OUCH! | Augustus 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Wat is Ransomware
- Zou Ik het Losgeld Betalen?
- Back-ups
- Bijkomende Maatregelen

Ransomware

Wat is Ransomware?

Ransomware is een speciaal type malware dat ermee dreigt om de documenten en bestanden van een slachtoffer te vernietigen. Het is tegenwoordig zeer actief op het Internet. Malware is software –een computerprogramma- dat schadelijke activiteiten uitvoert. Hoewel ransomware een bepaalde vorm is van malware, is het veruit de meest winstgevende voor criminelen. Eens dat ransomware jouw computer besmet, versleutelt het bepaalde bestanden of misschien jouw hele harde schijf. Hierdoor heb je geen toegang meer tot jouw belangrijke bestanden, zoals jouw documenten of foto's. De malware informeert je dan dat je jouw bestanden terug kan krijgen door losgeld te betalen aan de cybercrimineel (vandaar de naam ransomware). Vaak dien je het losgeld te betalen in een digitale munt, zoals Bitcoin. Ransomware wordt verspreid zoals andere vormen van malware. Criminelen versturen schadelijke e-mails waarbij men probeert om jouw een besmette bijlage te laten openen of te laten klikken op een link die je naar de website van de aanvaller leidt.

Gast redacteur

Lenny Zeltser beveiligt de IT-operaties van klanten bij NCR Corp en geeft les aan het SANS-instituut over hoe je malware kan bestrijden. Lenny is actief op Twitter als **@lennyzeltser** en heeft een security blog op **zeltser.com**.

Zou Ik Het Losgeld Betalen?

Er is geen duidelijk antwoord. Het probleem is dat hoe vaker men de criminelen betaalt hoe meer gemotiveerd de criminelen worden om anderen te besmetten. Soms heb je echter geen keuze dan te betalen om je bestanden terug te krijgen. Pas op want zelfs als je betaalt, is er geen garantie dat je jouw bestanden terugkrijgt. Je hebt hier te maken met criminelen, ze zullen mogelijk de bestanden niet decrypteren, of zelfs wanneer ze je een oplossing geven kan er iets mis gaan met het decryptieproces of kan jouw computer met extra malware worden besmet.

Back-Up Jouw Bestanden

De beste manier om te herstellen van een ransomware besmetting is door het losgeld niet te betalen en jouw bestanden te herstellen van back-ups. Op die manier zal je zelfs als je wordt besmet met ransomware, een manier hebben om jouw

Ransomware

systeem en bestanden te herstellen. Houd er rekening mee dat wanneer jouw back-ups kunnen worden geraadpleegd vanaf de besmette computer, de ransomware de back-ups zal verwijderen of zelfs versleutelen. Daarom is het belangrijk om back-ups op te slaan op externe schijven die niet altijd verbonden zijn met jouw systeem, of om back-up clouddiensten te gebruiken. Een vaak gemaakte fout is dat men veronderstelt dat back-ups werken, zonder regelmatig te testen of ze werken. Net daarom dien je regelmatig jouw back-ups te testen om zeker te zijn replace with: of je de bestanden kunt herstellen wanneer jouw systeem besmet raakt door ransomware. Back-ups zijn belangrijk omdat ze ook een oplossing zijn als je per ongeluk bestanden verwijdert of als jouw harde schijf crasht.

Ransomware is malware die eens het jouw computer besmet, al jouw bestanden versleutelt en de toegang ertoe blokkeert.

Bijkomende Maatregelen

Je kan jezelf beschermen tegen ransomware door een aantal andere maatregelen te nemen. Zorg ervoor dat jouw antivirus up-to-date is. Een antivirus of soms ook wel een antimalware oplossing genoemd, is ontworpen om malware te detecteren en te stoppen. Een antivirus kan niet ieder schadelijk programma blokkeren of verwijderen. Cybercriminelen innoveren constant en ontwikkelen betere en geavanceerdere malware die detectie vermijden. Het is een continue wapenwedloop waarbij beide partijen mekaar proberen te overtroeven. Helaas zijn de slechteriken vaak een stap voor, waardoor het belangrijk is om back-ups te maken en de volgende maatregelen te nemen:

- Cybercriminelen besmetten vaak computers en toestellen door kwetsbaarheden in de software te misbruiken. Hoe recenter jouw software, hoe minder kwetsbaarheden er zijn en hoe moeilijker het is voor cybercriminelen om deze te besmetten. Zorg er daarom voor dat jouw besturingssysteem, toepassingen en toestellen automatisch updates installeren.
- Op computers, gebruik een normale account met beperkte toegang dan een geprivilegieerd account zoals “Administrator” of “root”. Dit biedt extra bescherming doordat het voorkomt dat bepaalde types malware zichzelf kunnen installeren.
- Cybercriminelen leiden mensen vaak om de tuin zodat zij malware voor hen installeren. Zo wordt er bijvoorbeeld een mail verstuurd die er echt en authentiek uitziet met daarin een bijlage of een link. Misschien komt de e-mail

Ransomware

zelfs van jouw bank of van een vriend. Indien je de bijlage opent of als je op de link klikt, ga je mogelijk schadelijke code uitvoeren dat malware installeert op jouw systeem. Indien er een bericht een gevoel van urgentie creëert, verwarrend is, té mooi is om waar te zijn of taalfouten bevat, is het mogelijk een aanval. Wees daarom voorzichtig en gebruik jouw gezond verstand.

Bescherm jezelf tegen ransomware door waakzaam te zijn wanneer je e-mailbijlages of op links klikt. Zorg ervoor dat jouw antivirus up-to-date is en test of jouw back-ups werken.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives 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
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Microsoft Article:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 Course - Reverse Engineering Malware:	https://sans.org/for610

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