Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 6
MALWARE

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

“License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informazioni sulla licenza d’uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo “non-commerciale” verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo “doposcuola”.

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L’erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all’indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Hanno contribuito

Simon Biles, Computer Security Online Ltd.

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM

Doriano Azzena, centro CSAS del progetto Dschola IPSIA Castigliano - Asti

Sophia Danesino, centro CSAS del progetto Dschola ITIS Peano – Torino

Nadia Carpi, centro CSAS del progetto Dschola ITIS Peano – Torino

Fabrizio Sensibile, OPST&OPSA Trainer, @ Mediaservice.net Srl, Torino - ISECOM Authorized Training Partner

Claudio Prono, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

/// computer security online

mediaservice.net
CORPORATE SECURITY & IMAGE

6.1 Introduzione

I "Malware" sono programmi o parti di programmi che hanno un effetto spiacevole sulla sicurezza del vostro computer. La parola vuole indicare vari termini che avrete già sentito prima, come "Virus", "Worm" e "Trojan" ed anche altri meno noti quali "Rootkit", "Logicbomb" e "Spyware".

Questa lezione introdurrà, definirà e spiegherà le varie tipologie di malware, fornirà esempi e presenterà alcune contromisure che possono essere attivate per ridurre i problemi causati dai malware.

6.2 Virus

6.2.1 Introduzione

Virus – questo è il tipo più comune di malware di cui le persone dovrebbero essere a conoscenza. Il motivo per cui è noto come virus, piuttosto che altro, è storica. La stampa trattava le storie dei primi virus per computer allo stesso modo che gli articoli sulla diffusione dell'AIDS. Allora esistevano semplici paralleli tra i due, la propagazione attraverso l'interazione con una parte contaminata e la "morte" definitiva di qualunque cosa fosse stata infettata. Da ciò l'idea che le persone potessero venire "infettati" con un virus del computer.

6.2.2 Descrizione

I virus (o virii) sono parti di software auto-replicanti che, analogamente ad un virus biologico, si attaccano ad un altro programma, o, nel caso di "macro virus", ad un altro file. Il virus si attiva solo quando il programma o il file viene eseguito o aperto. E' proprio questo che differenzia i virus dai worm. Se non si attiva il programma o il file, il virus non viene eseguito e non si propaga ulteriormente.

Ci sono molti tipi di virus, tuttavia la forma più comune è oggi il macro virus, mentre altri, come i virus del settore di boot, si trovano solo "in cattività".

6.2.2.1 Virus del Settore di Boot

Il settore di boot è stato il primo tipo di virus ad essere creato. Si nasconde nel codice all'inizio dei dischi di boot. Questo significa che per infettare una macchina è necessario effettuare il boot da un floppy infetto. Molto tempo fa (circa 15 anni) l'accensione di una macchina da floppy era molto comune, quindi tali virus erano molto diffusi. Questo virus (e tutti gli altri tipi) dovrebbe lasciare una firma rilevabile dai successivi tentativi di infezione, in modo da non infettare ripetutamente lo stesso obiettivo. E' questa firma che consente agli altri software (noti come Anti-virus) di rilevare l'infezione.

6.2.2.2 I Virus nei File Eseguibili

I virus dei file eseguibili si attaccano ai file, quali .exe o .com files. Alcuni virus cercano programmi che sono parte del sistema operativo, in modo tale che vengono eseguiti ogni volta che il computer viene acceso aumentando la loro possibilità di propagazioni successive, Ci sono pochi modi per attaccare un virus ad un file eseguibile, alcuni dei quali funzionamo meglio di altri. La modalità più semplice (e la meno ingegnosa) è sovrascrivere la prima parte del file eseguibile con il codice del virus. Questo significa che il virus viene eseguito, ma il programma va successivamente in crash; è, quindi, abbastanza ovvio che ci si trova di fronte ad un'infezione – specialmente se il file è un importante file di sistema.

6.2.2.3 I virus "Termina e Stai Residente" (TSR)

TSR (*Terminate e Stay Resident*) è un termine del DOS che indica una applicazione che si carica in memoria e successivamente vi rimane in *background*, consentendo al computer di agire normalmente in *foreground*. I virus più complessi di questo tipo intercettano le chiamate di sistema e restituiscono risultati errati – altri si attaccano al comando 'dir' e infettano ogni applicazione della directory listata – altri ancora terminano (o cancellano) il software Anti-Virus installato sul sistema.

6.2.2.4 I Virus Polimorfi

I primi virus erano abbastanza facili da intercettare. Avevano una firma che li identificava, contenevano un metodo per prevenire una nuova infezione, o semplicemente avevano una struttura specifica che era possibile rilevare. Poi venne il virus polimorfo. Poli – che significa multiplo - e morfo – che significa forma. Questi virus si modificano ogni volta che si replicano, modificando il proprio codice, cambiando la crittografia e generalmente rendendosi completamente differente. Questo ha creato un enorme problema, poichè istaneamente c'erano firme molto più piccole: alcuni dei "migliori" virus si ridussero ad una firma di pochi bytes. Il problema aumentò con il rilascio di "kit polimorfi" da parte della comunità che scriveva virus che consentirono a qualunque virus di replicarsi come polimorfo.

6.2.2.5 Il Macro Virus

Il Macro Virus utilizza l'abilità che hanno molti programmi di eseguire codice. Programmi come Word and Excel hanno una versione del linguaggio di programmazione Visual Basic limitata, ma molto potente. Questo consente l'automazione di operazioni ripetitive e la configurazione automatica di settaggi specifici. Questi linguaggi di macro sono utilizzati per allegare ai documenti codice virale che si copierà automaticamente su altri documenti e si propagherà. Nonostante la Microsoft abbia eliminato la funzionalità di default su nuove installazioni, c'è Outlook che esegue automaticamente il codice allegato alle e-mail appena queste vengono lette. Cià implica che i virus si possono replicare molto velocemente inviandosi a tutti gli indirizzi di e-mail presenti nella macchina infetta.

6.2.2.6 Esercizi

1) Utilizzando Internet, cercate di trovare un esempio di ogni virus citato prima.

2) Cercate il virus Klez:

- qual è il suo effetto ?

- il virus Klez è noto come SPOOFING. Cos'è lo spoofing, e come lo usa Klez ?

- avete appena appreso che il vostro computer è infettato da Klez. Cercate come rimuoverlo.

3) Avete appena ricevuto una e-mail con il seguente oggetto:

Subject: "Warning about your email account".

Il corpo del documento spiega che l'uso inappropriato che avete dato della posta vi farà perdere i privilegi di Internet e rimanda all'allegato per ulteriori dettagli. Ma voi non avete fatto nulla di strano con la posta. Siete sospettosi ? Dovreste esserlo. Cercate questa informazione e determinate quale virus è attaccato a questo messaggio. (Aiuto: Quando iniziate a pensare alla colazione – siete sulla strada giusta).

6.3 I Worm

6.3.1 Introduzione

I Worm sono più vecchi dei virus. Il primo worm venne creato molti anni prima del primo virus. Questo worm fece uso di un'imperfezione nel comando UNIX finger per bloccare la maggior parte di Internet (che a quel tempo era molto più piccola). La sezione seguente tratta questi worm.

6.3.2 Descrizione

Un worm è un programma che, dopo essere stato avviato, si replica senza alcun bisogno di intervento umano. Si propaga da un host ad un altro, sfruttando uno o più servizi sprotetti. Attraversa una rete senza bisogno che un utente invii un file o un'emali infetta. La maggior parte degli incidenti recenti sono stati causati da worm piuttosto che da virus.

6.3.2.1 Esercizi

1) Utilizzando Internet, cercate il primo worm che sia stato mai creato.

2) Trovate quale vulnerabilità sfruttano i worm Code Red e Nimda per propagarsi.

6.4 Cavalli di troia e Spyware

6.4.1 Introduzione

Il primo Cavallo di Troia (Trojan Horse) fu creato dai greci migliaia di anni fa (pensate al film "Troia" se l'avete visto). Il concetto base è quello di introdurre qualcosa di sgradevole nel computer sicuro di qualcuno sotto la parvenza di qualcosa di piacevole. Questo varia da un trailer di un gioco, alla e-mail che promette foto della vostra celebrità preferita nuda. Questa sezione tratta trojans e spyware.

6.4.2 Descrizione

I Cavalli di Troia sono pezzi di software dannoso mascherato come qualcosa di utile o desiderabile per far sì che vengano eseguiti. A questo punti gli stessi danneggiano il computer installando una backdoor o rootkit (si veda la sezione 6.4), o – anche peggio – compongono un numero telefonico che vi costerà molto denaro.

Gli Spyware sono software che si installano clandestinamente, spesso da siti web che avete visitato. Una volta installati, essi cercheranno informazioni che considerano preziose. Si può trattare di statistiche relative alla vostra navigazione web o il numero della vostra carta di credito. Alcuni spyware inondano il vostro desktop con annunci.

6.4.2.1.Esercizi

1) Utilizzando Internet trovate un esempio di trojan e di spyware.

6.5 Rootkit e Backdoors

6.5.1 Introduzione

Spesso quando un computer è stato compromesso da un hacker, è stato installato un meccanismo per ottenere un facile accesso alla macchina. Ci sono molte varianti di questo, alcune delle qualli sono diventate abbastanza famose – cercate su Internet "Back Orifice" !

6.5.2 Descrizione

Rootkits e backdoors sono software che creano meccanismi per accedere ad una macchina. 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 una porta). Spesso creare una backdoor è semplice come creare un nuovo utente con privilegi da super-user in un file di password nella speranza che non venga individuato. Questo perchè una backdoor è progettata per superare la normale autenticazione di sistema. Entrambi i virus Sobig e MyDoom installano back doors.

6.5.2.1 Esercizi

1) Trovate su Internet esempi di rootkits e backdoors.

2) Cercate "Back Orifice" e confrontate le sue funzionalità confrontandolo con i prodotti commerciali disponibili per la gestione di sistemi remoti della Microsoft.

6.6 Logicbombs e Timebombs

6.6.1 Introduzione

I programmatori e amministratori di sistema possono essere persone abbastanza strane. Spesso impostano su un sistema delle azioni che vengono intraprese al verificarsi di determinati eventi. Ad esempio: può essere creato un programma che, nel caso in cui l'amministratore fallisca il login per più di 3 volte, inizi a cancellare a caso bit di dati dal disco. Questo è successo in un caso molto noto che ha coinvolto una società chiamata General Dynamics nel 1992. Un sistemista creò una logicbomb in grado di cancellare dati critici e che era programmata per essere attivata dopo che egli fosse stato licenziato. Egli si aspettava che la società gli pagasse una conspicua quantità di denaro per ritornare e risolvere il problema. Tuttavia, un altro programmatore trovò la logic bomb prima che si licenziasse, fu accusato di un crimine e condannato a pagare $5,000 US dollari. Il giudice fu clemente – la pena avrebbe potuto essere $500,000 US dollari, più un periodo di reclusione.

6.6.2 Descrizione

Logicbombs e Timebombs sono programmi che non hanno la capacità di replicarsi nè di creare un meccanismo di accesso, ma sono applicazioni o parti di applicazioni che causano danni ai dati quando attivati. Possono essere stand-alone, o parte di worms o viruses. Le Timebombs sono programmate per causare danni ad un'ora prefissata. Le Logicbombs sono programmate per causare danni quando si verifica un certo evento. L'idea dietro i timebombs, tuttavia, è anche una utile. Dopo un certo periodo dall'installazione – generalmente 30 giorni - il programma cessa la propria funzione a meno che venga fornito un codice di registrazione. Questo è un esempio di programmazione di timebomb non dannoso.

6.6.2.1 Esercizi

1) Quali altri usi ragionevoli (e legali) possono avere i codici timebomb and logicbomb?

2) Pensate a come potete rilevare tali programmi sul vostro sistema.

6.7 Contromisure

6.7.1 Introduzione

Ci sono molti modi con cui potete rilevare, rimuoveree preveniire software dannosi. Alcuni di essi sono il senso comune, altri sono alternative tecnologiche. La sezione seguente evidenzia alcune di queste, con una breve spiegazione e esempi.

6.7.2 Anti-Virus

I software Anti-Virus sono disponibili in molte versioni commerciali e Open Source. Tutti questi agiscono seguendo lo stesso metodo. Ognuno di essi ha un database con i virus noti e confronta le firme di questi con quelli del sistema per vedere se ci sono infezioni. Spesso tuttavia, con i virus moderni, queste firme sono molto piccole e ci posso spesso essere falsi positivi – cose che sembrano virus ma non lo sono. Alcuni scanner di virus utilizzano una tecnica nota come euristica: sanno a cosa assomiglia il virus e determinano se un'applicazione sconosciuta corrisponde a questi criteri. I recenti software AntiVirus si sono trasformati in Host Based Intrusion Detection, mantenendo una lista di files e checksums per aumentare la velocità della scansione.

6.7.3 NIDS

Un *Network intrusion Detection* è simile al software AntiVirus. Cerca una firma particolare o il comportamento da worm o virus. Può o allertare l'utente o fermare automaticamente il traffico di rete che trasporta il software dannoso.

6.7.4 HIDS

Gli *Host based Intrusion Detection Systems*, come *Tripwire*, sono in grado di rilevare i cambiamenti effettuati ai file. E' ragionevole aspettarsi che un'applicazione, una volta compilata, non abbia necessità di cambiare, così la esaminano (la sua dimensione, la data dell'ultima modifica e la checksum) evidenziando immediatamente che qualcosa è sbagliato.

6.7.5 Firewalls

I Worms si propagano attraverso la rete connettendosi ai servizi vulnerabili sui vari host.

Oltre ad assicurare che nessuno di questi servizi vulnerabili sia in esecuzione, la successiva cosa da fare è assicurare che il vostro firewall non consenta connessioni a questi servizi. Molti firewall moderni forniscono una forma di filtraggio dei pacchetti simile ai NIDS che elimina i pacchetti che corrispondono ad una certa firma.

6.7.6 Sandboxes

Il concetto di una sandbox è semplice. La vostra applicazione ha il suo piccolo mondo in cui agire e non può fare nulla al resto del computer. E' implementato nel linguaggio di programmazione Java e può anche essere implementato attraverso altre funzioni come chroot in Linux. Questo restringe il danno che ogni malware può fare ad un sistema operativo semplicemente negandoglli l'accesso richiesto. Un'altra opzione è far eseguire una macchina completa all'interno di un'altra macchina utilizzando un prodotto che crea macchine virtuali come VMWare. Questo isola la macchina virtuale dal sistema operativo consentendo l'accesso solo come definito dalll'utente.

Esempio http://www.vmware.com – VMWare virtual machines

6.7.6.1 Esercizi

1. Matching Game: cercate ognuno dei seguenti e e associateli al corretto tipo di contromisua:

    1. http://www.vmware.com NIDS
    2. http://www.tripwire.org Antivirus
    3. http://www.snort.org Firewalls
    4. http://www.checkpoint.com Sandboxes
    5. http://www.sophos.com HIDS

2. Cercate Search and Destroy e determinate da che tipo di malware protegge il vostro computer

3. Cercate come funzionano NIDS and HIDS

4. Cercate soluzioni Firewall in rete

5. cercate “chroot” su internet. Leggete circa questo tipo di “jail” o “sandbox”.

6.8 Consigli per una buona sicurezza

Ci sono alcune semplici cose che potete fare per minimizzare il vostro rischio di Malware.

- solo il download da sorgenti affidabili (ciò significa non W4R3Z, perfavore)
- non aprite allegati di e-mail provenineti da persone che non conoscete
- non lasciate macro abilitate di default nelle vostre applicazioni
- tenete il vostro sistema operativo e le applicazioni aggiornate
- effettuate il download e l' installazione di software con una checksum – verificate la checksum.

Ulteriori approfondimenti

AV Vendor Sites

http://www.sophos.com

http://www.symantec.com

http://www.fsecure.com

Tutti questi siti contengono liste dettagliate dei trojans, viruses ed altri malware. Trovate anche descrizioni dettagliate delle suddette funzionalità.

http://www.cess.org/adware.htm

http://www.microsoft.com/technet/security/topics/virus/malware.mspx

http://www.zeltser.com/sans/gcih-practical/revmalw.html

http://www.securityfocus.com/infocus/1666

http://www.spywareguide.com/

http://www.brettglass.com/spam/paper.html

http://www.lavasoft.nu/ - AdAware Cleaning Software (Freeware Version)

http://www.claymania.com/removal-tools-vendors.html

http://www.io.com/~cwagner/spyware.html

http://www.bo2k.com/

http://www.sans.org/rr/catindex.php?cat_id=36