~~Trojan di Stato~~ (Ops, captatori informatici)

ovvero come lo stato gioca a fare il blackhat

Andrea Ghirardini

Di cosa parleremo

- Cosa sono
- Perché ci sono
- Chi li usa
- Chi ne abusa
- Cosa fare
- Come difendersi

Chi sono …

- Andrea Ghirardini aka «Pila»
- Specialista in Digital Forensics
- Drogato di tecnologia
- Background come specialista di sistemi Enterprise
- Ho lavorato per una Telco
- Ho progettato sistemi per l'intercettazione per una nota azienda
- Ora con «Hermes Group» mi interesso di privacy

(No, non è così strano)

~~Trojan~~ Captatori di Stato

- E’ un agente software che viene inoculato (***verbo onomatopeico non trovate***?) all’interno di un sistema digitale (PC, Mac, Smartphone, Tablet ecc. ecc.) per motivazioni e per scopi diversi
- Il suo scopo primario è arrivare ad un livello di privilegi tale da poter interagire con l’hardware (System, Administrator, root…). A questo punto il sistema, semplicemente…

Non è più vostro

A voler essere del tutto sinceri non è che lo fosse molto anche prima ma è un altro discorso

Vi sentite meglio ora vero?

~~Trojan~~ Captatori di Stato

- Cosa può fare?
  - Più o meno tutto e per tutto intendo…

Registrare tutti i tasti che premete

Carpire tutte le vostre credenziali

Leggere qualunque file dal vostro siste

Permettere una tracciatura

Intercettare i dati in rete

Inserire dati!

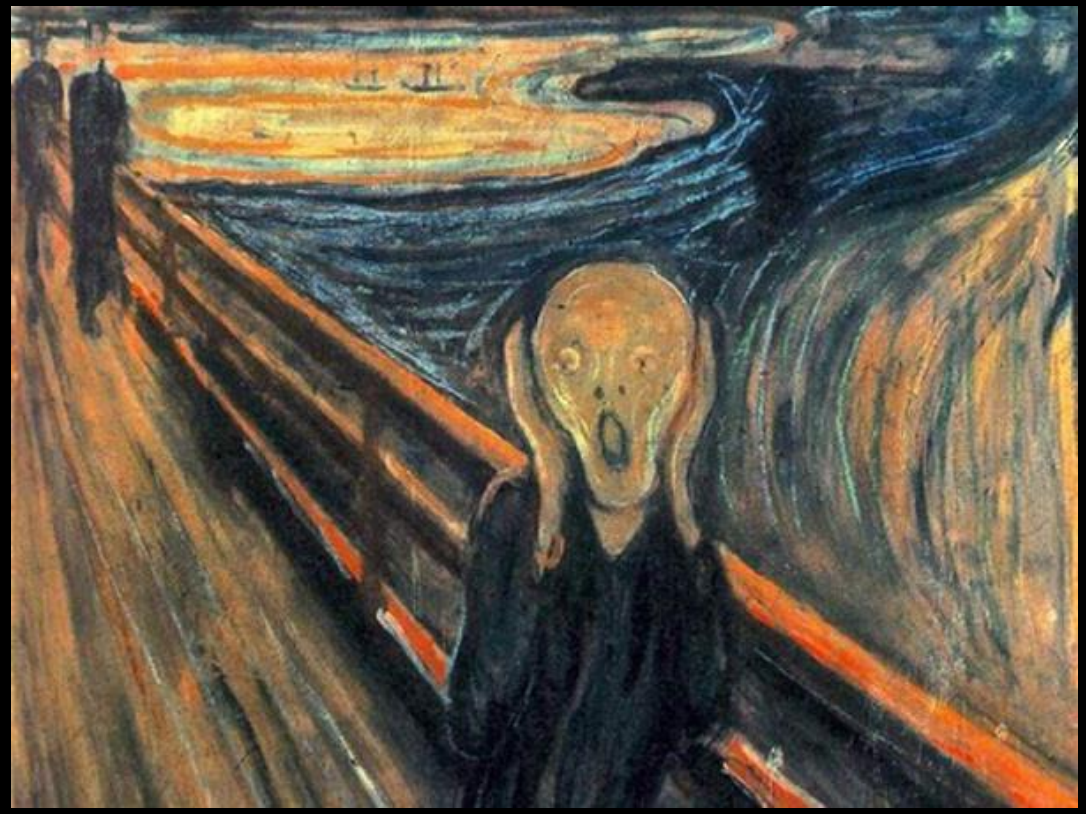
Gestire qualunque programma installato

Accedere a microfono e webcam

BE.iT

Oh mio Dio!!!

- Ma allora perché si usano?
- Perché lo Stato gioca a fare l'hacker?
- Non ci sono alternative?

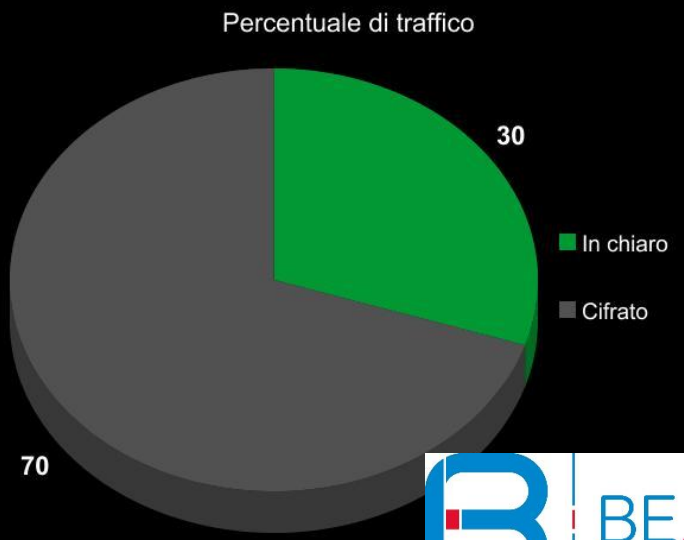


Perché si usano?

- Perché esiste la crittografia
- Avete presente quel bel lucchetto che si vede sul browser?
- Ora non solo le nostre preziosissime transazioni di e-commerce sono protette ma anche:

Perché si usano? II

- Da un certo punto di vista questa è una grande conquista
- Vuol dire che non solo il nostro denaro ma, ***IN TEORIA***, anche la nostra vita è protetta dalla crittografia
- Questo però vuole dire che, per un agente di polizia giudiziaria, le intercettazioni IP si risolvono con una gran fetta del traffico che non può essere utilizzato a fini di indagine
- Questo ha provocato, e sta provocando, non pochi grattacapi
- Il ~~trojan~~ captatore sta diventando l'unica soluzione utile



Perché si usano? III

- In realtà esistono anche altri motivi
- Il Cloud per esempio, che ha definitivamente scardinato l'unica certezza dei digital forensics expert, ovvero che il dato stesse nella memoria di massa dell'oggetto da esaminare
- L'enorme numero di sistemi che si usano: PC, Tablet, Smartphone sono diventati comuni e un «trittico» per molti utilizzatori
- Perché tutto sta diventando troppo interconnesso e quindi non è possibile controllare un individuo mettendo sotto controllo uno solo dei suoi mezzi di comunicazione

Chi li usa?

- La nostra fonte ufficiosa (che vuole restare anonima) ci ha indicato in maniera molto precisa chi sono i principali fruitori di ~~trojan~~ captatori informatici
- Rovistando tra qualche migliaia di E-Mail e di file troviamo:
  - Forze di polizia
  - Servizi di Intelligence
  - Forse Speciali
  - Agenzie investigative
- Tutto questo egualmente distribuito tra paesi «democratici» e a «democrazia alternativa»
- Ma è giusto tutto questo?

BE.iT

Chi li usa? II

- Riprendo una slide che ho presentato qualche giorno fa al Politecnico di Milano

Incident di sicurezza

- Chi sono i maggiori fornitori di captatori?
  - Gamma (Germania): Ha subito un hack due anni fa
  - Hacking Team (Italia): Ha subito un hack in Luglio 2015
  - NSO (Israele): Non risulta ~~ancora~~ hackerata (fatevi delle domande, datevi delle risposte)
- Fonti non ufficiali mi dicono che RCS ultimamente stia girando per le procure proponendo un nuovo prodotto…
- Esistono fornitori minori
- L'unico stato al mondo che si ufficialmente scritto un ~~trojan~~ captatore è la Germania

- Questo per dire che non solo sono usati da tutti i soggetti di cui abbiamo appena parlato ma anche che tutti vanno ad approvigionarsi dalle stesse fonti.
- E direi con non buoni risultati…

Chi ne abusa?

- La risposta è facile, TUTTI
- La cosa è talmente banale e risaputa che ci è arrivata perfino la Corte di Cassazione!
- Se ho dato dei concetti per scontati me ne scuso
  - Avete presenti tutte le funzioni che ho elencato prima?
  - Bene molti chiedono l'autorizzazione di livello inferiore per abilitare il servizio meno interessante
  - Però poi viene istanziato un trojan captatore con tutte le funzioni attive
  - Non parliamo del mercato privato, dove solo la fantasia pone dei limit

Cosa fare?

- Innanzitutto, come diceva Sun Tzu, «conosci il tuo nemico»
- Questo non significa che dobbiamo iniziare a fare OSINT sugli agenti di polizia giudiziaria
- Il nostro scopo invece è quello di essere più coscienti di tutto quello che ci portiamo sempre con noi
- Dobbiamo imparare per benino quali sono i principali vettori di infezione, così da poter mitigare il rischio
- Il nostro nemico non sono gli inquirenti o chi si serve di queste tecnologie per la protezione della popolazione, quanto chi si approfitta del vuoto normativo per abusare di questa tecnologia per riuscire a fare qualcosa che, normalmente, non sarebbe lecito

Come difendersi

- Capire come funzionano
- Tenere i propri sistemi aggiornati
- Non ragionare per luoghi comuni, leggende metropolitane e per sentito dire
- Non confidare troppo in noi stessi
- Diversificare al massimo la tecnologia utilizzata
- Usare un sistema quanto più sicuro possibile (e non è detto che debba essere necessariamente GNU/Linux)
- Spingere in tutti i modi per riuscire a creare una norma di legge che ne disciplini e ne regoli l'uso da parte degli ufficiali di PG

BE.iT

Buone intenzioni

- Alcuni hacker coinvolti anche nel gruppo Hermes (http://logioshermes.org/) sono stati invitati, assieme ad un avvocato (avv. Stefano Aterno) a partecipare ad una proposta di legge per normare l'uso del captatore informatico all'interno del nostro ordinamento
- Se qualche attivista di ONG come la FSF potrebbe storcere il naso in proposito, si ritiene che al momento la messa al bando dei ~~trojan~~ captatori, non sia una posizione gestibile
- A questo punto è molto meglio che si cerchi di gestire al meglio la cosa in modo che tutte le garanzie di legge siano rispettate

Premessa

il tentativo di introdurre il captatore informatico attraverso modifiche normative all'interno del nostro ordinamento passa attraverso alcuni principi e punti cardine

Preliminarmente si deve sottolineare che:

- Oggi il trojan è utilizzato ampiamente almeno dal 2004 MA è stato reso noto il suo utilizzo solo in 4 procedimenti penali;
- La tesi della Cassazione (2010) che ritiene trattarsi di "prova atipica" non è assolutamente sufficiente e rende lo strumento molto pericoloso per la riservatezza dei cittadini ;
- Una sentenza del 2015 che ha annullato le "intercettazioni ambientali" effettuate attraverso uno smartphone nel quale era stato introdotto il programma Trojan "captatore informatico" rischia di creare grandi problemi alle indagini e all'accertamento dei reati

Intervento Urgente

- È già da tempo urgente un intervento del legislatore
  di seguito si elencano principi e punti cardine:
  - Le norme vengono introdotte senza modificare la normativa esistente;
  - modifiche e integrazione del codice di procedura penale con commi e nuovi articoli in due ambiti ben precisi :
    - Intercettazioni: con acquisizione di dati a distanza (da remoto)
    - Perquisizione e sequestro occulti a distanza (da remoto) dei dati residenti nel sistema informatico con ritardata notifica all'indagato e al suo difensore per giustificare l'acquisizione dei dati occulta(istituto già utilizzato in tema di traffico di droga).
    - Garanzia dell'autorizzazione del Giudice per le indagini preliminari;

Intervento Urgente II

- Richiesta del Pubblico Ministero e necessario decreto autorizzazione/convalida del Giudice per le indagini preliminari su tutto il processo di inoculamento del programma sul sistema sotto controllo.
  - Assoluto ed espresso divieto di delegare ausiliari di polizia giudiziaria. Solo l'ufficiale di polizia giudiziaria potrà gestire l'attività del programma dall'inizio alla sua rimozione
  - Verbalizzazione dettagliata delle operazioni che compie l'ufficiale di polizia giudiziaria fino anche a prevedere e verbalizzare la tipologia dei dati acquisiti caso per caso dal sistema sotto controllo
  - I dati contenuti nel sistema controllato devono essere inviati presso i server della Procura della Repubblica

Intervento Urgente III

- CERTIFICAZIONE DEL SOFTWARE
  - Regolamento ministeriale (ministro di Giustizia e Ministro dell'Interno) con parere dell'Garante per la protezione dei dati personali e AGID con le specifiche di dettaglio e requisiti minimi e massimi necessaria a rilasciare da enti terzi la certificazione del software
  - Utilizzo a fini di indagine solo di software certificati
  - Garante Privacy con ruolo di coordinatore dei tavoli di lavoro e di garante sulla certificazione del software

Cosa si vuole chiedere per la certificazione?

- La possibilità di istanziare un ~~trojan~~ captatore che possa eseguire solo le operazioni per cui si è ottenuta autorizzazione
- Che tale ~~trojan~~ captatore sia integralmente allegato ai fascicoli
- Che i fornitori di questa tecnologia debbano depositare i sorgenti in apposito ufficio
- Che vi sia un sistema di gestione delle credenziali di accesso che si basino su chiave pubblica e privata e che questa sia embedded nel codice dell'agente
- Che venga conservata una lista dei sistemi sottoposti ad infezione
- Che non sia possibile utilizzare tecniche virali
- Che sia messo a disposizione un modulo per la pulizia dei sistemi

BE.iT

Domande? Dubbi?

Grazie per l’attenzione

Andrea Ghirardini
ghirardini@beitsa.ch +41 78 9466836 +39 377 1101101