

Hacker Highschool

SECURITY AWARENESS FOR TEENS



LEZIONE 6 HACKING MALWARE



ATTENZIONE

Il progetto Hacker Highschool è uno strumento di apprendimento e come tutti gli strumenti di apprendimento non è esente da pericoli. Alcune lezioni, se usate in modo improprio, possono causare danni fisici. Eventuali pericoli possono emergere anche in caso non si sia svolta una sufficiente ricerca in merito agli effetti di particolari tecnologie. Gli studenti che usano queste lezioni dovrebbero essere incoraggiati ad imparare, provare e testare. Ad ogni buon conto ISECOM non potrà essere ritenuto responsabile per un uso improprio di quanto esposto.

Le seguenti lezioni ed esercizi sono "open" e disponibili pubblicamente alle seguenti condizioni e termini stabiliti da ISECOM:

Tutti i contenuti del progetto Hacker Highschool vengono forniti per uso non-commerciale per gli studenti delle scuole elementari, scuole medie inferiori e scuole medie superiori sia per le istituzioni pubbliche che per quelle private, ammettendone l'uso per le esercitazioni a casa. Non è ammessa la riproduzione del materiale per la vendita. L'utilizzo del materiale presente in queste lezioni è consentito per i corsi di ogni tipo che prevedono il pagamento di una tassa/quota d'iscrizione o frequenza, previa acquisizione di regolare licenza. Sono soggetti a tale norma anche i corsi presso le università, campi estivi e tutto quanto sia inteso come formazione. Per acquistare una licenza è possibile visitare la sezione LICENSE della pagina web della HHS all'indirizzo web <http://www.hackerhighschool.org/licensing.html>.

Il progetto Hacker Highschool rappresenta lo sforzo di una comunità "open". Pertanto se trovi utile questo materiale ti invitiamo a supportarci tramite l'acquisto di una licenza, attraverso una donazione o una sponsorizzazione.



Indice

ATTENZIONE.....	2
Hanno contribuito.....	4
Introduzione.....	5
I Virus (Viri).....	6
Il Virus Polimorfico.....	7
Il Macro Virus.....	8
Game On: l'Insegnate di Malware.....	9
I Worm.....	10
Trojan e Spyware.....	11
Rootkit e Backdoor.....	12
Logic Bomb e Time Bomb.....	13
I malware oggi.....	15
Nutri la mente: Malware Flavors.....	16
Malware Mobile	17
Una mela al giorno.....	17
Botnet.....	18
Strumenti liberi.....	19
Tecniche di consegna.....	19
Contromisure.....	20
I Software Antivirus.....	20
Rimuovere ospiti sgraditi.....	21
Analisi di malware.....	21
NIDS/NIPS.....	23
HIDS/HIPS.....	23
Firewall.....	23
Sandbox.....	23
Patch, Patch, Patch, Back-up.....	24
Criptare.....	24
Conclusioni.....	26



Hanno contribuito

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Greg Playle, ISECOM
Bob Monroe, ISECOM
Simon Biles
Rachel Mahncke
Stephan Chenette
Fred Cohen
Monique Castillo

Per la versione in lingua italiana

Raoul Chiesa, ISECOM (Coordinatore Team di lavoro edizione italiana)
Matteo Benedetti, Security Brokers SCpA
Ing. Selene Giupponi, Security Brokers SCpA
Francesco Mininni, Ing. PhD, Uff. E.I.
Riccardo Trifonio, Mar.Ca. CC
Dott. Sandro Brusino, CISSP
Dott.ssa Sophia Danesino, I.I.S. "G.Peano" TO

ISECOM

Introduzione

È incredibile quanto facilmente il **malware** comprometta i sistemi. Nel 1984 il Dr. Fred Cohen scrisse la sua discussione per il dottorato sull'idea di un virus. Venne pubblicata nel 1985. L'università reputò la trattazione forte ed inizialmente ridicola fino a che il Dr. Cohen non dimostrò la sua idea. Il che avvenne all'incirca al tempo del worm Morris. Non appena gli accademici videro il potenziale di un virus, ne vennero spaventati a morte.

La scuola era preoccupata che la sua dissertazione avrebbe potuto suggerire alcune brutte idee a soggetti poco raccomandabili. Così rimandarono la pubblicazione al 1985, ma l'idea era ormai già venuta fuori e dimostrata ancora prima dei documenti di Cohen.

L'evoluzione di questi prodotti li ha portati ad essere delle vere e proprie armi, come ad esempio **Stuxnet**. Il più piccolo virus in grado di replicarsi era lungo solo 90 righe di codice (e saltò fuori alla Core Wars del MIT).

Nel malware i professionisti di sicurezza possono osservare social engineering, exploit software, novità e migliorie tecnologiche che mostrano le capacità di alcuni esperti programmatori. Nuove forme di programmi malevoli possono essere estremamente sofisticate e richiedono team di programmatori ben pagati per crearli. Altri sono semplici exploit preparati nella cameretta di qualcuno per aggirare i controlli di sicurezza e portare scompiglio.

All'inizio il malware non portava denaro o un qualche tangibile guadagno (a parte qualche occasionale ransomware) alla persona che scriveva il programma. Le cose sono cambiate negli anni, chi crea malware ha imparato a trarre vantaggio dal furto di dati, usando i dati delle carte di credito per accedere ai sistemi bancari con il virus Zeus. Da quel momento in poi, questo settore ha prosperato.

Molti nuovi tipi di malware cercano di sfruttarti tramite truffe, spam, bot-net e spiandoti. Inoltre ha creato un mercato per i produttori di antivirus del valore di un miliardo di dollari. Hmm, pensi ci sia una qualche forma di connessione?

Quando analizzi un virus, puoi vedere il funzionamento interno di programmi veramente meravigliosi. Polimorfismo, che idea straordinaria! Quello è un design intelligente, secondo noi. Perché non abbiamo sistemi di Intrusion Detection polimorfici? È difficile capire perché chi scrive malware usa queste tecniche fantastiche mentre i grandi produttori di software non lo fanno. Proprio come per un virus reale, possiamo imparare come pensano gli utenti e come questo software sfrutti il comportamento umano per sopravvivere (e prosperare).

Per lo più il Malware (o **malicious software**) è un programma, o parte di esso, che ha effetti nocivi o indesiderati sul tuo computer. Quando la gente pensa al malware pensano ad un **virus**, ma questo termine viene usato per descrivere molto altro. I nostri simpatici amici della rete hanno creato **worm** e **Trojan**, **rootkit**, **logic bomb**, **spyware**, e **botnet**. Il malware può assumere ciascuna di queste forme, o può racchiuderne svariate allo stesso tempo. È difficile etichettare oggi il malware solo come virus, worm o anche worm/trojan. Ed ecco perché il termine generico malware è più adatto alla nostra discussione.

Sei pronto ad approfondire?

L'AV-TEST Institute registra oltre 180,000,000 di programmi malevoli dall'inizio del 1984. Ogni giorno vengono aggiunti 20,000 nuovi campioni. Controlla personalmente su <http://www.av-test.org/en/statistics/malware/>.

Il problema è che non sappiamo come loro cataloghino il malware. Ad esempio, un malware polimorfico potrebbe sembrare come una serie di virus differenti, o lo stesso, non venire proprio rilevato. Inoltre i sistemi di intrusion detection vedranno cose differenti rispetto ai software antivirus. Prendi tutti questi numeri non proprio alla lettera.

I Virus (Virii)

Questo è quello a cui pensa la maggior parte delle persone quando pensano al malware. I **virus** per computer vengono da studi scientifici sulla vita artificiale – conosciuti quindi come automi cellulari – i quali gradualmente divennero più “simili alla vita reale”, con l'abilità di propagarsi (riprodurre più copie di se stessi), infettare più macchine, divenire persistenti, addirittura cacciare ed uccidersi tra loro. Essi si comportavano allo stesso modo dei virus presenti in natura, da cui il nome.

I virus o **virii** sono pezzi di codice auto-replicante che, come per i virus biologici, si attaccano ad un altro programma, o nel caso di macro-virus, ad un altro file. Il virus viene eseguito solo quando il programma o il file a cui sono attaccati viene eseguito o aperto. Questa è la differenza tra virus e worm. Se il programma o il file non viene aperto in qualche modo, allora il virus non entrerà in funzione e non si riprodurrà ulteriormente.

Le varianti di virus possono usare differenti meccanismi di innesco come ad esempio una ben precisa ora e data o una combinazione di tasti. Questi sono solitamente progettati per determinati eventi come ad esempio la commemorazione di rivolte, crimini, atti di guerra o quando la fidanzata dell'autore del virus ha richiesto l'applicazione di un ordine restrittivo contro di lui.

Alcuni malware consistono in programmi a se stanti che possono sembrare aggiornamenti software o immagini di qualcuno su una spiaggia. I file Adobe PDF sono stati spesso il meccanismo di lancio per molte epidemie di virus, come anche Java. Sono molti i casi riportati in cui software piratato in modo da sembrare legittimo in realtà conteneva malware. Ecco perché devi controllare il **checksum** del software prima di scaricarlo. Certo, anche gli **hash MD5** possono essere manipolati, ma vogliamo solo che tu sia più attento possibile quando prendi la copia legale di qualsiasi cosa tu stia scaricando.

Un virus ben progettato non verrà rilevato, eseguirà il suo payload e si diffonderà ad altre macchine senza che la vittima si accorga di che cosa sia successo almeno fino a che non sarà troppo tardi o addirittura mai.

L'autorevole Dr. Fred Cohen elenca alcuni altri modi in cui il malware può incasinare il tuo sistema ed i dati in esso contenuti:

- modificando i settaggi di protezione a caso
- file leggibili diventano illeggibili
- file illeggibili diventano leggibili
- file scrivibili diventano non scrivibili
- file non scrivibili diventano scrivibili

- i file eseguibili non lo sono più
- i file non eseguibili diventano eseguibili
- vengono impostati i privilegi setUID (livello di fiducia) per programmi non fidati
- nel caso in cui venga utilizzato nella linea di montaggio di un concorrente può abbassare il livello di qualità dei prodotti nel caso in cui controlli la produzione!!!

Oggigiorno, scoprirai che la maggior parte del malware viene usato come strumento per la consegna di un payload. Un virus potrebbe essere usato per localizzare i dati sensibili in una rete, aprire e tenere aperta una connessione per un attacco, avviare un DDoS, sniffare informazioni finanziarie, o interrompere servizi di produzione e infrastrutturali. I malware più sofisticati solitamente avranno molti meccanismi difensivi, conterranno molti tipi di exploit e verranno scritti per sopravvivere e diffondersi il più a lungo possibile.

Il Virus Polimorfico

Una volta capito che cosa fosse un virus (dopo il 1988), era abbastanza facile rilevarli. Essi presentavano una caratteristica distintiva, o per se stessi come metodo per evitare di re-infectare, o semplicemente avevano una struttura ben precisa che poteva essere rilevata come ad esempio un payload. Poi venne il virus **polimorfico**, da "polimorfo" che vuol dire "molte forme". Queste nuove specie di virus cambiavano aspetto ogni volta che si replicavano, riorganizzando il loro codice, cambiando crittografia e rendendo il loro aspetto completamente differente. Questo morfismo creò un enorme problema di rilevamento, perché all'improvviso non c'erano più firme valide per rilevare i virus.

Uno dei modi più semplici per far cambiare un virus è tramite l'utilizzo della crittografia. Tutto quello che un creatore di virus deve fare è usare un generatore casuale di chiavi per cambiare il virus e renderlo irricognoscibile ogni volta che viene copiato. L'idea rendeva difficile per i produttori di **antivirus (AV)** poter identificare una stringa di codice da usare nei loro software AV signature-based. La riga di codice sorgente era ogni volta diversa a causa della criptazione.

I produttori di AV hanno deciso di rivolgere l'attenzione a quali parti di un virus polimorfico non potevano cambiare, che dovrebbe essere la sezione del malware che si occupa di criptare/decriptare. Come potresti aspettarti, i creatori di virus hanno pensato a sistemi per modificare le funzioni di decriptazione e renderle tanto casuali quanto il resto del programma. Hanno aggiunto date che cambiano, tempi casuali, algoritmi ed operazioni differenti e tutta una serie di tecniche per rendere il loro virus polimorfico il più difficile possibile da rilevare.

Gli ideatori di questi virus hanno impiegato altri metodi per nascondere il loro malware come ad esempio spezzettare il codice in vari segmenti. Il primo segmento potrebbe sembrare un innocuo PDF ma all'interno del PDF c'è uno script che esegue il download di altre parti del virus. La seconda porzione del virus è criptata quindi i sistemi di rilevamento non notano l'installazione.

Chi crea i virus pensa a modi per farli sembrare tutto tranne che virus. Dal momento che i programmi antivirus cercano file, eventi, attività o comportamenti sospetti causati dai virus, gli autori di quelli polimorfici hanno deciso di simulare il comportamento del sistema operativo, delle periferiche e degli utenti.

In alcuni casi, il virus sostituisce i file legittimi del sistema con le sue proprie versioni. Simpatico: ogni volta che, ad esempio, apri il Notepad, il virus si replica.

Il Macro Virus

Il **macro virus** sfrutta la capacità di un certo numero di programmi di eseguire codice al loro interno. Programmi come Word ed Excel contengono versioni limitate, ma molto potenti, del linguaggio di programmazione Visual Basic. Il che consente di automatizzare operazioni ripetitive e la configurazione automatica di determinati settaggi. Queste macro possono essere sfruttate per attaccare codice virale ai documenti, che si copierà automaticamente su altri documenti e si propagerà.

Dal momento che Word ed Excel sono stati progettati per lavorare come parte di una suite di programmi (Microsoft Office), un macro virus potrebbe trarre vantaggio da quei privilegi speciali del sistema operativo per diffondere facilmente il suo payload all'interno di intere reti aziendali. I programmi del pacchetto Office possono usare speciali (non documentate) chiamate e script all'interno del sistema operativo per aumentare la produttività, i quali però forniscono anche ai macro virus l'accesso ad aree protette del sistema operativo e della rete.

In molti client email, puoi visualizzare un'anteprima dell'allegato senza aprire la mail. Qui è quando un macro virus attacca, perché un mini programma sta aprendo l'allegato. Quell'anteprima attiverà l'allegato anche se il file si chiama "cutepuppy.jpg". I nomi dei file possono essere manipolati. Vai a controllare la **Lezione 9: Hack delle Email** per maggiori informazioni.

Puoi aspettarti di trovare malware che sfruttano le macro ovunque ci siano script eseguibili, codice, form o sub-routine lato client. Il che capita spesso per HTML5, Java, Javascript e altri add-on dei browser. Puoi approfondire il discorso con la **Lezione 10: Sicurezza del Web**.

Esercizi

Rispondi a queste domande:

- 6.1 Qual è stato il primo virus? Non fidarti della prima risposta che trovi. Controlla varie fonti. Cinque punti extra per ogni compagno di classe che smentisci
- 6.2 Ora: qual è stato il primo virus ad aver effettivamente infettato dei computer? Come si è diffuso?
- 6.3 Il virus **Klez** è ben noto per lo **spoofing**. Che cos'è lo spoofing e come se ne serve Klez? Supponi che il tuo computer sia infettato da Klez. Come lo rimuovi? Come te ne accorgi?
- 6.4 Un virus può rivelarsi utile oltre che essere dannoso? Pensa al reale scopo di un virus prima di esprimere un parere.
- 6.5 Qual'era lo scopo del virus Stuxnet? Basandoti su quello che hai letto, il virus ha raggiunto il suo scopo?
- 6.6 Hai appena ricevuto una email con il seguente Soggetto: "Avviso riguardante il tuo account email". Il corpo del messaggio spiega che l'utilizzo inappropriato della posta elettronica causerà la perdita dei privilegi di accesso ad Internet e di leggere l'allegato per maggiori dettagli. Ma che tu sappia non hai fatto nulla di strano. Sei sospettoso? Dovresti esserlo. Fai una ricerca ed individua quale virus è allegato a questo messaggio. (AIUTINO: quando inizi a pensare alla colazione – sei sulla strada giusta).



Game On: l'Insegnate di Malware

La classe di tecnologia puzzava come pesce andato a male e forse pelo di topo ma almeno era disposta in file ordinate. Su ogni banco c'era un monitor in stand-by. Luci al neon incrostate dalle mosche sfarfallavano alla luce del sole fuori dalla fila di finestre. Uno studente ai primi banchi sbadigliò ed il resto della classe colse lo sbadiglio che si diffuse fino alle ultime file di banchi. L'insegnante, Mr. Tri, piegato verso lo schermo sulla sua cattedra, si incupì.

Se nella stanza non ci fosse stata quella puzza nauseabonda, i ragazzi avrebbero iniziato a mangiare il loro pranzo o gomma da masticare o a chiacchierare mentre il loro insegnante aveva problemi con competenze base di informatica. Ma in quel fetore si tappavano il naso o respiravano attraverso una manica. Parlare, mangiare o masticare una gomma erano le ultime cose che chiunque nella stanza avrebbe voluto fare. Molti avevano già gli occhi incollati all'orologio: ancora cinquantadue minuti.

Otto minuti dopo, Jace sgattaiolò dalla porta posteriore più silenziosamente che potè. L'olezzo la fece soffocare, in modo rumoroso. Mr.Tri sentì il rumore improvviso ed il cambiamento nella pressione dell'aria all'apertura della porta. Si mosse abbastanza velocemente da beccare Jace prima che potesse accovacciarsi dietro un banco. "Jace. Hai deciso di unirti a noi oggi. Che fantastica sorpresa".

La ragazza si guardò intorno cogliendo occhiate che gli dicevano di scappare fino a che ne aveva la possibilità, una fuga per la libertà. Corri, Jace, corri. Mettiti in salvo!

Lei fissò Mr.Tri negli occhi e replicò, "Mi scuso per il mio ritardo. Ero in bagno, non mi sentivo bene". Era una scusa che non reggeva ma l'insegnante era preoccupato da un qualcosa di ancora più noioso. L'hacker posò il suo zaino e si diresse al suo banco. Tappandosi il naso, chiese ad uno dei suoi compagni che cosa stesse accadendo. Lui rispose, "Lo scoprirai presto".

"Jace, visto che hai perso l'introduzione di questa mattina, ti aggiorno subito. Qualcuno, uno di voi studenti, ha installato un'influenza o un raffreddore su questi computer". Disse accusando tutti nella stanza. "Ora, fino a che qualcuno di voi non ammette il misfatto, resterete qui a godervi questo fantastico olezzo che vi ho portato", disse Mr.Tri. Jace si guardò intorno e vide l'oltraggiosa pelliccia con corredo di sardine nelle tasche, deposto al centro della stanza.


"Ms.Jace ne sai qualcosa di questa malattia per computer", le disse puntando il dito sullo schermo. Jace balzò in piedi e si diresse verso Mr.Tri come se stesse avvicinando una puzza affamata. Vide il testo sul monitor e si spostò rapidamente sulla tastiera digitando alcuni comandi per vedere come avrebbe risposto la macchina.

"Hmm", disse allo schermo. In un attimo, Jace prese il suo zaino, tirò fuori la custodia degli occhiali, l'aprì, e scelse una chiavetta USB, pensando *gunslinger*. La sua mano destra stava già digitando mentre la sinistra inseriva la chiavetta. "Qualcuno stava aggiornando il software su questi computer?" Il lungo silenzio le faceva immaginare l'espressione di Mr.Tri.

"Che cosa intendi con *aggiornare*?" le chiese?

"Lasciamo perdere".

Prima di tutto, il browser era due versioni indietro, e le estensioni Soda HTML erano notoriamente exploitabili tramite vulnerabilità di tipo zero day. Poi, lei notò un altro prodotto HTML5 chiamato Teepee vecchio di due anni, come minimo. Cliccando



tra le cartelle di strumenti sulla chiavetta USB, Jace trovò ed avviò Nmap per vedere su quali porte il computer fosse in ascolto. Nmap restituì una lunga lista di porte aperte. Jace si accigliò.

Wireshark mostrò tonnellate di traffico TCP/IP andare e venire da cinque porte sulla macchina. Per risolvere, lei tolse semplicemente la connessione di rete. Le cinque porte continuavano ad inviare pacchetti SYN, anche senza una connessione di rete. Quindi rivolse la sua attenzione ai file di avvio del sistema.

Jace non si era accorta che diceva continuamente "hmmm" quando esaminava un computer, ma il resto della classe lo notò. Essi cominciarono a disporsi intorno a lei in un semicerchio di curiosità. "Hmmm", disse Jace, individuando vari programmi inconsueti nel processo di avvio del sistema.

Controllò ogni directory in cerca di cartelle insolite e le date di ultimo accesso ai loro file. Di nuovo, questo portò alla luce una lista di programmi, cartelle e file altamente sospetti.

Tutta questo insieme di cose nocive portavano ad un nome utente. Jace si tappò la bocca appena in tempo, quindi si voltò a destra, abbassò la mano e disse gentilmente "Mr.Tri, sembra che quello che ha scaricato tutto questo malware sia un utente chiamato Super Tri." Fu solo dopo che partì la risata che si voltò e vide l'intera classe raccolta dietro alle sue spalle.

Oops.

Game Over

I Worm

I worm sono simili ai virus per quanto riguarda la capacità di propagarsi, ma si servono di servizi di rete per i loro spostamenti. La differenza fondamentale è che non hanno bisogno che qualcuno apra un file o faccia girare un programma per diffondersi; semplicemente si replicano non appena trovano una macchina vulnerabile.

Quindi un worm è un programma a se stante che, dopo essere stato avviato, si replica senza bisogno dell'intervento umano. Si sposterà di macchina in macchina, sfruttando un servizio od una rete non adeguatamente protetti. I Worm hanno saturato server ed intere reti dal momento che il loro fine è quello di moltiplicarsi. A seconda di come è stato progettato un worm, esso può avere o non avere uno specifico scopo od obiettivo.

I worm sono stati usati per mappare reti, per spulciare in aree nascoste e riportare le loro scoperte a ben precisi punti di raccolta delle informazioni. Questo tipo di malware può lavorare autonomamente o far parte di una struttura di "command and control".

Ci sono vari casi di worm su sistemi di una certa importanza che nessuno è stato in grado di rimuovere, o di capirne lo scopo o ancora di osservarne la provenienza. I worm sono ottimi per la fase di ricognizione perché solitamente non trasportano un payload ed usano dei canali secondari e nascosti di comunicazione, se e quando comunicano. Se il worm non effettua nessuna comunicazione, è impossibile capire dove sia e che cosa stia facendo.

La buona notizia riguardo ai worm è che solitamente infettano un sistema una sola volta. La cattiva notizia è che bisogna individuare l'infezione per rimuoverlo: Buona Fortuna.

Worm: Win32 Conficker

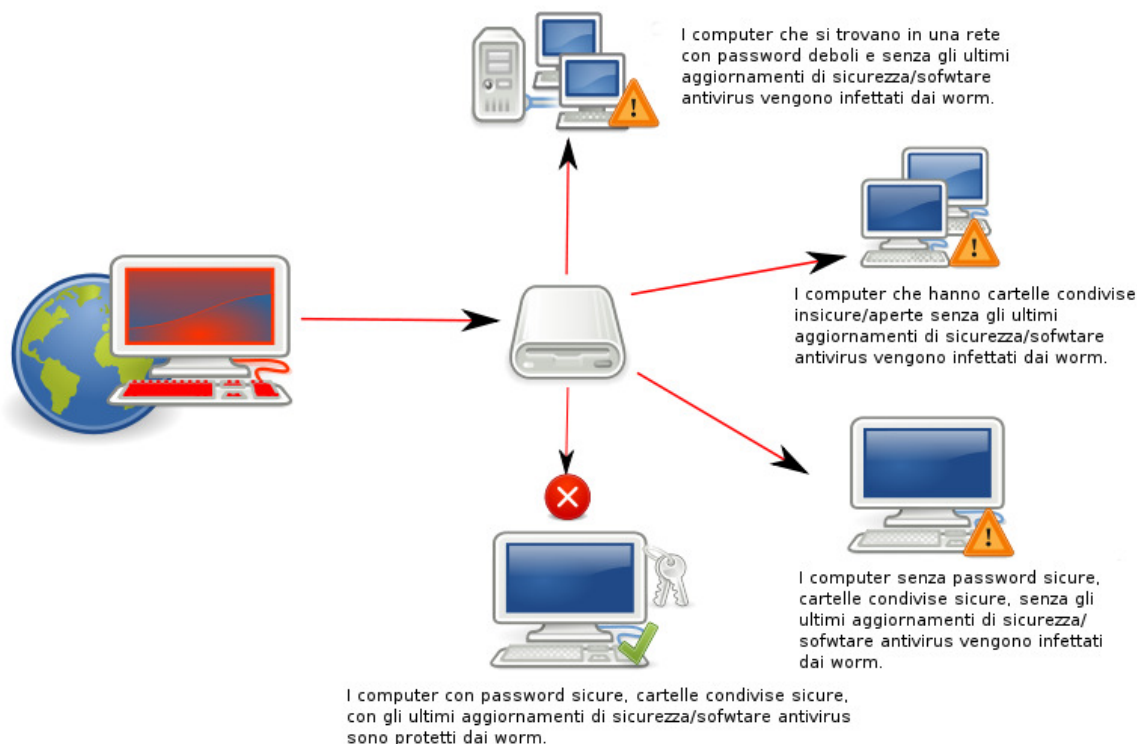



Figura 1. Come si propaga il worm **Conficker**. Foto prestata da Wikipedia sotto le Creative Commons. <http://en.wikipedia.org/wiki/File:Conficker.svg>

Esercizi

- 6.7 Quali sistemi operativi furono vulnerabili al primo worm che si è diffuso in Internet? Trova il codice sorgente. Sì, veramente. No, non ti colpirà il computer. Puoi aprire i file nel tuo browser e osservare quanto si stesse divertendo l'autore. Puoi maledirlo o invidiarlo, dipende.
- 6.8 Cerca dei video che mostrino come usare un *worm hack tool*. (Suggerimento: usa esattamente l'ultima frase.) NON CLICCARE SUI LINK. Considerando che i worm si propagano attraverso media infettati come i video, perché non dovresti necessariamente fidarti di questi video? O perfino di quei link?
- 6.9 Come puoi prendere una decisione corretta se fidarti o no di questi video? Per iniziare fai una ricerca in Internet e trova l'articolo "Ten Tricks to Make Anyone Trust You (Temporarily)." Hai usato qualcuno di questi trucchi?

Trojan e Spyware

La fonte di guadagno di un malware si trova nella categoria dello spam. Si tratta di **trojan** e **spyware** con un tocco di **adware** per un effetto ulteriore. L'originale **Trojan Horse** fu creato dai Greci migliaia di anni fa. Pensa al film "Troia" se lo hai visto). Il concetto di base è quello di offrire qualcosa che appare utile o benigno per intrufolare qualcosa di maligno in un computer sicuro. Alcuni esempi: trailer di giochi; e-mail che promettono foto della tua celebrità preferita nuda; un programma, uno strumento o utilità; un file, come un PDF; o video pirata. Li troverai spesso caricati nei cosiddetti



giochi **freeware**. Il concetto di freeware non è quello di riempire un prodotto gratuito con pubblicità o spazzatura, ma in qualche modo si è confuso con quell'idea.

I Trojan sono pezzi di malware che si mascherano come qualcosa di utile o attraente per farsi eseguire. Ci sono almeno due tipi di trojan. Il primo tipo di trojan malware si finge un programma utile, un'immagine, musica, film o è un allegato di un programma. Il secondo tipo è un programma falso che sostituisce quello legittimo sul tuo sistema. Una volta che si trovano all'interno di un sistema possono fare qualcosa di spiacevole al tuo computer come installare una backdoor o un rootkit, o – anche peggio – far diventare la tua macchina uno zombie. Segnale sinistro di musica di sottofondo.

Il primo indizio che un trojan sia stato installato sul tuo computer può essere una forte diminuzione della velocità e una perdita delle risorse. Del tuo computer, cioè non di te. Se il tuo corpo ha un forte rallentamento e/o perdita di risorse allora ti sei preso l'influenza. Vai a prendere una medicina dal tuo dottore. Il tuo computer non è così facile da sistemare. Avrai bisogno di tutta la tua forza.

Potresti notare che alcune applicazioni non si caricano, o che sono stati caricati programmi che non dovrebbero essere assolutamente in esecuzione. Non aspettarti che il tuo software antivirus ti aiuti perché se non ha impedito a quel trojan di installarsi perché dovrebbe funzionare proprio ora?

No, questo è tutto un problema tuo e se hai un trojan sul tuo computer, aspettati di trovare altro. Dal momento che i trojan sono solo contenitori per scaricare spazzatura sul tuo computer, dovrai capire da dove proviene. Qual è stata l'ultima cosa che hai scaricato, aperto o visto proveniente da un amico?

Per essere onesto con il tuo amico, anche organizzazioni molto grandi hanno passato ai propri impiegati, clienti e tra loro dei trojan. La Sony lo ha fatto. Valve lo ha fatto, due volte. Anche la Microsoft può averlo fatto, ma continua a chiamarlo "funzionalità non documentate".

Parleremo più tardi di come distruggere un malware.

Rootkit e Backdoor

Spesso quando un computer è stato compromesso da un attaccante, questo vuole tornare nella macchina. Ci sono molte varianti di questo, alcune delle quali sono abbastanza famose - cerca su Internet "**Back Orifice**".

I rootkit e le backdoor sono pezzi di malware che creano modi per continuare ad avere l'accesso ad una macchina o ad una rete. Possono essere molto semplici (un programma in ascolto su una porta) o molto complessi (programmi che nascondono processi in memoria, che modificano file di log e sono in ascolto su una porta). Entrambi i virus Sobig e MyDoom installano backdoors come parte del loro payload.

Sia i costruttori di hardware che i produttori di software sono stati accusati di aver installato delle backdoor nei loro prodotti. In alcuni casi si tratta di hacking di stato, mentre in altri casi si tratta semplicemente di aziende impiccione. Sony ha installato degli spyware sui dispositivi degli utenti per rinforzare il la Gestione dei Diritti Digitali (**Digital Rights Management DRM**). La Cina è stata incolpata di aver installato codici segreti su router, hub e altri prodotti costruiti nel loro paese. Queste tattiche hanno cancellato la fiducia dei consumatori in alcune marche e nei prodotti realizzati in certi paesi.

Quando avete a che fare con i rootkit, aspettatevi di perdere il vostro **master boot record (MBR)**, il *software* che avvia il sistema operativo. I rootkit hanno bisogno di caricarsi in memoria prima del sistema operativo. Lo fanno nascondendo porzioni di se stessi nell'MBR. Questo significa che la rimozione di un rootkit danneggia anche l'MBR.

Per ripristinare l'MBR avrete bisogno di utilizzare il prompt dei comandi attraverso il ripristino del sistema (system recovery). Al prompt dei comandi inserite il seguente comando e premete invio:

```
bootrec.exe /FixMbr
```

Se il comando avrà successo dovreste ricevere il messaggio **“L'operazione è stata completata con successo. Il Master Boot Record è stato riparato.”**

Anche se il precedente comandi ripara l'MBR, ci può ancora essere un errore nel settore di boot delle partizioni di sistema e nei **Boot Configuration Data (BCD)**, vale a dire che ci potrebbe essere un problema *fisico* da sistemare. Questo può accadere se installate un altro sistema operativo insieme a Windows 7, come Windows XP. Per scrivere un nuovo settore di boot, provate il seguente comando:

```
bootrec.exe /FixBoot
```

Esercizi

- 6.10 Cerca Back Orifice. Cosa fa esattamente? Chi lo ha creato?
- 6.11 Cerca Windows Remote Desktop. Cosa fa esattamente? Confrontalo con Back Orifice: in cosa sono diversi?
- 6.12 Immaginiamo che tu abbia un computer che vuoi far diventare con doppio sistema operativo (dual-bootable), capace di avviare due diverse versioni di Windows. C'è un trucco per farlo (come sempre). In che ordine devi installare le versioni di Windows per far sì che funzioni?

Logic Bomb e Time Bomb


Le logic bomb e time bomb sono programmi malware che risiedono silenziose fino a che non si verificano alcune condizioni – forse un particolare dato o una certa data. Normalmente non si propagano. Ad esempio: può essere creato un programma che, se l'amministratore non effettua il login per più di tre settimane, inizia a cancellare bit a caso dai dischi dati.

Questo si è verificato in un caso molto noto ed ha coinvolto un programmatore di una azienda chiamata General Dynamics nel 1992. Ha creato una logic bomb che cancellava dati critici, impostata per essere attivata dopo che se ne fosse andato. Si aspettava che l'azienda gli pagasse una bella quantità di denaro per ritornare e risolvere il problema. Tuttavia un altro programmatore ha scoperto la logic bomb prima che questa scoppiasse e il programmatore venne accusato del crimine e multato per \$5,000 dollari US. Il giudice fu clemente – l'accusa fatta dalla corte prevedeva multe fino a \$500,000 dollari US, più un periodo di reclusione.

Nel 2009, un impiegato licenziato dal gigante di prestiti e mutui Fannie May mise una logic bomb impostata per spazzare via i loro 4000 server. Fortunatamente il malware fu scoperto prima che si attivasse. Non fu una scoperta altrettanto fortunata per l'ex dipendente.

Una logic bomb/time bomb è generalmente un attacco ben informato commissionato da un impiegato scontento, un consulente esterno o un impiegato licenziato che abbia accesso alla rete. Il miglior modo per porre fine a queste minacce è la prevenzione. Rinforzare la separazione dei compiti in modo tale che nessuno abbia troppo potere su un sistema. Fate in modo che ogni dipendente prenda una vacanza ogni anno in modo tale che un attaccante non continui a seguire le sue tracce.

E soprattutto, se la vostra azienda licenzia qualcuno, prendete immediatamente il controllo sul loro accesso alla rete. Non lasciate che l'impiegato finisca la giornata o controlli le ultime mail. Accompagnatelo fuori dall'edificio in cui si trova l'ufficio, e subito



dopo cancellate le sue chiavi di accesso all'edificio (codici). Mettete il suo account di rete in una cartella speciale, ma rimuovete tutti i privilegi di accesso, in particolare quelli remoti. Questo dovrebbe aiutare in qualche modo (sempre che non conosca la password di qualche altro impiegato).

Esercizi

- 6.13 Quali usi ragionevoli (e legali) possono esistere per programmare time bomb e logic bomb?
- 6.14 Come potete rilevare tali programmi sul vostro sistema?

I malware oggi

I malware generalmente danno agli attaccanti accesso ai file o ai dati sul vostro computer, rete, tablet o smartphone. Sì, anche il vostro cellulare può prendere dei malware. **Nessun sistema di computer è immune da malware – inclusa tutta l'elettronica personale.**

Il vostro cellulare, o smartphone, è semplicemente un piccolo computer. Se state navigando sul web, utilizzando Facebook o aprendo degli allegati di mail, allora siete vulnerabili ai malware sul vostro cellulare. I malware possono anche essere preinstallati. I problemi sono gli stessi che con il vostro computer; ad esempio, rischiate di avere intercettata la vostra password. Più facilmente, il malware aspetterà che facciate delle operazioni bancarie online e o ripulirà il vostro conto corrente o vi ruberà le credenziali bancarie e le invierà all'attaccante.

Anche l'Internet TV è coinvolta. Oggi possiamo guardare la televisione e navigare in Internet allo stesso tempo. Possiamo connettere le cose ed avere una casa "smart". Di nuovo, ci sono gli stessi problemi che troviamo sui nostri computer. E' possibile introdursi nelle TV con accesso ad Internet, nei computer installati a bordo delle macchine e anche nei frigoriferi. Quasi tutto quello che ha un computer a bordo è suscettibile di attacco. Siate consapevoli che i criminali possono infiltrarsi nelle vostre case, uno spazio privato dove vi sentite sicuri, attraverso le vostre interazioni online.

Potete pensare di non avere nulla di valore sul vostro computer o smartphone, ma un attaccante può scoprire informazioni su di voi dal vostro computer o cellulare insieme alla informazioni pubblicamente disponibili su di voi, diciamo le vostre foto su Facebook, e ci possono essere informazioni sufficienti per un profilo dettagliato. L'attaccante potrebbe cercare di aprire le carte di credito, o prendere prestiti, a vostro nome. Questo è noto come **furto di identità**. I creditori si aspetteranno che li ripagiate per ciò che l'*attaccante* ha acquistato. Ci possono volere anni per provare che non siete stati voi a spendere il denaro e a ripristinare il vostro buon nome. Può ritardare la possibilità che vi venga concesso un prestito per acquistare la macchina "fast and furious" che avete sempre sognato di avere.

Siamo digitalmente connessi quasi 24 ore al giorno e ci aspettiamo che i nostri dispositivi rimangano parte di Internet anche quando non li usiamo. Questo piace ai creatori di malware. I nostri cellulari sono sincronizzati con i nostri tablet che a loro volta sono sincronizzati con i nostri computer che sono sincronizzati con i nostri account sul cloud. Tutte queste informazioni sono a portata di mano e vogliamo anche poter accedere alla nostra musica, file, film e dati personali ovunque noi siamo. Anche questo piace ai creatori di malware.

Attualmente molti obiettivi dei malware sono dispositivi mobili. Questi dispositivi hanno la minor quantità di sicurezza, ma hanno la stessa accessibilità dei dati presenti sui vostri computer. Sui vostri computer, avrete probabilmente installato un firewall, un software antivirus a un anti-spyware. Probabilmente i vostri dispositivi mobili non hanno alcuna di queste misure di protezione. Questo deve cambiare.

I creatori di malware possono modificare le proprie tattiche passando dal chiedere un riscatto e effettuare attacchi *denial of service* alla distruzione completa della rete di dati di un'organizzazione. La Sony venne attaccata nell'ottobre 2014 nello sforzo multiplo di rilasciare evidenza incriminatoria, mentre venivano distrutti dati vitali in sottofondo. Lo cyber assalto utilizzò malware sofisticato contro la Sony per fermare le operazioni giornaliere e rendere inutilizzabili i dati critici.

Nutri la mente: Malware Flavors

Secondo Kaspersky nel 2013 i principali 20 programmi maligni sono stati:

1. Malicious URL	93.01%
2. Trojan.Script.Generic	3.37%
3. AdWare.Win32.MegaSearch.am	0.91%
4. Trojan.Script.Iframer	0.88%
5. Exploit.Script.Blocker	0.49%
6. Trojan.Win32.Generic	0.28%
7. Trojan-Downloader.Script.Generic	0.22%
8. Trojan-Downloader.Win32.Generic	0.10%
9. Hoax.SWF.FakeAntivirus.i	0.09%
10. Exploit.Java.Generic	0.08%
11. Exploit.Script.Blocker.u	0.08%
12. Exploit.Script.Generic	0.07%
13. Trojan.JS.Iframe.aeq	0.06%
14. Packed.Multi.MultiPacked.gen	0.05%
15. AdWare.Win32.Agent.aece	0.04%
16. WebToolbar.Win32.MyWebSearch.rh	0.04%
17. AdWare.Win32.Agent.aeph	0.03%
18. Hoax.HTML.FraudLoad.i	0.02%
19. AdWare.Win32.Ibryte.heur	0.02%
20. Trojan-Downloader.HTML.Iframe.ahs	0.02%

Esercizi

- 6.15 Conoscere le ultime minacce malware. Cioè, quali nuove minacce malware sono emerse oggi? Vai sul sito web di un'azienda di software antivirus e cerca i loro rilevatori di minacce. Fai una ricerca in Internet su "threat research and response."
- 6.16 Esistono minacce che riguardano siti di reti sociali? Guarda alcuni siti web di antivirus. Sono concordi nell'identificare l'ultima minaccia? Quanto frequentemente cambiano le minacce malware (quante nuove minacce ci sono ogni giorno)? Quanto frequentemente dovresti aggiornare il tuo anti-malware?
- 6.17 Quali problematiche relative al malware potrebbero comparire quando porti il tuo dispositivo personale (BYOD), diciamo un laptop o uno smartphone, e ti connetti ad una rete a casa di un tuo amico, o al lavoro? E quali se ti connetti in un caffè o un ristorante?

Gli attaccanti hanno varie motivazioni, ma i moderni sviluppatori di malware generalmente vogliono guadagnare: rubare denaro alle persone. Non devono più entrare in casa vostra. Possono svuotare il vostro conto bancario, o spendere grandi quantità di denaro a nome vostro. L'altro modo di fare denaro con il malware è utilizzare il vostro computer per distribuire mail di spam o phishing emails. Gli attaccanti

possono guadagnare molto denaro in questo modo. Questo fino a quando il vostro ISP non vi blocca.

Mettendola in modo più ironico, i cracker sono usciti all'aperto, offrendo malware come servizio. Con una semplice ricerca potrete trovare una botnet da affittare o un cracker da assumere per scrivere malware personalizzato. Potete aver fiducia in uno sviluppatore di malware? Possono lasciare qualche backdoor nel vostro computer?

Malware Mobile

Gli attaccanti generalmente si focalizzano sulla rete, ma ora possono facilmente aggirare le difese della rete prendendo come obiettivo dispositivi mobili di lavoro. Nei prossimi esercizi, osserveremo come costruire malware per tablet e cellulari Android. Dal momento che tutti questi dispositivi sono connessi ad una rete una maniera o l'altra, c'è una buona possibilità che ad un certo punto si collegheranno alla rete aziendale. Naturalmente molte reti offrono accesso remoto, ma solo per segmenti isolati di quella rete. Questo però non è vero per servizi web based ed è diventato un punto debole per la sicurezza di molte aziende.

Android gira come una macchina virtuale (VM) con un simil-Linux, realizzato per piccoli dispositivi, ma costruito per la velocità. La VM è chiamata "Dalvik" nel caso ve lo steste chiedendo, che è una Java VM con molto meno overhead (richiesta di risorse). Il SO è scritto in C++ come tutte le librerie incluse nel Android Software Development Kit (SDK). Questo significa che c'è un kernel Linux sotto tutta quella GUI. Questo significa anche che Android può eseguire applicazioni Java all'interno dei browser e come programmi standalone.

Programmi di terze parti possono eseguire API native per accedere a funzioni interne di Android come la Gestione risorse, Gestione telefono e altri controlli principali. Questa è una delle maggiori vulnerabilità dal momento che non ci sono molte ragioni per cui un gioco debba avere accesso alla vostra posizione, foto, messaggi di testo o altri dati privati. Le applicazioni di terze parti sono spesso scritte in Java mentre applicazioni di sistema sono scritte in C++ (compilate per il processore in uso).

Esercizi

- 6.18 Esplora le Android APK (applicazioni) del tuo dispositivo personale. Vai a <http://developer.sonymobile.com/knowledge-base/tools/> e cerca APKAnalyser. Questo strumento gratuito ti mostrerà come funzionano le APK e quali API vengono chiamate. Ti mostrerà anche una grafica molto bella sotto forma di flowchart di come funziona quell'applicazione.
- 6.19 In quali modi possiamo determinare dove si trova il proprietario di un dispositivo?
- 6.20 Vai a <http://www.xray.io/#vulnerabilities> e cerca le vulnerabilità note degli Android che operano su processore Arm. Se stessi scrivendo un malware, quali di questi problemi sfrutteresti per primo? Ricorda che sono elencati in ordine alfabetico, non per popolarità. La maggior parte dei cellulari utilizzano un core Arm.

Una mela al giorno

Ora è il turno di ispezionare la Apple. La Apple si è sempre descritta come sicura da malware per via del sistema operativo chiuso e per le caratteristiche di sicurezza avanzate. In realtà, la sicurezza di iOS per tutti i dispositivi mobili Apple dipende dal fatto che gli utenti usano solo software proveniente dall'Apple Store ufficiale. Per dispositivi su cui sia stata eseguita la procedura di *jailbreak*, questa caratteristica di sicurezza può essere evitata, il che significa che l'uso dell'Apple Store non è un metodo efficace per proteggere questi dispositivi. Se l'azienda si affida unicamente sulla

protezione offerta dal fatto che gli utilizzatori acquistino software solo attraverso i canali ufficiali, allora non si tratta per nulla di un piano pratico.

Agli utenti piace condividere foto, allegati, messaggi, collegamenti e tutti i tipi di altri dati. I dati condivisi diventano un punto di accesso per infezioni malware esattamente come in qualunque altro sistema operativo. Una parte del motivo per cui non sentiamo parlare molto di questi malware per iOS è perché è una piattaforma popolare relativamente nuova. Via via che gli iPhone e gli iPad diventeranno più attrattivi, diventeranno anche un obiettivo di hackers malevoli. Ora che i prodotti Apple stanno diventando sempre più diffusi nella comunità dei dispositivi mobili, stanno anche suscitando più attenzione da parte degli sviluppatori di malware.

Uno dei programmi malevoli della prima ora per iPhone è chiamato **Wirelurker**. Questa applicazione si diffonde utilizzando il sistema di approvvigionamento aziendale, che è una funzione che consente ad una azienda di installare applicazioni personalizzate senza dover passare attraverso l'approvazione dell'Apple Store. Fortunatamente il malware non può fare molto di più che caricare un libro comico a meno che il cellulare non abbia subito la procedura di jailbreak. Su questi telefoni potranno essere acquisite le informazioni di pagamento ed inviate ad un comando o ad un server di controllo. Altre dimostrazioni delle vulnerabilità del sistema (*proof of concept*) sono state realizzate in passato e Apple le ha ignorate definendole "impossibili". Già, l'idea che c'è dietro a queste dimostrazioni è proprio dimostrare che ciò è possibile.

Qualunque cosa che si connette ad Internet può subire attacchi attraverso link malevoli, click-jacking, redirezioni, exploits Java più tonnellate di altre vulnerabilità. I prodotti Apple non sono diversi.


Esercizi

- 6.21 Si pensa che Wirelurker abbia compromesso fino a 800 milioni di utenti Apple utilizzando il desktop per effettuare un'infezione USB di iPhone e iPads. Perché pensate che un programma così potente usi un semplice payload per installare l'applicazione di un libro comico, mentre potrebbe installare software molto più pericoloso?
- 6.22 Cercate l'exploit CVE-2014-4377 per scoprire quali sistemi operativi e/o dispositivi possono esserne vittime. Come funziona questo exploit se l'utente non ha accesso ad Internet? Safari aprirà un PDF canaglia anche senza la connessione ad Internet. Questo è un problema relativo alla modalità con cui Safari tratta i PDF come immagini, più PDF possono essere caricati senza che l'utente ne sia a conoscenza, causando un buffer overflow che può essere sfruttato.
- 6.23 La pagina web <http://www.exploit-db.com/platform/?p=ios> elenca una collezione delle vulnerabilità note in iOS, che colpiscono dispositivi iPhone e iPad. Molti dei problemi elencati nel database coinvolgono vulnerabilità che vanno dall'accesso Wi-Fi al controllo della videocamera. Il database delle vulnerabilità elenca solo episodi a partire dal 2010. Quale anno ha il più alto numero di exploit documentati e quale credete che sia la ragione?

Botnet

Un **botnet** identifica generalmente da qualche centinaia fino a migliaia di computer che sono stati attaccati, compromessi e su cui sono stati installati un **rootkit** e una **backdoor** senza che il proprietario ne sia a conoscenza. Sono host inconsapevoli di malware, o **zombie**. L'attaccante (**bot master** o **bot herder**) può remotamente dare comandi su queste macchine in modo tale che facciano tutto quello che vuole, dall'invitare spam, a effettuare attacchi DDoS, a rubare informazioni finanziarie.

Se il vostro computer è stato infettato da un bot, può essere usato in un attacco. Un computer infettato può essere responsabile di un attacco ai server della polizia.



Legalmente voi siete responsabili del comportamento del vostro computer, esattamente come lo siete per il vostro cane e il vostro gatto. Cosa può accadere se il vostro computer è coinvolto in un attacco su infrastrutture critiche nel vostro paese, come impianti energetici o idrici?

Questi tipi di attacchi sono chiamati **cyberwar**, nonostante questa sia una parola pericolosa, perché ciò che la polizia fa è molto diverso da quello che fanno gli eserciti.

Chi c'è dietro i botnet? Qualche volta individui singoli, ma generalmente gruppi criminali organizzati. Certamente non volete avere nulla a che fare con loro! Si dice che la prossima guerra (sulla terra non nella galassia) verrà effettuata nello cyberspazio.

Vorresti essere un cacciatore di botnet? Ci sono pochi individui che lo fanno. Il problema è che, per poter stanare e buttare giù una botnet, è possibile che infrangiate qualche legge in tale operazione. Dovremmo lasciare questo a dei professionisti. Devono condurre le loro investigazioni nei limiti della legge.

I botnets vengono anche usati per attacchi **denial of service (DoS)**. Alcuni recenti attacchi DoS hanno richiesto denaro per non sferrare l'attacco. Nel passato, la maggior parte degli attacchi DoS si effettuavano su server potenti con richieste di dati tali da buttare giù i server o forzare un reboot del sistema. Alcune bot-nets hanno utilizzato decine di migliaia di macchine per sferrare un singolo attacco contro una rete per impedirne la comunicazione e il lavoro.

I bot-nets sono singoli computer dislocati in tutto il mondo ma controllati da uno o più server **comando e controllo (C&C)**. Ogni macchina è controllata dai server C&C e le viene detto cosa fare e chi attaccare. I server C&C sono a loro volta controllati da un altro server chiamato nave ammiraglia (mothership). Avendo livelli di comunicazioni separate tra gli hacker e le macchine attaccanti, la localizzazione dei criminali dietro un attacco è molto difficile.

Strumenti liberi


Le persone vogliono la loro musica preferita, gli spettacoli TV, film e altro gratuitamente. Pensaci di nuovo! Come pensi che un attaccante possa diffondere il proprio malware? Un modo efficace per diffondere malware (e costruire una botnet) sarebbe attaccarlo a qualcosa che tutti vogliono gratis. Se usi un sistema operativo non sicuro, non disattivare il tuo antivirus per rendere la macchina più veloce.

Cos'è un software antivirus e quali altre contromisure potrebbero aiutare ad evitare di prendere un malware? Ogni anno i venditori pubblicizzano i loro prodotti meglio di tutti quando si parla di rilevazione antivirus. I più grandi produttori di antivirus, Norton, McAfee, AVG e Kaspersky assumono organizzazioni di ricerca (riviste, news outlets, social media) per pubblicizzare i propri prodotti. In realtà, alcuni dei migliori software sono open source e quindi gratuiti. La chiave è fare le proprie ricerche per trovare strumenti che corrispondano alle proprie necessità, non a quelle di qualcun altro.

Tecniche di consegna

Pochissime persone installerebbero software malevolo nel proprio sistema, quindi gli sviluppatori di malware devono trovare un modo per installare i loro prodotti senza che il proprietario ne sia a conoscenza. Ci sono varie tecniche che si sono mostrate efficaci per installare programmi senza che il proprietario se ne accorgesse. Alcuni dei metodi migliori sono il repackaging (riconfezionamento), gli aggiornamenti e gli allegati (SMS, email, link web e altri URL malevoli).

Il repackaging consiste nell'usare programmi reali offerti come software legittimo attraverso i sistemi di distribuzione. Gli sviluppatori di malware prendono quel software e ci aggiungono il loro malware o ricompilano il codice per includere il proprio payload. Google Play ha avuto non poche difficoltà nel controllare i programmi legittimi per



dispositivi Android. Dal momento che molti utenti non fanno attenzione alla dimensione originale del programma corretto, è molto semplice rimpiazzare una copia corretta con una malevola.

Gli aggiornamenti di software sono un'altra area utilizzata dagli sviluppatori di malware per ingannare gli utenti e fargli installare i loro programmi. Un programmatore di malware è capace di persuadere un utente a effettuare il download di un aggiornamento di qualche software sul computer. L'avviso di aggiornamento sembra legittimo e può anche puntare all'URL iniziale di una vera patch software. L'URL o il link di aggiornamento in realtà sta caricando il malware mentre dice all'utente che il suo programma si sta aggiornando. Questa tecnica è stata utilizzata con Adobe, Microsoft, Java e altri produttori molto noti.

Abbiamo già discusso l'uso di allegati come mezzo per distribuire malware. Già, i link web sono ancora il modo più semplice per caricare malware su un sistema. I plug-in di un browser per eseguire Javascript, Ajax, aprire PDF, PHP, Flash e altri programmi consentono a malware di intrufolarsi da pagine web malevoli. Questo significa che dovete stare attenti per ogni possibile punto di accesso mentre siete dietro una tastiera.

Uno dei metodi più interessanti per installare malware è l'uso di *multi-stage insertion*. Il codice malevolo viene posto nel sistema dell'utente in più fasi per evitare che venga rilevato. Ad esempio, un utente può trovare un link su un sito web o una chiamata ad un'esecuzione corrotta (*corrupt execution call*) all'interno del browser da quell'indirizzo web. Questo evento consente ad un piccolo programma di girare in background sulla macchina. Il programma farà piccole modifiche al sistema che aprono una porta o superano alcune caratteristiche di sicurezza. Una volta che il passo è completato, viene caricato un altro programma che può essere solo un payload e potrebbe essere la seconda fase dell'attacco (*second-stage attack*).

Questo processo di caricamento di programmi in più fasi può continuare tanto quanto necessario per installare il malware ed effettuare un attacco. Generalmente un malware a più fasi è sufficientemente sofisticato per raccogliere informazioni da grandi quantità di dati, come i database di informazioni di istituzioni finanziarie o carte di credito. Un attacco massivo su un'azienda di commercio americana alla fine del 2013 utilizzò un attacco a più fasi che venne aggiornato almeno cinque volte diverse durante la violazione.

Oltre ai soliti meccanismi di invio file, alcuni programmatori di malware usano i canali di comunicazione presenti all'interno dei computer per propagarsi. Un programma chiamato **Flame** fu in grado di usare il sistema Bluetooth per trasmettere il malware alle macchine che si trovavano in prossimità. Anche il Wi-Fi è usato per trasmettere codice malevolo attraverso le onde radio. Ci sono state anche delle voci sulla possibilità di usare suoni ad alta frequenza per inviare bit ad altri dispositivi. E' stata dimostrata l'efficacia di questa tecnica in laboratori molto silenziosi. Non aspettatevi che funzioni bene attorno alla vostra casa. Parlate troppo forte e russate.

Contromisure

Ci sono vari modi per rilevare, rimuovere e prevenire il malware. Alcuni di questi sono dettati dal senso comune, altri sono soluzioni di tipo tecnico. Questa sezione fornisce una breve spiegazione e qualche esempio.

I Software Antivirus

Ci sono svariate versioni di antivirus sia commerciali che open source. Tutte usano mezzi simili. Solitamente si avvalgono di un database di virus conosciuti, e confrontano le loro "signature" con i file presenti sul sistema per identificare eventuali infezioni (questo metodo viene solitamente chiamato approccio di tipo **blacklist**). Spesso però, con i

moderni virus, queste signature sono molto piccole, e possono verificarsi dei falsi positivi, cioè si potrebbe pensare che un qualcosa è un virus ed invece non lo è.

Alcuni tipi di antivirus utilizzano una tecnica nota come **euristica**, che vuol dire che hanno l'idea di come si comporta un virus e cercano di determinare se un'applicazione sconosciuta corrisponde a tale criterio. Più recentemente, un software antivirus è anche entrato nel **Host-based Intrusion Detection**, tenendo una lista di file e checksum per aumentare la velocità dello scanning.

E sì, anche gli Apple Macs prendono malware. Le stime attuali mostrano 5000 tipi diversi di malware per i prodotti Apple. Ci sono kit di exploit costruiti specificatamente per attaccare i Mac. Ci sono ora molti software antivirus per Mac. Cerca online gli antivirus per Mac.

Vedi un antivirus sul tuo iPhone o iPad? Sul tuo cellulare o tablet Android? O sulla tua TV o lettore di dischi connessi ad Internet? O sulla tua Linux box? Perché? E' obbligatorio usare un software antivirus?

C'è una lista di software gratuiti e processi per risolvere problemi di malware in <https://www.soldierx.com/tutorials/Malware-Removal-Guide>.

Rimuovere ospiti sgraditi

Alcuni malware sono più facili da rimuovere di altri. Se ti sei imbattuto in un odioso virus, trojans o ransomware la maggior parte dei software antivirus possono rimuovere la minaccia in pochi secondi. Ci sono altri tipi di malware che non si possono eliminare così facilmente e richiedono alcune ricerche e lavoro per essere rimossi, come i rootkits. Alcuni tipi di malware sono quasi impossibili da rimuovere senza fare danni ai dati presenti sul sistema.

Uno dei primi passi per rimuovere software indesiderato è capire quale sia: hai bisogno di identificare il software malevolo. La maggior parte delle scansioni dei software antivirus forniscono il nome e sarà tuo compito cercare il tipo di software. Il segreto è avere vari scanner di antivirus a portata di mano perché uno non è mai sufficiente. Una volta scoperto il nome del malware, vai su <http://www.malwareremovalguides.info> e cerca cosa raccomandano di fare per rimuovere la minaccia.

Ogni tipo di malware può richiedere di essere trattato diversamente così fai le tue ricerche prima di iniziare a cancellare file dalla macchina.

Molto spesso, se hai un virus ne avrai molti altri che si nascondono da qualche parte. Non è raro localizzare varie dozzine di specie di trojan insieme a adware o rootkits. Sistemali tutti, iniziando da quelli peggiori.

Analisi di malware

Immagina di lavorare per un'azienda di antivirus e di scoprire un nuovo codice di malware che non è mai stato rilevato. Dovrai determinare il danno che può provocare e quali siano i suoi scopi, documentare e catalogare il nuovo malware e, cosa più importante, dargli il tuo nome! Immagina!

Sarebbe veramente una cattiva idea eseguire malware sul tuo computer, o su un computer condiviso connesso ad una rete, per ovvie ragioni. Se l'analisi di un malware di interessa veramente, c'è molto più da scoprire e avrai bisogno di un sistema di test esclusivamente per questo scopo.

E' abbastanza facile scrivere il proprio codice malware o cercare online del codice malware. Per favore siate prudenti quando vi addentrate nel "lato oscuro" di Internet. Gli scrittori di malware sono persone vere, spesso con intenti criminali; non vorrai uscire con loro o invitarli a casa tua.

Con l'analisi statistica è possibile studiare un programma senza veramente eseguirlo. Strumenti del mestiere sono **disassemblatori**, **decompilatori** e **analizzatori di codice sorgente**. Disassemblare un programma significa convertire il file del programma in una lista di istruzioni in linguaggio macchina; decompilare un programma significa convertire istruzioni in linguaggio macchina nell'equivalente codice sorgente in linguaggio ad alto livello; e l'analisi statistica esamina un programma senza eseguirlo veramente.

Cosa accade se il malware è cifrato? Se il codice è cifrato, il vostro lavoro diventa un po' più difficile, ma non impossibile. Un codice malvagio che è cifrato è generalmente un segno che il programma è un'applicazione a più fasi. La fase di codice che decifra il programma potrebbe già trovarsi da qualche parte nel tuo computer. Hai solo bisogno di cercare degli script o delle applicazioni che sono state scaricate circa nello stesso tempo in cui lo è stato il malware.

Per malware regolari la normale procedura è installarlo e eseguirlo su una macchina virtuale. A seconda del tipo di malware, se si tratta di un eseguibile stand alone, una app Java, uno script o altro, avrai bisogno di decompilare il programma in una *sandbox* su una virtual machine. Questo non è per i deboli di cuore. La maggior parte del malware è già stato decompilato e catalogato da altri ricercatori. Puoi risparmiare tempo fatica cercando queste informazioni e seguendole come una carta stradale.

Due siti per caricare malware sono <http://virusscan.jotti.org/en> o <https://www.virustotal.com/>. Questi siti eseguono il codice dei più noti software antivirus e ti dicono i risultati. Ci sono vari elementi a cui vorrai prestare particolare attenzione. Sono:


- **Propagazione:** come si diffonde il malware
- **Infezione:** come si installa e rimane installato nonostante tentativi di rimozione
- **Auto-Difesa:** come nasconde la propria presenza e resiste alle analisi
- **Capacità:** funzionalità software disponibili al proprietario del malware.

Aiuto: non fidarti mai o non cliccare su un pop up che ti offre software antivirus gratuito se ti dice che il tuo computer è infettato. Questo è quasi sempre malware!

Tieni a mente che l'estensione di un file JAR è un file Java compresso. Se vorrai ispezionare un elemento Java, dai un'occhiata a <http://en.wikipedia.org/wiki/Decompiler> o al progetto JAD su <http://varanekas.com/jad/>.

Esercizi

- 6.24 Vai online e trova **Sandboxie** (non fa mai male cercare anche tra i risultati di "like Sandboxie") Su quale OS è usato? Come funziona? Quali applicazioni useresti con Sandboxie?
- 6.25 Usi un software antivirus gratuito? Nessun problema, ma diamoci un'occhiata. Vai sul sito web del produttore e cerca il confronto tra il software gratuito e la versione commerciale (è altamente probabile che ce ne sia una). Qual è la differenza tra i due? Cosa riceveresti in cambio dei tuoi soldi se acquistassi la versione completa?

- 
- 6.26 Cerca nel tuo motore di ricerca preferito "confronta software antivirus". Cerca una versione recente (di quest'anno). Quale prodotto antivirus è valutato al primo posto? In cosa sono diversi?
- 6.27 Ora prova il tuo software antivirus per vedere se ha rilevato tutte le minacce sul tuo computer. Prima di tutto, vai al rilevatore di malware gratuito online disponibile all'indirizzo <http://quickscan.bitdefender.com>. Esegui lo scan online. Ci può volere un po' di tempo così usa il tuo tempo saggiamente mentre aspetti. Bitdefender ha rilevato qualche malware che il tuo antivirus non ha rilevato?
- 6.28 Prova il tuo software AV utilizzando un file di virus finto. Vai a http://www.eicar.org/anti_virus_test_file.htm e leggi attentamente le informazioni "Antivirus or Anti-malware test file". Il file che stai verificando non è un vero virus, ma piuttosto progettato per assomigliare ad un virus per il tuo software antivirus. Scarica il file. Aspetta di vedere cosa accade. Cosa fa il tuo software antivirus? Chiudi il messaggio dell'antivirus, se ne hai ricevuto uno, e completa la procedura di download.
- 6.29 Ora clicca eicar_com.zip. Questo file zip compresso contiene un virus falso. Cosa succede quando cerchi di aprire il file? Il tuo programma antivirus lo rileva come malevolo?
- 6.30 Utilizzando Internet, trova un esempio di un trojan e di spyware. Vedi di nuovo eicar.com.
- 6.31 Cerca su Internet esempi di rootkit e backdoor.
- 6.32 Ora considera: puoi proteggere il tuo browser in modo tale che tutto quello che scarichi rimanga chiuso in una *sandbox*? E' questa un'alternativa efficace ad un antivirus?

NIDS/NIPS

Network intrusion detection systems (NIDS) è simile a un software antivirus. Cerca una firma particolare o il comportamento di un worm o di un virus. Può o avvisare l'utente (come un **IDS**, o **Intrusion Detection System**), o automaticamente fermare il traffico di rete che trasporta il malware (come un **IPS**, o **Intrusion Prevention System**).

HIDS/HIPS

Host-based Intrusion Detection systems (HIDS), come **Tripwire**, sono capaci di rilevare modifiche effettuate sui file. E' ragionevole aspettarsi che un'applicazione, una volta installata, non si modifichi a meno che non venga aggiornata, così osservando le informazioni relative ai file, come la dimensione, la data dell'ultima modifica e la checksum, è possibile capire immediatamente se è accaduto qualcosa.

Firewall

I worm si propagano attraverso la rete scoprendo vulnerabilità su ogni host. A parte assicurarsi che non siano in esecuzione servizi vulnerabili, la prossima cosa da fare è assicurarsi che il tuo firewall non consenta connessioni. Molti firewall moderni forniscono una qualche forma di filtraggio di pacchetti simili a HIPS e scartano pacchetti che corrispondono ad una data signature.

Sandbox

Il concetto di sandbox è semplice. La tua applicazione ha il suo piccolo mondo in cui agire e non può fare nulla al resto del computer. Questo è implementato come standard nel linguaggio di programmazione Java, e può anche essere implementato

attraverso altri strumenti come **chroot** in Linux. Questo restringe i danni che un qualunque malware può arrecare al sistema operativo semplicemente negando l'accesso richiesto. In molti SO questo tipo di restrizione è sempre integrato. In almeno uno no (indovina quale).

Un'altra opzione è eseguire una macchina all'interno di un'altra macchina utilizzando una macchina virtuale come XEN o VirtualBox. Questo isola la macchina virtuale dal sistema operativo ospite, consentendo l'accesso solo in base a ciò che l'utente ha impostato.

Patch, Patch, Patch, Back-up

Questo è ciò che la maggior parte dei venditori ti diranno: applica ogni patch, applica tutte le patch, lasciaci installare tutte le patch, automaticamente, sempre! Questo ti renderà sicuro!

Eccetto per il fatto che:

1. la maggior parte delle patch che i venditori pubblicano non si applica al tuo particolare sistema
2. ogni patch che installi è un codice ancora più pieno di bug e propenso al malware che si trova sul tuo computer
3. le patch introducono errori con la stessa frequenza con cui li risolvono
4. le patch possono mandare in crash o distruggere altro software stabile sulla tua macchina o sul tuo server.

Il che equivale a dire che il gioco delle patch non è la cura di tutti i mali come asseriscono i predicatori. Le patch appropriate sono generalmente utili, nonostante possano causare problemi. Ma consentire aggiornamenti automatici (molti, molti amministratori di server lo hanno imparato a loro spese) è realmente molto pericoloso (Microsoft ha fatto a tutti un grande favore insegnandocelo, ripetutamente).

Il segreto è tenere aggiornato il proprio software su base regolare ma verificare le patch prima di installarle su macchine critiche. Se non potete verificare le patch, fate in modo di essere sicuri di poter annullare l'installazione una volta applicata. Lo storage sul cloud sta diventando più economico ogni giorno e potete impostare back-up automatici tra il vostro computer e l'account online. Non dimenticate di fare back-up incrementali localmente. I vostri dati sono importanti, teneteli al sicuro.

Criptare


La crittografia di un intero disco è un'altra buona idea per proteggere i vostri dati e il vostro sistema dal malware. Esiste software gratuito in grado di fornire un'eccellente cifratura e nello stesso tempo mantenere il tuo computer facile da usare. Uno dei trucchi che offre la cifratura del disco è che sostituisce il vostro settore di boot con il proprio bootstrap. Questo diminuisce il rischio di rootkit e di infezioni del boot sector.

Codice malevolo non può attaccare qualcosa che non può vedere. File cifrati tengono sotto il vostro controllo le informazioni sensibili in modo che non vengano inviate all'operatore di malware. Questo limita l'abilità del malware di catturare informazioni utili come password, dettagli dell'account, quelle foto in cui sputate latte dal naso e la vostra ultima pagella.

Non cifrate solo l'hard drive. Cifrate tutti i media e anche il vostro telefono.

Esercizi

- 6.33 Cerca il termine "automatic update causes." Quante cose provocano gli aggiornamenti automatici? O almeno quanti risultati hai ottenuto?

- 
- 6.34 Cerca software antivirus per cellulari. Cerca anche anti-malware per tablet (ad esempio iPad e Android). Sono efficaci questi strumenti? Chi li usa?
- 6.35 Cerca Stuxnet, Duqu e Flame. Per ognuno:
- Su quali sistemi agisce?
 - Quale era il suo payload?
 - Che cosa lo ha reso differente dagli altri malware?
 - Come si rimuove da un sistema?
- 6.36 Gioco sulle corrispondenze: fai corrispondere a ogni voce il tipo di contromisura:
- | | |
|---|-----------|
| http://www.virtualbox.org | NIDS/NIPS |
| http://www.tripwire.org | Antivirus |
| http://www.snort.org | Firewalls |
| http://www.checkpoint.com | Sandboxes |
| http://www.clamav.net | HIDS/HIPS |
- 6.37 Cerca come funzionano NIDS/NIPS e HIDS/HIPS.
- 6.38 Cerca soluzioni di Firewall in rete. Puoi analizzare i log del tuo firewall e sottomettere i log al SANS Internet Storm Center, DShield at <http://isc.sans.edu/howto.html>.
- 6.39 Cerca **chroot** su Internet. Cerca questo tipo di "jail" o "sandbox."
- 6.40 Disegna un **Attack Tree**. Fai una ricerca avanzata su "site:www.schneier.com."
- 6.41 Un malware non è mai buono per nessuno, oltre a chi cerca di trarne profitto e rischiare di essere beccato. Ognuno vuole evitare di essere infettato. Dai uno sguardo a questo flowchart per vedere esattamente cosa eviti quando proteggi te stesso dal malware: all'interno del business del malware <http://www.computerschool.org/computers/malware/>.
- 6.42 Computerschool.org ha una infografica sul Business del Malware. Trovala.

Conclusioni

Qualunque buona immunità dal malware si ottiene solo con una buona conoscenza del malware. Mentre non possiamo coprire ogni possibile tipo di malware (perché nel tempo in cui stai leggendo questa lezione ce ne saranno altri nuovi), ti abbiamo descritto alcuni punti critici. Per esempio, che puoi a malapena aver fiducia nelle *shortcut* sul desktop del tuo computer e che non puoi fidarti per nulla di qualunque file tu riceva senza averlo richiesto. La parola chiave è fiducia, che implica una forte consapevolezza di quanto tu diventi vulnerabile quando dai fiducia.

Non vogliamo che tu diventi fortemente diffidente su tutto; è un'attitudine che ti pregiudicherebbe molte opportunità. Invece, tieni ben chiaro in mente che quando dai accesso a qualcuno, gli stai dando fiducia. Gli stessi principi che rendono le reti sicure possono rendere sicuro anche te. La segmentazione della rete che consente solo una visibilità strettamente controllata, ad esempio, è una buona pratica sia nelle reti che nella vita reale.

Non stiamo neanche incoraggiandoti a costruire malware e scatenarlo nel mondo o ai tuoi amici. Oggi, probabilmente più che mai nella storia umana, le azioni hanno conseguenze. Non illuderti che non ti troveremmo se provassimo, e non siamo nemmeno lontanamente spaventosi come alcuni governi e forze dell'ordine.

Vogliamo, invece, che tu veda come funziona il malware e che diventi sensibile alle truffe in uso. Questo non solo ti rende più sicuro rispetto al malware, ma anche più sicuro nel tuo mondo.

Usa questo potere solo per il bene, giovane padawan.

Al giorno d'oggi i ragazzi vivono in un mondo in cui possono accedere ai principali canali di comunicazione, ma non hanno le conoscenze per difendersi contro le frodi, i furti d'identità, le violazioni della privacy ed altri attacchi che subiscono quotidianamente per il semplice fatto di utilizzare Internet. È per questo che esiste Hacker Highschool.

Il progetto Hacker Highschool punta a sviluppare dei materiali per l'apprendimento e la formazione su temi della sicurezza e della privacy per gli studenti delle scuole medie e superiori.

Hacker Highschool è composto da un set di lezioni ed esempi pratici per diventare degli hacker.

Oltre a renderli consapevoli riguardo a temi di cybersecurity ed a fornire le skill necessarie per navigare su Internet, dobbiamo insegnare ai giovani di oggi ad essere pieni di risorse, creativi e ad usare la logica, tutti tratti distintivi di un hacker. Il programma contiene materiali didattici su sicurezza e privacy e supporta gli insegnanti di scuole medie, superiori e private accreditate. Queste lezioni offrono delle sfide ai ragazzi per stimolarli ad essere creativi come un hacker e trattano l'utilizzo sicuro di Internet, la privacy sul web, le ricerche su Internet, evitare virus e trojan, temi legali ed etici ed altro.

Il programma HHS è sviluppato da ISECOM, un gruppo di ricerca no profit, open source, concentrato sulla sensibilizzazione alla sicurezza ed allo sviluppo della sicurezza professionale ed al suo accreditamento.



ISECOM