vzw katholiek secundair onderwijs TIELT RUISELEDE

Cryptolocker virussen

V1.0 – 25 april 2017

Centrale diensten:
Hulstplein 31
8700 Tielt
T 051 42 71 90
F 051 85 00 12
vzw.kso@molenland.be

Inhoudsopgave

Over deze handleiding

Deze handleiding legt uit wat een cryptolocker is, hoe je kunt herkennen wanneer je een besmet bent en wat je daarna moet doen.

Wat is een cryptolocker virus?

Cryptolocker of *cryptoware* is een ransomware[1], een vorm van malware[2], waarbij alle computerbestanden (inclusief back-ups) verloren kunnen gaan. Het sluipt binnen via het Windows-systeem en versleutelt computerbestanden. Hoewel Apple beweert dat het Mac OS-systeem hiertegen bestand is, zijn er toch gevallen van gekend.

De vergrendeling gebeurt via een encryptiemethode waarbij zowel een publieke als geheime sleutel nodig is. Cybercriminelen beschikken over deze sleutel en vragen dan losgeld zodat de bestanden ontgrendeld kunnen worden. De betaling gebeurt dan met bitcoins, de virtuele munt. Het eindresultaat is wel dat de herstelling meestal niet of slechts gedeeltelijk gebeurd is.

[1] **Ransomware** is een chantagemethode op het internet. Letterlijk vertaald betekend het *losgeld*. Het is een procedure waarbij bestanden vergrendeld worden en pas na het betalen van het losgeld worden de bestanden weer ontgrendeld. Betalen leidt echter niet altijd tot het ontgrendelen van de bestanden.

[2] **Malware** is software die gebruikt wordt om de werking van een computersysteem te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private systemen. De term is een samentrekking van het Engelse *malicious software*. Heel veel van deze software haalt de gebruiker onbewust binnen via louche websites, zoals pornosites of sites met gratis bestanden (zoals video's, mp3's, …).

Hoe word je besmet?

De virussen zijn steeds verstopt en cybercriminelen blijven steeds nieuwe manieren vinden om je om de tuin proberen te leiden. Belangrijk is om steeds je gezond verstand te gebruiken en bij de minste twijfel nergens op te klikken of bijlagen te openen. Meer hieronder in het hoofdstuk *Hoe merk je of je besmet bent?*.

Gekende manieren van besmetting

- E-mailberichten waarmee men probeert om je te verleiden om op een link te klikken. Deze mails bevatten meestal volgende inhoud:
    - Veel te hoge factuurbedragen
    - Boete's
    - Incasso's
    - Mislukte afleverpogingen van zogezegde verstuurde e-mailberichten
    - «Je hebt een prijs gewonnen!»
    - …
- Berichten met een bijlage waar het virus in vermomd zit. Meestal is het een zip, exe, doc, pdf, … van een factuur of betalingsherinnering. Zodra je de bijlage dan opent, start het virus automatisch.
- Men wordt opgebeld door een *medewerker* van een bedrijf zoals bijv. Microsoft of een bank met de vraag of ze van op afstand mogen inloggen op je computer om *een probleem op te lossen*.

De berichten zijn meestal afkomstig van:

- telecombedrijven (KPN, Telenet, …)
- transportbedrijven (DHL, UPS, …)
- scanapparaten (Xerox, HP, …)
- banken en financiële inrichtingen (KBC, Western Union, …)
- grote commerciële bedrijven (Amazon, Carrefour, …)
- …

Hoe merk je of je besmet bent?

Sommige varianten zijn heel agressief en dan merk je het meteen: melding op het scherm, browser geblokkeerd, … maar je hebt er ook die heel subtiel te werk gaan op de achtergrond.

Een mogelijk voorbeeld van een cryptolocker foutmelding.

Mogelijke manieren waarop je een besmetting kunt vaststellen

- Je krijgt een foutmelding zodra je een browser (Internet Explorer, Firefox, Chrome, …) opent.
- Je documenten hebben plots een extensie die je niet herkent.
- De harde schijfactiviteit gaat plots zonder reden de hoogte in; dat is een lichtje op je computer en bij oudere schijven zul je de schijf plots veel lawaai horen maken).
- Bestanden kunnen niet meer geopend worden.
- Als je een goed antiviruspakket hebt dat up-to-date is, krijg je misschien hier een melding over.

Wat te doen bij een besmetting?

Als je de zaken uit de vorige stapt vastgesteld hebt, of bij de minste twijfel, voer je volgende stappen uit:

1. Sluit **ONMIDDELLIJK** je pc af. We raden het normaal niet aan maar druk in dit geval op de grote aan/uit-knop tot het toestel uitstaat. Snelheid is een belangrijke factor hier.
2. Verwijder eventuele netwerkaansluitingen zoals een netwerkkabel.
3. Verwijder eventuele aangesloten externe media zoals een USB-stick, externe harde schijf, SD-kaart, …
4. Neem contact op met je computerleverancier of als het om een pc op school gaat, verwittig dan onmiddellijk de centrale IT-dienst. Hou er rekening mee dat in zo goed als alle gevallen de pc geformatteerd zal worden en je alle gegevens kwijt zult zijn.

Hoe kan ik een besmetting voorkomen?

Updates

Een besmetting kun je het best voorkomen door steeds je gezond verstand te gebruiken en je computersysteem zo goed mogelijk up-to-date te houden. Niet enkel het besturingssysteem (Windows) maar ook je browser (Internet Explorer, Edge, Firefox, Chrome, …), browserextensies en populaire software zoals Adobe Reader, Java, VLC, …

E-mails

Open nooit bijlages van e-mails of links als u:

- de afzender van het bericht niet kent.
- niet weet waarover de e-mail precies gaat.
- twijfelt aan de echtheid van de mail.

De echtheid van een e-mail kunt u meestal verifiëren door het domein na te kijken:

- als het e-mailbericht van *sysop@molenland.be* verstuurd is, dan komt het van de Centrale IT-dienst.
- komt het bijv. van *sysop@molenland.cx*, *sysopp@molenland.storage23.be*, *sysop.molenland.3@gmail.com*, … dan komt het bericht van elders.

Bovenstaande is ook toepasbaar op mails van bijv. bankinstellingen. Als het e-mailadres eindigt op *@kbc.be* dan is het meer te vertrouwen dan *@kbcc.xy.be* bijv. Maar zelfs als het e-mailadres betrouwbaar lijkt is oplettendheid aangewezen.

Als je de vraagt krijgt of je een programma wil uitvoeren die je niet zelf geopend hebt, antwoord dan altijd *Nee*.

Bijlages met een .exe- of .zip-extensie vragen altijd om oplettendheid!

Back-ups

Als je back-ups neemt van je bestanden, probeer dit altijd te doen op een *offline medium*. Dit kan bijv. een harde schijf zijn die je enkel connecteert met je computer als je een back-up wil maken en daarna meteen terug uit de computer haalt. Zo kan het virus deze bestanden niet bereiken.

Cloudopslag is niet beschermd tegen het cryptovirus. Als je OneDrive, Stack, Dropbox, … gebruikt, zorg dan ook nog voor een andere back-upoplossing. Als er een versiebeheer beschikbaar is kun je hier eventueel wel op terugvallen.

En misschien wel de belangrijkste tip…

Gebruik je gezond verstand!