OUCH! | March 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Wat Is Malware
- Wie Maakt Malware?
- Jezelf Beschermen

Wat Is Malware?

Overzicht

Je hebt allicht gehoord over begrippen als virus, trojan, ransomware of rootkit wanneer men het heeft over cyberbeveiliging. Elk van deze begrippen omschrijven hetzelfde, namelijk programma's die door criminelen worden gebruikt om computers en toestellen te besmetten. Het woord malware dient hier als overkoepelend begrip voor al deze schadelijke software. In deze nieuwsbrief leggen we uit wat malware is, wie het maakt, waarom en wat je kan doen om jezelf ertegen te beschermen.

Gast redacteur

Lenny Zeltser focust op het beschermen van de IT-operaties bij klanten van NCR Corp en geeft les in het bestrijden van malware bij het SANS-Instituut. Lenny is actief op Twitter als **@lennyzeltser** en heeft een security blog op **zeltser.com**.

Wat Is Malware

Malware is software -een computer programma- dat schadelijke activiteiten uitvoert. Het begrip malware is in feite een samenstelling van de woorden malicious (schadelijk) en software. Cybercriminelen installeren malware op computers of toestellen om de controle over te nemen of om toegang te krijgen tot gegevens. Na de installatie, kunnen deze aanvallers malware gebruiken om jouw online activiteiten te volgen, jouw wachtwoorden, bestanden te stelen of jouw systeem te gebruiken om andere systemen aan te vallen. Malware kan zelfs jouw gegevens gijzelen en in ruil voor losgeld, je terug toegang geven.

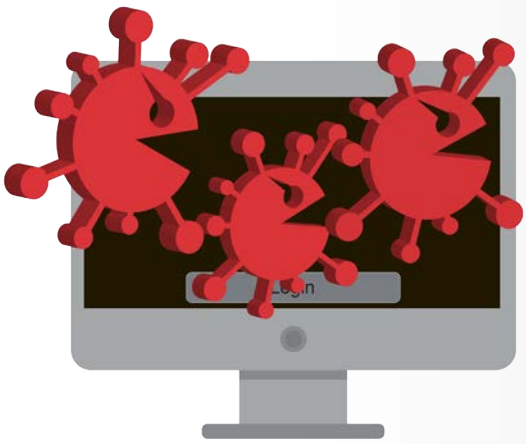
Veel mensen denken dat malware enkel een probleem is voor Windows computers. Hoewel Windows wijdverspreid is, en hierdoor een belangrijk doelwit is, kan malware ieder toestel besmetten, ook Mac computers, smartphones of tablets. Hoe meer computers en toestellen een cybercrimineel kan besmetten, hoe meer hij kan verdienen. Net daarom is iedereen een potentieel doelwit, zelfs jij.

Wie Maakt Malware?

Malware wordt niet meer enkel gemaakt door nieuwsgierige hobbyisten of amateur hackers, maar door beroepscriminelen. Hun doel is om geld te verdienen door jouw toestel of computer te besmetten, jouw gegevens te verkopen, spam e-mails te verzenden, denial of service aanvallen te starten, of zelfs door je te chanteren. De mensen die malware maken en

Wat Is Malware?

verdelen variëren van individuen tot georganiseerde misdaadbendes of zelfs overheidsinstanties. De mensen die de hedendaagse malware maken, doen dit vaak als fulltime job. Eens de malware is ontwikkeld, zal men dit verkopen aan andere individuen of organisaties, waarbij er zelfs ondersteuning en regelmatige updates worden voorzien aan de “klanten”.



Bescherm jezelf tegen malware door kritisch te zijn met verdachte berichten, jouw toestellen te updaten en een antivirus te installeren.

Jezelf Beschermen

Een belangrijke maatregel om jezelf te beschermen is door een antivirus te installeren van een vertrouwde verkoper. Deze tools, soms antimalware genaamd, zijn ontworpen om malware te detecteren en te stoppen. Maar een antivirus kan niet alle schadelijke software blokkeren of verwijderen. Cybercriminelen innoveren continu en ontwikkelen nieuwe en geavanceerde malware die deze detectie omzeilen. Het is tegenwoordig een wedloop geworden aan beide zijden om elkaar te slim af te zijn. Jammer genoeg zijn de slechteriken vaak een stap voor. Omdat je niet alleen op een antivirus kan vertrouwen, volgen er hier enkele extra maatregelen die je kan nemen om jezelf te beschermen:

- Cybercriminelen besmetten vaak computers of toestellen door zwakke plekken in software uit te buiten. Des te recenter jouw software, des te minder zwakke plekken jouw systemen zullen bevatten en des te harder het is om deze te besmetten. Zorg ervoor dat jouw besturingssystemen, toepassingen en toestellen automatische updates kunnen installeren.
- Een vaak gebruikte manier om mobiele toestellen te besmetten is door een valse mobiele app te voorzien, deze op het Internet te plaatsen en vervolgens gebruikers te overtuigen om deze te downloaden en te installeren. Net daarom download je enkel apps van vertrouwde en bekende bronnen. Installeer enkel mobiele apps die reeds een ruimte tijd online zijn, gedownload zijn door veel gebruikers en veel positieve recensies hebben.
- Op computers, gebruik een standaardaccount die beperktere privileges heeft dan een admin account zoals “Administrator” of “root”. Hierdoor voorzie je extra bescherming doordat je malware zal voorkomen om zichzelf te installeren.
- Cybercriminelen leiden vaak mensen om de tuin om voor hen malware te installeren. Zo kunnen ze bijvoorbeeld een e-mail naar jou sturen die er legitiem uitziet en een bijlage of link bevat. Misschien dat het bericht wel komt van jouw bank of een vriend. Maar indien je de bijlage opent of op de link klikt, activeer je schadelijke code dat malware installeert op jouw systeem. Indien je een bericht krijgt die verwarrend is, een dringende situatie betreft,

Wat Is Malware?

of te mooi lijkt om waar te zijn, dan is het mogelijk een aanval. Wees op je hoede, jouw gezond verstand biedt vaak de beste verdediging.

- Neem geregeld back-ups van jouw systeem en bestanden via cloud-gebaseerde diensten, of bewaar jouw back-ups offline op externe schijven die niet verbonden zijn met jouw systeem. Op die manier zullen jouw back-ups beschermd zijn indien malware deze ook probeert te versleutelen of te wissen. Back-ups zijn kritiek, aangezien ze vaak de enige manier zijn om te gegevens te herstellen na een malware besmetting.

Ten slotte, de beste manier om je te verdedigen tegen malware is door jouw software up-to-date te houden, een bekende antivirusoplossing te voorzien en aandachtig te zijn voor iedereen die je wil misleiden om jouw eigen systeem te besmetten.

Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Securely Using Mobile Apps:	https://securingthehuman.sans.org/ouch/2015#january2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Cybercrime:	https://veiliginternetten.nl/themes/basisbeveiliging/cybercrime/

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers