

RCS 8.0

The hacking suite for governmental interception

Manuale del tecnico

Proprietà delle informazioni

© COPYRIGHT 2012, 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 tipografi ci 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 5](#_Toc321318865)

[Introduzione a questa Guida 8](#_Toc321318866)

[Novità della guida 8](#_Toc321318867)

[Documentazione fornita 8](#_Toc321318868)

[Convenzioni tipografiche per le segnalazioni 2](#_Toc321318869)

[Convenzioni tipografiche per la formattazione 2](#_Toc321318870)

[Destinatari del prodotto e di questa guida 3](#_Toc321318871)

[Dati di identificazione dell'autore del software 4](#_Toc321318872)

[RCS (Remote Control System) 4](#_Toc321318873)

[Differenze rispetto alle versioni precedenti 4](#_Toc321318874)

[RCS Console per il Tecnico 5](#_Toc321318875)

[Ruolo del Tecnico 5](#_Toc321318876)

[Funzioni abilitate per il Tecnico 6](#_Toc321318877)

[Avvio di RCS Console 6](#_Toc321318878)

[Come si presenta la pagina di login 6](#_Toc321318879)

[Accedere a RCS Console 7](#_Toc321318880)

[Descrizione della homepage 7](#_Toc321318881)

[Introduzione 7](#_Toc321318882)

[Come si presenta 7](#_Toc321318883)

[Elementi e azioni comuni dell'interfaccia 8](#_Toc321318884)

[Come si presenta RCS Console 8](#_Toc321318885)

[Azioni sempre disponibili sull'interfaccia 13](#_Toc321318886)

[Procedure del Tecnico 15](#_Toc321318887)

[Introduzione 15](#_Toc321318888)

[Procedure 15](#_Toc321318889)

[I target 16](#_Toc321318890)

[Pagina del target 17](#_Toc321318891)

[Scopo 17](#_Toc321318892)

[Cose da sapere sulle factory e sugli agent 20](#_Toc321318893)

[Modalità di infezione 20](#_Toc321318894)

[Componenti della strategia di infezione 20](#_Toc321318895)

[Le factory 20](#_Toc321318896)

[I vettori di installazione 21](#_Toc321318897)

[Gli agent 21](#_Toc321318898)

[I moduli per l'acquisizione dei dati 21](#_Toc321318899)

[Dati della pagina target 22](#_Toc321318900)

[Visualizzazione a icone 22](#_Toc321318901)

[Visualizzazione a tabella 22](#_Toc321318902)

[Compilazione di una factory 23](#_Toc321318903)

[Scopo 23](#_Toc321318904)

[Passi successivi 23](#_Toc321318905)

[Gli agent 25](#_Toc321318906)

[Pagina dell'agent 25](#_Toc321318907)

[Scopo 25](#_Toc321318908)

[Cose da sapere sugli agent 27](#_Toc321318909)

[Sincronizzazione di un agent 27](#_Toc321318910)

[Prima sincronizzazione dell'agent 27](#_Toc321318911)

[Agent offline e online 27](#_Toc321318912)

[Disabilitazione temporanea di un agent 28](#_Toc321318913)

[Collaudo di un agent 28](#_Toc321318914)

[Configurazione di un agent 28](#_Toc321318915)

[Dati dello storico configurazioni di un agent 29](#_Toc321318916)

[Dati dello storico di un agent 30](#_Toc321318917)

[Trasferimento file da/a il target 30](#_Toc321318918)

[Scopo 30](#_Toc321318919)

[Factory e agent: configurazione base 31](#_Toc321318920)

[Configurazione base di una factory o di un agent 32](#_Toc321318921)

[Scopo 32](#_Toc321318922)

[Passi successivi 32](#_Toc321318923)

[Cose da sapere sulla configurazione base 34](#_Toc321318924)

[Configurazione base 34](#_Toc321318925)

[Dati della configurazione base 34](#_Toc321318926)

[Factory e agent: configurazione avanzata 35](#_Toc321318927)

[Configurazione avanzata di una factory o di un agent 36](#_Toc321318928)

[Scopo 36](#_Toc321318929)

[Passi successivi 36](#_Toc321318930)

[Cose da sapere sulla configurazione avanzata 39](#_Toc321318931)

[Configurazione avanzata 39](#_Toc321318932)

[Componenti della configurazione avanzata 40](#_Toc321318933)

[Lettura delle sequenze 40](#_Toc321318934)

[Eventi 41](#_Toc321318935)

[Azioni 41](#_Toc321318936)

[Relazioni tra azioni e moduli 42](#_Toc321318937)

[Relazioni tra azioni e eventi 42](#_Toc321318938)

[Moduli 42](#_Toc321318939)

[Dati globali dell'agent 43](#_Toc321318940)

[Gestione dei frontend 44](#_Toc321318941)

[Scopo della funzione 44](#_Toc321318942)

[I Network Injector 45](#_Toc321318943)

[Gestione dei Network Injector 45](#_Toc321318944)

[Scopo 46](#_Toc321318945)

[Cosa è possibile fare 46](#_Toc321318946)

[Cose da sapere su Network Injector e le sue regole 48](#_Toc321318947)

[Introduzione 48](#_Toc321318948)

[Tipi di risorse infettabili 48](#_Toc321318949)

[Come creare una regola 48](#_Toc321318950)

[Cosa succede quando si abilita/disabilita una regola 48](#_Toc321318951)

[Cosa succede quando si applica una regola 48](#_Toc321318952)

[Dati delle regole di injection 48](#_Toc321318953)

[Appendice: eventi, azioni, moduli e vettori 96](#_Toc321318954)

[Elenco degli eventi 96](#_Toc321318955)

[Elenco dei moduli 98](#_Toc321318956)

[Elenco delle sotto-azioni 100](#_Toc321318957)

[Elenco dei vettori di installazione 104](#_Toc321318958)

[Sistemi operativi supportati dagli agent 104](#_Toc321318959)

Glossario dei termini

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

Access Switch

Dispositivo di rete o nodo interno di rete che si occupa di commutazione a livello di indirizzamento e instradamento all'interno di reti locali attraverso indirizzi MAC.

Accounting

Sezione di RCS Console dedicata alla gestione degli accessi a RCS.

Agent

Sonde software installate presso le utenze o sorgenti dati di cui è stato disposto il controllo. Sono deputate a intercettare i dati e comunicarli a un Anonymizer o, in assenza di questo, direttamente al Collector.

Alerting

Sezione di RCS 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 intercettazioni in essere, gli obiettivi delle intercettazioni e il tipo di dati da rilevare.

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 all'analisi dei dati raccolti durante l'attività di intercettazione.

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 di RCS Console dedicata al controllo delle azioni dei vari utenti.

avvisi da Evidence

segnalazioni che generano Email verso gli analisti che informano quando è stata intercettata una prova importante (Evidence)

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 dal DSLAM verso la rete dell'ISP.

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.

Dashboard

Sezione di RCS Console dedicata all'Analista. Qui è possibile inserire Operation, Target e Agent che si vogliono tenere sotto controllo.

DSLAM

(Digital Subscriber Line Access Multiplexer) apparato elettronico di trasmissione di rete che esplica le funzioni di multiplazione/demultiplazione di linea di accesso numerica e modulazione da e verso il doppino dell'utente finale, cioè nella rete di accesso.

Evidence

Dati di una intercettazione che costituiscono una prova. Il formato dipende dal tipo di Agent installato (es.: immagine).

Factory

È un template per la configurazione e compilazione degli Agent in base al vettore di infezione scelto.

front end

Ambiente destinato a comunicare con la rete esterna, raccogliere le informazioni e controllare e configurare le entità remote di intercettazione. In architettura distribuita include il Collector e il Network Controller.

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.

Monitor

Sezione di RCS Console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

Network Controller

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

Network Injector

Componente hardware. Può essere installato presso un ISP (Internet Service Provider) in versione fissa, oppure può essere collegato ad un hotspot WiFi o ad una rete wired locale in versione portatile.

Network Injector Appliance

Versione appliance di Network Injector. Unità rack per installazione presso ISP. Cfr.: Tactical Network Injector.

Operation

Indagine composta da uno o più Target, a loro volta attaccati da uno o più Agent tramite uno o più vettori di infezione.

RCS

(Remote Control System) il sistema di monitoraggio in oggetto.

RCS Console

Software dedicato all'interazione con RCS Server.

RCS Server

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

regole di allerta

Regole che permettono di essere avvisati all'arrivo di prove particolari.

Regole di injection

Parametri che permettono la selezione del traffico HTTP originato dai dispositivi del Target e la successiva infezione delle risorse visualizzate e scaricate.

Sequenze di intercettazione

Insieme di eventi, azioni e moduli di registrazione complessi che costituiscono la configurazione avanzata di un Agent.

SSH

(Secure SHell) protocollo di comunicazione per stabilire una sessione remota cifrata.

System

Sezione di RCS Console dedicata alla gestione del sistema.

Tactical Network Injector

Versione portatile di Nework 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 da sottoporre a intercettazione attiva o passiva.

Tecnico

Colui che su mandato dell'Amministratore crea e gestisce gli Agent di intercettazione.

VPS

(Virtual Private Server) server remoto su cui installare l'Anonymizer. Disponibili come servizio a noleggio.

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 injection in 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

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

| Data rilascio | Codice | Versione software | Descrizione |
| --- | --- | --- | --- |
| 16 Aprile 2012 | Manuale del tecnico  1.0 FEB/2012  Technician's Guide  1.0 FEB/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 | Manuale dell'amministratore di sistema - 1.0 FEB/2012 | PDF |
| Manuale dell'amministratore | Amministratori | Manuale dell'amministratore - 1.0 FEB/2012 | PDF |
| Manuale del tecnico (questo manuale) | Tecnici | Manuale del tecnico - 1.0 FEB/2012 | PDF |
| Manuale dell'analista | Analisti | Manuale dell'analista - 1.0 FEB/2012 | 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.

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:

| Esempio | Stile | Descrizione |
| --- | --- | --- |
| Vedi "Dati degli utenti" | corsivo | 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. |
| <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 Aggiungi."  "Selezionare il menu File, Archivia dati" | 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. | Tecnico di reti esperto |
| Amministratore | Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze. | Responsabile dell'indagine |
| Tecnico | Crea gli agent e li configura. Configura le regole di un Network Injector. | Tecnico specializzato in intercettazioni |
| Analista | Analizza le evidence e le esporta. | Operativo |

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 uno strumento a supporto delle investigazioni che attua intercettazioni attive e passive di dati e informazioni relative alle attività 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

Di seguito le differenze rispetto alla versione RCS 7.5.

Terminologia

| RCS v. 7.5 | RCS 8.0 e successive |
| --- | --- |
| Activity | Operation |
| Agente | Module |
| Anonymizer chain | Anonymizing chain |
| Backdoor | Agent |
| 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. 7.5 | RCS 8.0 e successive |
| --- | --- |
| EXE | Melted application |
| CD | Offline Installation |
| USB | Offline Installation |
| EXPL | Exploit |

Terminologia vettori di infection per Mobile

| RCS v. 7.5 | RCS 8.0 e successive |
| --- | --- |
| SD | Local Installation |
| CAB | Installation Package |
| APP | Exploit |
| 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

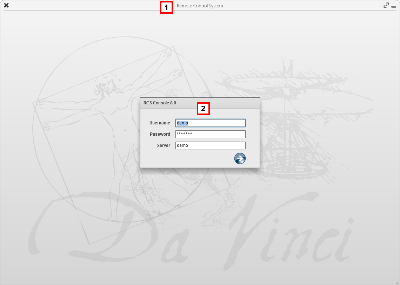
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

RCS Console all'avvio 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:  Uscita da RCS e 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. |
| 2 | Fare clic su : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. Vedi "Descrizione della homepage". |

Descrizione della homepage

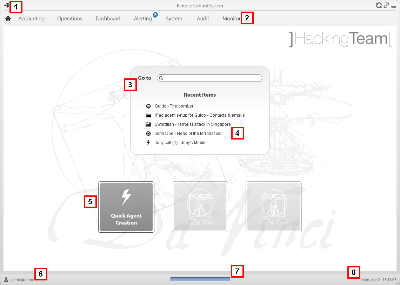
|  |  |
| --- | --- |
| Per visualizzare l'homepage: | * fare clic su |

Introduzione

RCS Console presenta all'avvio questa homepage. L'homepage è identica per tutti gli utenti. Solo i menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

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



| Area | Descrizione |
| --- | --- |
| 1 | Barra del titolo con pulsanti di comando. |
| 2 | Menu di RCS con le funzioni abilitate per l'utente. |
| 3 | Casella di ricerca per cercare tra i nomi di operation, target, agent. |
| 4 | Collegamenti agli ultimi cinque elementi aperti (operation, target e agent). |
| 5 | Pulsanti per avvio del Wizard. |
| 6 | Utente connesso con possibilità di cambiare la lingua e la password. |
| 7 | Area download con possibilità durante l'esportazione o una compilazione di vedere lo stato di avanzamento. |
| 8 | Data e ora attuale con possibilità di cambio fuso orario. |

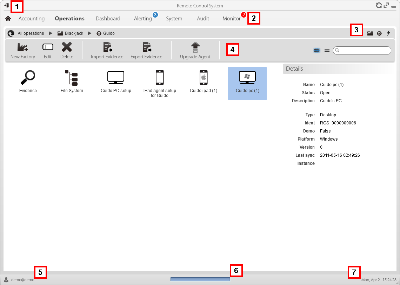
Elementi e azioni comuni dell'interfaccia

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 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 | | --- | --- | |  | Sale su di un livello. | |  | Mostra la pagina dell'operation | |  | Mostra la pagina del target | |  | Mostra la pagina della factory | |  | Mostra la pagina dell'agent | |
| 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 | Barra con i pulsanti della finestra. |
| 6 | Pulsanti e casella di ricerca:   | Oggetto | Descrizione | | --- | --- | |  | Casella di testo con ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite. | |  | Visualizza gli elementi in una tabella | |  | Visualizza gli elementi con le 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 Greenwitch (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. |

Altre azioni comuni

Di seguito la descrizione delle azioni su oggetti di interfaccia, comuni a più funzioni:

| Azione | Descrizione |
| --- | --- |
| Per ordinare una tabella | Fare clic sull'intestazione della tabella. |
| Per cambiare dimensione delle colonne | Selezionare il bordo della colonna e trascinarlo. |



Procedure del Tecnico

Introduzione

Il Tecnico deve occuparsi della strategia 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 strategie di injection.  Vedi "Gestione dei Network Injector"  Non è richiesta l'installazione di alcun agent. |

Infettare un computer non connesso a internet

Per infettare un computer non connesso a Internet.

| Passo | Azione |
| --- | --- |
| 1 | Creare una factory disabilitando la sincronizzazione.  Vedi "Pagina del target". |
| 2 | Compilare la factory selezionando il vettore di installazione adatto alla piattaforma del dispositivo e all'installazione fisica, quindi creare l'agent.  Vedi "Compilazione di una factory". |
| 3 | Installare l'agent presso il dispositivo del target nelle modalità scelte.  Vedi "Elenco dei vettori di installazione". |
| 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". |

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 del target" |
| 2 | Compilare la factory selezionando il vettore di installazione adatto alla piattaforma del dispositivo e all'installazione fisica, quindi creare l'agent.  Vedi "Compilazione di una factory". |
| 3 | Installare l'agent presso il dispositivo del target nelle modalità scelte.  Vedi "Elenco dei vettori di installazione". |
| 4 | Alla prima sincronizzazione l'agent compare nella pagina del target.  Vedi "Pagina del target" |
| 5 | Riconfigurare l'agent utilizzando la configurazione base o avanzata. Alla successiva sincronizzazione l'agent abilita la nuova configurazione.  Vedi "Configurazione base di una factory o di un agent"  Vedi "Configurazione avanzata di una factory o di un agent". |

Mantenere aggiornato il software degli agent

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

| Passo | Azione |
| --- | --- |
| 1 | * Nella sezione Operation, Target aggiornare gli agent. Vedi "Pagina del target"   oppure   * Nella sezione Operation, Target entrare in un agent e aggiornarlo. Vedi "Pagina dell'agent". |

I target

Presentazione

Introduzione

Il target può essere attaccato con diversi agent di infezione, uno per ogni dispositivo posseduto.

.

Contenuti

Questa sezione include i seguenti argomenti:

Pagina del target

|  |  |
| --- | --- |
| Per entrare in un target | * **sezione Operations, entrare in una operation, entrare in un target** |

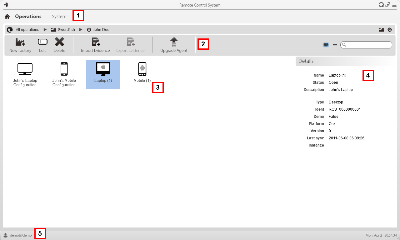
Scopo

Questa funzione permette di:

* gestire le factory, che compilate, diventeranno agent da installare sul dispositivo del target.
* entrare in una factory per la configurazione base vedi "Configurazione base di una factory o di un agent") o avanzata ("Configurazione avanzata di una factory o di un agent"
* importare/esportare le evidence del target.
* entrare in un agent installato (Vedi "Pagina dell'agent").
* aggiornare il software dell'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:  NOTA: il pulsante visualizza gli elementi in elenco con i loro dati.Vedi "Dati della pagina target"   | Icona | Descrizione | | --- | --- | |  | Compila la configurazione in uno o più agent da installare, in base ai vettori di installazione scelti. Vedi "Compilazione di una factory" | |  | Modifica una factory o un agent. | |  | Elimina una factory o un agent. | |  | Importa le evidence del target raccolte fisicamente sul dispositivo. | |  | Esporta le evidence del target in formato .tgz. | |  | Aggiorna il software di tutti gli agent con l'ultima versione ricevuta dall'assistenza HackingTeam.  PRUDENZA: l'aggiornamento non aggiorna la configurazione che viene comunicata agli agent alla successiva sincronizzazione. | |
| 4 | Icone/elenco delle factory create e degli agent installati.  : agent in modalità demo  Per la descrizione delle icone e dei dati della tabella vedi "Dati della pagina target". |
| 5 | Dati della factory o dell'agent selezionato. |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |

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 Edit: compaiono i suoi dati. * Nel menu a discesa Status, selezionare CLOSED. |
| 2 | Fare clic su Save.  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. * Selezionare la cartella dove si desidera salvare il file offline.ini |
| 2 | Fare clic su Save: le evidence sono salvate nella cartella specificata. |



Cose da sapere sulle factory e sugli agent

Modalità di infezione

È possibile infettare un dispositivo tramite:

* infezione fisica: il dispositivo viene infettato tramite file trasferito da memorie USB, CD, documento. La raccolta dei dati può avvenire sia fisicamente oppure via rete grazie all’agent installato, non appena il dispositivo effettua una connessione verso Internet.
* infezione da remoto: il dispositivo viene infettato tramite file trasferito via connessione internet o reso disponibile in una risorsa web. La raccolta delle registrazioni può avvenire sia fisicamente oppure oppure via rete grazie all’agent installato, non appena il dispositivo effettua una connessione verso Internet. L'infezione da remoto può essere potenziata tramite l'utilizzo di un Network Injector.

Componenti della strategia di infezione

I componenti che concorrono ad una buona strategia sono:

* Factory: template di base per la creazione degli agent.
* Vettori di installazione: canali di infezione.
* Agent: il singolo file 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. Vedi Manuale Amministratore di sistema.
* Registrazioni o sequenze di registrazione: i tipi di registrazioni che si vogliono raccogliere

Le factory

La factory è un template di base per 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: una factory può essere quindi usata per creare più agent, per esempio con eventi-azioni-moduli identici ma che devono essere installati tramite vettori di installazione diversi (es.: due computer con sistemi operativi diversi).

I vettori di installazione

I vettori di installazione sono scelti durante la compilazione e definiscono la modalità di installazione, fisica o da remoto, di un agent e variano in base al sistema operativo presente sul 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"

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"

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".

Dati della pagina target

|  |  |
| --- | --- |
| Per visualizzare i dati della pagina: | * sezione Operations, entrare in una operation, entrare in 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:   * OSX * Windows |
|  | Agent di tipo mobile, in stato Aperto, per sistemi operativi:   * Android, * BlackBerry, * iOS, * Symbian * Windows Mobile |

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



Visualizzazione a tabella

Di seguito la descrizione dei dati:

| Dato | Descrizione |
| --- | --- |
| Name | Nome della factory o dell'agent. |
| Description | 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. Ad ogni riconfigurazione 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. |

Compilazione di una factory

|  |  |
| --- | --- |
| Per compilare una factory: | * sezione Operations, entrare in una operation, entrare in un target, entrare in una factory, fare clic su Build * sezione Operations, entrare in una operation, entrare in un target, entrare in 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 a quanti vettori di installazione si decide di utilizzare e per quali piattaforme.

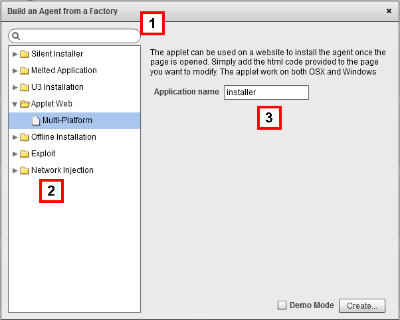
Per la descrizione dettagliata dei parametri di ogni vettore vedi "Elenco dei vettori di installazione"

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 di ogni vettore. |

Creare un agent

Per creare un agent:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare uno o più vettori di istallazione e impostare i parametri. |
| 2 | Fare clic su Create: viene creato un file ZIP o ISO e scaricato nella cartella RCS\_download 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 viene resa palese.

Per creare un agent da collaudare:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare uno o più vettori di istallazione e impostare i parametri. |
| 2 | Selezionare la casella di controllo Demo per il vettore di installazione interessato dal collaudo. |
| 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 installati in un dispositivo acquisiscono informazioni e prove importanti. La loro configurazione e il loro software possono essere aggiornati e possono essere trasferiti file in modo assolutamente invisibile al target.

Contenuti

Questa sezione include i seguenti argomenti:

Pagina dell'agent

|  |  |
| --- | --- |
| Per gestire  gli agent: | * sezione Operations, entrare in una operation, entrare in un target, entrare in un agent |

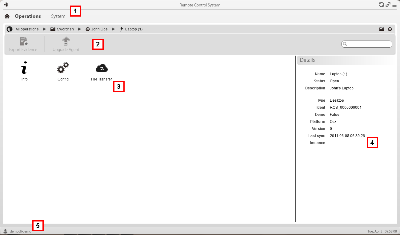
Scopo

Questa funzione permette di:

* verificare l'attività dell'agent tramite lo storico.
* 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
* aggiornare il software dell'agent

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Esporta le evidence dell'agent. | |  | Aggiorna il software dell'agent con l'ultima versione ricevuta dall'assistenza HackingTeam.  PRUDENZA: l'aggiornamento non aggiorna la configurazione che viene comunicata all'agent alla successiva sincronizzazione. | |
| 4 | Azioni possibili sull'agent. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Mostra lo storico delle configurazioni dell'agent, permettendo di modificare una configurazione esistente e salvarla come nuova. Vedi "Dati dello storico configurazioni di un agent". | |  | Apre la funzione per caricare o scaricare file dal dispositivo del target. Vedi "Trasferimento file da/a il target" | |
| 5 | Dettagli dell'agent. |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |



Cose da sapere sugli agent

Sincronizzazione di un agent

La sincronizzazione di un agent avviene solo se :

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

Prima sincronizzazione dell'agent

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

* : agent installato su un dispositivo Windows



* : agent installato su dispositivo BlackBerry



Dopo la prima sincronizzazione, se configurato opportunamente, l'agent inizia ad acquisire i dati.

Agent offline e online

L'agent ha un diverso comportamento in base al tipo di infezione che si è scelto:

| Se l'infezione è... | Allora... |
| --- | --- |
| fisica | se l'agent ha già dei moduli abilitati inizia a registrare i dati internamente al dispositivo. |
| da remoto | se l'agent ha effettuato la prima sincronizzazione è possibile:   * 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 registrazioni se sono state già inviate   Suggerimento: creare un agent con la sola sincronizzazione e solo dopo che è stato installato ed ha effettuato la prima sincronizzazione, riconfigurarlo per inserire gradualmente i moduli per le registrazioni. |

Disabilitazione temporanea di un agent

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

Collaudo di un agent

In fase di compilazione di una factory, è possibile collaudare un agent prima di installarlo sul dispositivo del target.

L'agent viene creato in versione demo e funziona analogamente agli altri agent, con le sole differenze che segnala in modo evidente (con segnalazioni audio, led e messaggi a video) la sua presenza sul dispositivo, in modo che sia facile identificare se il dispositivo è infettato.

NOTA: eventuali non ricezioni di evidence da un agent installato e in collaudo sono quindi il sintomo di errata configurazione del server, oppure impossibilità di raggiungerne l’indirizzo (es.: per problemi nella configurazione di rete) e non di una mancata installazione dell'agent.

Configurazione di un agent

La configurazione di un agent (base o avanzata) può essere modificata più volte. Ad 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 visualizzare lo storico vedi "Pagina dell'agent"

Per visualizzare i dati vedi "Dati dello storico configurazioni di un agent".

Dati dello storico configurazioni di un agent

Di seguito la descrizione:

| Campo | Descrizione |
| --- | --- |
| Description | Descrizione libera della configurazione. |
| User | Nome utente che ha modificato la configurazione. |
| Saved | Data salvataggio della configurazione. |
| Sent time | Data spedizione della configurazione tramite sincronizzazione.  AVVERTENZA:se questo valore è nullo, l'agent non sta sincronizzando. |
| Activated | Data installazione nuova configurazione nell'agent. |

Dati dello storico di un agent

Di seguito la descrizione:

| Campo | Descrizione |
| --- | --- |
| 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. |

Trasferimento file da/a il target

|  |  |
| --- | --- |
| Per trasferire file da/a l'agent: | * sezione Operations, entrare in una operation, entrare in un target, entrare in 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:

[IMAGE]

| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 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 | |
| 3 | Barre con i pulsanti della finestra. Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Carica un qualsiasi file nel dispositivo, nella cartella dove è installato l'agent. Ogni caricamento avvenuto viene registrato nello storico con data-ora e il nome del file. | |  | Esporta lo storico dei caricamenti. | |  | 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 desktop RCS\_Download. | |  | Elimina dalla cartella RCS\_Download il file selezionato. | |
| 4 | Storico dei caricamenti, con i pulsanti dei comandi. |
| 5 | Storico degli scaricamenti, con i pulsanti dei comandi. |
| 6 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |







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 parametrizzazioni complesse.

Contenuti

Questa sezione include i seguenti argomenti:

Configurazione base di una factory o di un agent

|  |  |
| --- | --- |
| Per configurare factory e agent: | * sezione Operations, entrare in una operation, entrare in un target, entrare in una factory * sezione Operations, entrare in una operation, entrare in un target, entrare in 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".
* aprire la funzione di configurazione avanzata (vedi "Configurazione avanzata di una factory o di un agent")

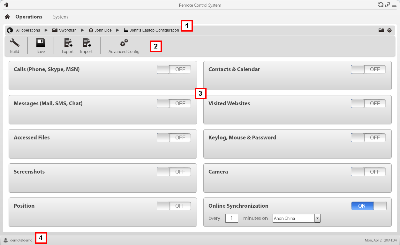
Passi successivi

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 attivata, altrimenti occorre procedere all'installazione fisica.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS.  Vedi "Descrizione della homepage" |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra 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" | |  | Salva la configurazione: se si tratta della configurazione di un agent, viene registrata nello storico e alla successiva sincronizzazione viene inviata all'agent.  Vedi "Dati dello storico configurazioni di un agent" | |  | Esporta la configurazione in un file in formato proprietario. | |  | Importa la configurazione da un file in formato proprietario. | |  | Apre la finestra della configurazione avanzata. Vedi "Configurazione avanzata di una factory o di un agent".  PRUDENZA: una volta modificato la configurazione con la funzione "avanzata" non è più possibile tornare a modificarla con la funzione "base". | |
| 4 | Area di lavoro principale con elenco dei moduli disponibili e relativo stato di attivazione.  NOTA: l'elenco dei moduli varia in base al tipo di dispositivo. Vedi "Dati della configurazione base". |
| 5 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |

Configurare una factory o un agent

Per attivare o disattivare semplicemente le registrazioni:

| Passo | Azione |
| --- | --- |
| 1 | * Fare clic su OFF in corrispondenza del dato che si desidera acquisire: il pulsante diventa ON ed è possibile impostare qualche parametro. |
| 2 | * In Online Synchronization lasciare ON se il dispositivo target avrà accesso a internet. Questo permette di procedere gradualmente a successive configurazioni. Lasciare OFF se il dispositivo target non avrà accesso a internet o se si desidera effettuare manualmente l’acquisizione delle evidence dal target. * Fare clic su Salva per salvare la configurazione corrente |
| 3 | Proseguire in modo diverso:   | Se si sta configurando... | Allora... | | --- | --- | | una factory | fare clic su Build per compilarla e ottenere i vari agent per le diverse piattaforme. Vedi "Compilazione di una factory". | | un agent | alla prossima sincronizzazione l'agent aggiorna automaticamente la propria configurazione. | |



Cose da sapere sulla configurazione base

Configurazione base

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

La configurazione base non prevede l'acquisizione di alcuni tipi di evidence, né la configurazione dettagliata delle modalità di acquisizione.

La configurazione base ha impostati 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".

IMPORTANTE: (solo per configurazioni degli agent) è possibile passare in qualsiasi momento dalla configurazione base a quella avanzata e vice versa, tuttavia se dalla configurazione avanzata si torna alla configurazione base, le impostazioni scelte fino a quel momento sono perdute e sono sostituite con quelle presenti nella configurazione base al momento del salvataggio.

Dati della configurazione base

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

| Registrazione | Descrizione |
| --- | --- |
| 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. |
| **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".  Se disabilitata indica che il dispositivo è sempre offline le evidence saranno recuperate fisicamente e importate nel database. Vedi "Pagina del target" |

Factory e agent: configurazione avanzata

Presentazione

Introduzione

La configurazione avanzata permette di costruire sequenze di registrazioni o di esecuzione comandi complesse. Attivate da un evento, tramite un’azione avviano/fermano un modulo o abilitano/disabilitano un evento. È possibile inserire anche sotto-azioni per segnalazioni a RCS.

Contenuti

Questa sezione include i seguenti argomenti:

Configurazione avanzata di una factory o di un agent

|  |  |
| --- | --- |
| Per aprire la configurazione avanzata: | * sezione Operations, entrare in una operation, entrare in un target, doppio clic sulla factory, fare clic su Config avanzata * sezione Operations, entrare in una operation, entrare in un target, doppio clic sull'agent, fare clic su Config avanzata |

Scopo

Questa funzione permette di:

* creare sequenze di esecuzioni comandi complesse. In una sequenza è possibile inserire delle sotto-azioni di allerta verso RCS.
* impostare i parametri generali di una factory/agent.

IMPORTANTE: una volta salvata la configurazione avanzata è sempre possibile passare alla configurazione base e vice versa, tuttavia se dalla configurazione avanzata si torna alla configurazione base, le impostazioni scelte fino a quel momento sono perdute e sono sostituite con la la configurazione base di default.

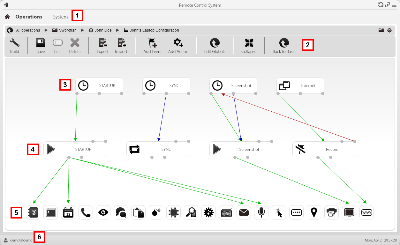
Passi successivi

Per una factory, dopo aver configurato le sequenze di intercettazione e impostato i suoi parametri, occorre compilarla per ottenere l'agent da installare. Vedi "Compilazione di una factory"

Per un agent, dopo aver configurato le sequenze di intercettazione è sufficiente salvare la nuova configurazione. Alla successiva sincronizzazione è il sistema che si occuperà di inviare all'agent la nuova configurazione.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS.  Vedi "Descrizione della homepage" |
| 2 | Barra di navigazione. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 3 | Barra 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" | |  | Salva la configurazione corrente | |  | Modifica l'evento o l'azione selezionati. | |  | Elimina l'evento, l'azione o la connessione logica selezionati. | |  | Torna alla configurazione di base senza salvare le eventuali modifiche apportate alla configurazione avanzata corrente  IMPORTANTE: una volta salvata la configurazione avanzata di un agent o di una factory è sempre possibile tornare alla configurazione base, perdendo però le impostazioni utilizzate fino a quel momento. | |  | Esporta la configurazione in un file in formato proprietario. | |  | Importa la configurazione da un file in formato proprietario. | |  | Inserisce un evento. | |  | Inserisce un'azione. | |  | Modifica i parametri globali dell'agent, vedi "Dati globali dell'agent". | |  | Comprime o espande i riquadri degli eventi e delle azioni per permettere una migliore visione della configurazione corrente. | |
| 4 | Area degli eventi. Gli eventi STARTUP e SYNC sono di default. |
| 5 | Area delle azioni. Le azioni STARTUP e SYNC sono di default. |
| 6 | Area dei moduli di registrazione. Cambiano in base al dispositivo desktop o mobile. |
| 7 | Barra di stato di RCS.  Vedi "Descrizione della homepage" |

Creare una sequenza di attivazione semplice

Per creare una sequenza semplice, ovvero all'accadere di un evento acquisire uno o più dati:

| 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 i parametri. Vedi "Elenco degli eventi" * 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 e l'azione al modulo:   * 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. |
| 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 avviare una registrazione, 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 i parametri. Vedi "Elenco degli eventi" * 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 i parametri |
| 3 | Collegare l'evento all'azione:   * Fare clic sui 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 sui tipi di dati che si vuole iniziare ad acquisire o di cui fermare l'acquisizione.   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 su cui agire. |
| 5 | Fare clic su Salva: la configurazione è pronta per essere compilata (se factory) o trasmessa al dispositivo alla prossima sincronizzazione (se agent). |



Cose da sapere sulla configurazione avanzata

Configurazione avanzata

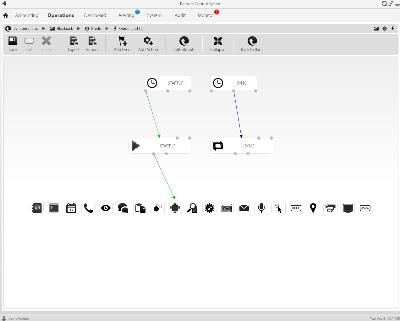
La configurazione avanzata di una factory/agent permette di creare delle sequenze complesse di attivazione tramite una semplice interfaccia grafica.

La sequenza avrà lo scopo di avviare/fermare le registrazioni (evidence), e/o eseguire un'azione sempre attraverso un evento.

La configurazione avanzata include sempre due sequenze base:

* Ad 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 dal dispositivo)
* le azioni eseguite a fronte di un evento (es.: l'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 registrare le informazioni desiderate o eseguono altre azioni sul dispositivo (es.: registrazione dell'audio della chiamata)
* le sequenze, termine usato per indicare l'insieme di eventi, azioni, sotto-azioni e moduli.

NOTA: la configurazione di eventi, azioni e di alcuni moduli particolari è disponibile solo nella configurazione avanzata.

Lettura 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 la segnalazione che la SIM è stata cambiata (azione verso evento)
* ...e così via

Le combinazioni tra eventi, azioni, sotto-azioni e moduli sono infinite. Di seguito la spiegazione dettagliata e i vincoli per una corretta progettazione.

Eventi

Gli eventi vengono intercettati dal sistema e possono avviare, ripetere o concludere un'azione.

NOTA: non è possibile avviare una registrazione (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 avviaerà/fermerà un modulo di registrazione.

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

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

| Relazione tra evento e azione | Descrizione | Connettore |
| --- | --- | --- |
| Start | Avvia un'azione quando l'evento viene scatenato. |  |
| Repeat | Ripete un'azione. È possibile specificare l'intervallo e il numero di ripetizioni. |  |
| End | Avvia un'azione quando l'evento termina. |  |

Un evento può gestire fino a tre azioni distinte contemporaneamente. L’azione Start viene avviata quando l’evento si scatena 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 che si desidera monitorare. L’azione Stop viene avviata quando l’evento scatenato termina (es.: l’evento StandBy scatena la End quando il dispositivo esce dalla modalità di standby).

Azioni

Le azioni sono innescate dagli eventi e possono:

* avviare o fermare un modulo di registrazione
* 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 ad un numero telefonico definito in fase di configurazione dell'agent).

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"

Relazioni tra azioni e moduli

La stessa azione può agire su un modulo in modi diversi, la relazione tra un'azione e uno o più moduli è rappresentata da un connettore:

| Relazione tra  azione e moduli | Descrizione | Connettore |
| --- | --- | --- |
| Start modules | Avvia uno o più moduli |  |
| Stop modules | Ferma uno o più moduli |  |

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:

| Relazione tra  azione e eventi | Descrizione | Connettore |
| --- | --- | --- |
| Enable events | Abilita uno o più eventi |  |
| Disable events | Disabilita uno o più eventi |  |

Un'azione può abilitare/disabilitare più eventi contemporaneamente.

Moduli

I moduli sono tipi di registrazioni effettuate sul dispositivo target. Possono essere avviati/fermati da un'azione e producono le evidence.

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 registrazione posizione + ferma registrazione degli screenshot). Per l'elenco completo vedi "Elenco dei moduli".

Dati globali dell'agent

Di seguito la descrizione dei parametri globali dell'agent:

| Campo | Descrizione |
| --- | --- |
| Minimum disk free | Quantità minima spazio disco libero sul dispositivo. |
| Maximum evidence size | Quantità massima spazio occupato dalle evidence sul dispositivo del target, fino alla successiva sincronizzazione. Il default è 1 GB.  Al raggiungimento di questo limite l'agent termina la registrazione in attesa di una sincronizzazione. Se la sincronizzazione non avviene, non saranno acquisite ulteriori evidence. |
| Wipe | Se abilitato, effettua il secure-wipe dei file generati dall'agent. Nessuna traccia dell'agent sarà rilevabile a seguito di un'analisi forense.  NOTA: questa modalità richiede un tempo maggiore. |
| Remove driver | Rimuove il driver alla disinstallazione. |
| No hide | Richiede assistenza: utilizzare solo su richiesta dell’assistenza tecnica HackingTeam. |
| Mask | Richiede assistenza: utilizzare solo su richiesta dell’assistenza tecnica HackingTeam. |

Gestione dei frontend

|  |  |
| --- | --- |
| Per gestire i front end: | * sezione System, Frontend |

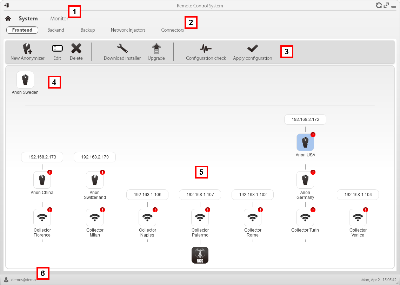
Scopo della funzione

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 vari VPS.

In fase di installazione, questa funzione permette di creare un nuovo "oggetto" Anonymizer che crea il collegamento logico tra RCS Console e la singola componente software da installare su VPS e di generare l'installer da eseguire sul VPS.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". |
| 2 | Menu System |
| 3 | Barra 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 in catena e funzionante  : Anonymizer non in catena.  : Anonymizer non raggiungibile  : Collector in funzione  : Collector non funzionante. |
|  |  |



I Network Injector

Presentazione

Introduzione

Network Injector permette di intercettare e isolare il traffico HTTP del target e eseguire delle azioni di intercettazione e injection sul dispositivo.

Contenuti

Questa sezione include i seguenti argomenti:

Gestione dei Network Injector 45

Cose da sapere su Network Injector e le sue regole 48

Dati delle regole di injection 48

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 sniffing e di injection su connessioni HTTP e inviarle al Network Injector.

Cosa è possibile fare

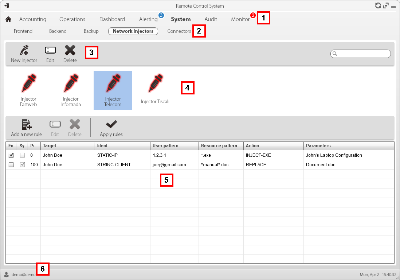
Con questa funzione è possibile:

* creare una regola di injection di un agent su un target e applicare le regola sul Network Injector.

Per creare una regola di injection non è necessario installare un agent.

Come si presenta la funzione

Ecco come viene visualizzata la pagina già popolata:



| Area | Descrizione | |
| --- | --- | --- |
| 1 | Menu di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". | |
| 2 | Menu System | |
| 3 | Barra con i pulsanti dedicati ai Network Injector. | |
| 4 | Elenco dei Network Injector. | |
| 5 | Barra con i pulsanti dedicati alle regole di injection. Di seguito la descrizione:   | Azione | Descrizione | | --- | --- | |  | Aggiunge una nuova regola. | |  | Apre la finestra con i dati della regola. Vedi "Dati delle regole di injection". | |  | Elimina la regola selezionata. | |  | Applica tutte le regole abilitate al Network Injector selezionato. | | |
| 6 | Elenco delle regole del Network Injector selezionato.  En: selezionare per abilitare le regole da applicare. | |
| 7 | Barra di stato di RCS. Vedi "Elementi e azioni comuni dell'interfaccia". | |
|  | |  | |



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". * Fare clic su Save: nell'area di lavoro principale compare la nuova regola. |
| 3 | **Abilitare le regole da applicare selezionando la casella di controllo En nella tabella.** |
| 4 | Fare clic su Apply rules: RCS invia al Network Injector selezionato le regole e un indicatore di stato mostra l'avanzamento dell'operazione. |



Cose da sapere su Network Injector e le sue regole

Introduzione

Network Injector controlla le connessioni HTTP del traffico di rete 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 migliore per identificare e isolare la connessione del target tra tutte le connessioni che Network Injector vede. Per esempio attraverso l'inserimento dell'indirizzo IP o MAC del target.
2. definire il metodo migliore 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.

Quando si è riusciti a identificare la connessione del target e si ha deciso il metodo migliore di attacco, occorre abilitare la regola e applicarla.

Cosa succede quando si abilita/disabilita una regola

Abilitare una regola vuol dire renderla disponibile per il processo di infezione da parte del sistema. 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.

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

Cosa succede quando si applica una regola

Applicare una regola significa dare inizio al processo di infezione del target. Il sistema invia le regole abilitate a Network Injector non appena viene contattato da Network Controller per la sincronizzazione(normalmente ogni 30 secondi).

Dati delle regole di injection

Di seguito la descrizione delle regole per definire la strategia di infezione più efficace:

| Dato | Descrizione |
| --- | --- |
| Enabled | Se selezionato, la regola sarà inviata al Network Injector al successivo comando di applicazione regole.  Se non selezionato, la regola è salvata ma non sarà inviata al successivo comando di applicazione regole. |
| Disable on sync | Se selezionato, RCS termina l'infezione delle risorse scaricate dal target dopo la prima sincronizzazione dell'agent.  Se non selezionato, RCS continua ad infettare le risorse scaricate dal target, anche dopo la prima sincronizzazione. In questo caso disabilitare manualmente la regola alla prima sincronizzazione dell'agent. |
| Probability | Probabilità (in percentuale) di infezione delle risorse scaricate dal target dopo la prima risorsa infettata.  0%: dopo aver infettato la prima risorsa, Network Injector non infetta più le altre risorse scaricate dal target.  100%: dopo aver infettato la prima risorsa, Network Injector infetta qualsiasi altra risorsa scaricata dal target.  SUGGERIMENTO: se si applica un valore superiore al 50%, si consiglia di riportare il valore allo 0% dopo avere verificato l'avvenuta installazione (sincronizzazione avvenuta) oppure utilizzare l'opzione Disable on sync. |
| Target | Nome del target da infettare. |
| 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:   | Dato | Descrizione | | --- | --- | | STATIC-IP | IP statico assegnato al target. | | STATIC-RANGE | Range di indirizzi IP potenzialmente 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 | |
| User pattern | Formato del metodo di identificazione del traffico del target. Il formato dipende dal tipo di Ident selezionato.   | Metodo | Formato | | --- | --- | | **DHCP**  **STATIC-IP**  **STATIC-MAC** | Indirizzo corrispondente (es.: "195.162.21.2") | | STATIC-RANGE | Range di indirizzi separati da '-' (es.: "195.162.21.2-195.162.21.5" | | **STRING-CLIENT**  **STRING-SERVER** | Stringa di testo (es.: "John@gmail.com") | | **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.\*") | |
| Resourse pattern | Formato della risorsa da attaccare, ovvero la risorsa che il target visualizzerà o scaricherà. Il formato dipende dal tipo di Action selezionata.  NOTA: non è utilizzato dall'azione INJECT-UPGRADE.   | Tipo azione | Contenuto di Pattern risorsa | | --- | --- | | INJECT-EXE | Nome dell'eseguibile da infettare. Utilizzare le wildcard per ottimizzare l'efficacia dell'attacco e ottenere un'infezione sicura.  Esempi di formati possibili:   * \*<nomeExe>\*.exe * www.mozilla.org/firefox/download/firefoxsetup.exe   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").  SUGGERIMENTO: digitare \*.exe\* per infettare tutti gli eseguibili, indipendentemente dalla URL.  IMPORTANTE: se si digita per esempio: \*exe\*, senza il carattere separatore '.'con l'estensione del file, saranno infettate tutte le pagine che contengono le parole che contengono le lettere "exe" (es.: "chief executive officer" oppure "executive lounge"). | | INJECT-HTML | URL della pagina web da infettare.  Esempi di formati possibili:   * www.oracle.com/ * www.oracle.com/index.html   NOTA: l'indirizzo della pagina deve comprendere il carattere '/' finale quando non è specificata una pagina precisa (es.: "www.oracle.com/" è equivalente a "www.oracle.com/index.html")  NOTA: non è possibile infettare una pagina di redirect. Verificare sul browser il path corretto della pagina web prima di indicarlo nella regola. | | INJECT-UPGRADE | Non utilizzato. | | REPLACE | Risorsa da sostituire, per esempio un file DOC, JPEG, PDF. | |
| Action | Metodo di infezione più appropriato che agisce sulla risorsa indicata in Pattern risorsa:   | Metodo | Descrizione | | --- | --- | | INJECT-EXE | Infetta in tempo reale il file EXE che il target desidera scaricare . L'installazione dell'agent avviene nel momento in cui il target esegue il file EXE. | | INJECT-HTML | Inserisce un'applet java nella pagina che il target desidera visualizzare. Quando il target apre la pagina, deve accettare l'esecuzione del codice java per installare l'agent.  Suggerimento: per evitare i messaggi di avviso da parte del sistema del target, si consiglia di fornirsi di un certificato valido per firmare l'applet. Salvare i certificati nella cartella: ...\RCS\db\config\certs\ | | INJECT-UPGRADE | Notifica il dispositivo del target della disponibilità di un aggiornamento per un software installato. L'agent si installa nel momento in cui il target esegue l'aggiornamento. Non fa riferimento a Pattern risorsa. | | REPLACE | Sostituisce la risorsa definita in Pattern risorsa con il nuovo file fornito.  Suggerimento: utilizzare questo tipo di azione insieme agli Exploit, che permettono di creare file DOC o PDF infettati e sostituirli ai file che il target desidera scaricare. | |
| Agent | Per tutte le azioni tranne le REPLACE. Agent preparato per essere installato sul dispositivo del target. |
| File | Solo per Action REPLACE. File da sostituire a quello indicato in Pattern risorsa. |

Appendice: eventi, azioni, moduli e vettori

Presentazione

Introduzione

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

Contenuti

Questa sezione include i seguenti argomenti:

Elenco degli eventi

Di seguito la descrizione degli eventi:

| Dato | Descrizione |
| --- | --- |
| Abilitato | Abilita o disabilita l'evento. |
| Nome | Nome arbitrario assegnato all'evento. |
| Tipo | Elenco dei tipi di evento:   | Evento | Dispositivo | Innesca un'azione quando.. | | --- | --- | --- | | AC | desktop, mobile | il cellulare viene collegato all'alimentazione. | | Battery | mobile | il livello di carica della batteria è entro il range specificato. | | Call | mobile | viene effettuata o ricevuta una chiamata. | | Connection | desktop, mobile | quando viene sostituita la scheda SIM. | | Position | mobile | il target raggiunge o lascia una posizione specifica. | | Process | desktop, mobile | sul dispositivo viene lanciato un eseguibile o se c'è una finestra aperta. | | Quota | desktop | l'occupazione disco delle evidence sul dispositivo supera il limite impostato. | | Screensaver | desktop | sul dispositivo target si avvia il salvaschermo. | | SimChange | mobile | viene sostituita la scheda SIM. | | SMS | mobile | viene ricevuto un messaggio SMS dal numero indicato. | | Standby | mobile | il dispositivo entra in modalità stand-by. | | Timer | desktop, mobile | scadono intervalli specificati. | | Window | desktop | si apre una finestra. | | WinEvent | desktop | il sistema operativo registra un evento Windows. | |

Elenco dei moduli

Di seguito la descrizione dei moduli di registrazione:

| Modulo | Configurazione | Dispositivo | Registrazione di... |
| --- | --- | --- | --- |
| Accessed files | base | desktop | (solo desktop) documenti o immagini aperti dal target |
| Addressbook | avanzata | desktop, mobile | contatti. |
| Application | avanzata | desktop, mobile | applicazioni utilizzate. |
| Calendar | avanzata | desktop, mobile | calendario |
| Call | avanzata | desktop, mobile | chiamate (telefono, Skype, MSN) |
| Calls | base | desktop, mobile | chiamate (telefono, Skype, MSN) |
| Camera | base, avanzata | desktop, mobile | immagini della webcam |
| Chat | avanzata | desktop, mobile | chat |
| Clipboard | avanzata | desktop, mobile | informazioni copiate nella clipboard |
| Contacts and Calendar | base | desktop, mobile | contatti e calendario |
| Device | avanzata | desktop, mobile | informazioni del sistema |
| File | avanzata | desktop, | file aperti dal target |
| Keylog | avanzata | desktop, mobile | tasti premuti sulla tastiera |
| Keylog, Mouse and Password | base | desktop | tasti premuti sulla tastiera, clic del mouse, password inserite |
| Messages | avanzata | desktop, mobile | email |
| Messages | base | desktop, mobile | email, SMS e chat |
| Mic | avanzata | desktop, mobile | audio |
| Mouse | avanzata | desktop | clic del mouse |
| Password | avanzata | desktop | password |
| Position | base, avanzata | desktop, mobile | posizione geografica del target |
| Print | avanzata | desktop | pagine stampate |
| Screenshots | base, avanzata | desktop, mobile | immagini attive sul display del target |
| URL | avanzata | desktop, mobile | pagine web visitate |
| Visited websites | base | desktop, mobile | pagine web visitate |

Di seguito la descrizione dei moduli di altro tipo:

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

Elenco delle sotto-azioni

Di seguito la descrizione delle sotto-azioni:

| Dato | Descrizione |
| --- | --- |
| Nome | Nome arbitrario assegnato all'azione. |
| Subaction | Elenco dei tipi di sotto-azioni:   | Azione | Dispositivo | Descrizione | | --- | --- | --- | | Destroy | desktop, mobile | Rende inutilizzabile il dispositivo del target. | | Execute | desktop, mobile | Esegue un comando arbitrario sulla macchina target. | | Log | desktop, mobile | Crea messaggio informativo personalizzato. | | SMS | mobile | Invia un SMS nascosto nel dispositivo del target. | | Synchronyze | desktop, mobile | Esegue la sincronizzazione con RCS. | | Uninstall | desktop, mobile | Rimuove completamente l'agent. | |

Elenco dei vettori di installazione

Sistemi operativi supportati dagli agent

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

| Dispositivo | Sistema Operativo |
| --- | --- |
| Desktop | * Windows * OSX |
| Mobile | * Android * BlackBerry * Windows Mobile * Symbian * IOS |

Di seguito l'elenco dei vettori:

| Installation Vector | Dispositivo | Descrizione |
| --- | --- | --- |
| Applet Web | Desktop | Genera codice HTML da inserire in una pagina web. |
| Exploit | Desktop, Mobile | Inserisce l'agent all'interno di un qualsiasi documento. |
| Installation Package | Mobile | Crea un file autoinstallante con l'agent. |
| Local Installation | Mobile | Installa l'agent sul dispositivo del target o tramite USB o tramite memory card SD/MMC. |
| Melted Application | Desktop | Inserisce l'agent in un qualsiasi file autoinstallante. |
| Network Injection | Desktop | Rimanda alla pagina di creazione delle regole di injection. Vedi "Gestione dei Network Injector". |
| Offline Installation | Desktop | Crea un file ISO per la generazione di un CD/DVD/USB di avvio da utilizzare su un computer spento. |
| QR Code/Web Link | Mobile | Genera un codice QR per siti o stampati, che se il target fotograferà, installerà l'agent. |
| Silent Installer | Desktop | Crea un file eseguibile vuoto che, quando eseguito sul dispositivo del target, installa solamente l'agent. |
| U3 Installation | Desktop | Crea una chiave U3 che installa l'agent sul dispositivo del target. |
| Wap Push Message | Mobile | Invia un messaggio WAP, che se il target accetterà, installerà l'agent. |



|  |  |
| --- | --- |
| RCS8.0Manuale dell'amministratore di sistema  Manuale dell'amministratore di sistema 1.0 FEB/2012  © COPYRIGHT 2012  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 |