Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 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.

Informatie over de “Gebruiksvoorwaarden”

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Op al het werk berust copyright van ISECOM, 2004.

Inhoudsopgave

Auteurs

Simon Biles, Computer Security Online Ltd.
Kim Truett, ISECOM
Pete Herzog, ISECOM
Marta Barceló, ISECOM

Vertaald door:

Raoul Teeuwen

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

/// computer security online

6.0 Introductie

Onder "Malware" verstaan we programma's en delen van programma's die een kwaadaardig (Engels: malicious > "Mal"ware) of vervelend effect op je computer (beveiliging) hebben. Het begrip malware omvat vele anderen begrippen waar je wellicht ook weleens van hebt gehoord, zoals , "Virus", "Worm" en "Trojan" en ook een paar waar je wellicht nog niet van hebt gehoord zoals "Rootkit", "Logische bom" en "Spyware". Deze les introduceert en omschrijft deze vormen van malware, geeft voorbeelden, en legt uit wat je kunt doen om de problemen die malware veroorzaakt te beperken.

6.1 Virussen (Virii)

6.1.1 Introductie

Virussen – dit is de meest voorkomende vorm van malware waar mensen van weten. De oorzaak dat het bekend staat als een virus heeft een historische oorzaak. Virussen kwamen voor het eerst in het nieuws op het moment dat ook de verspreiding van AIDS enorm in het nieuws was. Men zag al snel overeenkomsten tussen die twee: verspreiding via contact met een besmette partij, de noodzaak van een gastheer en de uiteindelijke 'dood' van de besmette partij. Hierdoor ontstond zelfs de zorg dat mensen besmet konden raken door een computervirus.

6.1.2 Omschrijving

Virussen of virii zijn zich zelf-kopieerende stukjes software die, net als een biologisch virus, zichzelf aan een ander programma vasthechten, of, in het geval van een "macro virus", aan een ander bestand. Het virus wordt alleen actief wanneer het programma of bestand wordt gestart of geopend. Dit is ook het onderscheid tussen een virus en een worm. Wanneer het programma of bestand op geen enkele manier benaderd wordt, zal het virus niet actief worden en zich niet kunnen verspreiden.
Er zijn verschillende soorten virussen, maar de meest voorkomende soort is nu het macro-virus, terwijl boot-sector-virussen eigenlijk alleen nog voorkomen in "gevangenschap"/laboratoriums.

6.1.2.1 Boot sector virussen

Het boot sector virus was het eerste virussoort. Het verstopt zich in het deel van opstartbare disks waar zich code bevindt waarmee een computer opstart. Om een computer te besmetten moest dus worden opgestart met een besmette disk, vaak een diskette (floppy). Een hele tijd geleden, zo rond 1994, was het heel normaal om met een diskette op te starten, en konden boot-sector-virussen zich prima verspreiden voordat mensen doorhadden dat er iets aan de hand was. Dit virus, en alle andere soorten, laat een handtekening achter die bij een volgende besmettingspoging werd gedetecteerd, zodat een besmette gastheer niet meerdere malen werd besmet. Deze handtekening wordt ook door andere software, zoals anti-virus-software, gebruikt om een besmetting vast te stellen.

6.1.2.2 Het bestands-virus

Het bestands-virus hecht zich aan uitvoerbare bestanden zoals .exe en .com bestanden. Sommige virussen probeerden specifieke bestanden te vinden die onderdeel waren van het besturingssysteem, in de hoop dat die bij elke keer opstarten van de computer worden aangeroepen, zodat ook het virus actief werd en zich kon verspreiden. Er waren verschillende manieren om een virus aan een uitvoerbaar bestand te koppelen, sommige manieren werkten beter dan andere. De eenvoudigste (en minst subtiele) was het overschrijven van het eerste deel van de uitvoerbare code door de virus code. Dit zorgde ervoor dat het virus werd geactiveerd, maar dat het programma vervolgens crashte, zodat al snel duidelijk werd dat er sprake van een besmetting was – zeker wanneer het om een belangrijk systeembestand ging.

6.1.2.3 Het Terminate and Stay Resident (TSR) virus

TSR is een term uit de DOS-tijd, waarbij een programma in het geheugen werd geladen en actief werd in de achtergrond, waarna de computer 'net als anders' kon worden gebruikt 'in de voorgrond' (in die tijd kon je als gebruiker meestal maar 1 programma starten, met TSR-programma's kon je er dus meer tegelijkertijd laten draaien). De meer complexe virussen van dit soort onderschepten aanroepen van systeemcommando's waarmee ze zichtbaar werden gemaakt en gaven foute antwoorden terug – anderen koppelden zich aan het 'dir'
commando, en besmette elk programma in de directory die werd opgevraagd – sommige schakelden zelfs anti-virus-software uit of verwijderden dit geheel.

6.1.2.4 Het polymorphische virus

De eerste virussen waren vrij eenvoudig te vinden. Ze hadden een bepaalde specifieke handtekening: van zichzelf waarmee ze zelf probeerde te voorkomen dat ze een gastheer meerdere keren besmette, of ze hadden een specifieke structuur waardoor ze konden worden geidentificeerd als een bepaald virus. Toen ontstond het polymorphische virus.
Poly – betekent meervoudig en morphisch – betekent vorm. Deze virussen wijzigen zichzelf elke keer dat ze zichzelf verspreiden, door de volgorde van hun eigen programmacode te wijzigen, hun codering (encryptie) te wijzigen en zichzelf een geheel ander uiterlijk te geven. Dit zorgde voor een groot probleem, omdat ineens nog maar heel korte handtekeningen overbleven die hetzelfde bleven – enkele van de "beste" virussen hadden nog maar een detecteerbare handtekening van enkele bytes. Het probleem werd nog groter toen er een aantal polymorpische viruskits werd vrijgegegeven binnen de virus-programmeurs-community, waarmee elk virus polymorpisch kon worden .

6.1.2.5 Het macro virus

Het macro-virus maakt gebruik van de ingebouwde mogelijkheid van een aantal programma's om code uit te voeren. Programma's zoals Word en Excel bevatten beperkte, maar zeer krachtige, versies van de Visual Basic programmeertaal. Dit maakt het mogelijk om herhalende taken te automatiseren of bepaalde instellingen automatisch te configureren. Deze macro-talen worden misbruikt om er virale code aan documenten toe te voegen die zichzelf automatisch hecht aan andere documenten en zichzelf verspreidt. Alhoewel Microsoft de instelling bij nieuwe installaties standaard uit zet, was het ooit zo dat Outlook automatisch code die als bijlage van een e-mail aanwezig was, uitvoerde zodra de mail gelezen werd. Dit betekende dat virussen zich heel snel konden verspreiden door zichzelf eenvoudigweg naar alle e-mail-adressen uit het adresboek van de geinfecteerde machine te sturen.
Oefeningen:

1) Probeer met behulp van het internet van elk van de hiervoor beschreven virussoorten een voorbeeld te vinden.
2) Onderzoek het Klez virus:
- wat is zijn "payload" (wat laat het virus achter en probeert het te bereiken)?
- het Klez virus is bekend omdat het gebruik maakt van SPOOFING. Wat is spoofing, en hoe maakt Klez er gebruik van?
- je hebt net geconstateerd dat je computer besmet is met Klez. Onderzoek hoe je het moet verwijderen.
3) Je hebt zojuist een email ontvangen met als onderwerp "Warning about your email account". In de tekst van de email wordt uitgelegd dat je misbruik maakt van je email-mogelijkheden, en dat je daarom bepaalde rechten en mogelijkheden verliest. Er staat dat in de bijlage meer uitleg volgt.
Maar voor zover jij weet heb je helemaal niets vreemds gedaan met je email. Ben je achterdochtig?
Dat zou je wel moeten zijn. Onderzoek de informatie en stel vast welk virus zich in de bijlage bevindt. (HINT: Als je aan een hondensoort begint te denken – dan zit je goed.)

6.2 Wormen

6.2.1 Introductie

Wormen zijn oudern dan virussen. De eerste worm werd vele jaren eerder gemaakt dan het eerste virus.
De betreffende worm maakt gebruik van een foutje in het UNIX finger commando en legde snel bijna het hele internet, dat toen nog heel klein was, plat. De volgende tekst gaat over wormen.

6.2.2 Omschrijving

Een worm is een programma dat, nadat het geactiveerd is, zichzelf vermenigvuldgt zonder menselijke tussenkomst. Het verspreidt zichzelf van gastheer naar gastheer (computer naar computer), gebruik makend van een onbeschermde service of services. Het reist van het ene naar het andere netwerk zonder dat een gebruiker een besmet bestand of besmette email hoeft te versturen. Bij de meeste recent in de pers verschenen berichten over besmettingen ging het om wormen in plaats van om virussen.
Oefeningen:
1) Zoek via het internet uit wat de allereerste worm was.
2) Zoek uit van welke kwetsbaarheid de Code Red en Nimda wormen gebruikten om zich te verspreiden.

6.3 Trojans en Spyware

6.3.1 Introductie

Het eerste Trojaanse paard (trojan horse) werd duizenden jaren geleden gemaakt door de Grieken. (wellicht heb je de film "Troy" gezien). Het recept/principe van een trojaans paard is dat je iets kwaadaardigs binnensmokkelt in een beveiligde computer, omdat je het verstopt in iets onschuldigs. Dit kan varieeren van een gedownloade spel-demo tot een email waarin naaktfoto's van je favoriete ster worden beloofd. In dit deel gaat het over trojans en spyware.

6.3.2 Omschrijving

Trojans zijn stukjes malware die zich voordoen als iets nuttigs of iets dat je graag wil hebben in de hoop dat je ze daarmee zult activeren. Zodra ze geactiveerd worden kunnen ze iets vervelends doen met je computer, zoals het installeren van een backdoor of rootkit (zie sectie 6.4), of erger, ze bellen een duur telefoonnummer waar je de rekening van dan van krijgt.
Spyware is software welke zichzelf op slinkse wijze installeert, vaak vanaf bezochte websites. Zodra het geinstalleerd is gaat het op zoek naar informatie die mogelijk waardevol is. Daarbij kan het gaan om gegevens over welke websites je bezoekt, of om je credit card nummer. Sommige spyware is makkelijk te ontmaskeren doordat het behoorlijke irritant reclame-pop-up-berichten toont.

Oefeningen:
1) Zoek op het internet een voorbeeld van een trojan en van spyware.

6.4 Rootkits en Backdoors

6.4.1 Introductie

Wanneer een hacker eenmaal toegang heeft gekregen tot een computer, dan zal hij vaak willen zorgen dat hij de volgende keer makkelijker op diezelfde computer binnenkomt. Hiervoor bestaan verschillende manieren, en enkele ervan zijn behoorlijk beroemd geworden – zoek op het internet maar eens op "Back Orifice" !

6.4.2 Omschrijving

Rootkits en backdoors zijn stukjes malware die zorgen dat er weer makkelijk toegang tot de machine te verkrijgen is. Ze varieren van heel simpele manieren (een programma die op een bepaalde poort staat te luisteren) tot heel complexe (programma's die processen in het geheugen onzichtbaar maken, log-bestanden aanpassen, en luisteren op een bepaalde poort). Vaak bestaat een backdoor uit niet meer dan een nieuw aangemaakte gebruiker met beheerders-rechten, waarbij de hacker er van uitgaat dat die extra gebruiker toch niet wordt opgemerkt. Zowel het Sobig als het MyDoom virus installeren een backdoor als onderdeel van hun schadelijke lading (payload).

Oefeningen:
1) Zoek op het internet voorbeelden van rootkits en backdoors.
2) Onderzoek "Back Orifice", en vergelijk zijn functionaliteit met het commercieel verkrijgbare produkt van Microsoft om systemen op afstand te beheren.

6.5 Logische bommen en tijdbommen

6.5.1 Introductie

(Systeem)programmeurs en beheerders kunnen vreemde mensen zijn. Er zijn gevallen bekend waarbij maatregelen geactiveerd werden als aan bepaalde voorwaarden werd voldaan. Een voorbeeld: je zou een programma kunnen maken dat, als de beheerder 3 weken lang niet inlogde, willekeurige bits uit bestanden gaat wissen. Dit gebeurde in een bekend geval uit 1992 waarbij een programmeur van het bedrijf General Dynamics betrokken was.

Hij maakte een logische bom (logic bomb) die belangrijke data zou wissen en geactiverd zou worden nadat hij was vertrokken. Hij was er van uitgegaan dat het bedrijf hem dan veel geld zou betalen om terug te komen om het probleem op te lossen. Maar een andere programmeur ontdekte de logische bom voordat hij af kon gaan, en de kwaadwillende programmeur werd veroordeeld en moest $5,000 betalen. De man had geluk dat de rechter genadig was: in de rechtzaal werd een boete van $500,000 geeist, en daarbovenop nog gevangenisstraf.

6.5.2 Omschrijving

Logische bommen en tijdbommen zijn programma's die zichzelf niet kunnen verspreiden en geen mogelijkheid hebben toegang tot een systeem open te zetten, maar applicaties of delen van applicaties die schade aan gegevens veroorzaken zodra ze actief worden. Ze kunnen op zichzelf staan, of deel uitmaken van een worm of virus. Tijdbommen zijn geprogrammeerd om hun lading op een bepaald tijdstip los te laten.
Logische bommen zijn geprogrammeerd om hun lading los te laten zodra aan bepaald voorwaarden is voldaan.
Het idee achter tijdbommen kan ook nuttig worden toegepast. Het wordt bijvoorbeeld gebruikt om te zorgen dat je een programma kunt downloaden en een bepaald aantal dagen uit te proberen, meestal 30 dagen. Na die periode kan het programma niet meer gebruikt worden, tenzij een registratiecode wordt ingevoerd. Dit is een voorbeeld van niet schadelijke tijdbom-programmacode.

Oefeningen:

1) Op welke andere acceptabele (en legale) manieren is het principe van een tijdbom en een logische bom te gebruiken?
2) Denk eens na over hoe je zo'n programma op je computer op het spoort kunt komen.

6.6 Tegenmaatregelen

6.6.1 Introductie

Er zijn een aantal manieren waarop je malware kunt ontdekken, verwijderen en voorkomen. Sommige komen neer op logisch nadenken, anderen zijn technische alternatieven. In de hierna volgende tekst behandelen we er een paar, met een korte uitleg en voorbeelden.

6.6.2 Anti-Virus

Anti-Virus-software is er in vele commerciele en open source varianten. Ze werken ruwweg allemaal op dezelfde manier. Ze hebben een database van bekende virussen en vergelijken de handtekeningen daarvan met alle op het systeem langskomende bestanden om te zien of er sprake is van besmetting.
Bij moderne virussen is die handtekening echter vaak heel klein, en de kans op valse meldingen (false positives) neemt dan toe – iets lijkt op een virus, maar is dat niet. Sommige virus scanners gebruiken daarom tevens een techniek die men heuristisch scannen noemt, wat betekent dat ze een idee hebben van hoe een virus werkt en daarmee kunnen vaststellen of iets onbekends er wel of niet als een virus uit ziet. Sinds kort doet bepaalde antivirus software ook aan wat ment noemt Host Based Intrusion Detection, waarbij er een lijst met bestanden en controlegetallen (checksum) wordt bijgehouden om de snelheid van de viruscontrole te verhogen.

6.6.3 NIDS

Network intrusion detection (inbraak-alarm) werkt op een zelfde manier als antivirus-software. Het let op een bepaalde handtekening of worm- of virusachtig gedrag. Zodra er iets gevonden wordt kan de gebruiker worden gewaarschuwd of kan het netwerkverkeer met de malware worden geneutraliseerd.

6.6.4 HIDS

Host based Intrusion Detection systems, zoals Tripwire, zijn in staat veranderingen aan bestanden waar te nemen. Je mag aannemen dat zodra een programma gecompileerd is (tot een EXE), normaal gesproken niet meer verandert. Door een aantal zaken te bewaken, zoals de omvang, de bestandsdatum en het controlegetal (checksum), is makkelijk vast te stellen of er iets vreemds aan de hand is.

6.6.5 Firewalls

Wormen reizen van netwerk naar netwerk door gebruik te maken van kwetsbare services. Naast zorgen dat alleen de noodzakelijke services draaien (vaak staan in een besturingssysteem veel meer services geactiveerd dan nodig) en dat eventueel ontdekte kwetsbaarheden gelijk via een update worden gedicht, is het beste dat je vervolgens kunt doen zorgen dat je firewall niet toestaat dat verbinding met die services gemaakt wordt. Veel moderne firewalls hebben ook de mogelijkheid om aan een vorm van packet filtering te doen, vergelijkbaar met een NIDS, waarmee pakketjes die aan een bepaalde handtekening voldoen, onschadelijk worden gemaakt. (Firewalls worden in meer detail besproken in hoofdstuk 7.1.2).

6.6.6 Zandbakken

Het principe van een zandbak (sandbox) is simpel. Je application heeft zijn eigen kleine wereld waarin hij kan doen wat hij wil, maar hij kan niets doen in/aan/tegen/met de rest van de computer. Deze manier van werken gebruikt men ondermeer bij de Java programmeertaal, en kan ook worden toegepast via andere hulpmiddelen zoals chroot in Linux. Hiermee beperk je de schade die malware eventueel kan aanrichten in het besturingssysteem van de host-computer, door het simpelweg er de mogelijkheden en rechten niet voor te geven. Een andere optie is een volledige machine te laten draaien binnen/op een machine, door gebruik te maken van produkten voor "virtuele machines", zoals VMWare. Hiermee isoleer je de virtuele machine van het besturingssysteem op de (fysieke) machine, waarbij de virtuele machine alleen de rechten heeft die het expliciet krijgt toebedeeld door de gebruiker.
Voorbeeld – http://www.vmware.com – VMWare virtuele machines.

Oefeningen:

1. Onderzoek de volgende zaken en bepaal welk soort tegenmaatregel ze vormen of bieden:
1. http://www.vmware.com NIDS
2. http://www.tripwire.org Antivirus
3. http://www.snort.org Firewalls
4. http://www.checkpoint.com Zandbak
5. http://www.sophos.s.com HIDS
2. Onderzoek "Spybot Search and Destroy" en bepaal tegen welk type malware het je beschermt.
3. Onderzoek hoe NIDs en HIDS werken.
4. Onderzoek Firewall oplossingen op het net.

5. Zoek "chroot" op op het internet. Lees meer over dit type "gevangenis" of "zandbak".

6.7 Goed veiligheids advies

Er is een aantal simpele dingen die je kunt doen om de kans te verkleinen dat je last krijgt van malware.

· Download alleen zaken van bronnen die als goed en betrouwbaar bekend staan (dat betekent dus ook: geen W4R3Z, alstublieft.)
· Open geen bijlages in mails van mensen die je niet kent.
· Laat macro's niet standaard aan staan in je applicaties.
· Houd je besturingssysteem en applicaties up to date door eer regelmatig patches te installeren.
· Als je software download en installeert waar een checksum bij is geleverd – controleer dan die checksum.

Verder lezen

AV Vendor Sites -
http://www.virusalert.nl
http://www.waarschuwingsdienst.nl
http://www.sophos.com
http://www.symantec.com
http://www.fsecure.com
Al deze websites hebben databases met informatie over de vele trojans, virussen en andere malware. Ze bevatten vaak ook informatie over de werking van het bovenstaande.
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