Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 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.

Informationen zur Nutzungslizenz

Die folgenden Lektionen und Arbeitsmaterialien sind öffentlich verfügbar unter den folgenden Bedingungen seitens ISECOM:

Alle Materialien der Hacker Highschool werden für den nicht-kommerziellen Einsatz in Grund-, Haupt-, Realschulen und Gymnasien zur Verfügung gestellt, sowohl für öffentliche und private Bildungseinrichtungen, als auch für Privatunterricht zu Hause. Die Materialien dürfen in keiner Form für den Wiederverkauf reproduziert werden. Der kommerzielle Einsatz der Materialien, welche käuflich erworben werden können, in jeglicher Form von Schulstunde, Unterricht, Training, Meeting, Kongress, Vorlesung, Fortbildung, Sommer- oder Abendschulen ist ohne vorigen Erwerb einer Lizenz explizit untersagt. Um eine Lizenz zu erwerben, besuchen Sie bitte http://www.hackerhighschool.org/license.

Das Hacker Highschool (HHS) Projekt ist ein Unterrichtswerkzeug. Der Einfluss auf die Lernenden liegt beim Lehrer, nicht jedoch beim Werkzeug. Aus diesem Grund erkärt sich ISECOM nicht für Schäden verantwortlich, welche aus einem eventuellen Missbrauch der hier publizierten Informationen hervorgeht. Das HHS Projekt ist die Arbeit einer offenen Gemeinschaft. Wir hoffen, dass die Lesenden Nutzen in unsem Projekt finden werden und bitten um Unterstützung unserer Arbeit, sei es durch den Erwerb einer Lizenz, durch eine Spende, Sponsoring oder in anderer Form.

Für das gesamte Material: © ISECOM 2004

Inhalt

Mitwirkende

Simon Biles, Computer Security Online Ltd.

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM

ÜBERSETZUNG

Georg Berky

Karl Pausch

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

/// computer security online

6.0 Einleitung

„Malware“ sind Programme, die einen unerwünschten, negativen (lat. „malus“ - böse) Effekt auf die Sicherheit deines Computer haben. Die Bedeutung beinhaltet mehrere andere Begriffe, die du wahrscheinlich schon gehört hast, etwa „Virus“, „Wurm“ und „Trojanisches Pferd“, oder solche, die du vielleicht noch nicht kennst: „Rootkit“, „Logische Bombe“ („logic bomb“) und „Spyware“. Diese Lektion soll dir eine Einführung, Beschreibung und Erklärung zu jeder dieser verschiedenen Untergruppen des Begriffes „Malware“ geben, und einige Gegenmaßnahmen erkären, mit denen man die Probleme, die mit Malware verbunden sind, einschränken kann.

6.1 Viren

6.1.1.Einführung

Der Virus ist wohl die bekannteste Form der Malware, deren sich die Leute bewusst sind. Der Grund, weswegen diese Form als „Virus“ bekannt ist, ist eher historischer als logischer Natur. Die Presse brachte die Berichte über die ersten Computerviren zur selben Zeit wie Artikel über die Verbreitung von AIDS. Damals gab es für die Leute leicht zu entdeckende Gemeinsamkeiten zwischen den beiden Phänomenen, nämlich die Interaktion mit einem bereits infizierten Opfer, die Abhängigkeit von einem Wirtskörper und der sichere Tod nach der Infektion. Das resultierte in der Sorge, man könne sich mit einem Computervirus „infizieren“.

6.1.2.Beschreibung

Viren sind selbsreplizierende Software, die sich – ähnlich einem biologischen Virus – an ein anderes Programm oder (im Falle eines Makrovirus) an eine andere Datei anhängen. Das Virusprogramm wird also nur ausgeführt, wenn das Wirtsprogramm gestartet, oder die Wirtsdate des Makrovirus geöffnet wird. Diese Eigentschaft unterscheidet auch Viren von Würmern. Wird der Wirt nicht geöffnet oder gestartet, wird auch der Virus nicht aktiv und verbreitet sich nicht weiter.

Es gibt eine Vielzahl verschiedener Virentypen, wobei die am weitverbreitetste Sorte wohl der Makrovirus ist. Die meisten anderen Arten findet man oft nur noch in speziellen Testumgebungen, die der Erforschung solcher Viren dienen („in captivity“, Gegenteil: „in the wild“).

6.1.2.1. Bootsektorviren

Der Bootsektorvirus war die erste Sorte Virus. Er versteckt sich im ausführbaren Code am Anfang eines bootbaren Datenträgers. Um also einen Computer zu infizieren, musste man von einer infizierten Diskette booten. Vor ziemlich langer Zeit (vor etwa 15 Jahren) war es ganz normal, von einer Diskette zu booten, weswegen sich auch solche Viren sehr schnell verbreiteten, bis die Leute herausfanden, was eigentlich los war. Da der Virus (und alle anderen Arten) keinen Wirt zweimal infizieren wollte, hinterließ er auf schon befallenen Opfern eine Markierung, genannt „Signatur“. Durch diese Signatur war es aber auch anderer Software (meistens Antivirensoftware) möglich, die Infektion zu erkennen.

6.1.2.2. Viren in ausführbaren Dateien

Dieser Virus befällt eine ausfürbare Datei („executable"), etwa an eine .exe oder eine .com Datei. Einige Viren suchen nach speziellen Programmdateien, die Teil des Betriebssystems sind, und deswegen immer gestartet werden, wenn der Computer verwendet wird, wodurch sich der Virus schnell verbreitet. Es gibt mehrere Methoden, wie sich ein Virus eine ausführbare Datei befällt. Die einfachste und brutalste davon besteht darin, einfach den Anfang des Wirts mit dem Viruscode zu überschreiben, was natürlich zur Folge hat, dass das Wirtsprogramm nicht mehr funktioniert und crasht und dass die Infektion ziemlich schnell erkannt wird – besonders, wenn es sich um eine wichtige Datei des Betriebssystems handelte.

6.1.2.3. Der „Terminate and stay resident" (TSR) Virus

TSR („terminate and stay resident" - „beende und bleib im Speicher") ist ein Begriff des DOS Betriebssystems, der besagt, dass ein Programm in den Speicher geladen, dann aber weiter im Hintergrund ausgeführt wird. Dadurch kann der Benutzer wie normal andere Programme im Vordergrund ausführen. Die komplexeren Mitglieder dieser Sorte Virus fangen Funktionsaufrufe an das Betriebssystem am, die dazu führen würden, dass die Infektion entdeckt wird. Statt der normalen Ergebnisse geben sie falsche zurück. Einige fangen beispielsweise den „dir" Befehl ab und infizieren alle Programme im Verzeichnis, das gerade angezeigt wird, andere beendeten oder löschten sogar Antiviren Software auf dem infizierten System.

6.1.2.4. Der polymorphe Virus

Die ersten Viren waren ziemlich leicht zu entdecken. Entweder schrieben sie eine Signatur in den Wirt oder hatten eine in sich selbst, um mehrfache Infektionen zu verhindern, oder sie hatten eine charakteristische Programmstruktur anhand welche es möglich war, sie zu entdecken. Dann kamen die Polymorphen Viren. Polymorphe Viren (lat. „polymorphus" - vielgestaltig) ändern ihre Struktur, den Aufbau ihres Codes oder ihre Verschlüsselung, sobald sie sich reproduzieren. Nach jeder Infektion sehen sie also komplett anders aus. Dies stellte ein großes Problem dar, da es viel weniger Signaturen gab, die gleich blieben – einige der ausgefeiltesten Viren hatte eine Signatur von nur wenigen Bytes, anhand welcher man sie identifizieren konnte. Das Problem vergrößerte sich noch weiter, als in der Virenschreiber-Szene einige Ploymorephie-Kits auftauchten, mit denen man für jeden Virus eine Polymorphe Variante erstellen konnte.

6.1.2.5. Der Makrovirus

Ein Makrovirus nutzt die Tatsache, dass einige Programme Code ausführen können, der in in den Dateien, die sie erzeugen oder wenigstens lesen, gespeichert ist. Programme wie Excel und Word unterstützen eine eingeschränkte aber dennoch mächtige Version der Programmiersprache VisualBasic. Das hat für den Anwender den Vorteil, dass er für immer wiederkehrende Aufgaben einfach ein Programm, ein sogenanntes „Makro", schreiben kann und so Arbeitszeit spart, aber diese Makros können auch dazu verwendet werden, Virencode an ein Dokument anzuhängen, der sich selbständig in andere Dokumente schreibt und sich so verbreitet. Obwohl diese „Features" jetzt nicht mehr schon direkt nach der Installation des Programms aktiviert sind, führte Outlook dennoch bestimmten Code in einer HMTL E-Mail aus, sobald diese gelesen wurde. Das hatte zur Folge, dass sich solche Viren schnell verbreiteten, indem sie sich an alle auf dem Computer gespeicherten Mail-Adressen verschickten.

Übungen:

1.Suche im Web nach Beispielen für jede der oben beschriebenen Virusarten

2.Versuche, mehr über den Klez Virus herauszufinden

Was ist seine „payload"?

Der Klez Virus ist bekannt dafür, zu „spoofen". Was ist bedeutet das, und wie wird es von Klez verwendet?

Nehmen wir an, dass du erfährst, dass dein Computer mit Klez infiziert ist. Wie entfernst du diesen Virus?

3.Nehmen wir an, du hast gerade eine E-Mail mit dem Betreff „Warning about your E-Mail account" erhalten. Die Mail sagt, dass du Mails falsch verschickt hast, dass dir deswegen dein Internetzugang gesperrt wird und dass du die Datei im Anhang lesen sollt, um Details zu erfahren. Du hast deines Wissens nach natürlich nichts falsches mit deinen E-Mails gemacht. Wirst du misstrauisch? Das solltest du. Suche nach Informationen und finde heraus, welcher Virus im Anhang steckt. Tip: wenn du anfängst, an Frühstuck oder „breakfast" zu denken, liegst du richtig.

6.2 Würmer

6.2.1. Einführung

Würmer sind älter als Viren. Der erste Wurm existierte schon viele Jahre vor dem ersten Virus und nutzte einen Fehler im UNIX Befehl „finger" aus, um ziemlich schnell fast das ganze Internet, das damals noch recht klein war, lahmzulegen. Im folgenden Abschnitt befassen wir uns mit Würmern.

6.2.2. Beschreibung

Ein Wurm ist ein Programm, das sich, sobald es gestartet worden ist, ohne dass der Benutzer eingreifen muss reproduziert. Es verbreitet sich von Host zu Host, indem es Fehler in den angeboteten Diensten auf dem Zielrechner ausnutzt. Würmer verbreiten sich über Netzwerke, ohne dass ein Benutzer eine E-Mail schreiben oder eine infizierte Datei abschicken muss. Der Großteil der Vorfällte, über die in der Presse berichtet worden ist, wurde von Würmern, nicht von Viren verursacht.

Übungen:

Suche im Web über Informationen zum ersten Wurm

Finde heraus, welche Schwachstellen Nimda und Code Red ausnutzen, um sich zu verbreiten

6.3 Trojanische Pferde und Spyware

6.3.1. Einführung

Das erste trojanische Pferd wurde von den Griechen vor einigen tausend Jahren verwendet. Erinnere dich an Homers Ilias (http://de.wikipedia.org/wiki/Ilias) oder den Film „Troja“, falls du ihn gesehen hast. Die Idee bei einem Trojaner ist, dass man etwas gemeines in ein sonst sicheres System einschleust, indem man es in etwas nettem versteckt. Das kann sowohl durch Demoversionen des neusten Spielehits, als auch durch E-Mails mit Nacktfotos einer Filmschönheit geschehen. Dieser Abschnitt befasst sich mit Trojanern und Spyware.

6.3.2. Beschreibung

Trojaner sind Malware, die sich als etwas interessantes, begehrenswertes oder nützliches verkleiden, um dich dazu zu bringen, sie auszuführen. An diesem Punkt angelangt können sie deinem Computer unangenehme Dinge antun, etwa das Installieren einer Hintertür oder eines Rootkits (siehe Abschnitt 6.4) oder schlimmer: sie lassen deinen Computer eine Telefonnummer anrufen, die sehr viel Geld kostet.

Spyware ist Software, die sich heimlich auf deinem Computer installiert, oft von einer Website, die du besucht hast. Nach der Installation wird das Programm versuchen, nach Informationen über dich zu suchen, die es als nützlich oder wertvoll ansieht. Das kann sowohl eine Statistik über deine besuchten Webseiten sein, als auch deine Kreditkartennummer. Einige Vertreter der Sorte Spyware enttarnen sich selbst dadurch, dass sie Werbungs-Popups überall auf deinem Desktop anzeigen.

Übung:
Suche im Web nach einem Beispiel für ein Trojanisches Pferd und für Spyware

6.4 Rootkits und Hintertüren

6.4.1. Einführung

Wenn ein Computer kompromittiert worden ist, wird der Angreifer versuchen, einen Weg zu finden, wie er ohne großen Aufwand wieder Zugriff auf den Computer bekommt. Dafür gibt es viele Möglichkeiten, von denen einige berühmt geworden sind, etwa „Back Orifice“ (Hintereingang, oder vulgärer „hintere Öffnung“).

6.4.2. Beschreibung

Rootkits und Hintertüren („backdoors“) sind Porgramme, die Zugriff auf einen Computer gewähren. Die Varianten reichen von einfach (ein Programm, das auf einen bestimmten Port hört) zu komplex (ein Programm, das sich im Speicher versteckt, Logdateien umschreibt und auf einen Port hört). Manchmal sind sie so einfach gebaut, dass sie nur einen neuen Benutzer mit Administratorprivilegien erstellen und hoffen, dass der zusätzliche Account übersehen wird. Das geschieht zu dem Zweck, die normale Anmeldung am System zu umgehen. Sowohl Sobig und MyDoom installieren als Teil ihrer Payload eine Hintertür.

Übungen:

Suche im Web nach Beispielen für Rootkits und Hintertüren

Suche nach Informationen über „Back Orifice“ und vergleiche die angebotenen Funktionen mit denen eines kommerziellen remote-administration-Tools, etwa dem von Microsoft.

6.5 Logische Bomben und Zeitbomben

6.5.1. Einführung

Programmierer und Administratoren können manchmal ziemlich schräge Vögel sein. Es ist bekannt, dass es Methoden gibt, ein Programm auszuführen, sobald auf dem System bestimmte Kriterien zutreffen. Beispielsweise könnte man ein Programm schreiben, das anfängt, zufällige Bits auf der Festplatte zu löschen, sollte sich der Administrator für mehr als drei Wochen nicht am System anmelden. Dieser ziemlich bekannte Fall trat 1992 in einer Fima namens „General Dynamics“ auf, wo der Programmierer dieser Firma das Programm nach seinem Ausscheiden aus dem Betrieb starten wollte, um von der Firma viel Geld für die Reparatur des Schadens zu erpressen. Glücklicherweise fand ein anderer Programmierer die logische Bombe bevor sie losging und der Übeltäter wurde zu einer Zahlung von 500'000$ und einiger Zeit im Gefängnis verurteilt.

6.5.2. Beschreibung

Logische Bomben („logic bombs“) und Zeitbomben („time bombs“) sind Programme, die sich weder reproduzieren noch gestatten sie jemandem Zugriff auf dein System. Sie sind Programme oder Teil eines Programms, das schaden anrichtet, sobald es aktiv wird. Sie können selbständig oder Teil eines Wurm oder Virus sein. Zeitbomben lassen ihre Payload zu einem bestimmte Zeitpunkt los, logische Bomben warten damit, bis ein bestimmtes Ereignis auf dem System eintritt.

Das konzeppt der „Zeitbombe“ kann natürlich auch für etwas sinnvolles verwendet werden, beispielsweise dazu, dass ein Programm innerhalb eines bestimmten Zeitraumes (meistens 30 Tage) getestet werden kann, danach aber nicht mehr lauffähig ist, bis ein Registrationscode eingegeben wird. Das ist ein Beispiel für nützliche Zeitbombenprogrammierung.

Übungen

Welche anderen sinnvollen (und legalen) Gründe könnte es für den Einsatz von logischen Bomben und Zeitbomben geben?
Wie könnte man solche Programme auf deinem System ausfindig machen?

6.6 Gegenmaßnahmen

6.6.1. Einführung

Es gibt mehrere Möglichkeiten, Malware zu entdecken, zu entfernen und eine Infektion damit zu verhindern. Einige davon lassen sich auf gesunden Menschenverstand zurückführen, andere sind technischer Natur. Im folgenden Abschnitt werden wir uns einige davon zusammen mit einem kurzen Beispiel und einer Erklärung ansehen.

6.6.2. Anti-Virus

Antivirenprogramme sind sowohl kommerziell als auch in Open Source Form verfügbar und arbeiten alle nach der selben Methode: die Programme haben eine Datenbank voll von Signaturen, auf die sie alle Dateien auf einem System überprüfen, um zu sehen, ob sie infiziert sind oder nicht. Bei modernen Viren sind die Signaturen jedoch oft klein und die Programme können falsche Meldungen über eine angebliche Infektion liefern. Manche Programme verwenden eine „heuristische" Suche, was bedeutet, dass sie nach Code suchen, der für Viren charakteristisch ist, und so auch unbekannte Formen entdecken können. Neuerdings haben Antivirenprogramme auch die Grenze zum host-basierten IDS („intrusion detection system"- System zur Erkennung von Einbrüchen) überschritten, indem sie Prüfsummen der der Dateien auf einem System speichern, und so die Zeit, die zum Überprüfen benötigt wird, verkürzen.

6.6.3. NIDS

Network intrusion detection systems (Systeme, die Einbrüche in ein Netzwerk melden) arbeiten ähnlich wie Antivirenprogramme. Sie suchen nach der Signatur oder dem typischen Verhalten eines Wurms oder Virus. Sie können dann entweder eine Meldung an den Benutzer schicken, oder automatisch den Netzwerkverkehr, der die Malware entält stoppen.

6.6.4. HIDS

Host based intrusion detection systems (Systeme, die Einbrüche in einen Host melden) wie Tripwire („Stolperdraht") erkennen, wenn Dateien modifiziert worden sind. Bei Programmen erwartet man normalerweise nicht, dass sie sich ändern, nachdem sie kompiliert worden sind. Wenn sich also die Größe der Datei, das Datum der letzten Änderung der Datei oder ihre Prüfsumme ändert, ist es normalerweise ziemlich schnell klar, dass etwas falsch läuft.

6.6.5. Firewalls

Würmer verbreiten sich über Netzwerke, indem sie sich mit angreifbaren Diensten auf jedem Zielhost verbinden. Neben der Tatsache, dass man keine angreifbaren Dienste auf seinen Host laufen lässt, ist es wohl eine gute Idee keine Verbindungen zu diesen Diensten zuzulassen. Viele moderne Firewalls beherrschen die eine oder andere Form des „packet filtering" (Filterung von Paketen), die Pakete verbietet, welche einer bestimmten Signatur entsprechen.

6.6.6. Sandboxes

Das Prinzip einer Sandbox (eines Sandkasten) ist einfach: Ein Programm bekommt seine eigene kleine Welt zum spielen, kann aber nichts mit dem Rest des Computers anfangen. In der Programmiersprache Java ist das standartmäßig der Fall, eine Sandbox kann aber auch anders realisiert werden, etwa durch den Linux Befehl chroot. Ein Sankasten beschränkt den Schaden, den Malware auf einem System anrichten kann also auf die Umgebung des Sandkastens. Eine andere Methode stellt die virtuelle Maschine dar, eine Maschine, die nicht wirklich existiert, sondern nur durch ein Programm auf deinem Computer nachgestellt wird, etwa durch VMWare (http://www.vmware.com). Dies isoliert die virtuelle Maschine vom Rest des Systems und lässt nur dem vom Benutzer erlaubten Zugriff daruf zu.

Übungen:

Suche nach Informationen auf den folgenen Seiten und gib an, um welches Sicherheitssystem es sich handelt

http://www.vmware.com

NIDS

http://www.tripwire.org

Antivirus

http://www.snort.org

Firewall

http://www.checkpoint.com

Sandbox

http://www.sophos.com

HIDS

Suche nach „Spybot Search and destroy“ und finde heraus, gegen welche Sorte Malware es dich schützt.

Finde heraus, wie NIDS und HIDS funktionieren

Suche im Web nach Firewall Systemen

Suche nach einer Beschreibung von chroot, finde heraus wie diese Art der Sandbox funktioniert

6.7 Sicherheitsratschläge

Es gibt ein paar einfache Dinge, die dein System um einiges sicherer machen:

Lade Software nur von vertrauenswürdigen Seiten herunter (keine W4R3Z bitte)

Öffne keine Mail-Anhänge von Leuten, die du nicht kennst

Deaktiviere standartmäßig Makros in den Programmen die du meistens benutzt und aktiviere sie nur, wenn du sie brauchst

Halte dein Betriebssystem und deine Programme mit Updates und Patches auf dem neusten Stand

Wenn es Checksummen fuer die Programme, die du herunterlädst, gibt, überprüfe sie

Weitere interessante Informationen

Anbieter von Antivirenprogrammen -

http://www.sophos.com

http://www.symantec.com

http://www.fsecure.com

Auf allen diesen Seiten findest du Datenbanken mit Details zu Viren, Würmern und Trojanern. Es gibt auch detaillierte Beschreibungen der Funktionsweise der aufgefürten Exemplare.

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