Ordine degli Ingegneri di Pisa

Nair Congressi

Via Scornigiana 1, Ospedaletto (PI)

16 novembre 2017 – 14:00 – 19:00

IISFA European Chapter

Cryptolocker, se lo conosci lo eviti

Cosa e' il malware, cosa e' Cryptolocker e come evitarli.

Marco A. Calamari

marco.calamari@ordineingegneripisa.it

IISFA – International Information Systems Forensics Association: Italian Chapter

Il vostro anfitrione

https://www.linkedin.com/in/marcocalamari/

- **Marco Calamari, classe 1955, ingegnere nucleare, si cimenta a rotazione tra attivita' di consulenza tecnica informatica, Computer Forensics, editoriali e di formazione.**
- **Qualche sigla: IISFA, AIP, Opsi, Hermes Center, PWS.**
- **Appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.**
- **Fondatore del Progetto Winston Smith e tra i fondatori del *Centro Hermes per la Trasparenza ed i diritti digitali*.**
- **In concorrenza con i veri giornalisti, dal 2003 scrive su Punto Informatico ed altre riviste la rubrica settimanale "Cassandra Crossing", che ad oggi ha superato le 400 puntate.**

  (www.cassandracrossing.org)

Di cosa parleremo oggi

Prima parte

Breve storia del malware e del business del crimine informatico

Seconda parte

Morris Worm, Conflicker, Stuxnet, Ransomware

Terza Parte

Tutto su Cryptolocker

Quarta Parte

Non solo antivirus ma igiene informatica
Le cose da fare e quelle da non fare.

Storia del Malware

Una tassonomia del malware

Tassonomia vuole semplicemente dire "classificazione".

E' un tradizionale metodo di analisi scientifica, che cerca di creare ordine in una materia complessa.

Il malware, quando questo termine ancora non esisteva (ed il mondo informatico era molto piu' semplice) veniva classificato in tre categorie, definite dalla modalita' di propagazione:

- **Virus**
- **Worm**
- **Trojan horse**

Virus

Un Virus e' un software autonomo che puo' riprodursi senza l'intervento diretto di un utente, ma si diffonde solo tramite esso.

La definizione di virus informatico che troviamo su Wikipedia e' piuttosto confusionaria, ed in realta' non segue questa tassonomia, ma e' interessante dal punto di vista storico ed informativo.

Il primo virus ad avere una diffusione significativa e' stato Brain.

Infettava il boot sector di qualsiasi disco.
Al boot si copiava in memoria e quando veniva inserito un floppy disk, si copiava nel boot sector.
Lo scambio di floppy propagava cosi' l'infezione.

Worm

Un Worm e' un software autonomo che si riproduce e si diffonde senza l'intervento diretto di un utente.

Il capostipite di questa tipologia e' stato il Morris Worm, che paralizzo' Internet per un'intera giornata il 2 novembre 1988.

Si diffondeva attraverso servizi non protetti da un computer all'altro, e ricompilava se' stesso prima di tentare di infettare un nuovo computer, potendo cosi' diffondersi tra computer con sistemi operativi diversi.

Internet allora era abitata solo da "buoni"; la sicurezza informatica non esisteva ancora.

Trojan Horse

Un Trojan Horse e' un software non autonomo che si riproduce e si diffonde solo tramite l'intervento diretto ma inconsapevole di un utente.

Il primo trojan con diffusione significativa e' apparso nel 1985; battezzato Gotcha, si mascherava dentro un programma grafico di gestione di file, e eliminava invece dati su disco.

Un trojan non si preoccupa di diffondersi; sono gli utenti stessi che, con lo scambio di software, lo diffondono inconsapevolmente.

Una parola chiave nel contesto del malware e' proprio consapevolezza; la sua ricerca e' anche (speriamo) il motivo per cui siete qui.

Una tassonomia non basta...

Dagli anni ‘80 il malware e’ cresciuto in complessita’ ad un livello tale da rendere obsoleta la tassonomia che abbiamo visto.

Creare una nuova tassonomia non e’ una buona idea; sarebbe complicatissima ed in continua evoluzione.

Approcciamo il problema in un modo diverso; non dal punto di vista di cosa e’ uno specifico malware, ma di come funziona.

Per far questo ci servono delle definizioni precise, una terminologia moderna; ci viene in soccorso la moderna sicurezza informatica, che ce li ha gia’ preparati.

Sistema informatico

Un sistema informatico e' l'oggetto che, nel particolare caso in esame, puo' essere attaccato e deve essere difeso.

Puo' essere uno smartphone, un laptop, un'applicazione distribuita, un server, un'intera rete locale, un servizio Internet o l'intera Internet.

Nella stragrande maggioranza dei casi consiste in un singolo PC connesso ad Internet.

In molti casi, particolarmente nell'attivita' professionale, un pc opera, almeno part-time, connesso ad una rete locale; in questo caso e' necessario analizzare la rete locale e non il pc.

Superficie di attacco

La superficie di attacco di sistema informatico e' l'area materiale, funzionale o concettuale che e' raggiungibile dall'attacco o dall'attaccante da cui vogliamo difenderci.

Nel caso di una rete locale la superfice di attacco e' rappresentata dalle connessioni verso l'esterno, quindi dal modem/router ADSL e dal/dagli access point WiFi … ma non e' cosi' semplice come sembra, perche' magari avete il Bluetooth attivo.

Analizzando la possibilita' di essere infettati da un sito compromesso, la superficie di attacco e' rappresentata dal browser e dal programma di posta elettronica … ma il il vostro sistema operativo vi permette di aprire un link da un documento? Allora vanno aggiunti i programmi che visualizzano link.

Vettore di attacco

Un vettore di attacco di un sistema informatico e' il percorso tramite il quale un agente di minaccia è potenzialmente in grado di ottenere un accesso non autorizzato ad una risorsa informatica; quando sfruttato e' il particolare punto che e' stato usato per portare un particolare attacco.

Un link ad un sito compromesso in un messaggio di posta elettronica e' un esempio di vettore di attacco.

L'inserimento di una chiavetta infetta, oppure aprire un documento di provenienza ignota contenente un exploit sono altri esempi

Vettore

Il vettore di un'infezione/attacco e' il programma che effettua materialmente l'infezione (da non confondere con "vettore d'attacco").

Nel caso ad esempio di una infezione di Cryptolocker, il vettore piu' comune e' un messaggio di posta rogue, contenente un allegato eseguibile, che appare come file pdf.

Se cliccato, l'eseguibile inocula il carico pagante

Carico pagante

Il carico pagante di un'infezione/attacco e' il programma che effettua materialmente l'infezione (la terminologia deriva da quella missilistica).

Nel caso ad esempio di una infezione di Cryptolocker, il carico pagante non e' l'eseguibile allegato al messaggio di posta, ma viene inoculato dall'eseguibile stesso..

Il carico pagante vero e proprio e' il software che l'eseguibile installa sul computer.

Tipologie di Malware

Bomba logica

Una Bomba logica (logic bomb o time bomb) e' un software non in grado di replicarsi o di diffondersi, che una volta installato su un computer rimane inattivo in attesa del verificarsi di una certa condizione.

Le Timebombs sono programmate per attivarsi ad un'ora prefissata.

CTU

Le Logicbombs sono programmate per attivarsi quando si verifica un certo evento.

Possono essere non dannose; un programma in modalita' demo che si disattiva dopo 30 giorni dall'installazione o 30 esecuzioni ne e' un esempio.

Rootkit

Un Rootkit (talvolta impropriamente chiamato backdoor) e' un software che crea meccanismi nascosti per accedere ed utilizzare un computer senza lasciare tracce.

CTU

Variano dal semplice (un programma che ascolta su una porta) al complesso (programmi che nascondono processi in memoria, modificano file di log e ascoltano su piu' porte).

Sono sempre progettati per superare la normale autenticazione di sistema.

Botnet

Una Botnet e' un super-organismo informatico che, come un rootkit su un singolo computer, permette di utilizzare un elevato numero di computer infettati (chiamati Zombie) come una unica entita' in grado di compiere azioni a comando, il tutto all'insaputa dell'utente dei computer zombie.

CTU

Ogni zombie contatta un particolare server di C&C (comando e controllo), spesso anche questo un computer infetto, da cui l'attaccante puo' comandare la botnet come una unica entita'.

Puo' ad esempio istruire gli zombie ad inviare grandi quantita' di messaggi di spam, o collegarsi ripetutamente ad un sito da attaccare in modo da realizzare un attacco di negazione di servizio distribuito (DDoS).

Botnet - 2

Nelle botnet piu' grandi e recenti esistono piu' server di C&C, ed anche piu' livelli di tali server, in modo da permettere all'attaccante di meglio nascondersi.

In questi casi esistono meccanismi che permettono agli zombie di selezionare il proprio server di C&C, e di trovarne un altro se il primo scomparisse, ad esempio perche' identificato come computer infetto e riformattato.

CTU

Eliminare una botnet e' sostanzialmente impossibile, dovendo "ripulire" singolarmente centinaia di migliaia od anche milioni di computer. In molti casi per lottare contro una botnet si "attaccano" non gli zombie ma i server di C&C.

Alcuni malware "famosi"

Conficker

Le botnet Conficker nasce nel 2009 ed e' stata, per un periodo, la piu' grande botnet esistente, arrivando ad essere costituita da oltre 6 milioni di zombie contemporaneamente attivi.

Possiede un sistema di C&C a due livelli; gli zombie contattano un server C&C di primo livello utilizzando un nome di dominio pseudocasuale deciso da un particolare algoritmo.

Per lottare contro Conficker si era costituito un gruppo di lavoro il Conficker Working Group – CWG che ha tentato di disabilitare la botnet.
Sono riusciti ad "affondarla", registrando i nomi di dominio che sarebbero stati usati dagli Zombie, impedendogli quindi di localizzare i server C&C.

Conficker - 2

Scopo ideale del gruppo di lavoro sarebbe stato di eliminare tutti gli zombie, sovvertendo i meccanismi di diffusione del malware.

Impedire il contatto con i server C&C non ha cancellato gli zombie, che ovviamente sono rimasti vitali, ma ha reso dal 2010 la botnet sostanzialmente "acefala".

Il risultato e' che un milione di pc infetti sono sopravvissuti fino ad oggi, persi in un "*mar dei Sargassi*" digitale. I proprietari non si sono mai accorti di niente, i pc "zombificati" non verranno mai aggiornati e resteranno "vivi" probabilmente fino a quando l'hardware funzionera'.

Stuxnet

Stuxnet e' stato il primo malware ad essere utilizzato come arma in una guerra elettronica.
Gli esperti di geopolitica e guerra elettronica sono ormai concordi che questa azione di guerra non dichiarata sia stata condotta da Stati Uniti ed Israele contro l'Iran, che stava realizzando un impianto di arricchimento dell'uranio a Natanz.

Questi impianti sono altamente modulari, e sono formati da centinaia o migliaia di moduli centrifuga, connessi tra di loro da tubazioni. Ogni centrifuga e' riempita di un gas (esafluoruro di uranio) e ruota a velocita' altissima (30.000+ rpm) al fine di separare gli atomi di U238 da quelli di U235 sulla base della loro diversa massa.

Stuxnet - 2

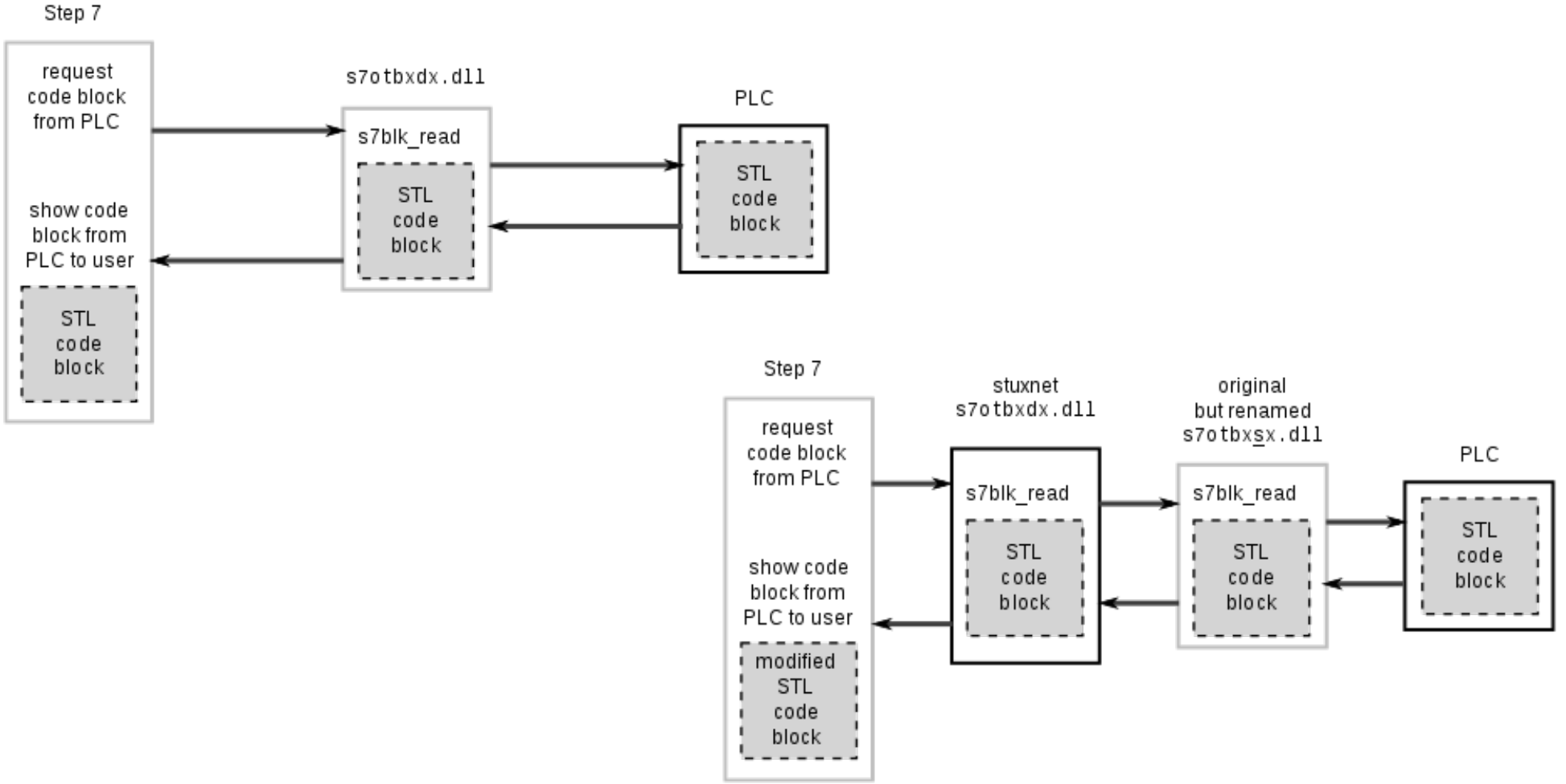
Da un punto di vista ingegneristico il parametro piu' importante e' il controllo della velocita' di rotazione in funzione delle vibrazioni della centrifuga. Il controllo viene realizzato tramite PLC – Programmable Logic Controller che, nel caso in esame, erano Siemens Step7, ed in particolare il sistema SIMATIC WinCC.

WinCC e' in grado di scambiare informazioni con il PLC (inviare parametri, leggere risultati, ma anche di riprogrammare il codice installato sui PLC stessi.

Stuxnet, una volta installatosi, sovvertiva il sistema installando una falsa DLL tra l'applicazione di controllo e la vera DLL di comando.

Stuxnet - 3

In pratica installava un vero e proprio rootkit, volto a nascondere il malware e ad ingannare chi monitorava le prestazioni attraverso WinCC.



Stuxnet - 4

Dopo che l'utente aveva programmato i PLC delle centrifughe e ne monitorava il funzionamento, Stuxnet prendeva il controllo della situazione, e riprogrammava i PLC con parametri diversi che facessero funzionare le centrifughe a velocita' distruttiva (ma non troppo).

Contemporaneamente mostrava all'utente il programma originale e falsi dati di funzionamento, coerenti con i parametri originariamente programmati.

Le centrifughe quindi funzionavano male, non arricchendo correttamente l'uranio, e si rompevano in maniera apparentemente casuale ma con tassi elevatissimi. Si ritiene che oltre 1000 centrifughe su 4000 siano state distrutte da Stuxnet.

Stuxnet - 5

Ma se Stuxnet era un'arma di precisione che doveva colpire solo Natanz, perche' e' stato rilevato in altri 8 paesi del mondo oltre l'Iran? Essendo la rete dell'impianto isolata, il metodo di infezione con una nuova versione di Stuxnet consisteva nell'infettare "a mano" le reti locali delle 5 aziende che si occupavano di manutenzione degli impianti a Natanz, e poi aspettare che uno dei tecnici che avevano l'accesso fisico al sito inserisse una chiavetta infetta in un pc.

La modalita' di infezione e trasmissione sono state rese molto piu' virulente dopo le prime versioni, che erano molto "silenti" ma non abbastanza infettive.

Kim Zetter, autore del testo di riferimento su Stuxnet "*Countdown to Zero Day*", sostiene che gli israeliani forzarono la mano agli americani, diffondendo una versione piu' virulenta. D'altra parte l'alternativa proposta era il bombardamento nucleare dell'impianto.

Cryptolocker

Ransomware

Come tipo di malware Cryptolocker ha avuto un grande successo, creandone addirittura una nuova categoria chiamata Ransomware (da ransom – riscatto).

I ransomware infettano in vari modi i computer; una volta infettato il computer cerca di infettare gli altri computer connessi alla rete locale, e poi cripta tutti i file dati presenti sul computer con un algoritmo a chiave doppia.

Una volta criptati i file, il computer visualizza in vari modi una richiesta di pagamento di un riscatto, con la promessa di inviare una chiave di decrittazione a pagamento ricevuto.

Modello di business (criminale)

La diffusione di Cryptolocker e dei successivi ransomware e' stata letteralmente esplosiva; vediamo perche'.

Il fatto che i ransomware siano in grado di generare direttamente un flusso di denaro contante e' stata la chiave del successo di questo malware, e dell'attivita' criminale di diffonderlo e gestirlo.

La possibilita' di ottenere un riscatto e' stata "regalata" ai criminali dall'esistenza di due recenti innovazioni, figlie dello sviluppo di software open source, che tutti i ransomware usano:

- **Tor hidden service**
- **Bitcoin**

Tor hidden service

Tor – The Onion Router, e' un software per la navigazione anonima su Internet.
Nato originariamente nei laboratori di ricerca della marina americana, e' stato poi ulteriormente sviluppato da una comunita' di programmatori di FOSS, successivamente costituitasi in Fondazione.

Sfruttando collaudati algoritmi di crittografia forte, permette di fruire di qualsiasi servizio TCP/IP (socket) in forma anonima. Normalmente utilizzato per accedere servizi http/https, permette effettuare navigazione web non tracciabile.

Consente anche di "pubblicare" un servizio TCP/IP in modo che sia anonimo, perche' raggiungibile solo attraverso la navigazione Tor (Tor hidden service).

Bitcoin

Una moneta elettronica (da non confondere con un pagamento elettronico) e' un sistema che permette di generare e scambiare una valuta sintetica.

Una valuta sintetica e' una valuta accettata in un sistema economico, che le riconosce un valore di scambio.

Bitcoin e' la piu' nota moneta elettronica, che possiede anche la bizzarra caratteristica di essere stata progettata e realizzata da un programmatore anonimo, Satoshi Nakamoto.
Puo' essere scambiata anche in maniera anonimizzata ed in questo caso e' difficilmente tracciabile.

Bitcoin - 2

IISFA European Chapter

Bitcoin e' realizzato come sistema peer-to-peer utilizzando il metodo delle Blockchain; permette di coniare nuova moneta, e rende quindi conveniente contribuire tecnicamente alla gestione del sistema.

Non e' una cosa solo per nerd o criminali; un bitcoin nel momento in cui scrivo questa slide (8/11/2017) vale 7519.25 dollari, ed il suo circolante vale 120 miliardi di dollari.

Inoltre Bitcoin ha provocato la nascita di una dozzina di altre valute sintetiche.

La piu' nota, Ethereum, vale attualmente 300 dollari.

Come arriva Cryptolocker

Cryptolocker infetta il computer in maniera "classica", aprendo un allegato infetto, lanciando un programma di non certa provenienza, cliccando su un link di una mail di scam

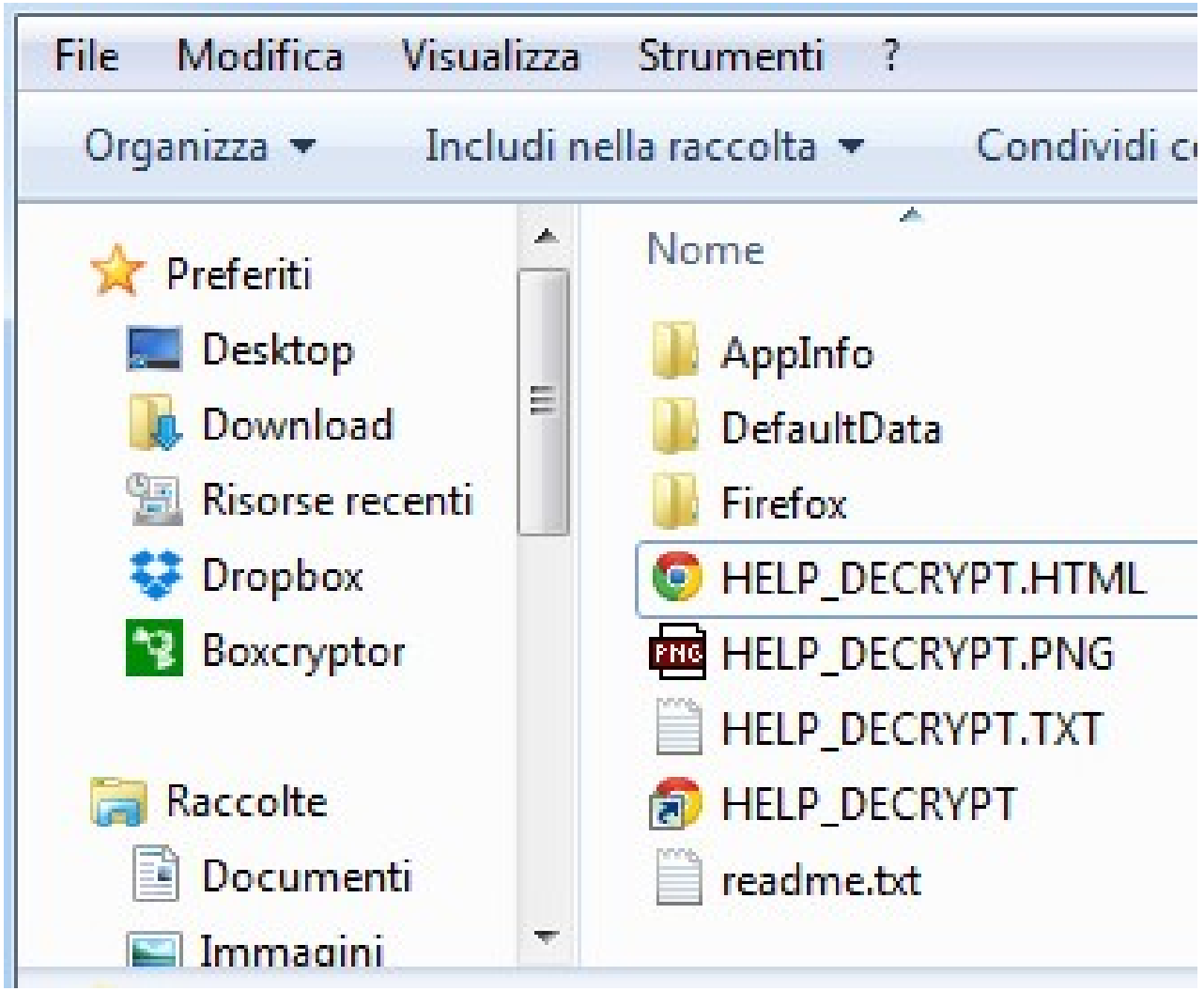
Tutte queste azioni scaricano un Injector (malware installer) che installa, oppure a sua volta scarica ed installa il carico pagante del malware, il quale:

- **Tenta di infettare i computer della rete locale**
- **Enumera i dischi/share su cui puo' scrivere**
- **Cripta i file dati mantenendo i permessi di accesso fino a criptatura completata.**
- **Visualizza in vario modo il messaggio di riscatto (schermate, file in ogni directory) e le istruzioni per ottenere la chiave.**

Come arriva Cryptolocker -2

IISFA European Chapter

Se tutte le vostre directory contengono questi file, siete stati infettati.



Putting it all together

Riassumiano il "funzionamento" di un ransomware:

- **Il ransomware infetta il computer**
- **Il ransomware si installa e cripta i file dati**
- **Il ransomware comunica la richiesta di un riscatto da pagare in Bitcoin, dando spiegazioni su come effettuare il pagamento e l'URL (Tor hidden service) da contattare**
- **La vittima si crea un wallet Bitcoin**
- **La vittima compra l'ammontare necessario di Bitcoin**
- **La vittima installa Tor o Tor Browser**
- **La vittima contatta l'URL via Tor e trova il numero di un wallet su cui effettuare il pagamento**
- **La vittima effettua il pagamento**
- **La vittima fornisce l'ID della transazione al server, che gli rivela la password e la procedura per decrittare i file**

Cosa fare per evitare Cryptolocker?

Prima di Cryptolocker

IISFA European Chapter

Immagini dei dischi di sistema dei computer, da rigenerare dopo aggiornamenti importanti.

- **Backup completo periodico (minimo mensile, meglio settimanale) delle aree dati (implica la segregazione e la conoscenza delle aree dati).**

- **Backup incrementale delle aree dati con cadenza minimo settimanale, meglio giornaliera.**

- **Hardening delle permission sui computer.**

Eseguendo queste operazioni, aiutati se necessario la prima volta da un esperto, potete ripartire anche dopo la criptatura totale di tutti i vostri computer, in circa una giornata, avendo perso solo un giorno/una settimana di lavoro.

Dopo Cryptolocker...

...avendo i backup

- **Per scrupolo, fare un immagine dei computer infetti**
- **Reinstallare i computer con le immagini salvate**
- **Ricaricare i dati dall'ultimo backupo totale**
- **Ricaricare i dati dell'ultimo backup incrementale**

… et voila'!!!

I backup non sono una spesa, sono un investimento

Dopo Cryptolocker...

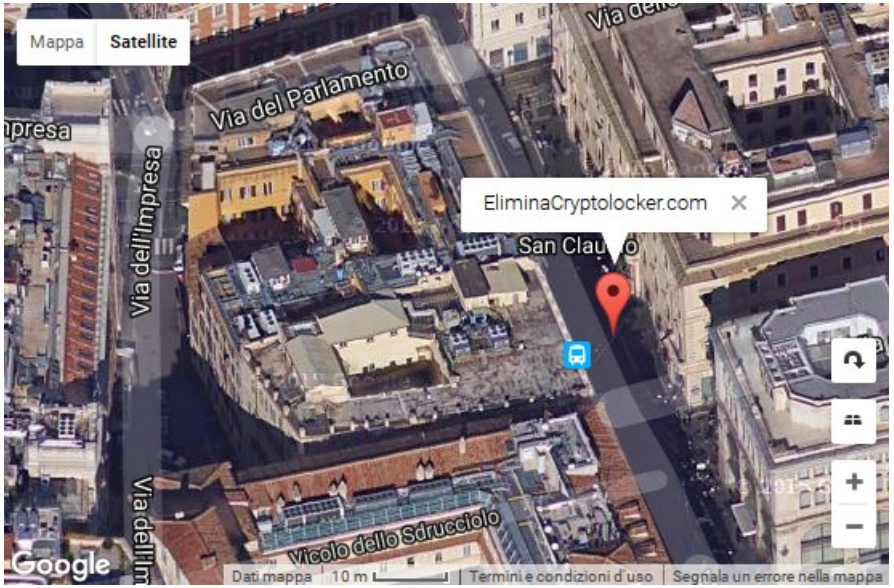
...non avendo i backup

Opzione A

Pagare seguendo le istruzioni e sperare in bene

Opzione B

rivolgersi agli "stregoni", pagarli e sperare in bene



Nessuna certezza!

Backup delle aree dati

Non ci sono scuse! Oggi (8/11/17) un disco esterno USB3 da 2.5" che non richiede alimentazione da 1TB si compra con 47,99 Euro, IVA e spedizione incluse. **Non ci sono giustificazioni** per non avere tutti i backup dati e le immagini necessarie su hard disk, in piu' copie (hard disk = materiale consumabile).

I backup si intendono eseguiti **solo** quando **l'hard disk e' scollegato** e messo in cassaforte/cassetto, meglio se in un'altra stanza/edificio.

Tenere nota del contenuto con nomi file/directory **autoesplicativi** che contengano la data di backup.

Annotare data e tipo del backup su **etichetta autoadesiva** attaccata sull'hard disk,

Programmi per il backup

Robocopy – parte del Microsoft® Windows® Server 2003 Resource Kit. Gratuito, non libero, da linea comandi. Utile per veloci backup incrementali/ completi dei dati.

Clonezilla – Scaricabile da Sourceforge – Libero, gratuito, immagine di boot per CD/USB.
Utile per creare immagini dei sistemi.

Active@ Disk Image – commerciale, installabile/live
Utile per creare immagini dei sistemi.

Hardening dei permessi

Sulle varie versioni di Windows a partire da XP e' possibile disabilitare l'esecuzione dei percorsi e dei moduli tipici di una infezione ransomware.

Si deve utilizzare l'editor di criteri/ policy/profili, diverso tra versioni di windows.

Il materiale in bibliografia vi aiutera' se fosse necessario realizzare l'hardening.

Si tratta sostanzialmente di modificare una mezza dozzina di chiavi di registro, ma usando l'editor specifico, non Regedit.

L'hardening affianca, ma non sostituisce, una igiene informatica di base, di cui abbiamo parlato.

Link utili

Articolo su hardening dei permessi (inglese)
https://www.computerworld.com/article/2485214/microsoft-windows/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are.html

Articolo su come aprire l'Editor Criteri di gruppo locali (italiano)
https://technet.microsoft.com/it-it/library/cc731745(v=ws.11).aspx

Articolo su come si manifesta Cryptolocker e sull'hardening (inglese)
https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information#files

Articolo su Conflicker e gli zombie ancora attivi (italiano)
http://punto-informatico.it/4264189/PI/Commenti/cassandra-crossing-zombie-nella-rete.aspx

Paper su Conflicker e la sua storia (inglese)
https://www.documentcloud.org/documents/2191004-post-mortem-of-a-zombie-conficker-cleanup-after.html

Azienda che sostiene di saper eliminare Cryptolocker
(link solo informativo, non e' un endorsement, non e' un consiglio)
http://www.eliminateslacrypt.com/

Link utili - 2

Windows Server 2003 Resource Kit Tools - Robocopy (inglese)
https://www.microsoft.com/en-us/download/details.aspx?id=17657

Robocopy GUI (italiano)
https://technet.microsoft.com/it-it/library/2006.11.utilityspotlight.aspx

Robocopy reference (inglese)
https://technet.microsoft.com/it-it/library/cc733145(v=ws.10).aspx

Programma commerciale per disk imaging (inglese)
http://www.disk-image.com/

Versione free del programma commerciale per disk imaging (inglese)
http://www.disk-image.com/disk-image-freeware.htm

Programma libero e gratuito per il disk imaging – Clonezilla (inglese)
https://sourceforge.net/projects/clonezilla/

Sito di riferimento di Clonezilla (inglese)
http://clonezilla.org/

Q&A time

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+
| |
| PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698 |
| DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B |
| Tel: (+39) 050 576031 Cell: (+39) 347 8530279 |
| Fax: (+39) 050 7849817 Skype-Twitter: calamarim |
| |
+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ---------------+

Grazie per l'attenzione

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+
| |
| PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698 |
| DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B |
| Tel: (+39) 050 576031 Cell: (+39) 347 8530279 |
| Fax: (+39) 050 7849817 Skype-Twitter: calamarim |
| |
+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ------------+