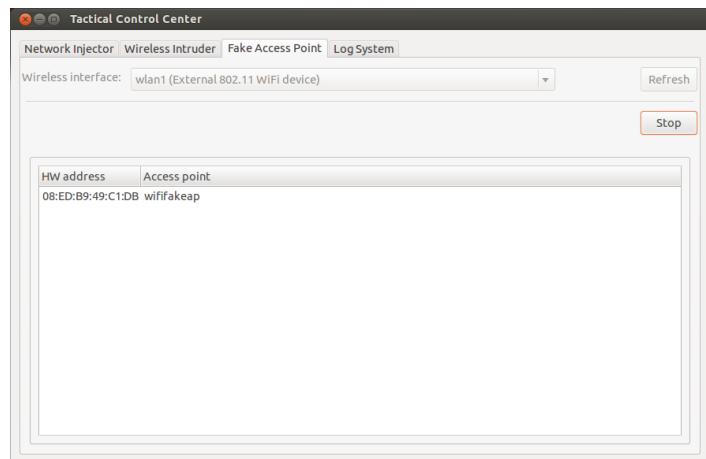


IMPORTANTE: prima di attivare l'emulazione dell'Access Point, fermare un eventuale attacco attivo nella scheda Network Injector .

Per trasformare Tactical Network Injector in un Access Point conosciuto dai target:

Passi

1. Nella scheda **Fake Access Point** selezionare nella casella di riepilogo **Wireless Interface** l'interfaccia di rete su cui ci si vuole mettere in ascolto.

Risultato

2. Fare clic su **Start**: Tactical Network Injector recupera i nomi delle reti WiFi cui i dispositivi sono soliti connettersi e li mostra nella scheda **Network Injector**.
3. Parallelamente stabilisce la comunicazione con i singoli dispositivi emulando l'access point di ogni rete
4. In Network Injector, nella casella di riepilogo **Network interface** selezionare la stessa interfaccia di rete esposta come access point
5. Premere **Start**: i dispositivi connessi vengono visualizzati
6. Procedere nell'infezione manuale come descritto dalla procedura *vedi "Infettare i target tramite identificazione manuale" a pagina 97*.

Spegner il Tactical Network Injector

Non è prevista alcuna procedura particolare. Spegner normalmente il computer.

Visualizzare i dettagli dell'infezione

Per visualizzare i dati registrati selezionare la scheda **Log System**.

Dati del Tactical Control Center





Dati scheda Network Injector


Di seguito la descrizione dei dati:

<i>Dato</i>	<i>Descrizione</i>
Network interface	Elenco delle interfacce di rete già connesse. Selezionare l'interfaccia di injection connessa alla rete dove è collegato il dispositivo da attaccare. In caso di simulazione di Access Point qui comparirà anche l'interfaccia utilizzata nella sezione Fake Access Point .
Sniffing interface	Come Network Interface oppure altra interfaccia di rete da utilizzare solo per lo sniffing.
Regular expression	Espressione usata per filtrare i dispositivi connessi alla rete. Viene applicata a tutti i dati trasmessi e ricevuti dal dispositivo tramite rete, di qualsiasi genere. <i>Vedi "Cose da sapere su Tactical Control Center" a pagina 84 .</i>
BPF network filter	Serve per filtrare con maggiore precisione utilizzando la sintassi BPF (Berkeley Packet Filter). Questa sintassi prevede l'inserimento di parole chiave accompagnate da qualificatori. <i>Vedi "Cose da sapere su Tactical Control Center" a pagina 84 .</i>

Dati dei dispositivi rilevati

Di seguito la descrizione dei dati:

<i>Dato</i>	<i>Descrizione</i>
Status	Stato dei dispositivi connessi alla rete:  : dispositivo sconosciuto. Non può essere infettato per problematiche legate alla autenticazione. Forzare l'autenticazione.  : dispositivo in fase di identificazione.  : dispositivo identificato e può essere infettato.  : dispositivo infettato.
HW address	Indirizzo hardware della scheda di rete del dispositivo.
IP address	Indirizzo IP del dispositivo nella rete.
Vendor	Marca della scheda di rete (abbastanza affidabile).

<i>Dato</i>	<i>Descrizione</i>
Hostname	Nome del dispositivo.
OS	Sistema operativo del dispositivo.
Browser	Browser web usato dal dispositivo.
Last web Traffic	Ultimi siti visitati dal dispositivo rilevati e analizzati negli ultimi cinque minuti.  NOTA: se al termine dei cinque minuti il dispositivo non genera più traffico web, allora comparirà la scritta Idle . Tipicamente questo accade quando nessuno sta utilizzando il dispositivo.
Last web attack	Tipo e risultato dell'ultimo attacco. Per controllare ulteriori dettagli consultare la scheda Log System .

Dati scheda Wireless Intruder

Di seguito la descrizione dei dati:

<i>Dato</i>	<i>Descrizione</i>								
Wireless interface	Elenco delle interfacce di rete non connesse. Selezionare l'interfaccia da connettere alla rete WiFi protetta cui si vuole accedere.								
ESSID network	Nome della rete locale in cui accedere.								
Attack type	Tipi di individuazione password disponibili: <table border="1" data-bbox="336 1272 1423 1655"> <thead> <tr> <th><i>Tipo</i></th> <th><i>Descrizione</i></th> </tr> </thead> <tbody> <tr> <td>WPA/WPA2 dictionary attack</td> <td>Raccoglie gli handshake tra il client e il punto di accesso e cerca di scoprire la password utilizzando un dizionario di parole comuni.</td> </tr> <tr> <td>WEP bruteforce attack</td> <td>Fa una injection simulando uno dei client connessi a raccoglie i dati per forzare la password cifrata.</td> </tr> <tr> <td>WPS PIN bruteforce attack</td> <td>Prova tutte le possibili combinazioni per poter recuperare la configurazione del punto di accesso tramite un protocollo WiFi Protected Setup.</td> </tr> </tbody> </table>	<i>Tipo</i>	<i>Descrizione</i>	WPA/WPA2 dictionary attack	Raccoglie gli handshake tra il client e il punto di accesso e cerca di scoprire la password utilizzando un dizionario di parole comuni.	WEP bruteforce attack	Fa una injection simulando uno dei client connessi a raccoglie i dati per forzare la password cifrata.	WPS PIN bruteforce attack	Prova tutte le possibili combinazioni per poter recuperare la configurazione del punto di accesso tramite un protocollo WiFi Protected Setup.
<i>Tipo</i>	<i>Descrizione</i>								
WPA/WPA2 dictionary attack	Raccoglie gli handshake tra il client e il punto di accesso e cerca di scoprire la password utilizzando un dizionario di parole comuni.								
WEP bruteforce attack	Fa una injection simulando uno dei client connessi a raccoglie i dati per forzare la password cifrata.								
WPS PIN bruteforce attack	Prova tutte le possibili combinazioni per poter recuperare la configurazione del punto di accesso tramite un protocollo WiFi Protected Setup.								

Dati scheda Fake Access Point

Di seguito la descrizione dei dati:

<i>Dato</i>	<i>Descrizione</i>
Wireless interface	Elenco delle interfacce di rete non connesse. Selezionare l'interfaccia che si vuole esporre come rete WiFi.
HW address	Indirizzo hardware della scheda di rete del dispositivo.
Access point	Nome dell'Access Point atteso dal dispositivo.

Appendice: azioni

Presentazione

Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati le singole azioni con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

Contenuti

Questa sezione include i seguenti argomenti:

Elenco delle sotto-azioni	105
Azione Destroy	105
Azione Execute	106
Azione Log	107
Azione SMS	107
Azione Synchronize	108
Azione Uninstall	110

Elenco delle sotto-azioni

Descrizione dati sotto-azioni

Di seguito la descrizione delle sotto-azioni:

<i>Dato</i>	<i>Descrizione</i>
Name	Nome arbitrario assegnato all'azione.
Subaction	Elenco dei tipi di sotto-azioni.

Descrizione tipi di sotto-azioni

Di seguito la descrizione dei tipi di sotto-azioni:

<i>Azione</i>	<i>Dispositivo</i>	<i>Descrizione</i>
Destroy	desktop, mobile	<i>Rende il dispositivo target inutilizzabile.</i>
Execute	desktop, mobile	<i>Esegue un comando arbitrario sulla macchina target.</i>
Log	desktop, mobile	<i>Crea messaggio informativo personalizzato.</i>
SMS	mobile	<i>Invia un SMS nascosto dal dispositivo del target.</i>
Synchronize	desktop, mobile	<i>Avvia una sincronizzazione con il Collector.</i>
Uninstall	desktop, mobile	<i>Rimuove l'agent dal dispositivo.</i>



Azione Destroy

Scopo

L'azione **Destroy** rende il dispositivo target temporaneamente o permanentemente inutilizzabile.

Sistemi operativi

Desktop: Windows, OS X

Mobile: BlackBerry, WinMobile

Parametri

Nome	Descrizione
------	-------------

Permanent	Il dispositivo è reso inutilizzabile in modo permanente.
------------------	--



AVVERTENZA: potrebbe essere necessario portare il dispositivo in assistenza .



Azione Execute

Scopo

L'azione **Execute** esegue un comando arbitrario sulla macchina target. Se richiesto, possono essere specificate impostazioni del comando e variabili di ambiente. Il programma sarà eseguito con i privilegi dell'utente che in quel momento è registrato nel sistema.

L'eventuale output del comando è visibile nella pagina **Commands**. Vedi "[Pagina dei comandi](#)" a pagina49 .



AVVERTENZA: anche se tutti i comandi sono eseguiti utilizzando il sistema di occultamento dell'agent e risultano quindi invisibili, qualsiasi modifica al file system (es.: un file creato sul desktop) sarà visibile dall'utente. Fare attenzione.



ATTENZIONE: evitare programmi che richiedono interazione da parte dell'utente o che aprono interfacce grafiche.



Suggerimento: utilizzare applicazioni lanciate da linea di comando e file batch perché i loro processi (e la corrispondente finestra per la linea di comando) saranno nascosti dall'agent.

Riferimento a cartella dell'agent

Alla stringa di comando si può aggiungere la variabile di ambiente virtuale \$dir\$ che si riferisce alla cartella di installazione (nascosta) dell'agent.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, WinMobile

Dati significativi

<i>Campo</i>	<i>Descrizione</i>
--------------	--------------------

Command	Comando da eseguire.
----------------	----------------------



Suggerimento: utilizzare un percorso assoluto.

Azione Log

Scopo

L'azione **Log** crea messaggio informativo personalizzato.



NOTA: i messaggi personalizzati e i log provenienti da un agent sono visualizzati nella sezione **Info**. Vedi "[Pagina dell'agent](#)" a pagina 42

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

<i>Nome</i>	<i>Descrizione</i>
-------------	--------------------

Text	Testo del messaggio che comparirà nella sezione Info .
-------------	---



Azione SMS

Scopo

L'azione **SMS** invia un SMS nascosto dal dispositivo del target, con i dati della posizione del dispositivo e della SIM.

Sistemi operativi

Mobile: Android, BlackBerry, Symbian, WinMobile

Parametri

Nome **Descrizione**

Number	Telefono destinatario del messaggio.
Text	Testo del messaggio.
Position	Inserisce nel messaggio la posizione della cella GPS o GSM del target.
Sim	Inserisce nel messaggio le informazioni relative alla SIM del telefono.

Azione Synchronize

Scopo

L'azione **Synchronize** sincronizza l'agent e il server RCS.
Il processo di sincronizzazione si divide nei seguenti passi:

Passo **Descrizione**

- 1 Autenticazione reciproca agent/server RCS.
- 2 Sincronizzazione temporale agent/server RCS.
- 3 Eventuale rimozione dell'agent in caso di chiusura dell'attività relativa.
- 4 Aggiornamento configurazione dell'agent.
- 5 Caricamento di tutti i file nella coda "upload".
- 6 Scaricamento di tutti i file nella coda "download".
- 7 Scaricamento di tutte le evidenze raccolte dall'agent, con contestuale rimozione sicura.
- 8 Rimozione sicura nell'agent di tutte le evidenze scaricate.

Sistemi operativi

Desktop: Windows, OS X

Mobile: **Android, BlackBerry, iOS, Symbian, WinMobile**

Parametri desktop

<i>Nome</i>	<i>Descrizione</i>
Hostname	Nome dell'Anonymizer o Collector da connettere per la sincronizzazione. Nella casella combinata selezionare il nome del server oppure inserire l'FQDN (nome DNS) oppure l'indirizzo IP.
Bandwidth	Massima ampiezza di banda da utilizzare durante la sincronizzazione.
Min delay	Minimo ritardo in secondi tra l'invio una evidence e quella successiva.
Max delay	Massimo ritardo in secondi tra l'invio una evidence e quella successiva.
Stop on success	Se abilitato, la catena di sottoazioni viene interrotta al corretto completamento della sincronizzazione. Le rimanenti sottoazioni nella coda non sono eseguite.

Parametri mobile

<i>Nome</i>	<i>Descrizione</i>
Hostname	Nome o indirizzo IP dell'Anonymizer o Collector cui connettersi per la sincronizzazione. Nella casella combinata selezionare il nome del server oppure inserire l'FQDN (nome DNS) oppure l'indirizzo IP.
Stop on success	La catena di sottoazioni viene interrotta al corretto completamento della sincronizzazione. Le rimanenti sottoazioni nella coda non sono eseguite.
Type	<p>Internet: sincronizzazione tramite connessione Internet.</p> <ul style="list-style-type: none"> • Force WiFi: sincronizzazione via rete WiFi. Forza una connessione dati WiFi con una qualsiasi rete WiFi aperta o preconfigurata disponibile, prima di avviare la sincronizzazione. • Force Cell: sincronizzazione via rete GPRS/UMTS/3G . Forza una connessione dati GPRS/UMTS/3G verso il fornitore di telefonia prima di iniziare la sincronizzazione. <p>APN: specifica le credenziali per l'accesso a un APN che il telefono può usare per raccogliere i dati. Utile per non addebitare al target i costi del traffico generato dall'agent.</p>



IMPORTANTE: questo metodo è supportato solo su BlackBerry e Symbian.

Azione Uninstall

Scopo

L'azione **Uninstall** rimuove completamente l'agent dal sistema del target. Tutti i file vengono eliminati.



NOTA: su BlackBerry la rimozione comporta un riavvio automatico. Se su Android il dispositivo non ha i privilegi di root l'utente dovrà autorizzare la disinstallazione.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nessuno

Appendice: eventi

Presentazione

Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati i singoli eventi con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

Contenuti

Questa sezione include i seguenti argomenti:

Elenco degli eventi	112
Evento AC	113
Evento Battery	113
Evento Call	114
Evento Connection	114
Evento Idle	115
Evento Position	115
Evento Process	116
Evento Quota	117
Evento Screensaver	117
Evento SimChange	118
Evento SMS	118
Evento Standby	119
Evento Timer	119
Evento Window	120
Evento WinEvent	120

Elenco degli eventi

Descrizione dati eventi

Di seguito la descrizione degli eventi:

<i>Dato</i>	<i>Descrizione</i>
Abilitato	Abilita o disabilita l'evento.
Nome	Nome assegnato all'evento.
Type	Elenco dei tipi di evento. Vedi tabella sottostante.

Descrizione tipi eventi

Di seguito la descrizione tipi di evento:

<i>Evento</i>	<i>Dispositivo</i>	<i>Innesca un'azione quando..</i>
AC	mobile	<i>il cellulare viene collegato all'alimentazione.</i>
Battery	mobile	<i>il livello di carica della batteria è entro il range specificato.</i>
Call	mobile	<i>viene effettuata o ricevuta una chiamata.</i>
Connection	desktop, mobile	<i>l'agent rileva una connessione alla rete attiva.</i>
Idle	desktop	<i>l'utente non interagisce col computer per un determinato periodo di tempo.</i>
Position	mobile	<i>il dispositivo raggiunge o lascia una posizione specifica.</i>
Process	desktop, mobile	<i>sul dispositivo viene lanciato un'applicazione o se c'è una finestra aperta.</i>
Quota	desktop	<i>l'occupazione disco delle evidenze sul dispositivo supera il limite impostato.</i>
Screensaver	desktop	<i>sul dispositivo target si avvia il salvaschermo.</i>
SimChange	mobile	<i>viene sostituita la scheda SIM.</i>
SMS	mobile	<i>viene ricevuto un messaggio SMS dal numero indicato.</i>
Standby	mobile	<i>il dispositivo è in modalità stand-by.</i>
Timer	desktop, mobile	<i>scadono intervalli specificati.</i>
Window	desktop	<i>si apre una finestra.</i>
WinEvent	desktop	<i>il sistema operativo registra un evento Windows.</i>

Evento AC

Scopo

L'evento **AC** innesca un'azione quando il cellulare viene collegato all'alimentazione.

Sistemi operativi

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nessuno

Evento Battery

Scopo

L'evento **Battery** innesca un'azione quando il livello di carica della batteria è entro il range specificato.



Suggerimento: se si vuole ridurre l'impatto sull'uso della batteria, è sensato associare all'evento **Battery**, impostato su valori 0%-30%, le azioni **Start** e **Stop Crisis**. In questo modo, se il livello di carica della batteria scende sotto il valore prefissato, sono sospese le attività più dispendiose dell'agent.



ATTENZIONE: il modulo Crisis può essere configurato in modo da inibire la sincronizzazione!

Sistemi operativi

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nome Descrizione

<i>Nome</i>	<i>Descrizione</i>
Min	Minima percentuale di batteria richiesta. Percentuali superiori a questo limite innescano l'evento.
Max	Massima percentuale di batteria richiesta. Percentuali inferiori a questo limite innescano l'evento.

Evento Call


Scopo

L'evento **Call** innesca un'azione quando viene effettuata o ricevuta una chiamata.

Sistemi operativi

Mobile: WinMobile, BlackBerry, Symbian, Android

Parametri

<i>Nome</i>	<i>Descrizione</i>
Number	numero telefonico (o parte di esso) da cui viene effettuata/o ricevuta la chiamata.  Suggerimento: lasciare vuoto per innescare l'evento con qualsiasi numero.

Evento Connection

Scopo

L'evento **Connection** innesca un'azione quando l'agent rileva una connessione alla rete attiva.

Nel caso di dispositivo desktop indicare l'indirizzo del destinatario della connessione.

Nel caso di dispositivo mobile innesca un'azione non appena il dispositivo disporrà di un indirizzo IP valido su una qualsiasi delle interfacce di rete (es.: WiFi, Activesync, GPRS/3G+), e disinnescherà l'azione quando tutte le connessioni sono terminate.

Sistemi operativi

Desktop: Windows, OS X



Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri mobile

Nessuno

Parametri desktop

Nome *Descrizione*

IP Address	Indirizzo IP di destinazione per la connessione
	 NOTA: Inserire 0.0.0.0 per indicare un qualsiasi indirizzo.
	 NOTA: le connessioni a indirizzi locali nella stessa sottorete del target non vengono considerate.
Netmask	Netmask applicata all'indirizzo IP.
Port	Porta utilizzata per identificare la connessione.

ZZ Evento Idle

Scopo

L'evento **Idle** innesca un'azione quando l'utente non interagisce con il computer per un determinato periodo di tempo.

Sistemi operativi

Desktop: Windows, OS X

Parametri

Nome *Descrizione*

Time Secondi di inattività allo scadere dei quali viene innescato l'evento.

Evento Position

Scopo

L'evento **Position** innesca un'azione quando il target raggiunge o lascia una posizione specifica. La posizione può essere identificata dalle coordinate GPS e da un raggio d'azione oppure dall'ID di una cella GSM.

Sistemi operativi

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nome *Descrizione*

Type Tipo di posizione da utilizzare.

GPS

- **Latitude, Longitude:** coordinate
- **Distance:** raggio a partire dalle coordinate.

GSM Cell

- **Country, Network, Area, ID:** dati della cella GSM. Inserire '*' per ignorare un campo. Per esempio, se si mantiene il valore di **Country** e si mette il simbolo '*' negli altri tre campi, l'evento è innescato quando il dispositivo entra o esce dalla nazione specificata.



Evento Process

Scopo

L'evento **Process** innesca un'azione quando sul dispositivo viene lanciata un'applicazione o viene aperta una finestra.

Sistemi operativi


Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nome *Descrizione*

Type **Process Name:** l'evento innesca un'azione all'avvio del processo specificato.
Window Title: l'evento innesca un'azione quando il focus viene dato alla finestra specificata.

<i>Nome</i>	<i>Descrizione</i>
String	Nome o parte del nome del programma o del titolo della finestra.  Suggerimento: utilizzare caratteri jolly per specificare un programma (es.: "*Calculator*")
On Focus	(solo desktop) Se selezionato, l'evento innesca l'azione solo quando il processo o la finestra sono in primo piano.

Evento Quota

Scopo

L'evento **Quota** innesca un'azione quando l'occupazione disco delle evidenze sul dispositivo supera il limite impostato.

Quando lo spazio disco torna al di sotto del limite, alla successiva sincronizzazione l'azione sarà terminata.

Sistemi operativi

Desktop: Windows

Parametri

<i>Nome</i>	<i>Descrizione</i>
Quota	Spazio disco da usare per salvare le evidenze raccolte.

Evento Screensaver

Scopo

L'evento **Screensaver** innesca un'azione quando sul dispositivo target si avvia il salvaschermo.

Sistemi operativi

Desktop: Windows, OS X

Parametri

Nessuno

Evento SimChange

Scopo

L'evento **SimChange** innesca un'azione quando viene sostituita la scheda SIM.

Sistemi operativi

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nessuno

Evento SMS

Scopo

L'evento **SMS** innesca un'azione quando viene ricevuto uno specifico messaggio SMS dal numero indicato. Il messaggio non comparirà tra i messaggi ricevuti dal telefono.



ATTENZIONE: i messaggi in arrivo vengono cancellati soltanto su **BlackBerry OS 5.x**.




NOTA: il messaggio ricevuto non viene visualizzato sul dispositivo del target.

Sistemi operativi

Mobile: Android, BlackBerry, Symbian, WinMobile

Parametri

<i>Nome</i>	<i>Descrizione</i>
Number	Numero telefonico del mittente del messaggio SMS. Qualsiasi SMS proveniente da questo numero verrà nascosto.
Text	Parte del testo che deve corrispondere.  IMPORTANTE: nella stringa non si fa distinzione fra maiuscole e minuscole.

Evento Standby

L'evento **Standby** innesca un'azione quando il dispositivo entra in modalità stand-by (retroilluminazione spenta).

Sistemi operativi

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nessuno

Evento Timer

Scopo

L'evento **Timer** innesca un'azione agli intervalli indicati.

Quando l'evento si verifica, viene eseguita l'azione connessa all'azione **Start**.

Durante il periodo di tempo che intercorre tra l'innescò e il disinnescò dell'evento, viene ripetuta l'azione **Repeat**, con il periodo specificato dal connettore relativo.

Quando l'evento viene disinnescato, viene eseguita l'azione **Stop**.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

Nome *Descrizione*

Type Tipo di intervallo:

- **Loop:** innesca un'azione ripetendola indefinitivamente ogni periodo di tempo specificato dall'azione **Repeat**.
- **Daily:** innesca un'azione quotidiana all'interno degli orari indicati da **From** e **To**.
- **Date:** innesca un'azione nel periodo indicato da **From** e **To**.



NOTA: selezionare **Forever** affinché l'azione continui nel tempo.

- **AfterInst:** innesca un'azione dopo un certo numero di giorni (**Days**) dall'installazione dell'agent.

Evento Window

Scopo

L'evento Window innesca un'azione all'apertura di ogni finestra.

Sistemi operativi

Desktop: Windows

Parametri

Nessuno.

Evento WinEvent

Scopo

L'evento **WinEvent** innesca un'azione quando il sistema operativo registra un evento Windows.

Sistemi operativi

Desktop: Windows

Parametri

<i>Nome</i>	<i>Descrizione</i>
-------------	--------------------

Event ID	ID dell'evento Windows.
-----------------	-------------------------

Source	Sorgente dell'evento Windows (es.: sistema, applicazione)
---------------	---

Appendice: moduli

Presentazione

Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati i singoli moduli con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

Contenuti

Questa sezione include i seguenti argomenti:

Elenco dei moduli	122
Modulo Addressbook	123
Modulo Application	124
Modulo Calendar	124
Modulo Call	125
Modulo Camera	125
Modulo Chat	126
Modulo Clipboard	127
Modulo Conference	127
Modulo Crisis	128
Modulo Device	129
Modulo File	130
Modulo Infection	131
Modulo Keylog	131
Modulo Livemic	131
Modulo Messages	132
Modulo Mic	133
Modulo Mouse	134
Modulo Password	135
Modulo Position	135
Modulo Screenshot	136
Modulo Url	136

Elenco dei moduli

Di seguito la descrizione dei moduli di registrazione:

Modulo	Configurazione	Dispositivo	Registrazione di...
Accessed files	base	<i>desktop</i>	documenti o immagini aperti dal target.
Addressbook	avanzata	<i>desktop, mobile</i>	contatti.
Application	avanzata	<i>desktop, mobile</i>	applicazioni utilizzate.
Calendar	avanzata	<i>desktop, mobile</i>	calendario.
Call	avanzata	<i>desktop, mobile</i>	chiamate (telefono, Skype, MSN).
Calls	base	<i>desktop, mobile</i>	chiamate (telefono, Skype, MSN).
Camera	base, avanzata	<i>desktop, mobile</i>	immagini della webcam.
Chat	avanzata	<i>desktop, mobile</i>	chat (Skype, BlackBerry Messenger).
Clipboard	avanzata	<i>desktop, mobile</i>	informazioni copiate nella clipboard.
Contacts and Calendar	base	<i>desktop, mobile</i>	contatti e calendario.
Dispositivo	avanzata	<i>desktop, mobile</i>	informazioni del sistema.
File	avanzata	<i>desktop,</i>	file aperti dal target.
Keylog	avanzata	<i>desktop, mobile</i>	tasti premuti sulla tastiera.
Keylog, Mouse and Password	base	<i>desktop</i>	tasti premuti sulla tastiera, clic del mouse, password salvate.
Messages	avanzata	<i>desktop, mobile</i>	e-mail, SMS, MMS.
Messages	base	<i>desktop, mobile</i>	e-mail, SMS e chat.
Mic	avanzata	<i>desktop, mobile</i>	audio proveniente dal microfono.

Modulo	Configurazione	Dispositivo	Registrazione di...
Mouse	avanzata	<i>desktop</i>	clic del mouse.
Password	avanzata	<i>desktop</i>	password salvate.
Position	base, avanzata	<i>desktop, mobile</i>	posizione geografica del target.
Screenshots	base, avanzata	<i>desktop, mobile</i>	schermata attive sul display del target.
URL	avanzata	<i>desktop, mobile</i>	URL visitati.
Visited websites	base	<i>desktop, mobile</i>	URL visitati.

Di seguito la descrizione dei moduli di altro tipo:

Modulo	Configurazione	Dispositivo	Azione
Conference	avanzata	<i>mobile</i>	Crea una chiamata a tre.
Crisis	avanzata	<i>desktop, mobile</i>	Riconosce situazioni di pericolo (es.: esecuzione di uno sniffer). Può disabilitare temporaneamente la sincronizzazione e l'esecuzione di comandi.
Infection	avanzata	<i>desktop</i>	Propaga l'agent su altri dispositivi.
Livemic	avanzata	<i>mobile</i>	Ascolta in tempo reale conversazioni.
Online Synchronization	base	<i>desktop, mobile</i>	Sincronizza l'agent con RCS permettendo la ricezione delle evidence e la riconfigurazione dell'agent.



Modulo Addressbook

Scopo

Il modulo **Addressbook** registra tutte le informazioni trovate nella rubrica del dispositivo. La versione per desktop recupera i contatti da Outlook, Skype ed altre fonti.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, WinMobile

Dati significativi

Nessuno



Modulo Application

Scopo

Il modulo **Application** registra il nome e le informazioni relative all'avvio e alla chiusura di un processo sul dispositivo del target.

Le evidenze riporteranno tutte le applicazioni utilizzate dal target in ordine cronologico.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Dati significativi

Nessuno



Modulo Calendar

Scopo

Il modulo **Calendar** registra tutte le informazioni trovate nel calendario del dispositivo del target. La versione per desktop recupera il calendario da Outlook, e altre fonti.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, WinMobile

Dati significativi

Nessuno

Modulo Call

Scopo

Il modulo **Call** a cattura l'audio e le informazioni (ora di inizio, durata, numeri di origine e destinazione della chiamata) di tutte le telefonate effettuate e ricevute dal target.

Su un dispositivo desktop, il modulo **Call** intercetta le conversazioni voce effettuate da applicazioni supportate.

Su un dispositivo mobile, il modulo **Call** intercetta tutte le chiamate.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry (solo informazioni), Symbian (senza soppressione del segnale acustico), WinMobile

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
Enable call recording	(solo mobile) Abilita la registrazione delle chiamate. Se disabilitato l'audio delle chiamate non viene registrato.
Buffer size	Dimensioni del buffer di acquisizione utilizzato per i settori audio.
Quality	Qualità audio (1=massima compressione, 10=migliore qualità).

Modulo Camera

Scopo

Il modulo **Camera** cattura un'immagine dalla fotocamera integrata.



ATTENZIONE: la cattura dell'immagine su un desktop provoca il lampeggio del led della fotocamera.

Sistemi operativi

Desktop: Windows, OS X

Mobile: iOS, Symbian (solo fotocamera frontale, quando disponibile), WinMobile

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
--------------	--------------------

Quality	Qualità immagine (1=massima compressione, 10=migliore qualità).
----------------	---

Modulo Chat

Scopo

Il modulo **Chat** registra tutte le sessioni di chat del target. Ogni messaggio viene catturato come una evidenza distinta.



IMPORTANTE: su Android le chat vengono catturate solo se il dispositivo ha ottenuto i privilegi di root e se nella compilazione del vettore è stata abilitata l'opzione Require Administrative Privilege.



IMPORTANTE: su BlackBerry questo modulo, per attivarsi al riavvio del dispositivo, richiede che il telefono rimanga in standby (retroilluminazione spenta) per qualche minuto.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry

Dati significativi

Nessuno

Modulo Clipboard

Scopo

Il modulo **Clipboard** copia e registra il contenuto in formato testo della clipboard.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, WinMobile

Dati significativi

Nessuno

Modulo Conference

Scopo

Il modulo **Conference** chiama il numero indicato creando una teleconferenza ogni volta che il target effettua una chiamata. Il numero ricevente potrà ascoltare la conversazione in tempo reale.



IMPORTANTE: il funzionamento del modulo dipende dalle caratteristiche dell'operatore telefonico. Il target potrebbe accorgersi della teleconferenza se l'operatore telefonico inserisce un segnale acustico in attesa dell'inizio chiamata.

Sistemi operativi

Mobile: WinMobile

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
Number	numero telefonico ricevente

Modulo Crisis

Comportamento su dispositivi desktop

Il modulo **Crisis** viene abilitato (automaticamente o su una specifica azione) e riconosce le situazioni di pericolo sul dispositivo che possono far scoprire la presenza dell'agent (es.: esecuzione di uno sniffer). Può disabilitare temporaneamente la sincronizzazione e l'esecuzione di comandi.

Questo modulo aumenta il livello di occultamento nei confronti dei software di protezione.



NOTA: **Crisis** può essere abilitato di default sul dispositivo desktop per permettere all'agent di rilevare automaticamente la condizione di pericolo e agire di conseguenza (es.: diventare invisibile).

Comportamento su dispositivi mobile

Il modulo **Crisis** viene usato per sospendere il funzionamento di attività che fanno uso pesante della batteria. In base ai parametri impostati, questo modulo può disabilitare temporaneamente alcune funzioni.

Su un dispositivo mobile **Crisis** deve essere avviato manualmente da un'azione specifica (es.: avvio dell'agent con carica della batteria troppo bassa) e arrestato quando la situazione anomala termina.



NOTA: questo modulo non crea evidence.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, WinMobile

Dati significativi desktop


Sui dispositivi desktop non si dovrebbero modificare le impostazioni di default a meno di diversa indicazione da parte dei tecnici HackingTeam.

<i>Campo</i>	<i>Descrizione</i>
Inhibits Network	Abilita inibizione della sincronizzazione in presenza di processi potenzialmente pericolosi.
Network Inhibitors	Elenco dei processi che, se in esecuzione, possono impedire la sincronizzazione.
Inhibits Hooking	Abilita inibizione dell'hooking dei programmi in presenza di processi potenzialmente pericolosi.

<i>Campo</i>	<i>Descrizione</i>
Hooking inhibitors	Elenco dei processi che, se in esecuzione, possono impedire l'hooking.
Process	Processo da aggiungere all'elenco.

Dati significativi mobile

Nella versione mobile è possibile specificare le funzionalità da bloccare:

<i>Campo</i>	<i>Descrizione</i>
Mic	se selezionato, impedisce la registrazione audio Mic
Call	se selezionato, impedisce la registrazione audio Call
Camera	se selezionato, impedisce l'istantanea Camera
Position	se selezionato, impedisce l'uso del GPS
Synchronize	se selezionato, impedisce la sincronizzazione
	AVVERTENZA: operazioni altamente rischiose! Prima di impedire la sincronizzazione contattare i tecnici HackingTeam! È possibile perdere l'agent in modo permanente.



Modulo Device

Scopo

Il modulo **Device** registra le informazioni del sistema (es.: tipo di processore, memoria in uso, sistema operativo installato). Può essere utile per monitorare l'uso del disco fisso sul dispositivo e ricavare la lista delle applicazioni installate.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Dati significativi mobile

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
Retrieve application list	Oltre alle informazioni di sistema, registra l'elenco delle applicazioni installate.

Modulo File

Scopo

Il modulo **File** registra tutti i file che vengono aperti sul computer del target. Può anche catturare il file nel momento in cui viene aperto.

Sistemi operativi

Desktop: Windows, OS X

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
Include Filters	Elenco delle estensioni dei file da registrare. Specificare opzionalmente il processo per registrare il file solo quando viene eseguito o aperto da quel processo.
Exclude filters	Elenco delle estensioni dei file da non registrare. Specificare opzionalmente il processo per ignorare il file solo quando viene eseguito o aperto da quel processo.
Mask	Stringa per filtrare il processo e il file da registrare o ignorare. Sintassi <processo> <filtro> Esempio caratteristiche per inclusione "skype.exe *.*" "word.exe *John*.doc" Esempio caratteristiche per esclusione "skype.exe *.dat"
Log path and access mode	Registra il percorso del file e il tipo di accesso (es.: lettura, scrittura)
Capture file content	Se abilitato, il file viene copiato e scaricato al primo accesso.

<i>Campo</i>	<i>Descrizione</i>
Min/Max size	Minima e massima dimensione ammessa per il file da scaricare.
Newer than	Data minima di creazione del file da scaricare.

Modulo Infection



IMPORTANTE: il modulo è stato deprecato a partire dalla versione RCS 8.4.

Modulo Keylog

Scopo

Il modulo **Keylog** registra tutto quello che viene digitato dal target.



NOTA: supporta tutti i caratteri unicode via IME.

Sistemi operativi

Desktop: Windows, OS X

Mobile: iOS

Dati significativi

Nessuno

Modulo Livemic

Scopo

Il modulo **Livemic** permette di ascoltare in tempo reale eventuali conversazioni già in corso.




PRUDENZA: questo modulo è fornito "as is" e il suo utilizzo può risultare pericoloso. Ogni apparecchio si comporta diversamente. Si consiglia di fare test approfonditi prima di utilizzarlo sul campo.

Sistemi operativi

Mobile: WinMobile

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
Number	Numero del telefono usato per l'ascolto. Deve comprendere il prefisso internazionale, es.: "+341234567890".
	 ATTENZIONE: non nascondere l'ID del chiamante e disabilitare il microfono mentre si ascolta la conversazione.

Modulo Messages

Scopo

Il modulo **Messages** registra tutti i messaggi ricevuti o inviati dal target. Questo modulo cattura:

- e-mail
- SMS (solo Mobile)
- MMS (solo Mobile)

Sistemi operativi

Desktop: Windows

Mobile:

<i>Sistemi operativi</i>	<i>e-mail</i>	<i>MMS</i>	<i>SMS</i>
Android	x (*)	-	x
BlackBerry	x	-	x
iOS	-	x	x
WinMobile	x	x	x



IMPORTANTE (*): su Android vengono catturate solo le e-mail di Gmail e solo se il telefono ha ottenuto i privilegi di root e se nella compilazione del vettore è stata abilitata l'opzione Require Administrative Privilege.

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
--------------	--------------------

Abilitato	Abilita la registrazione.
------------------	---------------------------

From	Registra i messaggi a partire dalla data indicata.
-------------	--

To	Registra i messaggi fino alla data indicata.
-----------	--

Max size	Dimensione massima del messaggio da registrare.
-----------------	---



Modulo Mic

Scopo

Il modulo **Mic** registra i suoni circostanti utilizzando il microfono del dispositivo.

Piattaforme

Desktop: Windows, OS X




Mobile: Android (disabilitato durante le chiamate), BlackBerry (disabilitato durante le chiamate), iOS, Symbian (disabilitato durante le chiamate), WinMobile



IMPORTANTE: non attivare il microfono per registrare chiamate dati (es.: Skype, Viber) senza aver fatto test approfonditi sullo stesso modello di telefono con la stessa versione di sistema operativo. Si rischia di disabilitare l'audio sul client, rendendo la relativa applicazione inutilizzabile.

Dati significativi

Di seguito la descrizione dei dati:

Campo	Descrizione
Silence between voices	<p>Numero massimo di secondi di silenzio ammessi nella registrazione. Superato il periodo impostato, l'agent sospende la registrazione e si riavvia alla ricezione di nuovi suoni.</p> <p> AVVERTENZA: se il valore è troppo basso la registrazione escluderà tutti i silenzi e si otterrà una conversazione continua senza pause. Se il valore è troppo alto la registrazione includerà tutti i silenzi e si otterrà una conversazione molto lunga.</p>
Voice recognition	<p> NOTA: non supportata da iOS, BlackBerry, Android e Symbian.</p> <p>Valore per identificare la voce umana ed escludere dalla registrazione eventuali rumori di fondo.</p> <p> AVVERTENZA: 0.2-0.28 è l'intervallo suggerito per identificare la voce umana. Valori più alti si adattano meglio alle voci femminili ma causano la registrazione di maggiori rumori di fondo.</p>
Autosense	<p>Se abilitato, l'agent cerca di modificare le impostazioni del mixer audio (attiva/disattiva microfono, selezione linea e volume) per ottimizzare la qualità della registrazione audio, evitando volumi troppo bassi e o interruzioni nella registrazione.</p>

Modulo Mouse

Scopo

Il modulo **Mouse** cattura a ogni clic l'immagine di una piccola area dello schermo attorno al puntatore.

Utile per intercettare tastiere virtuali utilizzate per evitare le intercettazioni dei tasti della tastiera. Vedi "[Modulo Keylog](#)" a pagina 131.

Sistemi operativi

Desktop: Windows, OS X

Dati significativi

Di seguito la descrizione dei dati:

Campo *Descrizione*

Width dimensioni immagine catturata**Height** **Modulo Password****Scopo**

Il modulo **Password** registra tutte le password salvate nei vari account degli utenti. Vengono raccolte le password salvate dai browser, dagli Instant Messenger, e dai client web-mail.

Sistemi operativi**Desktop:** Windows**Dati significativi**

Nessuno

 **Modulo Position****Scopo**

Il modulo **Position** registra la posizione del dispositivo utilizzando il sistema GPS, la cella GSM o le informazioni WiFi.

Sistemi operativi**Desktop:** (solo WiFi) Windows, OS X**Mobile:** Android, BlackBerry, Symbian, WinMobile**Dati significativi mobile**

Di seguito la descrizione dei dati:

Campo *Descrizione*

GPS Ricava la posizione dalle informazioni GPS.**Cell** Ricava la posizione dalle informazioni della cella GSM o CDMA.**Wifi** Ricava la posizione dal BSSID delle stazioni WiFi.

Modulo Screenshot

Scopo

Il modulo **Screenshot** cattura un'immagine dello schermo del dispositivo del target.



IMPORTANTE: su Android gli screenshot vengono catturati solo se il telefono ha ottenuto i privilegi di root e se nella compilazione del vettore è stata abilitata l'opzione Require Administrative Privilege.


Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Dati significativi

Di seguito la descrizione dei dati:

<i>Campo</i>	<i>Descrizione</i>
Quality	Qualità finale dell'immagine catturata. Low: immagini di qualità peggiore, con massima compressione High: immagini di qualità migliore, con minima compressione  Suggerimento: lasciare il valore di default.
Only foreground window	(solo Desktop) Cattura un'istantanea della finestra in primo piano.

Modulo Url

Scopo

Il modulo **Url** registra i nome delle pagine visitate dal browser target.

Sistemi operativi

Desktop: Windows, OS X

Mobile: BlackBerry, iOS, Symbian, WinMobile.



IMPORTANTE: (BlackBerry) il modulo richiede che il telefono resti in standby (retroilluminazione spenta) per qualche minuto, per potersi attivare al riavvio del dispositivo.

Dati significativi

Nessuno

Appendice: vettori di installazione

Presentazione

Introduzione

Un agent è un complesso insieme di eventi, azioni, moduli e vettori di installazione. Qui sono elencati i singoli vettori di installazione con la descrizione dettagliata dei parametri disponibili nella configurazione avanzata.

Contenuti

Questa sezione include i seguenti argomenti:

Ottenere un certificato per il Code Signing	139
Elenco dei vettori di installazione	139
Vettore Exploit (desktop)	140
Vettore Melted Application	141
Vettore Network Injection	142
Vettore Offline Installation	142
Vettore Silent Installer	143
Vettore U3 Installation	144
Vettore Exploit (mobile)	145
Vettore Installation Package	146
Vettore Local Installation	148
Vettore QR Code/Web link	149
Vettore WAP Push Message	150
Ottenere un certificato Symbian	151

Ottenere un certificato per il Code Signing

Introduzione

Per poter utilizzare la funzione di firma del codice disponibile in fase di compilazione di alcuni vettori è necessario acquistare un certificato per Code Signing emesso da una Certification Authority riconosciuta.

La maggior parte delle Certification Authority offre certificati per Code Signing, fra cui le seguenti:

- Verisign (<http://www.verisign.com>)
- Thawte (<http://www.thawte.com>)
- GoDaddy (<http://www.godaddy.com>)

Installazione del certificato Code Signing

Sul sistema Backend, dalla cartella C:\RCS\DB\bin digitare il seguente comando:

```
> rcs-db-config --sign-cert <file certificato> --sign-pass <password  
certificato>
```

Risultato: il certificato viene installato nel sistema e da questo momento è possibile utilizzare la funzione di firma.

Elenco dei vettori di installazione

Sistemi operativi supportati dagli agent

Di seguito i sistemi operativi supportati per i vari dispositivi desktop e mobile:

<i>Dispositivo</i>	<i>Sistema Operativo</i>
Desktop	<ul style="list-style-type: none">• Windows• OS X
Mobile	<ul style="list-style-type: none">• Android• BlackBerry• Windows Mobile• Symbian• IOS

Di seguito l'elenco dei vettori:

Installation Vector	Dispositivo	Descrizione
Applet Web	Desktop	<i>Deprecata a partire dalla versione RCS 8.4.</i>
Exploit	Desktop, Mobile	<i>Inserisce l'agent in un qualsiasi documento (il formato del documento può dipendere dagli exploit disponibili).</i>
Installation Package	Mobile	<i>Crea un file autoinstallante con l'agent.</i>
Local Installation	Mobile	<i>Installa l'agent sul dispositivo del target o tramite USB o tramite memory card SD/MMC.</i>
Melted Application	Desktop	<i>Inserisce l'agent in un qualsiasi file eseguibile.</i>
Network Injection	Desktop	<i>Rimanda alla pagina di creazione delle regole di injection. Vedi "Gestione dei Network Injector" a pagina 71 .</i>
Offline Installation	Desktop	<i>Crea un file ISO per la generazione di un CD/DVD/USB di avvio da utilizzare su un computer spento o ibernato.</i>
QR Code/Web Link	Mobile	<i>Genera un codice QR per siti o stampati, che se il target fotograferà, installerà l'agent.</i>
Silent Installer	Desktop	<i>Crea un file eseguibile vuoto che, quando eseguito sul dispositivo del target, installa l'agent.</i>
U3 Installation	Desktop	<i>Crea un pacchetto da installare su chiave U3. La chiave U3 installa l'agent automaticamente al suo inserimento sul dispositivo del target.</i>
Wap Push Message	Mobile	<i>Invia un messaggio WAP, che se il target accetterà, installerà l'agent.</i>

Vettore Exploit (desktop)

Scopo

La compilazione crea un installer, che una volta aperto sul dispositivo del target, sfrutta la vulnerabilità di un programma specifico. In base al tipo di Exploit possono anche esserci comportamenti diversi (es.: il programma in esecuzione si interrompe).

Installazione

L'installer viene creato e automaticamente viene salvato nella cartella C:\RCS\Collector\public il pacchetto di file utili. Questi file potranno essere usati in molti tipi di attacchi (es.: tramite collegamento da un sito Web).

Eliminazione file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, vedi "[Gestione dei frontend](#)" a pagina 67.

Sistemi operativi

OS X, Windows

Parametri

<i>Nome</i>	<i>Descrizione</i>
File type	Tipo di file che verrà infettato (es.: .PDF).
Choose an Exploit	Nome per esteso dell'applicativo usato dal target per aprire il file (es.: Adobe Acrobat Reader 10).
URL Document	URL che punta al pacchetto di installazione dell'agent desiderato.
...	URL: collegamento a un Anonymizer dove l'installer è stato salvato. Document: per la selezione del file da infettare.

Vettore Melted Application

Scopo

In compilazione modifica un eseguibile esistente inserendovi un agent.



I componenti dall'agent sono criptati per evitare eventuali attacchi di reverse engineering.

Sistemi operativi

Android, OS X, Windows

Parametri

<i>Nome</i>	<i>Descrizione</i>
Require administrative privileges	Durante l'installazione dell'agent saranno necessari i privilegi di amministratore.

<i>Nome</i>	<i>Descrizione</i>
Application to be used as dropper	<p>File eseguibile a cui inserire aggiungere l'agent. Il tipo di file è diverso in base al sistema operativo:</p> <ul style="list-style-type: none">• Android: applicazione APK di terze parti.  IMPORTANTE: fare un test dell'applicazione finale. Infatti alcune applicazioni eseguono dei controlli di sicurezza addizionali a runtime.• OS X: file MacOS compresso .app. È quindi necessario comprimere l'applicazione (è una cartella) con il comando zip dalla console Terminal.app.  IMPORTANTE: non utilizzare la voce di menu Compress dall'applicazione Finder.• Windows: qualsiasi file EXE.

Vettore Network Injection

Scopo

La pagina conduce direttamente alla funzione Network Injector della sezione System.

Sistemi operativi

-

Parametri

-

Vettore Offline Installation

Scopo

La compilazione crea un autoinstallante ISO da copiare su un CD o su una USB Thumbdrive (solo Windows).

Inserire il CD o la chiave USB e quindi accendere il computer del target. Fare il boot dal supporto inserito e attendere la comparsa di un menu. L'infezione può essere fatta in modo selettivo scegliendo dall'elenco degli utenti disponibili sul sistema.

Sistemi operativi

Multipiattaforma.

Parametri

<i>Nome</i>	<i>Descrizione</i>
Bootable CD/DVD	Crea un autoinstallante ISO per CD o DVD.
Bootable USB drive	(solo Windows) Crea un autoinstallante ISO per chiave USB.
Dump Mask	<p>Estrae automaticamente i documenti appartenenti ad un determinato utente. I documenti potranno poi essere salvati su una periferica USB, per poi essere importati nel database di RCS in un secondo tempo.</p> <p>Sono disponibili tre opzioni per la cattura dei documenti:</p> <ul style="list-style-type: none"> • Documents: documenti MS Office, PDF e file di testo • Images: foto ed immagini • Custom: seleziona le estensioni dei file da catturare, separate dal carattere pipe (" ").

Vettore Silent Installer

Scopo




La compilazione crea un eseguibile che installa l'agent in modo silente. Nessun output è visibile sul dispositivo.

Sistemi operativi

OS X, Windows

Parametri

<i>Nome</i>	<i>Descrizione</i>
Require administrative privileges	<p>Durante l'installazione dell'agent sono necessari i privilegi di amministratore. I comportamenti sono diversi in base al sistema operativo:</p> <ul style="list-style-type: none"> • OS X: se selezionato, l'agent richiederà la password di root ingannando il dialogo di autenticazione. Se non selezionato, alcuni moduli non funzioneranno. • Windows: se selezionato, saranno richiesti i privilegi di amministratore per procedere con l'installazione dell'agent. L'opzione deve essere selezionata quando si è diretti a dispositivi Windows Vista, quando l'utente è un membro del gruppo Amministratori. In tutti gli altri casi lasciare l'opzione non selezionata.

<i>Nome</i>	<i>Descrizione</i>
Include 64bit support (100 KiB)	(solo Windows) L'eseguibile supporta macchine a 64bit (la sua dimensione aumenterà di 100 KiB).
Include audio codec (200 KiB)	(solo Windows) L'eseguibile include algoritmo codec (la sua dimensione aumenterà di 200 KiB).  NOTA: anche se questa opzione non è selezionata, alla prima sincronizzazione l'agent scarica il codec audio necessario ai tipi di evidenze da acquisire.
Use the certificate to sign the dropper	Firma l'eseguibile utilizzando il certificato digitale. La firma digitale può elevare notevolmente il livello di invisibilità agli antivirus.  IMPORTANTE: per utilizzare questa funzione seguire la procedura di ottenimento del certificato. Vedi " Ottenerne un certificato per il Code Signing " a pagina139 .  Richiede assistenza: per maggiori informazioni su come ottenere e configurare un certificato digitale contattare il personale di supporto di HackingTeam.



NOTA: 1 KiB è 1024 byte.

Vettore U3 Installation

Scopo

La compilazione crea un autoinstallante ISO da scrivere su una chiave U3 (SanDisk) tramite il programma **U3 customizer** (il software può essere scaricato da Internet).

Quando la chiave è inserita nel dispositivo compare direttamente un menu (nessun disco USB viene visto automaticamente) per l'installazione degli agent.

Sistemi operativi

Windows

Parametri

Nessuno.

Vettore Exploit (mobile)

Scopo

La compilazione crea un installer che una volta eseguito sul dispositivo del target, lo infetta. In base al tipo di Exploit possono anche esserci comportamenti diversi (es.: il programma in esecuzione si interrompe).

Installazione

L'installer deve essere copiato manualmente sul dispositivo e occorre eseguire install.sh dalla cartella copiata.



IMPORTANTE: il dispositivo deve essere sbloccato.

Il pacchetto di file utili viene copiato automaticamente nella cartella C:\RCS\Collector\public. Questi file potranno essere usati in molti tipi di attacchi (es.: tramite collegamento da un sito Web).

Eliminazione file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, vedi "[Gestione dei frontend](#)" a pagina 67.

Esempio comandi per copiare installer nel dispositivo 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
```

Sistemi operativi

iOS

Parametri

<i>Nome</i>	<i>Descrizione</i>
File type	Tipo di file che verrà infettato (es.: .PDF).
Choose an Exploit	Nome per esteso dell'applicativo usato dal target per aprire il file (es.: Adobe Acrobat Reader 10).

<i>Nome</i>	<i>Descrizione</i>
URL	Parametri che identificano il file da infettare.
Document	URL: collegamento a un Anonymizer dove l'installer è stato salvato. .
...	Document: seleziona il file da infettare.

Vettore Installation Package

Scopo

La compilazione crea un eseguibile che installa l'agent in modo silente.

L'eseguibile può essere caricato sul dispositivo con uno qualsiasi di questi metodi:

- download da URL,
- link tramite SMS o MMS,
- (solo Windows mobile) copia diretta sulla scheda SD,
- direttamente da computer via cavo USB

Note per sistemi operativi Android (preparazione del vettore)

Se il vettore contiene i moduli Screenshot, Chat e Messages è necessario abilitare l'opzione **Require Administrative Privilege**.

La compilazione genera due vettori APK (Android Application Package File):

- <application name>.v2.apk: vettore per Android 2.x
- <application name>.default.apk: vettore per Android 3.x e 4.x

Note per sistemi operativi Android (installazione)

Di seguito la procedura per l'installazione:

Passo Azione


- 1** Sul dispositivo abilitare l'opzione **Origini sconosciute** nelle impostazioni del dispositivo (tipicamente sotto **Impostazioni, Applicazioni**). Terminata l'installazione è possibile disabilitare nuovamente l'opzione.



NOTA: se non si abilita questa opzione, durante l'installazione compare una richiesta di autorizzazione a installare un'applicazione che non appartiene all'Android Market.

- 2** Se il vettore contiene i moduli Screenshot, Chat e Messages, è necessario ottenere i privilegi di root del dispositivo. Altrimenti i moduli non potranno funzionare.
- 3** Sul dispositivo selezionare ed eseguire il vettore APK appropriato.

Passo Azione

- 4 Durante l'installazione del vettore APK, accettare i permessi richiesti dall'agent.
Per Android 3.x e 4.x, fare clic sul pulsante **Apri** per avviare il vettore, altrimenti il vettore non sarà installato.
 **IMPORTANTE: il vettore APK di default per Android 3.x e 4.x si mostra come una normale applicazione denominata DeviceInfo, che mostra le informazioni del dispositivo.**

- 5 Durante l'esecuzione del vettore, se è stata abilitata l'opzione **Require Administrative Privilege**, compare una richiesta per ottenere i privilegi.


Note per sistemi operativi Windows Mobile

È possibile specificare un installer CAB esistente per aggiungervi l'agent.

Se non viene specificato un CAB, il sistema utilizzerà un CAB di default che non installa nulla.

Note per sistemi operativi BlackBerry

Per permettere il download dell'agent da parte di un BlackBerry estrarre i contenuti del file zip creato su un server Web cui il dispositivo possa accedere.

-  **NOTA:** il server Web deve correttamente supportare i tipi MIME per i file .jad e .cod, .text/vnd.sun.j2me.app-descriptor e application/vnd.rim.cod. rispettivamente. La cartella public del Collector già esegue questa funzione.

Una volta che l'installer viene eseguito sul dispositivo, accettare i permessi richiesti dall'agent.

Note per sistemi operativi Symbian

-  **IMPORTANTE:** per i Symbian seguire la procedura di ottenimento del certificato. Vedi ["Ottenere un certificato Symbian" a pagina 151](#).

Sistemi operativi

Android, BlackBerry, iOS, Symbian, WinMobile

Parametri Android, iOS, WinMobile

<i>Nome</i>	<i>Descrizione</i>
Application name	Nome dell'applicazione (visibile al target)

<i>Nome</i>	<i>Descrizione</i>
Require Administrative Privilege	Opzione necessaria per far funzionare i moduli Screenshot, Chat e Messages

Parametri BlackBerry

<i>Nome</i>	<i>Descrizione</i>
Application name	Nome dell'installer (visibile al target)
Name	(solo BlackBerry) Dati dell'applicazione usati per "nascondere" l'agent.
Description	
Vendor	
Version	

Parametri Symbian

<i>Nome</i>	<i>Descrizione</i>
Application name	Nome dell'applicazione (visibile al target)
Certificate bound to phone IMEI	Certificato per il dispositivo.
S60 Edition	Versione sistema operativo.
Symbian configuration	Parametri: <ul style="list-style-type: none"> • UID 1-6: elenco degli UID legati al certificato • Key: file di chiave

Vettore Local Installation

Scopo

La compilazione installa l'agent direttamente sul dispositivo BlackBerry del target, oppure crea una cartella sulla scheda SD da inserire nel dispositivo.



IMPORTANTE: per completare con successo l'installazione su dispositivo BlackBerry, su un computer Windows deve essere installata l'applicazione Blackberry Desktop Software. La console produrrà un file .zip contenente tutti i file necessari ad infettare il BlackBerry collegato. Copiare il file .zip sul computer Windows (se necessario) e poi decomprimerlo. Collegare il BlackBerry al PC usando un cavo USB, poi eseguire il file install.bat. Se il BlackBerry è protetto da PIN, inserire il PIN richiesto.

Sistemi operativi

BlackBerry, WinMobile

Parametri

Nessuno.

Vettore QR Code/Web link

Scopo

La compilazione crea un QR Code da inserire in un qualsiasi sito web o documento cartaceo. Non appena il target cattura il codice QR, l'agent viene installato nel suo dispositivo.

Funzionamento

Non appena il target si connette all'Anonymizer chiedendo l'installer, il Collector scarica l'installer adatto al sistema operativo del dispositivo del target dalla cartella C:\RCS\Collector\public.

Eliminazione file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, vedi "[Gestione dei frontend](#)" a pagina 67.

Sistemi operativi

Android, BlackBerry, Symbian, WinMobile



NOTA: se il sistema operativo del target è sconosciuto, usare la versione Multiplatforma.

Parametri

<i>Nome</i>	<i>Descrizione</i>
Application name	Nome dell'installer (visibile al target).
URL	Collegamento a un Anonymizer dove l'installer è stato salvato.
Name	(solo BlackBerry) Dati dell'applicazione usati per "nascondere" l'agent.
Description	
Vendor	
Version	

<i>Nome</i>	<i>Descrizione</i>
Certificate bound to phone IMEI	(solo Symbian) Certificato per il dispositivo.
S60 Edition	(solo Symbian) Versione sistema operativo.

Vettore WAP Push Message

Scopo

Creare un messaggio WAP-Push che invita il target a visitare un collegamento.

Funzionamento

Invia un messaggio WAP-Push contenente o testo o il link all'installer dell'agent. Se il messaggio è accettato sul dispositivo target, l'agent sarà installato.



IMPORTANTE: per i Symbian seguire la procedura di ottenimento del certificato. Vedi *"Ottenere un certificato Symbian"* alla pagina successiva .

Installazione

La compilazione crea un installer e automaticamente salva il pacchetto dei file utili nella cartella C:\RCS\Collector\public.

Eliminazione file non più utilizzati

I pacchetti salvati nella cartella C:\RCS\Collector\public possono essere eliminati con la funzione **File Manager**, vedi *"Gestione dei frontend"* a pagina67 .

Sistemi operativi

Android, BlackBerry, Symbian, WinMobile



NOTA: se il sistema operativo del target è sconosciuto, usare la versione Multipiattaforma. Questa crea più installer, uno per piattaforma supportata e li salva nella cartella Public del Collector. Non appena il target si connette all'Anonymizer chiedendo l'installer, il Collector scarica l'installer adatto al sistema operativo del dispositivo del target.

Parametri

<i>Nome</i>	<i>Descrizione</i>
Application name	Nome dell'installer (visibile al target)
Phone Number	Numero telefonico del target, compreso di prefisso internazionale.
URL	Collegamento a un Anonymizer dove l'installer è stato salvato. Se si è salvato il pacchetto su un altro sito Web, specificarne l'URL.
Service Type	Tipo di servizio richiesto: <ul style="list-style-type: none">• Loading: il telefono target è reindirizzato automaticamente alla risorsa indicata in URL. In base alle impostazioni di sicurezza del telefono, l'applicazione può essere installata automaticamente o può apparire un messaggio per l'utente su come procedere.• Indication: sarà visualizzato un messaggio con un testo specifico, per richiedere all'utente come proseguire.• SMS: manda il link preceduto dal testo specificato
Text	(solo per Indication e SMS) Testo per l'utente target.
Name	(solo BlackBerry) Dati dell'applicazione usati per "nascondere" l'agent.
Description	
Vendor	
Version	
Certificate bound to phone IMEI	(solo Symbian) Certificato per il dispositivo.
S60 Edition	(solo Symbian) Versione sistema operativo.

Ottenere un certificato Symbian

Introduzione

A partire dalla versione Symbian OS 9.1, viene richiesto un Symbian Development Certificate per installare ed eseguire un agent su un dispositivo Symbian. Attualmente, ogni certificato emesso supporta fino a 1000 IMEI e fino a 17 funzionalità.

Sequenza consigliata

Completare i seguenti passi per richiedere un certificato:

Passo Azione

- 1 Ottenere l'ID dell'editore
- 2 Creare le chiavi Certificate Public e Private
- 3 Creare il Development Certificate

Ottenere l'ID del Editore (voi)

Seguire la seguente procedura:

Passo Azione

- 1 Acquistare il certificato in TrustCenter (https://www.trustcenter.de/en/products/tc_publisher_id_for_symbian.htm).
NOTA: il certificato deve essere di tipo "Developer Certificate" e non "Test House Certificate".
- 2 Dopo l'acquisto del certificato (valido un anno), occorre fornire la seguente documentazione del richiedente:
 - Una copia della registrazione ufficiale della società richiedente (fornita dalle autorità competenti) o equivalente.
 - Una richiesta scritta firmata da persona autorizzata della società.
 - Una copia firmata dal richiedente della carta d'identità o del passaporto (con foto e firma).

Creare le chiavi Certificate Public e Private

Seguire la seguente procedura:

Passo Azione

- 1 Dopo qualche giorno dalla consegna dei documenti (solitamente entro quattro giorni) si riceve da TrustCenter una e-mail di conferma con il link al certificato e l'ID dell'editore.
- 2 Salvare il certificato sul computer.
- 3 Scaricare e installare lo strumento TC- Converter da: <http://wiki.forum.nokia.com/index.php/File:TC-ConvertP12.zip>
- 4 Copiare YourDeveloperCert.p12 nella cartella di TC-Converter.
- 5 Eseguire "tcp12p8 YourDeveloperCert.p12 YourPasswordtc.keytc.cer": le chiavi Tc.key e il certificato Tc.cer vengono creati.

Creare il Development Certificate


Dopo aver creato le diverse chiavi, è necessario creare il certificato con i numeri IMEI che interessano. Questa procedura può essere eseguita più volte mano a mano che serve aggiungere nuovi numeri IMEI.



NOTA: per approfondimenti vedi http://www.developer.nokia.com/Community/Wiki/User_guide:Symbian_Signed.

Seguire la seguente procedura:

Passo Azione

- 1 Creare un account in <https://www.symbiansigned.com>
 - 2
 - Fare clic su **My Dashboard** e selezionare la scheda **My Profile**.
 - Verificare che Country sia valorizzato con lo stesso dato presente nell'ID dell'editore.
 - Fare clic su **Verify Account**
 - 3
 - Scaricare il file .sys
 - Firmare il file .sys con il file .cer e .key corrispondenti allo stesso ID dell'editore, usando questo comando:`signsis symbian_signed_account_verification_sis.sis signed.sis tc.cer tc.key`
 - Caricare il file .sis firmato
 - 4 Fare di nuovo la login nell'accout creato
 - 5
 - Fare clic su **My Dashboard** e selezionare la scheda **Manage UIDs**.
 - Richiedere sei UID (entro il range protetto) e lasciare vuoti gli altri campi.
 - Ottenuti gli UID selezionare la scheda **Development Certificate**
 - Inserire i numeri IMEI dei dispositivi (per ottenere il numero digitare `*#06#*` oppure leggere il codice dal vano batteria)
 - Fare clic su **Download Certificate**.
-  **IMPORTANTE: non caricare l'agent RCS .sis nel sito symbian firmato. Per ogni nuovo target inserire il nuovo numero IMEI e scaricare di nuovo il Development Certificate. Non scaricare nuovamente il file .sis.**
- Usare il Development Certificate per firmare gli agent RCS per Symbian.

]HackingTeam[

RCS 8.4 Manuale del tecnico
Manuale del tecnico 1.4 LUG-2013
© COPYRIGHT 2013
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
