Malware e Trojan di Stato - AvANa - Groups - we.riseup.net

ed altri metodi invasivi di controllo dei computer.

Un malware e' una sorta di virus: e' un programma che si nasconde nel computer con finalita' malevoli. Alcuni malware vendono i tuoi dati alle aziende che si occupano di pubblicita', altri scoprono la password della tua email per utilizzare il tuo indirizzo per mandare email di spam. I malware della polizia sono utilizzati principalmente per:

- registrare cio' che appare sullo schermo (*screenshot*)
- registrare i tasti che premi e le parole che digiti sulla tastiera (*keylogger*)
- permettere da remoto di vedere i dati contenuti nel tuo disco e copiarli.

Telecom-Sismi

In questo caso il malware ancora non veniva utilizzato come strumento di repressione, ma solo come pratica per recuperare informazioni per operare dei ricatti ad uso e consumo dei servizi segreti.

Il caso telecom e del tiger team di fabio ghioni, di cui trovi anche su wikipedia volendo. Anche loro ci davano di backdoor e attacchi mirati a recuperare informazioni.

> Tra gli arrestati, Marco Mancini (arrestato anche in relazione al sequestro di Abu Omar), ex numero 2 del SISMI, Giuliano Tavaroli, ex direttore della Security del Gruppo Telecom Italia, ed Emanuele Cipriani, investigatore che da anni ha aperto una fiorente società di investigazioni a Firenze, la Polis d'Istinto (i cui uffici sono in un appartamento della nuora di Licio Gelli, del cui marito Cipriani è amico), oltre ad alcuni membri del Tiger Team, il gruppo di hacker gestiti da Tavaroli.
>
> Cipriani avrebbe costruito illecitamente, per conto di Tavaroli (all'epoca a capo della security di Telecom), numerosi dossier su varie personalità politiche, economiche e dello spettacolo, oltre a giornalisti e calciatori[2]: non solo dossier con regolare mandato, ma arricchiti di informazioni raccolte con metodi illegali (detti "pratiche grigie", dal colore della copertina), ma addirittura dossier per i quali era stato dato incarico a Cipriani per le "vie brevi", non risultante pertanto da nessun mandato scritto (le "pratiche celesti")
>
> Presso Mirko Meacci gli investigatori trovano dei DVD contenenti i back-up degli hard-disk con tutto l'archivio "Z", ossia le "pratiche celesti". L'accesso è criptato e solo la confessione del Cipriani, dopo un lungo periodo di detenzione cautelare, permette di stampare quei dossier, che vengono immediatamente segretati.
> In una pen-drive trovata a Tavaroli gli inquirenti trovano "bozze delle decisioni dell'Antitrust, comunicazioni di funzionari, atti di legali difensori nella causa di Telecom davanti all'Antitrust".
>
> Nel gennaio e nel marzo 2007 altri provvedimenti di arresto colpiscono varie persone coinvolte nella vicenda, tra cui Fabio Ghioni e il suo Tiger Team (Andrea Pompili, Rocco Lucia e altri), di Telecom, e nuovamente Giuliano Tavaroli (all'epoca già in carcere) e Mancini. Tra gli arresti del marzo 2007 rientrano anche ex poliziotti ed un ex agente della CIA.
>
> A Ghioni i magistrati contestano anche di aver ottenuto, oltre che da fornitori di Telecomitalia, da Cipriani e Bernardini ingenti somme di danaro per svolgere intrusioni informatiche,su incarichi che egli stesso commissionava. Tali somme, riversate su conti esteri di prestanomi e della fiduciaria neozelandese Finefin, sono state solo in parte recuperate.
>
> I vari capi di imputazione comprendono i reati di associazione a delinquere finalizzata alla corruzione di pubblici ufficiali, rivelazione del segreto d'ufficio, appropriazione indebita, falso, favoreggiamento e riciclaggio.

Operazione Ardire

blog culmine: negli atti che aveva pubblicato sul proprio sito il tgcom mi sembra, si parlava di una backdoor installata sul pc di uno di loro e c'erano degli screenshot di attivita' svolte al pc in corrispondenza di intercettazioni ambientali.

> Un ruolo fondamentale ce l'avevano internet e i blog. In particolare, si legge nell'ordinanza del giudice per le indagini preliminari, emerge "la centralità, funzionale alla stessa esistenza dell'associazione sovversiva in esame, dei 'blogs' gestiti da Fosco Stefano Gabriele , in ciò coadiuvato da Di Bernardo Elisa, in particolare, tramite il blog Culmine".

fonti: Yahoo

Cile

Poi c'e' il caso del cile di cui avevamo parlato anche su cavallette

> Su cryptome.org e' apparso un contributo dal Cile, che descrive i metodi di intercettazioni utilizzati in una grossa inchiesta che ha coinvolto piu' di 200 persone e portato all'arresto di 14 attivisti, liberati solo quest'anno, senza piu' accuse a loro carico, nel frattempo pero' hanno fatto due anni di carcere.
> Il materiale citato fino al 2010 comprende trascrizioni di telefonate e di chat su msn, screenshot di sessioni web ottenute da file temporanei recuperati dall'indagine forense, screenshot di account gmail crackati, un'analisi superficiale di alcuni siti frequentati dagli indagati, tra i quali nodo50.org, indymedia.org, riseup.org. In ultimo chat con Otr e mail cifrate con Gpg, che compaiono pero' cifrate.
> Dal 2010 fino ad oggi si nota una maggiore attenzione al web. Trascrizioni di chat su crypto.cat, accesso a piu' di 20 account su gmail e altri su facebook, ancora chat con Otr e mail con Gpg, con annessa richiesta di aiuto all'Fbi per la decifratura. Un'analisi piu' approfondita dei servizi di media "alternativi" utilizzati dagli indagati. C'e' un analisi piuttosto approfondita di riseup.net.

Descrizione approfondita su cryptome.org/2012/07/chile-comments.htm

Syria

Poi ci sono storie interessanti tipo: DarkComet Analysis – Understanding the Trojan used in Syrian Uprising

> On February 17th the CNN published an interesting article, where some Syrian's regime opponents claimed that the government was using a Trojan to monitor and disrupt the protestor's network. Apparently the regime has been using a well-known social engineering technique: impersonate a trusted person then attack from the inside. It is not possible to confirm the story but this is what is being told by the opponents of the regime: apparently one of the protestors was brought to jail and promptly forced to hand over his passwords. Those passwords were used later on to access his Skype account and infiltrate the network of protestors, spreading via chat a program containing some malicious code. In other cases the same file was delivered as a Facebook Chat security update, together with a Facebook icon, while some other people claim that it was also sent by mail. Whatever the means, the common sign among all the stories is that this file, after being opened, did simply nothing and even the antivirus didn't complain at all.

altri link:

Fake YouTube Site Targets Syrian Activists With Malware
New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan
Campaign Targeting Syrian Activists Escalates with New Surveillance Malware
New Trojan Spread Over Skype as Cat and Mouse Game Between Syrian Activists and Pro-Syrian-Government Hackers Continues
Fake Skype Encryption Tool Targeted at Syrian Activists Promises Security, Delivers Spyware

Il CCC ed il Trojan di stato tedesco

In breve

La polizia tedesca si dota di uno strumento potentissimo per mettere malware molto potenti su larga scala. In pratica, sono in grado di infettare computer in modo da poterli controllare, registrare quello che avviene sopra, prendere dati e molto altro.

Chi lo voleva:

La legalizzazione di questo "strumento" fu promossa dall'ex ministro degli Interni Wolfgang Schäuble, e dal presidente del Bundeskriminalamt (Polizia criminale federale), Jörg Ziercke, e **promosso dal 2007** con i soliti argomenti.
Uno di questi argomenti diceva che le autorità dovrebbero essere in grado di agire sullo stesso terreno degli jihadisti, per impedire il loro reclutamento attraverso la rete.

già in passato lo stesso Ziercke si era lamentato della difficoltà della polizia tedesca di poter intercettare le telefonate via skype:

> A piangere questa volta è nientemeno che Joerg Ziercke (nella foto qui sopra), uno dei papaveri più importanti tra le forze dell'ordine tedesche: è presidente dell'Ufficio della Polizia Federale, BKA. A suo dire "la cifratura del software telefonico Skype ci sta creando grandi difficoltà. Non lo possiamo decifrare. Ed è per questo che ora parliamo di sorveglianza delle telecomunicazioni alla fonte, il che significa intercettare la fonte prima che la cifratura venga effettuata o dopo che il contenuto viene decifrato".

peraltro trojan annunciato:

> "Berlino – Suscita attenzione una notizia pubblicata nei giorni scorsi dal quotidiano tedesco Suddeutsche Zeitung secondo cui i cybercop tedeschi si doteranno a breve di un nuovo strumento di indagine, ovvero della possibilità di penetrare da remoto nei PC delle persone sospette."

La scoperta:

La scoperta per merito del chaos computer club 1 (spiega tecnica in tedesco 3).

> **fine 2011** Il famigerato "trojan di stato" teutonico, da anni spauracchio di tutti i difensori della privacy e dei diritti digitali, sarebbe stato finalmente individuato: il collettivo hacker noto come Chaos Computer Club (CCC) ha pubblicato un rapporto con tanto di file binari appartenenti al malware, accusando in maniera diretta il governo di pratiche spionistiche.

Perquisizione:

da punto-informatico.it

```
 L'oscura attrazione delle autorità di sicurezza tedesche per Skype, per l'intercettazione delle chiamate VoIP e per i sequestri a distanz
```

L'Ammissione:

da punto-informatico

```
Roma - Dopo le rivelazioni dei giorni scorsi da parte del Chaos Computer Club sull'esistenza di un virus trojan finalizzato a un vero e pr
Oltre al Ministro degli Interni della Baviera, Joachim Herrmann, i Ministri degli Interni di altri quattro stati, Baden-Württemberg, Branc
```

Quanti utenti coinvolti?

le autorita' svagheggiano

da punto-informatico.it

```
Un'interrogazione parlamentare per appurare cifre e obiettivi dell'attività di sorveglianza informatica statale agita lo spauracchio del t
Nelle 46 pagine di confronto parlamentare, il ministro interpellato non manca di rispondere con perizia ai quesiti relativi all'entità del

Risposte che confermerebbero l'atteggiamento elusivo delle autorità tedesche, ma che, a ben vedere, appaiono ben lungi da convalidare le p
```

Trojan Skype:

Inoltre legato alla vicenda del trojan di stato c'è la pubblicazione di wikileaks (è il partito pirata tedesco che ha sottrato documenti al governo bavarese) che riguarda lo SKYPE TROJAN:

```
The pdf file obtained by Wikileaks and also released by the german political party PiratenPartei, contains two scanned documents relating
```

"Skype Capture Unit"
nel 2008, l'azienda DigiTask si è evidenziata quando su Wikileaks apparve l'offerta che la magistratura penale di Baviera aveva presentato. I documenti rivelano che la DigiTask offrì una specifica "Skype Capture Unit" al prezzo di 3.500 euro mensili per posto di lavoro.
Con essa si potrebbero ascoltare parallelamente dieci conversazioni telefoniche su Skype. Il Trojan inoltre faciliterebbe l'accesso ai servizi Skype come chat o invio di file, così come l'elenco dei contatti.

"Software di protezione specifico"
La società DigiTask si è inoltre presentata in diverse mostre dei sistemi di sorveglianza come produttore di "software per analisi forense a distanza".
"DigiTask S.L. è un leader nazionale che fornisce soluzioni per la sicurezza e comunicazioni alle amministrazioni pubbliche", secondo il sito web della società. ORF.at ha presentato domenica in DigiTask una richiesta scritta d'informazioni dettagliate.

Dettagli Tecnici:

dal comunicato del ccc:

```
L'analisi del CCC rivela funzionalità del "Bundestrojaner luce" (Bundestrojaner significa "trojan federale" ed è il termine colloquiale te
Ciò significa, un "percorso di aggiornamento" di Quellen-TKU alle funzionalità del Bundestrojaner completo è integrato fin dall'inizio.  L

L'analisi conclude che non gli sviluppatori del Trojan anche cercato di mettere in garanzie tecniche per assicurarsi che il malware può es
L'analisi conclude che gli sviluppatori del Trojan non hanno cercato di garanzie tecnicamente che il malware può essere utilizzato
esclusivamente per le intercettazioni di telefonia internet, come stabilito dal giudice costituzionale. Al contrario, il disegno incluso f

L'analisi ha inoltre rivelato gravi falle di sicurezza del Trojan. Le schermate e file audio che manda fuori vengono crittografati male, i
E 'anche concepibile che le forze dell'ordine "infrastrutture potrebbe essere attaccato attraverso questo canale. Il CCC non ha ancora ese

"Siamo rimasti sorpresi e sconvolto per la mancanza di sicurezza, anche elementare nel codice. Qualsiasi utente malintenzionato potrebbe a
Per evitare di rivelare la posizione del server di comando e controllo, tutti i dati vengono reindirizzati tramite un server dedicato in a
```

da altre fonti:

```
Il malware apre una backdoor per Windows, contiene una libreria dinamica (.dll) e un driver di livello kernel, con all'interno un ulterior
Un'altra importante caratteristica del malware è la capacità di catturare screenshot e registrare audio - incluse le chiamate su Skype - u
```

da f-secure:

```
The backdoor includes a keylogger that targets certain applications. These applications include Firefox, Skype, MSN Messenger, ICQ and oth
The backdoor also contains code intended to take screenshots and record audio, including recording Skype calls.
In addition, the backdoor can be remotely updated. Servers that it connects to include 83.236.140.90 and 207.158.22.134.
We do not know who created this backdoor and what it was used for.
We have no reason to suspect CCC's findings, but we can't confirm that this trojan was written by the German government. As far as we see,
```

Risvolti Legali:

da punto-informatico:

```
Lo ha deciso la massima corte tedesca: se i cittadini sapessero che girano sui PC trojan di stato potrebbero trattenersi dal comunicare in

Corte Costituzionale tedesca non ha alcuna intenzione di consentire alle forze dell'ordine di infettare i computer degli utenti Internet c

In particolare, il tribunale di Karlsruhe ha stabilito che la sola nozione dell'utilizzo di strumenti di questo tipo potrebbe tradursi in

"Raccogliere dati di quel tipo in modo così diretto comprime i diritti del cittadino - hanno spiegato i magistrati - dato che la paura di
```

da punto-informatico

```
La Corte Costituzionale tedesca si era pronunciata a riguardo: le intercettazioni a mezzo trojan avrebbero compresso le libertà fondamenta

Una proposta difficile, da un lato perché i criminali veri, o i terroristi organizzati, difficilmente potranno essere ingannati da un malw
```

Legislazione

Sarebbe carino capire come è andata a finire questa faccenda 5, ed allo stato attuale a che punto siamo a livello di legislazione

cito da punto-informatico.it:

"Per facilitare queste sinergie, il Consiglio propone di istituire una piattaforma comune a cui fare riferimento, presso la quale segnalar

ancora da punto-informatico.it, sempre un articolo piuttosto datato (2008):

"Sarà dunque legale distribuire spyware e vigilare sul computer del sospetto, le forze dell'ordine potranno battere a tappeto i dispositiv

Malware di stato in Spagna

In Spagna il Ministro della Giustizia ha presentato il progetto di legge “Borrador del Código Procesal Penal”, nel quale si autorizzano le forze di polizia ad installare malware sui device (PC o altro).

In base all’Art. 350 di questa bozza, gli inquirenti possono richiedere al giudice l’autorizzazione “all’installazione di software che permetta l’analisi remota dei contenuti di computer e altri device, di sistemi informatici in generale, di strumenti per lo storage e l’archiviazione, di database – senza che l’oggetto di tale osservazione ne sia consapevole”.

Secondo la bozza, la magistratura potrebbe rilasciare l’autorizzazione per i casi di investigazione di delitti con pene massime superiori ai tre anni di reclusione, per terrorismo, per le organizzazioni criminali e per i reati telematici.

Una volta ottenuta l’autorizzazione, "Le autorità e gli agenti coinvolti nelle indagini potranno ordinare a qualsiasi persona che conosca il funzionamento del sistema informatico o le misure applicate per proteggere i dati contenuti esso di collaborare al recupero delle informazioni necessarie per il buon esito della procedura”

Le autorità e gli agenti coinvolti nelle indagini potranno impartire ordini a qualsiasi persona che conosca il funzionamento del sistema informatico o le misure applicate per proteggere i dati informatici contenuti nel sistema che faciliti le informazioni necessarie per il buon esito della procedura".

“Borrador del Código Procesal Penal” in pdf
www.fiscal.es/cs/Satellite?c=FG_Multime...

rif.: www.edri.org/edrigram/number11.12/spain...

Spanish police might use trojans to spy computers (4.06.2013)
www.neurope.eu/article/spanish-police-m...

The police will be able to use Trojans to investigate computers and tablets (only in Spanish, 3.06.2013)
sociedad.elpais.com/sociedad/2013/06/03...

Trojans in my computer? Possible? So what? (only in Spanish, 5.06.2013)
www.internautas.org/html/7603.html

El troyano de Gallardón sería ilegal y “fácilmente detectable” por el antivirus
www.elconfidencial.com/tecnologia/2013/...

Legalising the use of Trojan viruses by the police puts in question citizen fundamental rights (only in Spanish, 6.06.2013)
www.internautas.org/html/7604.html

DaVinci/RCS e l’Hacking Team di Milano

Reporto completo su due casi di utilizzo di un malware commerciale forkato per attività illecite.

In this report, Citizen Lab Security Researcher Morgan Marquis-Boire describes analysis performed on malicious software used to compromise a high profile dissident residing in the United Arab Emirates. The findings indicate that the software is a commercial surveillance backdoor distributed by an Italian company known as Hacking Team. The report also describes the potential involvement of vulnerabilities sold by the French company, VUPEN.

rif.: citizenlab.org/2012/10/backdoors-are-fo...

Android Malware

Malware used to spy on Tibetan activists and other ethnic groups in China is nothing new. But a new Trojan discovered by researchers at Kaspersky Labs has widened the scope of this digital espionage and intimidation. The malware uses a combination of e-mail hacking, “spear phishing,” and a Trojan built specifically for Android smartphones. Kaspersky claims this is the first discovery of a targeted attack that uses mobile phone malware.

When opened, the Trojan installs an app called “Conference” on the Android devices’ desktops. If the app is launched, it displays a fake message from the chairman of the WUC—while sending back a message to a command and control server to report its successful installation. The malware provides a backdoor to the device via SMS messages sent by the server. On command, it returns the phone’s contact lists, call logs, data about the smartphone, its geo-location data, and any SMS messages stored on it to a server via a Web POST upload.

rif.: www.securelist.com/en/blog/208194186/An...

h3: Altri link

Android Malware Genome Project will catalog, share Android malware

First targeted attack to use Android malware discovered

More malware found hosted in Google’s official Android market

La Spagna vuole i trojan di stato

Conclusioni

Trojan, Malware e Backdoor non sono uno strumento d'indagine particolarmente frequente in Italia. Anche perche' appunto le intercettazioni di robe telematiche sono una molto piccola percentuale delle intercettazioni, tipo molto meno del 10%, la stragrande maggioranza sono telefoniche, e poi ambientali, secondo le statistiche pubbliche formite dal ministero.

Probabilmente siamo ancora lontani da scenari come quello tedesco o cileno, probabilmente non vengono ancora sviluppati software dedicati… ma siamo sicuri che sia uno scenario molto prossimo.

In generale, sul comportamento generale dei servizi segreti nei confronti delle ICT (specie in relazione ai moderni social network) c'è questo articoletto abbastanza interessante, per quanto generico: www.valigiablu.it/come-i-servizi-segret...

cose ancora da guardare

hakcing team

analisi
leaks
slides

Comments