OUCH! | mei 2014

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Overzicht
- Indicatoren van aantasting
- Hoe reageren

Ik ben gehackt, wat nu?

Overzicht

We snappen jouw bezorgdheid wanneer het gaat over het beschermen van jouw computer en jouw gegevens. Het maakt niet uit –net als met autorijden- hoe veilig je ook rijdt, vroeg of laat kan je betrokken raken in een ongeval. In deze nieuwsbrief leren we je op welke zaken je moet letten om te bepalen of jouw computer is gehackt en wat je er aan kan doen. Des te sneller je opmerkt dat jouw computer gehackt is en hoe sneller je hierop reageert, des te beter je de schade aan jezelf of jouw organisatie kan beperken.

Gastredacteur

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) werkt als Chief Scientist bij CSRgroup Computer Security Consultants. Hij is tevens medeauteur van de SANS cursussen Memory Forensics (FOR526) en Malware Reserve Engineering (FOR610).

Indicatoren van aantasting

Allereerst moet je begrijpen dat in de meerderheid van de gevallen er geen eenvoudige manier is om te bepalen of jouw computer is gehackt. Om dit te bepalen worden er verschillende indicatoren gebruikt. Indien je er een aantal herkent, ben je gehackt. Enkele voorbeelden:

- Jouw antivirus programma geeft de melding dat jouw computer besmet is, vooral indien het onmogelijk is om de besmette bestanden te verwijderen of in quarantaine te plaatsen.
- De standaardpagina in jouw browser is onverwacht gewijzigd of communiceert met websites die je niet hebt bezocht.
- Jouw computer heeft nieuwe gebruikersaccounts die je niet zelf hebt aangemaakt.
- Er worden nieuwe programma's uitgevoerd die je niet hebt geïnstalleerd.
- Jouw computer crasht voortdurend of werkt zeer langzaam.
- Een programma vraagt om jouw toestemming om wijzigingen toe te passen op jouw systeem, ook al heb je recent zelf geen programma's geïnstalleerd of bijgewerkt.
- Jouw firewall meldt dat een programma, dat je niet herkent, om toestemming vraagt voor toegang tot het Internet.

Ik ben gehackt, wat nu?

Hoe reageren

Als je een vermoeden hebt dat jouw computer aangetast is, dan is snel handelen de boodschap. Indien de computer wordt voorzien door jouw werkgever of enkel voor werk-gerelateerde zaken wordt gebruikt, probeer dan zeker niet om de computer zelf te herstellen en schakel de computer niet uit. Hierdoor kan je mogelijk waardevol bewijsmateriaal vernietigen dat in later onderzoek nodig is. Daarom meld je best het incident meteen aan jouw werkgever, door contact op te nemen met de help desk, security team of met jouw leidinggevende. Indien je om een bepaalde reden jouw organisatie niet kan contacteren, schakel de computer dan in slaapstand, sluimerstand of hybride slaapmodus. Ook als je twijfelt of je daadwerkelijk bent gehackt, is het veel beter om dit te melden dan dit niet te doen. Jouw organisatie zal mogelijk beschikken over de nodige procedures en medewerkers die met dergelijke situaties weten om te gaan.

Vroeg of laat kan jouw computer worden aangetast, hoe sneller je een incident opmerkt en hoe sneller je reageert, des te beter.

Indien het je eigen computer is, volg dan deze stappen:

- **Backups**: De beste voorbereiding is het maken van backups. Voorzie regelmatige backups van jouw data en test de backups zodat je weet dat je de bestanden kunt herstellen. Wanneer een computer aangetast is, zal het volledig wissen van de harde schijf vaak de enige uitweg bieden samen met een herinstallatie van het besturingssysteem, of de aanschaf van een nieuwe computer. In elk geval dien je jouw persoonlijke data te herstellen van een backup.
- **Wijzig wachtwoorden**: Wijzig al je wachtwoorden, niet enkel diegenen op jouw computer en mobiele toestellen, maar ook al jouw online wachtwoorden. Zorg er voor dat je de wachtwoorden wijzigt vanaf een andere computer, waarvan je zeker weet dat het een veilige computer is.
- **Antivirus**: Als jouw antivirus een melding maakt van een besmet bestand, kies dan uit één van de voorgestelde acties. Meestal kan je het bestand in quarantaine plaatsen, opschonen of verwijderen. De meeste antivirus oplossingen geven links met meer informatie over de specifieke besmetting. Als je twijfelt, plaats dan het bestand in quarantaine. Is dit niet mogelijk, verwijder dan het bestand.
- **Herinstallatie**: indien de antivirus er niet in slaagt om de computer op te schonen, kan je de meest veilige methode toepassen, nl. het opnieuw installeren van jouw computer. Ontkoppel jouw computer eerst van het netwerk, volg dan de instructies van de computerleverancier. In de meeste gevallen betekent dit dat je de ingebouwde recovery partitie gebruikt om jouw computer te herinstalleren. Indien de recovery

Ik ben gehackt, wat nu?

partitie ontbreekt, besmet of beschadigd is, contacteer dan de computerleverancier en vraag of er een recovery DVD kan worden bezorgd. Herinstalleer het besturingssysteem zeker niet via jouw persoonlijke backups, want deze kunnen dezelfde kwetsbaarheden bevatten als diegenen die de hacker oorspronkelijk toegang gaven tot de computer. Indien de computer verouderd is, is het eenvoudiger (en misschien zelfs goedkoper) om een nieuwe aan te schaffen dan nog veel uren te besteden aan een herinstallatie.

- **Professionele Hulp**: Ben je bezorgd dat je mogelijk bent gehackt, maar heb je niet de vaardigheden of de kennis om dit zelf te repareren, dan is het raadzaam om een professional te raadplegen. Bijvoorbeeld nadat je gehackt bent, realiseer je dat jouw backups onvolledig of oud zijn. Hierdoor wil je misschien belangrijke bestanden als afbeeldingen, documenten en video tussen jouw besmette machine en de nieuwe machine uitwisselen. Maar door deze actie kan je onvoorzien malware uitwisselen waardoor de nieuwe computer ook wordt besmet. Een veel veiligere oplossing is om de besmette computer naar een gekwalificeerde technieker te brengen, die de bestanden op een veilige manier overzet zonder risico op een nieuwe besmetting.

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.

Nederlandse Editie

Cegeka is een full-service ICT-bedrijf: u kan bij ons terecht voor advies, detachering, softwareontwikkeling, bouw van websites, on-site en remote beheer van ICT-infrastructuur en outsourcing. Voor meer informatie: http://www.cegeka.com of volg ons op Twitter via @cegeka.

Resources

OUCH! Backups:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! What Is Malware:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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