

RCS 8.2

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 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 14](#_Toc337471071)

[Introduzione a questa Guida 17](#_Toc337471072)

[Novità della guida 3](#_Toc337471073)

[Documentazione fornita 3](#_Toc337471074)

[Convenzioni tipografiche per le segnalazioni 4](#_Toc337471075)

[Convenzioni tipografiche per la formattazione 4](#_Toc337471076)

[Destinatari del prodotto e di questa guida 5](#_Toc337471077)

[Dati di identificazione dell'autore del software 6](#_Toc337471078)

[RCS (Remote Control System) 6](#_Toc337471079)

[Differenze rispetto alle versioni precedenti 7](#_Toc337471080)

[RCS Console per il Tecnico 8](#_Toc337471081)

[Avvio di RCS Console 9](#_Toc337471082)

[Come si presenta la pagina di login 9](#_Toc337471083)

[Accedere a RCS Console 9](#_Toc337471084)

[Descrizione della homepage 10](#_Toc337471085)

[Introduzione 10](#_Toc337471086)

[Come si presenta 10](#_Toc337471087)

[Descrizione dei wizard da homepage 11](#_Toc337471088)

[Introduzione 11](#_Toc337471089)

[Come si presenta 11](#_Toc337471090)

[Investigation Wizard 12](#_Toc337471091)

[Elementi e azioni comuni dell'interfaccia 13](#_Toc337471092)

[Come si presenta RCS Console 13](#_Toc337471093)

[Azioni sempre disponibili sull'interfaccia 16](#_Toc337471094)

**[Cambiare la lingua dell'interfaccia o la propria password](#_Toc337471095)** [16](#_Toc337471095)

**[Convertire le date-ora di RCS Console al proprio fuso orario](#_Toc337471096)** [16](#_Toc337471096)

[Azioni sulle tabelle 16](#_Toc337471097)

[Procedure del Tecnico 19](#_Toc337471098)

[Introduzione 19](#_Toc337471099)

[Procedure 19](#_Toc337471100)

**[Effettuare l'injection su connessioni HTTP](#_Toc337471101)** [19](#_Toc337471101)

**[Infettare un computer non connesso a internet](#_Toc337471102)** [19](#_Toc337471102)

**[Infettare un computer connesso a Internet](#_Toc337471103)** [20](#_Toc337471103)

**[Mantenere aggiornato il software degli agent](#_Toc337471104)** [20](#_Toc337471104)

[I target 21](#_Toc337471105)

[Pagina del target 22](#_Toc337471106)

[Scopo 22](#_Toc337471107)

**[Come si presenta la funzione](#_Toc337471108)** [22](#_Toc337471108)

[Per saperne di più 24](#_Toc337471109)

**[Creare una factory](#_Toc337471110)** [24](#_Toc337471110)

**[Chiudere una factory o un agent](#_Toc337471111)** [24](#_Toc337471111)

**[Eliminare una factory o un agent](#_Toc337471112)** [25](#_Toc337471112)

**[Importare le evidence del target](#_Toc337471113)** [25](#_Toc337471113)

**[Esportare le evidence del target](#_Toc337471114)** [25](#_Toc337471114)

[Cose da sapere sulle Factory e sugli Agent 25](#_Toc337471115)

[Modalità di infezione 25](#_Toc337471116)

[Componenti della strategia di infezione 26](#_Toc337471117)

[Le factory 26](#_Toc337471118)

[I vettori di installazione 26](#_Toc337471119)

[Gli agent 27](#_Toc337471120)

[I moduli per l'acquisizione dei dati 27](#_Toc337471121)

[Dati della pagina target 28](#_Toc337471122)

[Visualizzazione a icone 28](#_Toc337471123)

[Visualizzazione a tabella 28](#_Toc337471124)

[Compilazione di una factory 29](#_Toc337471125)

[Scopo 29](#_Toc337471126)

[Passi successivi 29](#_Toc337471127)

**[Come si presenta la funzione](#_Toc337471128)** [29](#_Toc337471128)

[Per saperne di più 30](#_Toc337471129)

**[Creare un agent](#_Toc337471130)** [30](#_Toc337471130)

**[Creare un agent da collaudare in modalità demo](#_Toc337471131)** [31](#_Toc337471131)

[Gli agent 31](#_Toc337471132)

[Pagina dell'agent 32](#_Toc337471133)

[Scopo 32](#_Toc337471134)

**[Come si presenta la funzione](#_Toc337471135)** [32](#_Toc337471135)

[Per saperne di più 34](#_Toc337471136)

[Cose da sapere sugli agent 34](#_Toc337471137)

[Installazione di un agent 34](#_Toc337471138)

[Acquisizione evidence per analisi ambiente installazione 34](#_Toc337471139)

[Analisi ambiente di installazione 35](#_Toc337471140)

[Aggiornamento dello scout agent 35](#_Toc337471141)

[Sincronizzazione di un agent 35](#_Toc337471142)

[Agent offline e online 35](#_Toc337471143)

[Disabilitazione temporanea di un agent 36](#_Toc337471144)

[Collaudo di un agent 36](#_Toc337471145)

[Configurazione dell'agent 36](#_Toc337471146)

[Dati dello storico configurazioni di un agent 37](#_Toc337471147)

[Dati dello storico eventi di un agent 38](#_Toc337471148)

[Dati dello storico sincronizzazioni dell'agent 39](#_Toc337471149)

[Trasferimento file da/a il target 39](#_Toc337471150)

[Scopo 39](#_Toc337471151)

**[Come si presenta la funzione](#_Toc337471152)** [39](#_Toc337471152)

[Per saperne di più 41](#_Toc337471153)

[Factory e agent: configurazione base 41](#_Toc337471154)

[Configurazione base di una factory o di un agent 42](#_Toc337471155)

[Scopo 42](#_Toc337471156)

[Passi successivi 42](#_Toc337471157)

**[Come si presenta la funzione](#_Toc337471158)** [42](#_Toc337471158)

[Per saperne di più 43](#_Toc337471159)

**[Configurare una factory o un agent](#_Toc337471160)** [44](#_Toc337471160)

[Cose da sapere sulla configurazione base 45](#_Toc337471161)

[Configurazione base 45](#_Toc337471162)

[Esportazione e importazione di configurazioni 45](#_Toc337471163)

[Salvataggio della configurazione come template 45](#_Toc337471164)

[Dati della configurazione base 45](#_Toc337471165)

[Factory e agent: configurazione avanzata 47](#_Toc337471166)

[Configurazione avanzata di una factory o di un agent 48](#_Toc337471167)

[Scopo 48](#_Toc337471168)

[Passi successivi 48](#_Toc337471169)

**[Come si presenta la funzione](#_Toc337471170)** [48](#_Toc337471170)

[Per saperne di più 50](#_Toc337471171)

**[Creare una sequenza di attivazione semplice](#_Toc337471172)** [50](#_Toc337471172)

**[Creare una sequenza di attivazione complessa](#_Toc337471173)** [50](#_Toc337471173)

[Cose da sapere sulla configurazione avanzata 52](#_Toc337471174)

[Configurazione avanzata 52](#_Toc337471175)

[Componenti della configurazione avanzata 52](#_Toc337471176)

[Lettura delle sequenze 53](#_Toc337471177)

[Eventi 53](#_Toc337471178)

[Azioni 54](#_Toc337471179)

[Relazioni tra azioni e moduli 54](#_Toc337471180)

[Relazioni tra azioni e eventi 54](#_Toc337471181)

[Moduli 54](#_Toc337471182)

[Esportazione e importazione di configurazioni 55](#_Toc337471183)

[Salvataggio della configurazione come template 55](#_Toc337471184)

[Dati globali dell'agent 56](#_Toc337471185)

[Gestione dei frontend 57](#_Toc337471186)

[Scopo della funzione 57](#_Toc337471187)

**[Come si presenta la funzione](#_Toc337471188)** [57](#_Toc337471188)

[Per saperne di più 58](#_Toc337471189)

[I Network Injector 58](#_Toc337471190)

[Gestione dei Network Injector 59](#_Toc337471191)

[Scopo 59](#_Toc337471192)

[Cosa è possibile fare 59](#_Toc337471193)

**[Come si presenta la funzione](#_Toc337471194)** [59](#_Toc337471194)

[Per saperne di più 60](#_Toc337471195)

**[Aggiungere una nuova regola di injection e applicarla al target](#_Toc337471196)** [60](#_Toc337471196)

[Dati di un Network Injector 61](#_Toc337471197)

[Cose da sapere su Network Injector e le sue regole 62](#_Toc337471198)

[Introduzione 62](#_Toc337471199)

[Tipi di risorse infettabili 62](#_Toc337471200)

[Come creare una regola 62](#_Toc337471201)

[Cosa succede quando si abilita/disabilita una regola 62](#_Toc337471202)

[Dati delle regole di injection 62](#_Toc337471203)

[Appendice: azioni 66](#_Toc337471204)

[Elenco delle sotto-azioni 67](#_Toc337471205)

[Descrizione dati sotto-azioni 67](#_Toc337471206)

[Descrizione tipi di sotto-azioni 67](#_Toc337471207)

[Azione Destroy 67](#_Toc337471208)

[Scopo 67](#_Toc337471209)

[Sistemi operativi 67](#_Toc337471210)

[Parametri 67](#_Toc337471211)

[Azione Execute 68](#_Toc337471212)

[Scopo 68](#_Toc337471213)

[Riferimento a cartella dell'agent 68](#_Toc337471214)

[Sistemi operativi 68](#_Toc337471215)

[Dati significativi 68](#_Toc337471216)

[Azione Log 68](#_Toc337471217)

[Scopo 68](#_Toc337471218)

[Sistemi operativi 68](#_Toc337471219)

[Parametri 69](#_Toc337471220)

[Azione SMS 69](#_Toc337471221)

[Scopo 69](#_Toc337471222)

[Sistemi operativi 69](#_Toc337471223)

[Parametri 69](#_Toc337471224)

[Azione Synchronyze 69](#_Toc337471225)

[Scopo 69](#_Toc337471226)

[Sistemi operativi 70](#_Toc337471227)

[Parametri desktop 70](#_Toc337471228)

[Parametri mobile 70](#_Toc337471229)

[Azione Uninstall 71](#_Toc337471230)

[Scopo 71](#_Toc337471231)

[Sistemi operativi 71](#_Toc337471232)

[Parametri 71](#_Toc337471233)

[Appendice: eventi 71](#_Toc337471234)

[Elenco degli eventi 73](#_Toc337471235)

[Descrizione dati eventi 73](#_Toc337471236)

[Descrizione tipi eventi 73](#_Toc337471237)

[Evento AC 74](#_Toc337471238)

[Scopo 74](#_Toc337471239)

[Sistemi operativi 74](#_Toc337471240)

[Parametri 74](#_Toc337471241)

[Evento Battery 74](#_Toc337471242)

[Scopo 74](#_Toc337471243)

[Sistemi operativi 74](#_Toc337471244)

[Parametri 74](#_Toc337471245)

[Evento Call 75](#_Toc337471246)

[Scopo 75](#_Toc337471247)

[Sistemi operativi 75](#_Toc337471248)

[Parametri 75](#_Toc337471249)

[Evento Connection 75](#_Toc337471250)

[Scopo 75](#_Toc337471251)

[Sistemi operativi 75](#_Toc337471252)

[Parametri mobile 75](#_Toc337471253)

[Parametri desktop 75](#_Toc337471254)

[Evento Idle 76](#_Toc337471255)

[Scopo 76](#_Toc337471256)

[Sistemi operativi 76](#_Toc337471257)

[Parametri 76](#_Toc337471258)

[Evento Position 76](#_Toc337471259)

[Scopo 76](#_Toc337471260)

[Sistemi operativi 76](#_Toc337471261)

[Parametri 76](#_Toc337471262)

[Evento Process 77](#_Toc337471263)

[Scopo 77](#_Toc337471264)

[Sistemi operativi 77](#_Toc337471265)

[Parametri 77](#_Toc337471266)

[Evento Quota 77](#_Toc337471267)

[Scopo 77](#_Toc337471268)

[Sistemi operativi 77](#_Toc337471269)

[Parametri 78](#_Toc337471270)

[Evento Screensaver 78](#_Toc337471271)

[Scopo 78](#_Toc337471272)

[Sistemi operativi 78](#_Toc337471273)

[Parametri 78](#_Toc337471274)

[Evento SimChange 78](#_Toc337471275)

[Scopo 78](#_Toc337471276)

[Sistemi operativi 78](#_Toc337471277)

[Parametri 78](#_Toc337471278)

[Evento SMS 78](#_Toc337471279)

[Scopo 78](#_Toc337471280)

[Sistemi operativi 78](#_Toc337471281)

[Parametri 79](#_Toc337471282)

[Evento Standby 79](#_Toc337471283)

[Sistemi operativi 79](#_Toc337471284)

[Parametri 79](#_Toc337471285)

[Evento Timer 79](#_Toc337471286)

[Scopo 79](#_Toc337471287)

[Sistemi operativi 79](#_Toc337471288)

[Parametri 79](#_Toc337471289)

[Evento Window 80](#_Toc337471290)

[Scopo 80](#_Toc337471291)

[Sistemi operativi 80](#_Toc337471292)

[Parametri 80](#_Toc337471293)

[Evento WinEvent 80](#_Toc337471294)

[Scopo 80](#_Toc337471295)

[Sistemi operativi 80](#_Toc337471296)

[Parametri 80](#_Toc337471297)

[Appendice: moduli 81](#_Toc337471298)

[Elenco dei moduli 82](#_Toc337471299)

[Modulo Addressbook 84](#_Toc337471300)

[Scopo 84](#_Toc337471301)

[Sistemi operativi 84](#_Toc337471302)

[Dati significativi 84](#_Toc337471303)

[Modulo Application 84](#_Toc337471304)

[Scopo 84](#_Toc337471305)

[Sistemi operativi 84](#_Toc337471306)

[Dati significativi 84](#_Toc337471307)

[Modulo Calendar 85](#_Toc337471308)

[Scopo 85](#_Toc337471309)

[Sistemi operativi 85](#_Toc337471310)

[Dati significativi 85](#_Toc337471311)

[Modulo Call 85](#_Toc337471312)

[Scopo 85](#_Toc337471313)

[Sistemi operativi 85](#_Toc337471314)

[Dati significativi 85](#_Toc337471315)

[Modulo Camera 86](#_Toc337471316)

[Scopo 86](#_Toc337471317)

[Sistemi operativi 86](#_Toc337471318)

[Dati significativi 86](#_Toc337471319)

[Modulo Chat 86](#_Toc337471320)

[Scopo 86](#_Toc337471321)

[Sistemi operativi 86](#_Toc337471322)

[Dati significativi 86](#_Toc337471323)

[Modulo Clipboard 87](#_Toc337471324)

[Scopo 87](#_Toc337471325)

[Sistemi operativi 87](#_Toc337471326)

[Dati significativi 87](#_Toc337471327)

[Modulo Conference 87](#_Toc337471328)

[Scopo 87](#_Toc337471329)

[Sistemi operativi 87](#_Toc337471330)

[Dati significativi 87](#_Toc337471331)

[Modulo Crisis 87](#_Toc337471332)

[Comportamento su dispositivi desktop 87](#_Toc337471333)

[Comportamento su dispositivi mobile 88](#_Toc337471334)

[Sistemi operativi 88](#_Toc337471335)

[Dati significativi desktop 88](#_Toc337471336)

[Dati significativi mobile 88](#_Toc337471337)

[Modulo Device 89](#_Toc337471338)

[Scopo 89](#_Toc337471339)

[Sistemi operativi 89](#_Toc337471340)

[Dati significativi mobile 89](#_Toc337471341)

[Modulo File 90](#_Toc337471342)

[Scopo 90](#_Toc337471343)

[Sistemi operativi 90](#_Toc337471344)

[Dati significativi 90](#_Toc337471345)

[Modulo Infection 91](#_Toc337471346)

[Scopo 91](#_Toc337471347)

[Sistemi operativi 91](#_Toc337471348)

[Dati significativi 91](#_Toc337471349)

[Modulo Keylog 91](#_Toc337471350)

[Scopo 91](#_Toc337471351)

[Sistemi operativi 91](#_Toc337471352)

[Dati significativi 92](#_Toc337471353)

[Modulo Livemic 92](#_Toc337471354)

[Scopo 92](#_Toc337471355)

[Sistemi operativi 92](#_Toc337471356)

[Dati significativi 92](#_Toc337471357)

[Modulo Messages 93](#_Toc337471358)

[Scopo 93](#_Toc337471359)

[Sistemi operativi 93](#_Toc337471360)

[Dati significativi 93](#_Toc337471361)

[Modulo Mic 93](#_Toc337471362)

[Scopo 93](#_Toc337471363)

[Piattaforme 93](#_Toc337471364)

[Dati significativi 93](#_Toc337471365)

[Modulo Mouse 95](#_Toc337471366)

[Scopo 95](#_Toc337471367)

[Sistemi operativi 95](#_Toc337471368)

[Dati significativi 95](#_Toc337471369)

[Modulo Password 96](#_Toc337471370)

[Scopo 96](#_Toc337471371)

[Sistemi operativi 96](#_Toc337471372)

[Dati significativi 96](#_Toc337471373)

[Modulo Position 97](#_Toc337471374)

[Scopo 97](#_Toc337471375)

[Sistemi operativi 97](#_Toc337471376)

[Dati significativi mobile 97](#_Toc337471377)

[Modulo Print 98](#_Toc337471378)

[Scopo 98](#_Toc337471379)

[Sistemi operativi 98](#_Toc337471380)

[Dati significativi 98](#_Toc337471381)

[Modulo Screenshot 99](#_Toc337471382)

[Scopo 99](#_Toc337471383)

[Sistemi operativi 99](#_Toc337471384)

[Dati significativi 99](#_Toc337471385)

[Modulo Url 100](#_Toc337471386)

[Scopo 100](#_Toc337471387)

[Sistemi operativi 100](#_Toc337471388)

[Dati significativi 100](#_Toc337471389)

[Appendice: vettori di installazione 100](#_Toc337471390)

[Ottenere un certificato per il Code Signing 101](#_Toc337471391)

[Introduzione 101](#_Toc337471392)

[Installazione del certificato Code Signing 101](#_Toc337471393)

[Elenco dei vettori di installazione 101](#_Toc337471394)

[Sistemi operativi supportati dagli agent 101](#_Toc337471395)

[Vettore Applet Web 102](#_Toc337471396)

[Scopo 102](#_Toc337471397)

[Sistemi operativi 103](#_Toc337471398)

[Parametri 103](#_Toc337471399)

[Vettore Exploit (desktop) 103](#_Toc337471400)

[Scopo 103](#_Toc337471401)

[Installazione 103](#_Toc337471402)

[Eliminazione file non più utilizzati 103](#_Toc337471403)

[Sistemi operativi 103](#_Toc337471404)

[Parametri 103](#_Toc337471405)

[Vettore Melted Application 104](#_Toc337471406)

[Scopo 104](#_Toc337471407)

[Sistemi operativi 104](#_Toc337471408)

[Parametri 104](#_Toc337471409)

[Vettore Network Injection 105](#_Toc337471410)

[Scopo 105](#_Toc337471411)

[Sistemi operativi 105](#_Toc337471412)

[Parametri 105](#_Toc337471413)

[Vettore Offline Installation 105](#_Toc337471414)

[Scopo 105](#_Toc337471415)

[Sistemi operativi 105](#_Toc337471416)

[Parametri 105](#_Toc337471417)

[Vettore Silent Installer 106](#_Toc337471418)

[Scopo 106](#_Toc337471419)

[Sistemi operativi 106](#_Toc337471420)

[Parametri 106](#_Toc337471421)

[Vettore U3 Installation 107](#_Toc337471422)

[Scopo 107](#_Toc337471423)

[Sistemi operativi 107](#_Toc337471424)

[Parametri 107](#_Toc337471425)

[Vettore Exploit (mobile) 107](#_Toc337471426)

[Scopo 107](#_Toc337471427)

[Installazione 107](#_Toc337471428)

[Eliminazione file non più utilizzati 107](#_Toc337471429)

[Esempio comandi per copiare installer nel dispositivo iOS 107](#_Toc337471430)

[Sistemi operativi 107](#_Toc337471431)

[Parametri 108](#_Toc337471432)

[Vettore Installation Package 108](#_Toc337471433)

[Scopo 108](#_Toc337471434)

[Note per sistemi operativi Android 108](#_Toc337471435)

[Note per sistemi operativi Windows Mobile 109](#_Toc337471436)

[Note per sistemi operativi BlackBerry 109](#_Toc337471437)

[Sistemi operativi 109](#_Toc337471438)

[Parametri Android, iOS, WinMobile 109](#_Toc337471439)

[Parametri BlackBerry 109](#_Toc337471440)

[Parametri Symbian 109](#_Toc337471441)

[Vettore Local Installation 110](#_Toc337471442)

[Scopo 110](#_Toc337471443)

[Sistemi operativi 110](#_Toc337471444)

[Parametri 110](#_Toc337471445)

[Vettore QR Code/Web link 110](#_Toc337471446)

[Scopo 110](#_Toc337471447)

[Funzionamento 110](#_Toc337471448)

[Eliminazione file non più utilizzati 110](#_Toc337471449)

[Sistemi operativi 111](#_Toc337471450)

[Parametri 111](#_Toc337471451)

[Vettore WAP Push Message 111](#_Toc337471452)

[Scopo 111](#_Toc337471453)

[Funzionamento 111](#_Toc337471454)

[Installazione 111](#_Toc337471455)

[Eliminazione file non più utilizzati 111](#_Toc337471456)

[Sistemi operativi 111](#_Toc337471457)

[Parametri 112](#_Toc337471458)

[Ottenere un certificato Symbian 113](#_Toc337471459)

[Introduzione 113](#_Toc337471460)

[Sequenza consigliata 113](#_Toc337471461)

[Ottenere l'ID del Editore (voi) 113](#_Toc337471462)

[Creare le chiavi Certificate Public e Private 113](#_Toc337471463)

[Creare il Development Certificate 114](#_Toc337471464)

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.

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

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 in ambienti WiFi.

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.

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

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

| Data rilascio | Codice | Versione software | Descrizione |
| --- | --- | --- | --- |
| 15 Ottobre 2012 | Manuale del tecnico  1.2 OTT-2012 | 8.2 | Aggiunto salvataggio configurazioni base o avanzate come template. Vedi "Cose da sapere sulla configurazione base" a pagina 45 e Vedi "Cose da sapere sulla configurazione avanzata" a pagina 52.  Aggiunto wizard per creazione rapida di una investigazione. Vedi "Descrizione dei wizard da homepage" a pagina 11  Aggiunta gestione dello scout agent. Vedi "Cose da sapere sugli agent" a pagina 34. |
| 30 Giugno 2012 | Manuale del tecnico  1.1 GIU 2012 | 8.1 | Aggiunte funzioni sull'agent vedi "Pagina dell'agent" a pagina 32.  Aggiunto evento Idle vedi "Evento Idle" a pagina 76.  **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 pagina 101**.**  Modificato processo per ottenere certificato per Symbian vedi "Ottenere un certificato Symbian" a pagina 113.  Certificato Code Signing per vettori Melted Application e Silent Installer vedi "Ottenere un certificato per il Code Signing" a pagina 101. |
| 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 | Manuale dell'amministratore di sistema  1.2 OTT-2012 | PDF |
| Manuale dell'amministratore | Amministratori | Manuale dell'amministratore  1.2 OTT-2012 | PDF |
| Manuale del tecnico (questo manuale) | Tecnici | Manuale del tecnico  1.2 OTT-2012 | PDF |
| Manuale dell'analista | Analisti | Manuale dell'analista  1.2 OTT-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.

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:

| 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 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. | 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 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

Di seguito le differenze rispetto alla versione RCS 7.6.

Glossario dei termini

| RCS v. 7.6 | RCS 8.0 e successive |
| --- | --- |
| 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 |
| 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

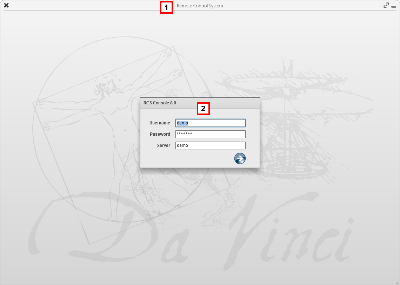
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

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. |
| 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" più sotto. |

Descrizione della homepage

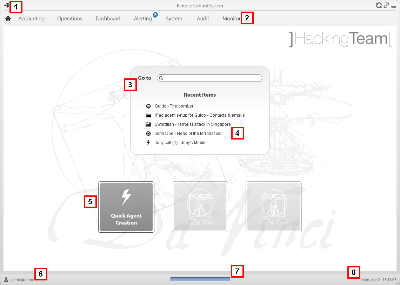
|  |  |
| --- | --- |
| Per visualizzare l'homepage: | * fare clic su |

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. |
| 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

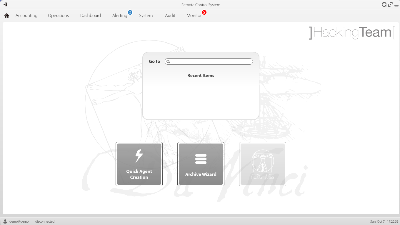
|  |  |
| --- | --- |
| Per visualizzare l'homepage: | * fare clic su |

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 |
| --- | --- |
|  | Apre il wizard per la creazione rapida di un agent.  NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Tecnico. |
|  | Apre il wizard per la gestione 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 42

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. |
| Remove all data from the live system | **Elimina dal database tutte le evidence dell'operation o del target selezionato.**  L'operation o il target restano aperti e funzionanti. Solo il database viene ridotto di dimensione.  PRUDENZA: se combinate questa opzione con il backup istantaneo date un nome particolare al backup in modo che sia evidente che le evidence corrispondenti sono stati eliminate dal sistema. |
| Mark the item as closed | **Chiude l'operation o il target selezionato.**  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 evidence già ricevute. |
| Delete the item from the system | 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 evidence.  PRUDENZA: eliminare un'operation/target è un'azione irreversibile e causa la perdita dei dati associati a quella operation/target. |

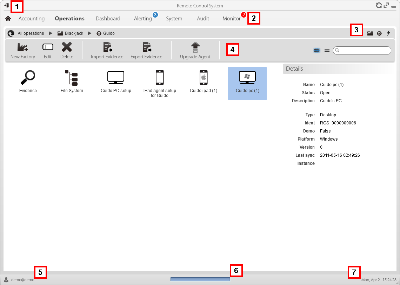
Elementi e azioni comuni dell'interfaccia

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. | |
| 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 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. |

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. |
| Filtrare un testo | Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.  L'esempio mostrerà elementi con descrizioni tipo:   * "myboss" * "bossanova" |
| Filtrare in base a un'opzione | Selezionare un'opzione: compaiono gli elementi che corrispondono all'opzione scelta. |
| Filtrare in base a più opzioni | Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte. |
| Cambiare la dimensione delle colonne | Selezionare il bordo della colonna e trascinarlo. |

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 injection.  Vedi "Gestione dei Network Injector" a pagina 59  NOTA: 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" a pagina 22. |
| 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 pagina 29. |
| 3 | Installare l'agent presso il dispositivo del target nelle modalità scelte.  Vedi "Elenco dei vettori di installazione" a pagina 101. |
| 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 pagina 32. |

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" a pagina 22 |
| 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 pagina 29. |
| 3 | Installare l'agent presso il dispositivo del target nelle modalità scelte.  Vedi "Elenco dei vettori di installazione" a pagina 101. |
| 4 | Alla prima sincronizzazione l'agent compare nella pagina del target.  Vedi "Pagina del target" a pagina 22 |
| 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 pagina 42  Vedi "Configurazione avanzata di una factory o di un agent" a pagina 48. |

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 pagina 22   oppure   * Nella sezione Operations, Target entrare in un agent e aggiornarlo. Vedi "Pagina dell'agent" a pagina 32. |

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:

Pagina del target

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

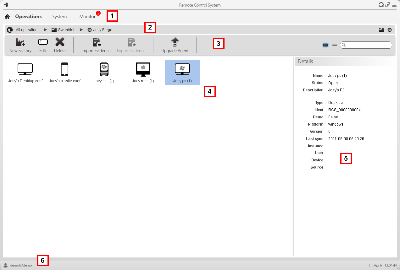
Scopo

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 pagina 42) o per la configurazione avanzata (vedi "Configurazione avanzata di una factory o di un agent" a pagina 48
* 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. |
| 3 | Barre con i pulsanti della finestra. Di seguito la descrizione:  NOTA: il pulsante visualizza gli elementi in elenco con i loro dati.   | 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 pagina 29 | |  | 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 nuovo target. | |  | 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 trasmessa agli agent alla successiva sincronizzazione. | |
| 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 pagina 13.

Per la descrizione dei dati presenti sulla finestra vedi "Dati della pagina target" a pagina 28.

Per saperne di più sui target vedi "Cose da sapere sulle Factory e sugli Agent" a pagina 25

Per gestire rapidamente i dati di un target vedi "Descrizione dei wizard da homepage" a pagina 11.

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. |
| 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. |

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).

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 59

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 pagina 82

Per saperne di più sugli agent vedi "Cose da sapere sugli agent" a pagina 34.

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 pagina 82.

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:

| Dato | Descrizione |
| --- | --- |
| 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. |

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.

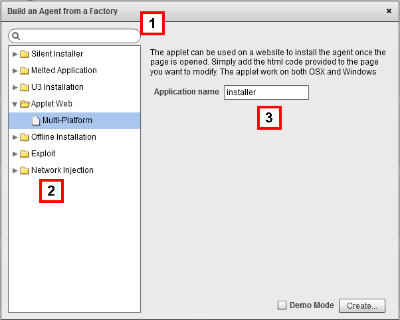
NOTA: per la descrizione dettagliata di ogni vettore di installazione vedi "Elenco dei vettori di installazione" a pagina 101

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 pagina 13.

Per saperne di più sulle factory vedi "Cose da sapere sulle Factory e sugli Agent" a pagina 25.

Per la descrizione dettagliata di ogni vettore di installazione vedi "Elenco dei vettori di installazione" a pagina 101

Creare un agent

Per creare un agent:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare uno o più vettori di istallazione e impostare le opzioni richieste. |
| 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 istallazione 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:

Pagina dell'agent

|  |  |
| --- | --- |
| Per gestire  gli agent: | * sezione Operations, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent |

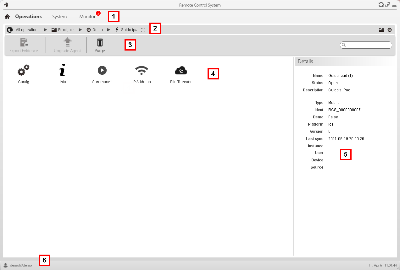
Scopo

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. |
| 3 | Barre con i pulsanti della finestra.  Di seguito la descrizione:   | Icona | Descrizione | | --- | --- | |  | Esporta le evidence dell'agent. | |  | 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. | |
| 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" a pagina 39. | |  | 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" a pagina 37. | |  | Apre la funzione per caricare o scaricare file dal dispositivo del target. Vedi "Trasferimento file da/a il target" a pagina 39 | |
| 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 pagina 13.

Per saperne di più sugli agent vedi "Cose da sapere sugli agent" più sotto.

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.

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 il pseudo 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... | Allora... |
| --- | --- |
| 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:   * 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 evidence 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 evidence 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 29).

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 pagina 37.

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. |
| 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:

| 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. |

Dati dello storico sincronizzazioni dell'agent

Di seguito la descrizione:

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

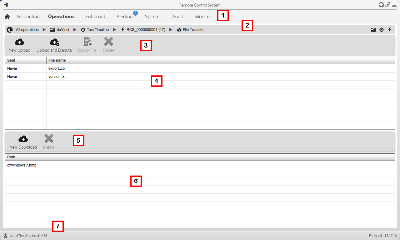
|  |  |
| --- | --- |
| Per trasferire file da/a l'agent: | * sezione Operations, doppio-clic su una operation, doppio-clic su un target, doppio-clic su un agent, doppio clic su File Transfer |

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. | |
| 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. | |  | 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".  Ogni caricamento avvenuto viene registrato nello storico con data-ora e il nome del file. | |  | 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. |
| 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 pagina 13.

Per la descrizione dei dati degli agent vedi "Pagina dell'agent" a pagina 32.

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:

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 29.
* aprire la funzione di configurazione avanzata (vedi "Configurazione avanzata di una factory o di un agent" a pagina 48)

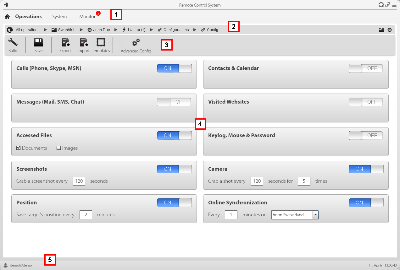
Passi successivi

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 pagina 29 | |  | 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 pagina 37 | |  | 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 pagina 45. | |  | Apre la finestra della configurazione avanzata. Vedi "Configurazione avanzata di una factory o di un agent" a pagina 48.  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 pagina 13.

Per saperne di più sulla configurazione base vedi "Cose da sapere sulla configurazione base" a pagina 45.

Per la descrizione dei dati presenti sulla finestra vedi "Dati della configurazione base" a pagina 45.

Per l'elenco dei moduli disponibili nelle due configurazioni vedi "Elenco dei moduli" a pagina 82

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:   | Se si sta configurando... | Allora... | | --- | --- | | una factory | fare clic su Build per compilarla e ottenere gli agent per diverse piattaforme. Vedi "Compilazione di una factory" a pagina 29. | | 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 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" più sotto.

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.

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" a pagina 57.  Se disabilitata indica che il dispositivo è sempre offline le evidence saranno recuperate fisicamente e importate nel database. Vedi "Pagina del target" a pagina 22 |

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:

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.

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

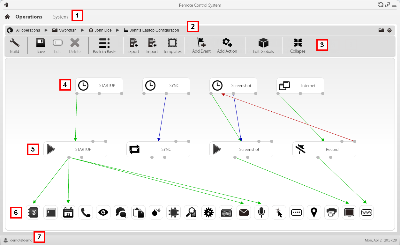
Passi successivi

Per una factory, terminare la sua configurazione e compilarla per ottenere l'agent da installare.Vedi "Compilazione di una factory" a pagina 29

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. |
| 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 pagina 29 | |  | 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 pagina 52. | |  | Inserisce un evento. | |  | Inserisce un'azione. | |  | Modifica i dati globali dell'agent vedi "Dati globali dell'agent" a pagina 56. | |  | 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 pagina 13.

Per saperne di più sulla configurazione avanzata vedi "Cose da sapere sulla configurazione avanzata" a pagina 52.

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 pagina 73 * 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 pagina 82. |
| 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 evidence, 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 pagina 73 * 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 pagina 67. |
| 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 pagina 82.   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). |

Cose da sapere sulla configurazione avanzata

Configurazione avanzata

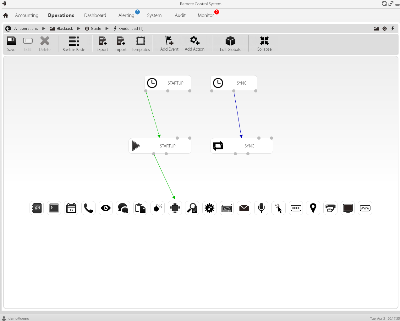
La configurazione avanzata di una factory/agent permette di creare delle sequenze complesse di attivazione tramite una semplice interfaccia grafica.

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.

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 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 73.

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 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 67

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:

| Relazione tra  azione e moduli | Descrizione | Connettore |
| --- | --- | --- |
| 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:

| Relazione tra  azione e eventi | Descrizione | Connettore |
| --- | --- | --- |
| 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 evidence dal dispositivo del 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 modulo posizione + ferma modulo screenshot). Per l'elenco completo vedi "Elenco dei moduli" a pagina 82.

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.

Dati globali dell'agent

I dati globali dell'agent sono descritti di seguito:

| 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 della successiva sincronizzazione. Se la sincronizzazione non avviene, non vengono acquisite ulteriori evidence. |
| Wipe | Se abilitato, cancella in modo sicuro i file generati dall'agent. Nessuna traccia dell'agent sarà rilevabile in caso di un'analisi forense.  NOTA: questa modalità richiede un tempo maggiore rispetto alla normale eliminazione del file. |
| 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 |

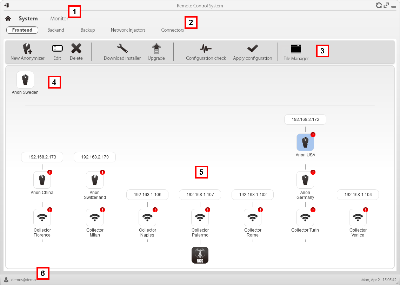
Scopo della funzione

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 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.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



| Area | Descrizione |
| --- | --- |
| 1 | Menu di RCS. |
| 2 | Menu System. |
| 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 pagina 13.

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:

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.

Cosa è possibile fare

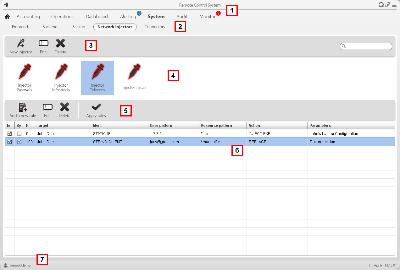
Con questa funzione è possibile:

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

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. |
| 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. | |  | Elimina la regola selezionata. | |  | Aggiorna la configurazione del 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. . |

Per saperne di più

Per la descrizione degli elementi di interfaccia Vedi "Elementi e azioni comuni dell'interfaccia" a pagina 13.

Per la descrizione dei dati delle regole di injection vedi "Dati delle regole di injection" a pagina 62.

Per saperne di più sulle regole di injection vedi "Cose da sapere su Network Injector e le sue regole" a pagina 62.

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" a pagina 62. * 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:

| Dato | Descrizione |
| --- | --- |
| Name  Description | Descrizioni libere. |
| Version | Versione software. |
| Address | Indirizzo IP dell'apparato. |
| Port | 4444. |
| 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 | Ultimi messaggi registrati nei log.  : aggiorna l'elenco.  : elimina i log visualizzati. |

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.
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.

Quando si è riusciti a identificare la connessione del target e si è deciso il metodo di attacco, 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 di Network Injector. 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.

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 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 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 | Metodo di identificazione del traffico del target. Il formato dipende dal tipo di Ident selezionato.   | Metodo | Formattazione | | --- | --- | | **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 | Metodo di identificazione della risorsa da infettare, applicato all'URL della risorsa Web. Il formato dipende dal tipo di Action selezionata.  NOTA: lasciare vuoto se l'azione selezionata è INJECT-UPGRADE.   | Tipo azione | Contenuto di Pattern risorsa | | --- | --- | | INJECT-EXE | URL del file eseguibile da infettare. Utilizzare le wildcard per aumentare il numero di URL corrispondenti.  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 '.' dell'estensione del file, saranno infettate tutte le pagine che contengono accidentalmente le lettere "exe". | | INJECT-HTML | URL della pagina web da infettare.  Esempi di formati possibili:  www.oracle.com/  www.oracle.com/index.html  NOTA: se non si specifica una pagina HTML o dinamica, includere nell'indirizzo del sito il carattere '/' finale (es.: "www.oracle.com/").  NOTA: non è possibile infettare una pagina di redirect. Verificare sul browser il path corretto del sito web prima di indicarlo nella regola. | | INJECT-UPGRADE | Non utilizzato. | | REPLACE | URL della risorsa da sostituire. | |
| Action | Metodo di infezione che verrà applicato sulla risorsa indicata in Resource pattern:   | Metodo | Descrizione | | --- | --- | | 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 | Aggiunge un applet Java alla pagina Web. 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 acquistare un certificato valido per firmare l'applet Java.  Richiede assistenza: contattare i tecnici HackingTeam per ulteriori dettagli. | | 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.  Suggerimento: 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. |

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

Descrizione dati sotto-azioni

Di seguito la descrizione delle sotto-azioni:

| Dato | Descrizione |
| --- | --- |
| 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:

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

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".

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

| Campo | Descrizione |
| --- | --- |
| 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 32

Sistemi operativi

Desktop:Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri

| Nome | Descrizione |
| --- | --- |
| **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 Synchronyze



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 evidence raccolte dall'agent, con contestuale rimozione sicura. |
| 8 | Rimozione sicura nell'agent di tutte le evidence scaricate. |

Sistemi operativi

Desktop:Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Parametri desktop

| Nome | Descrizione |
| --- | --- |
| **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

| Nome | Descrizione |
| --- | --- |
| **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 | Internet: sincronizzazione tramite connessione Internet.   * 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.   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.  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.

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

Descrizione dati eventi

Di seguito la descrizione degli eventi:

| Dato | Descrizione |
| --- | --- |
| 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:

| Evento | Dispositivo | Innesca un'azione quando.. |
| --- | --- | --- |
| AC | 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 | l'agent rileva una connessione alla rete attiva. |
| Idle | desktop | l’utente non interagisce col computer per un determinato periodo di tempo. |
| Position | mobile | il dispositivo raggiunge o lascia una posizione specifica. |
| Process | desktop, mobile | sul dispositivo viene lanciato un'applicazione 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 è 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. |

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 |
| --- | --- |
| **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

| Nome | Descrizione |
| --- | --- |
| **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. |

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. |
| 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 evidence 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

| Nome | Descrizione |
| --- | --- |
| **Quota** | Spazio disco da usare per salvare le evidence 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'eventoSimChange 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 BlackBerry non cancellano i messaggi in ingresso.

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

Sistemi operativi

Mobile: Android, BlackBerry, Symbian, WinMobile

Parametri

| Nome | Descrizione |
| --- | --- |
| 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'eventoStandby 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’innesco e il disinnesco 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

| Nome | Descrizione |
| --- | --- |
| **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

Di seguito la descrizione dei moduli di registrazione:

| Modulo | Configurazione | Dispositivo | Registrazione di... |
| --- | --- | --- | --- |
| Accessed files | base | 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 (Skype, BlackBerry Messenger). |
| Clipboard | avanzata | desktop, mobile | informazioni copiate nella clipboard. |
| Contacts and Calendar | base | desktop, mobile | contatti e calendario. |
| Dispositivo | 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 salvate. |
| Messages | avanzata | desktop, mobile | e-mail, SMS, MMS. |
| Messages | base | desktop, mobile | e-mail, SMS e chat. |
| Mic | avanzata | desktop, mobile | audio proveniente dal microfono. |
| Mouse | avanzata | desktop | clic del mouse. |
| Password | avanzata | desktop | password salvate. |
| Position | base, avanzata | desktop, mobile | posizione geografica del target. |
| Print | avanzata | desktop | pagine inviate alla stampante. |
| Screenshots | base, avanzata | desktop, mobile | schermata attive sul display del target. |
| URL | avanzata | desktop, mobile | URL visitati. |
| Visited websites | base | desktop, mobile | URL visitati. |

Di seguito la descrizione dei moduli di altro tipo:

| Modulo | Configurazione | Dispositivo | Azione |
| --- | --- | --- | --- |
| Conference | avanzata | mobile | Crea una chiamata a tre. |
| Crisis | avanzata | desktop, mobile | Riconosce situazioni di pericolo (es.: esecuzione di uno sniffer). Può disabilitare temporaneamente la sincronizzazione e l'esecuzione di 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. |

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 evidence 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:

| Campo | Descrizione |
| --- | --- |
| 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:

| Campo | Descrizione |
| --- | --- |
| 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 evidence distinta.

Sistemi operativi

Desktop: Windows, OS X

Mobile: BlackBerry

Dati significativi

Nessuno

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

NOTA: il BlackBerry supporta l'applicazione BBM e Google Talk.

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 delle 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:

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

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

| Campo | Descrizione |
| --- | --- |
| 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 della applicazioni installate.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Dati significativi mobile

Di seguito la descrizione dei dati:

| Campo | Descrizione |
| --- | --- |
| 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:

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



Scopo

Il modulo Infection viene utilizzato per propagare l'agent su dispositivi diversi dal quello attuale. L'infezione può essere propagata su:

* un apparecchio mobile collegato al computer (es: via USB).
* altri utenti dello stesso computer (è necessario avere infettato almeno un utente).
* Virtual Machine installate
* chiavi USB. Una volta infettata la chiave USB diffonderà l'agent su tutti i computer che la apriranno utilizzando la funzione di Autoplay.

Se la propagazione va a buon fine, si vedranno comparire nella stessa attività dell’agent in questione le istanze relative ai nuovi dispositivi infettati.

NOTA: questo modulo non crea evidence.

Sistemi operativi

Desktop: Windows

Dati significativi

Di seguito la descrizione dei dati:

| Campo | Descrizione |
| --- | --- |
| Infect mobile devices | Abilita l'infezione di dispositivi Windows Mobile o BlackBerry collegati al computer. |
| Infect other local users | Copia l'agent su altri utenti dello stesso computer. |
| Infect USB drives | Diffonde l'agent su tutte le chiavi USB inserite nel computer. |
| Infect VMWare virtual machines | Infetta le Virtual Machine installate nel computer. |

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:

| Campo | Descrizione |
| --- | --- |
| 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: Android, BlackBerry (solo e-mail e SMS), iOS (solo SMS e MMS), WinMobile

Dati significativi

Di seguito la descrizione dei dati:

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

Dati significativi

Di seguito la descrizione dei dati:

| Campo | Descrizione |
| --- | --- |
| Silence between voices | 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.  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. |
| Voice recognition | NOTA: non supportata da iOS, BlackBerry e Symbian.  Valore per identificare la voce umana ed escludere dalla registrazione eventuali rumori di fondo.  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. |
| Autosense | 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. |

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 91.

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.

Sistemi operativi

Desktop: Windows, OS X

Mobile: Android, BlackBerry, iOS, Symbian, WinMobile

Dati significativi

Di seguito la descrizione dei dati:

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

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](http://www.verisign.com/))
* Thawte ([http://www.thawte.com](http://www.thawte.com/))
* GoDaddy ([http://www.godaddy.com](http://www.godaddy.com/))

Installazione del certificato Code Signing

Sul sistema Backend, dalla cartellaC:\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:

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

Di seguito l'elenco dei vettori:

| Installation Vector | Dispositivo | Descrizione |
| --- | --- | --- |
| Applet Web | Desktop | Genera codice HTML ed una applet Java da inserire in una pagina Web. |
| Exploit | Desktop, Mobile | Inserisce l'agent in un qualsiasi documento (il formato del documento può dipendere dagli exploit disponibili). |
| 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 eseguibile. |
| Network Injection | Desktop | Rimanda alla pagina di creazione delle regole di injection. *Vedi "*Gestione dei Network Injector*"* a pagina 59*.* |
| Offline Installation | Desktop | Crea un file ISO per la generazione di un CD/DVD/USB di avvio da utilizzare su un computer spento o ibernato. |
| 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 l'agent. |
| U3 Installation | Desktop | Crea un pacchetto da installare su chiave U3. La chiave U3 installa l'agent automaticamente al suo inserimento sul dispositivo del target. |
| Wap Push Message | Mobile | Invia un messaggio WAP, che se il target accetterà, installerà l'agent. |

Vettore Applet Web

Scopo

La compilazione crea un file .zip che contiene del codice HTML e un applet associata, compatibile con tutti i sistemi operativi desktop.

È possibile aggiungere questo il codice HTML a qualsiasi sito Web dove è possibile modificare le pagine sorgente. I visitatori delle pagine Web infettate si troveranno l'agent automaticamente installato sul dispositivo usato per la navigazione.

NOTA: questa operazione è simile a quanto fanno le regole di injection di un Network Injector. Con la sola differenza che le regole identificano il flusso dati e vi iniettano l'applet, mentre l'applet Web viene appositamente inserita in un sito web creato all'occorrenza o esistente.

Sistemi operativi

Multipiattaforma.

Parametri

| Nome | Descrizione |
| --- | --- |
| Application name | Norme libero dell'applet |

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 57.

Sistemi operativi

OS X, Windows

Parametri

| Nome | Descrizione |
| --- | --- |
| 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

OS X, Windows

Parametri

| Nome | Descrizione |
| --- | --- |
| Require administrative privileges | Durante l'installazione dell'agent sono necessari i privilegi di amministratore. |
| Application to be used as dropper | File eseguibile a cui inserire aggiungere l'agent.  Il tipo di file è diverso in base al sistema operativo:   * 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. |
| 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). |
| 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 "Ottenere un certificato per il Code Signing" a pagina 101.  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 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

| Nome | Descrizione |
| --- | --- |
| 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 | 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.  Sono disponibili tre opzioni per la cattura dei documenti:   * 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

| Nome | Descrizione |
| --- | --- |
| Require administrative privileges | Durante l'installazione dell'agent sono necessari i privilegi di amministratore.  I comportamenti sono diversi in base al sistema operativo:   * 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. |
| 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 evidence 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 "Ottenere un certificato per il Code Signing" a pagina 101.  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 57.

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

| Nome | Descrizione |
| --- | --- |
| 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  ... | Parametri che identificano il file da infettare.  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

IMPORTANTE: per i Symbian seguire la procedura di ottenimento del certificato. Vedi "**Ottenere un certificato Symbian**" a pagina 113.

Note per sistemi operativi Android

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

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

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

Di seguito la procedura per l’installazione:

| Passo | Azione |
| --- | --- |
| 1 | Selezionare ed eseguire sul dispositivo l’installer APK appropriato. |
| 2 | Dopo l’esecuzione dell’installer APK, accettare i permessi richiesti in fase di installazione. |
| 3 | Se il dispositivo Android ha installato il package SU (root) accettare i permessi aggiuntivi richiesti.  IMPORTANTE: l’installer di default per Android 3.x e 4.x si mostra come una normale applicazione denominata BitCompress, che finge di ottimizzare le trasmissioni di rete del dispositivo. |

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.

Sistemi operativi

Android, BlackBerry, iOS, Symbian, WinMobile

Parametri Android, iOS, WinMobile

| Nome | Descrizione |
| --- | --- |
| Application name | Nome dell'applicazione (visibile al target) |

Parametri BlackBerry

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

Parametri Symbian

| Nome | Descrizione |
| --- | --- |
| 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:   * 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 57.

Sistemi operativi

Android, BlackBerry, Symbian, WinMobile

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

Parametri

| Nome | Descrizione |
| --- | --- |
| 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 |
| 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**" a pagina 113.

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 pagina 57.

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

| Nome | Descrizione |
| --- | --- |
| 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 ha installato il pacchetto su un altro sito Web, specificarne l’URL. |
| Service Type | Tipo di servizio richiesto:   * 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](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. |

|  |  |
| --- | --- |
| RCS 8.2 Manuale del tecnico  Manuale del tecnico 1.2 OTT-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 |