Maandelijkse Beveiligingsnieuwsbrief voor Computer gebruikers

OUCH!

IN DEZE EDITIE...

- Wat is Malware
- Wie en Waarom
- Bescherming

Wat is Malware

Inleiding

Iedereen heeft wel eens gehoord van virussen, trojans of rootkits. Deze termen beschrijven verschillende soorten programma's waarmee een computer of mobiel apparaat geinfecteerd kan worden door cyber criminelen. Tegenwoordig worden al deze termen simpelweg malware genoemd. In deze editie bespreken we wat malware is, door wie het ontwikkeld en gebruikt wordt en wat je kan doen om je hier tegen te beschermen.

Auteur
De gast auteur van deze editie van OUCH! is Lenny Zeltser. Lenny houdt zich bezig met het beveiligen van de IT omgevingen van klanten van NCR Corp en hij doceert malware beveiliging bij het SANS Institute. Lenny is actief op Twitter als **@lennyzeltser** en schrijft in zijn beveiligingsblog **blog.zeltser.com**.

Wat is Malware

Malware is software; computerprogramma's die speciaal gemaakt zijn om kwaadaardige acties uit te voeren. Malware is een samenvoeging van de woorden malicious (kwaadaardig) en software. Het doel van de meeste cybercriminelen is om malware op computers en mobiele apparaten te installeren waardoor zij controle krijgen over het apparaat. Veel mensen denken dat dit alleen een probleem is voor Windows computers, maar ieder apparaat kan geinfecteerd worden; zelfs smartphones en tablets.

Windows wordt wel door heel veel mensen gebruikt en daarom is het een interessant doelwit voor criminelen. Er wordt echter steeds meer malware voor mobiele apparaten ontwikkeld omdat vrijwel iedereen tegenwoordig een smartphone heeft. Vergeet niet; iedereen is een potentieel doelwit. Hoe meer apparaten criminelen kunnen infecteren, hoe meer geld zij kunnen verdienen. Meestal maakt het ze niet uit wie er precies geinfecteerd wordt, als het er maar zoveel mogelijk zijn.

Wie en waarom

Malware wordt niet langer uitsluitend ontwikkeld door nieuwsgierige hobbyisten of amateur hackers, maar door cyber criminelen die gebruik maken van geavanceerde technieken. Het doel kan zijn om vertrouwelijke informatie te stelen, inlognamen en wachtwoorden te achterhalen, het verzenden van spam, uitvoeren van DOS aanvallen (Denial of Service), afpersing of identiteitsdiefstal. Cryptolocker malware wordt bijvoorbeeld door criminelen gebruikt om alle bestanden op een computer te infecteren en versleutelen zodat ze niet

© The SANS Institute 2014

Wat is Malware

meer te gebruiken zijn. Eenmaal versleuteld vragen de cybercriminelen om losgeld voor het ontsleutelen van je bestanden.

De beste bescherming tegen malware is up-to-date software, een recente virusscanner en waakzaamheid.

De mensen die malware ontwikkelen en installeren kunnen individuele criminelen zijn, maar ook grote, professionele bendes of organisaties en zelfs overheidsinstanties. Het is zelfs zo dat de meeste malware ontwikkelaars hier tegenwoordig een full-time dagtaak aan hebben; zij doen niets anders dan malware schrijven en verbeteren. Vaak wordt de malware doorverkocht aan andere criminele organisaties, brengen ze er updates voor uit en leveren ze zelfs support aan hun klanten. Een organisatie die malware aankoopt, wil dit vervolgens op zoveel mogelijk machines installeren. Op deze manier wordt een botnet gecreeerd dat kan bestaan uit enkele duizenden tot vele miljoenen geinfecteerde apparaten. Dit botnet kan je zien als een op afstand beheersbaar leger van apparaten dat gebruikt kan worden door de criminelen, of dat weer doorverkocht of verhuurd kan worden aan andere cybercriminelen.

Bescherming

Een belangrijke eerste stap om apparaten te beschermen is de installatie van anti-virus software van een gerenommeerde partij. Anti-virus software, tegenwoordig ook wel anti-malware software genoemd, is software die specifiek ontwikkeld is om malware te detecteren en te stoppen. Anti-malware producten kunnen echter nooit volledige bescherming bieden omdat cybercriminelen contant op zoek zijn naar nieuwe manieren om anti-malware producten te omzeilen. Op hun beurt proberen anti-malware fabrikanten hun producten constant te updaten zodat de laatste malware ook herkent en gestopt kan worden. Het is een constant kat en muis spel tussen malware schrijvers en anti-malware fabrikanten. Dat de anti-malware fabrikanten moeten reageren op malware ontwikkelaars, is er een voordeel voor cybercriminelen; zij ontwikkelen nieuwe malware versies die nog niet gedetecteerd kunnen worden. Je kan dus niet uitsluitend op je anti-malware programma vertrouwen voor bescherming; je moet nog een paar andere dingen doen.

Zorg er ten eerste voor dat je besturingssysteem en applicaties zo ingesteld zijn dat ze automatisch veiligheidsupdates installeren. Hoe beter je systeem is bijgewerkt, hoe lastiger het is voor cybercriminelen om malware op je machine te installeren.

© The SANS Institute 2014

Wat is Malware

Verder ben je zelf één van de belangrijkste beschermingen tegen malware. Malware maakt vaak gebruik van 'social engineering' wat zoveel wil zeggen dat geprobeerd wordt je er van te overtuigen dat je bepaalde software moet installeren. Dit kan bijvoorbeeld via een email (phishing) waarin je gevraagd wordt om op een link te klikken of een bijgevoegd document te openen. Uiteraard wordt de link of het document vervolgens gebruikt om je computer te infecteren.

Social engineering kan ook via andere kanalen dan email, bijvoorbeeld via de telefoon. Je wordt bijvoorbeeld gebeld door iemand die zich voordoet als een support medewerker van Microsoft. Ze hebben gedetecteerd dat er iets mis is met je computer en willen graag dat een programmaatje installeert, een bepaalde website bezoekt, of op afstand toegang tot je computer verschaft zodat ze het kunnen oplossen voor je. Trap er niet in, men probeert malware te installeren en er is hoogstwaarschijnlijk niets aan de hand met je computer. Gebruik je gezonde verstand, als een telefoontje vreemd lijkt, verdacht, of te mooi om waar te zijn, dan is het dat doorgaans ook.

Tenslotte; de beste manier om je te beschermen tegen malware is dat je je software up-to-date houdt, anti-virus producten van bekende fabrikanten installeert en dat je op je hoede bent voor iedereen die je probeert te overtuigen dat je bepaalde software moet installeren waarmee je dan vervolgens je eigen machine infecteert.

Meer Weten?

Ga naar http://www.securingthehuman.org om je in te schrijven voor de maandelijkse OUCH! nieuwsbrief, toegang tot het OUCH! archief en om meer te weten te komen over SANS Security Awareness programma's.

Nederlandse Editie

De Nederlandse editie van OUCH! wordt gesponsord door Breukel IIS. Wij brengen enterprise information security naar het midden- en klein bedrijf. Voor meer informatie: info@breukeliis.com

Bronnen (Engels)

OUCH Phishing:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
OUCH Securing Your Computer:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012
You Are The Target Poster:
http://www.securingthehuman.org/resources/posters

OUCH! is een publicatie van SANS Securing The Human en wordt gedistribueerd onder de Creative Commons BY-NC-ND 3.0 license. Deze nieuwsbrief mag gebruikt worden in uw eigen Security Awareness programma's en vrijelijk verder worden gedistribueerd, zolang de inhoud niet gewijzigd wordt. Stuur een bericht naar ouch@securingthehuman.org voor meer informatie en vertalingen.

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Jan-Adam Breukel