Ransomware

How to protect and respond v.1

CERT.be

TLP: WHITE

15 maart 2017

CERT.be
The Federal Cyber Emergency Team

CENTRE FOR
CYBER SECURITY
BELGIUM

Inhoud

1 RANSOMWARE

Introductie

Ransomware is de benaming voor kwaadaardige software (malware) die computergebruikers probeert af te persen. Hiervoor blokkeert ransomware de toegang tot een informaticasysteem of versleutelt het de gegevens zodat ze onbruikbaar worden. Het slachtoffer verneemt via een boodschap op het scherm dat de toestand opnieuw genormaliseerd zal worden na het betalen van losgeld (ransom).

In de meeste gevallen kan het slachtoffer het losgeld uitsluitend betalen met cryptovaluta; een digitale munteenheid die wordt gebruikt als alternatief betalingssysteem. Voorbeelden van cryptovaluta zijn Bitcoin en Litecoin.

Ransomware kan opgedeeld worden in twee grote categorieën: ransomware die het informaticasysteem gijzelt en ransomware die de bestanden op het informaticasysteem versleutelt:

Locker — De toegang tot het informaticasysteem wordt geblokkeerd. Het slachtoffer is niet meer in staat om het informaticasysteem te gebruiken zolang het losgeld niet betaald is.

Cryptor — Een Cryptor, ook wel gekend onder de naam cryptoware, versleutelt de bestanden op het informatica- en netwerksysteem met geavanceerde versleutelingsalgoritmen. Meer geavanceerde vormen van ransomware beschikken over technologie om, naast het lokale informaticasysteem, ook netwerkschijven, databases, back-ups, gegevens in de cloud en USB-sticks te versleutelen.

---

bitcoin

Ransomware blokkeert de toegang tot een informaticasysteem of versleutelt de gegevens zodat ze onbruikbaar worden. De toestand wordt opnieuw genormaliseerd na het betalen van losgeld (ransom), in de meeste gevallen uitsluitend te betalen met cryptovaluta zoals bijvoorbeeld Bitcoins.

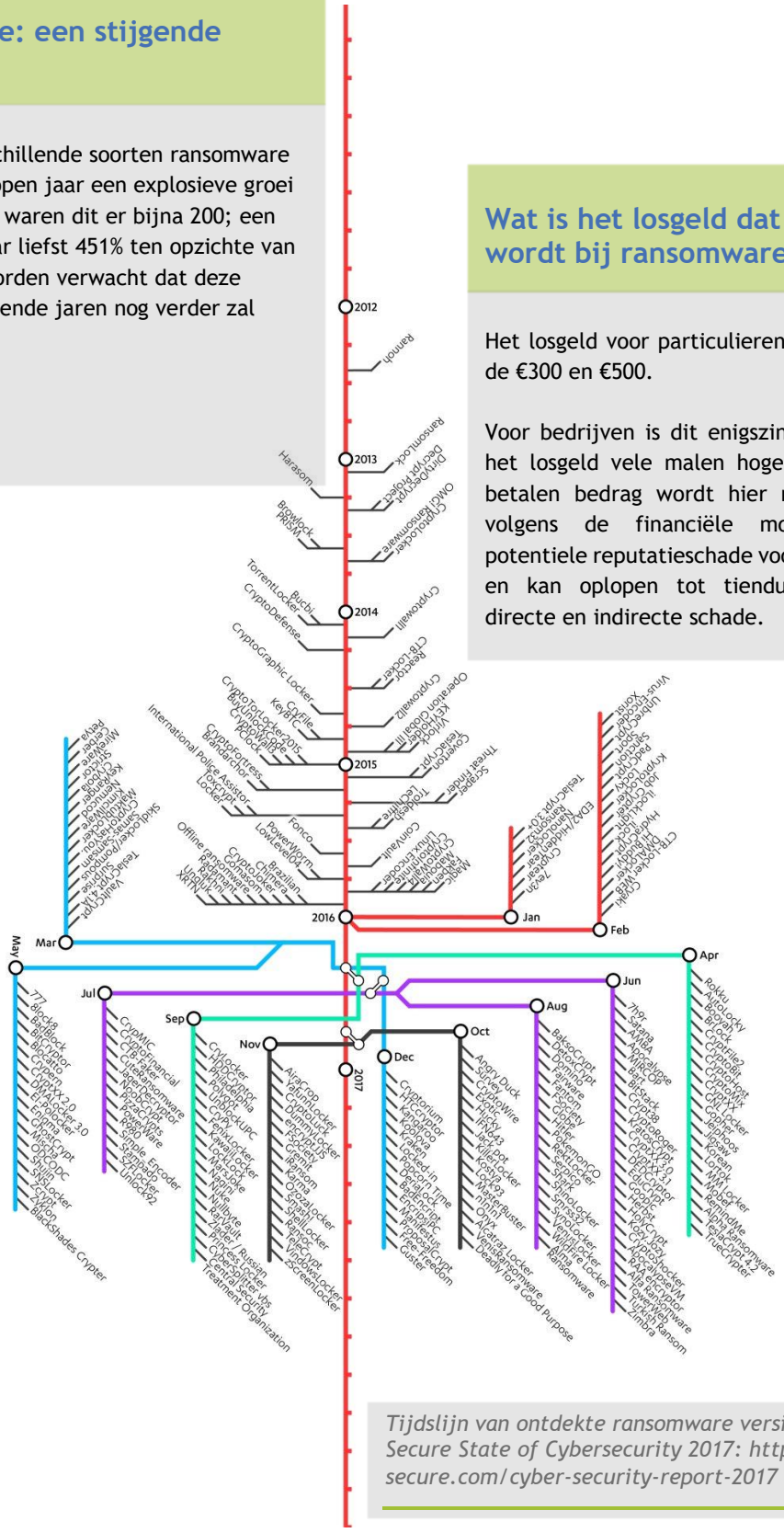
Ransomware: een stijgende dreiging

Het aantal verschillende soorten ransomware heeft het afgelopen jaar een explosieve groei gekend. In 2016 waren dit er bijna 200; een stijging van maar liefst 451% ten opzichte van 2015! Er mag worden verwacht dat deze dreiging de komende jaren nog verder zal stijgen.

Wat is het losgeld dat gevraagd wordt bij ransomware?

Het losgeld voor particulieren ligt vaak tussen de €300 en €500.

Voor bedrijven is dit enigszins anders en kan het losgeld vele malen hoger liggen. Het te betalen bedrag wordt hier meestal bepaald volgens de financiële mogelijkheden of potentiele reputatieschade voor het slachtoffer en kan oplopen tot tienduizenden euro's, directe en indirecte schade.



Tijdslijn van ontdekte ransomware versies. Bron F-Secure State of Cybersecurity 2017: http://www.f-secure.com/cyber-security-report-2017

Naast de directe kost voor bedrijven, namelijk het gevraagde losgeld, hoort men ook nog rekening te houden met andere kosten zoals geen of een beperkte toegang tot het informaticasysteem, verlies van inkomsten, de kost om het IT-systeem te herstellen, reputatieschade en de mogelijke diefstal van intellectuele eigendom.

De gebruikte ransomware methoden worden technisch steeds complexer, kennen een beter georganiseerde aanpak en gebruiken steeds betere versleutelingsalgoritmen.

Cybercriminelen ondernemen ook steeds vaker gerichte aanvallen wat een toenemend gevaar impliceert voor Belgische particulieren en ondernemingen.

Kleine of middelgrote ondernemingen zijn voor cybercriminelen een interessant doelwit omdat ze vaak minder geld kunnen besteden aan beveiliging, maar toch over voldoende financiële middelen beschikken om losgeld te kunnen betalen.

Hoe wordt een informaticasysteem geïnfecteerd

Cybercriminelen worden steeds creatiever in hun aanvalstechnieken. De onderstaande lijst is daarom zeker niet volledig maar is wel een goede indicatie:

(Spear) Phishing: Het slachtoffer ontvangt een e-mail met een geïnfecteerde bijlage of een link naar een geïnfecteerde webpagina. Het slachtoffer wordt gevraagd de geïnfecteerde bijlage te openen of naar de website te surfen. Veel slachtoffers downloaden en installeren op deze manier zelf de ransomware zonder zich daar echt bewust van te zijn. Het is voor gebruikers van een informaticasysteem belangrijk om kwaadaardige e-mails te herkennen en deze bij ontvangst te verwijderen.

Geïnfecteerde Webpagina: Het bezoeken van een geïnfecteerde webpagina kan resulteren in het downloaden en installeren van ransomware. Een up-to-date antivirus pakket kan gebruikers hiertegen beschermen.

Hoe gebeurt een cryptoware infectie

1. Het informaticasysteem van het slachtoffer wordt geïnfecteerd met cryptoware, meestal via een e-mail of een programma dat door de eindgebruiker geopend of geïnstalleerd wordt.

2. De cryptoware versleutelt de bestanden op het informatica- en netwerksysteem.

3. Op het scherm verschijnt de melding dat de gebruiker slachtoffer is van een cryptoware-infectie gevolgd door een uitleg over hoe het slachtoffer de criminelen geld kan overmaken.

   Het slachtoffer krijgt meestal tussen 24 en 72 uur de tijd om het losgeld te betalen. Indien de betaling niet binnen de maximale periode wordt uitgevoerd, kan de prijs van het losgeld stijgen of wordt de (digitale) sleutel, noodzakelijk voor het ontcijferen van de bestanden, voorgoed verwijderd.

2 PREVENTIE

Het risico op besmetting in een organisatie kan worden beperkt door enkele preventieve en meestal zeer eenvoudige maatregelen te nemen zoals:

Basis

Informeer gebruikers over de gevaren van ransomware en hoe ze zelf verschillende besmettingsmogelijkheden kunnen herkennen.

- Breng gebruikers op de hoogte van (spear) phishing technieken en hoe deze ermee moeten omgaan.
- Wees voorzichtig met e-mails van onbekende afzenders. Zeker wanneer deze onverwacht worden ontvangen en wanneer er onzekerheid is over de inhoud van een toegevoegde bijlage.
- Controleer steeds de correctheid van het e-mailadres van de afzender. Vaak worden valse e-mailaccounts gebruikt die erg goed op bestaande accounts lijken: gebruiker@yahoo.com is niet hetzelfde als gebruiker@yahoe.com.
- Let op het taalgebruik van de ontvangen e-mail. Vaak bevatten deze taalfouten of zijn ze in een andere dan de te verwachten taal opgesteld.
- Tips om phishing te herkennen kunnen teruggevonden worden op de website van Safe on Web[1].

Maak een back-up van alle gegevens.

- Belangrijk is dat het back-up systeem slechts tijdelijk verbonden is met het informaticasysteem. Nieuwe vormen van ransomware versleutelen eveneens back-ups en gegevens in de cloud. Wanneer een back-up toestel niet verbonden is met een besmette computer kan deze ook niet versleuteld worden door de ransomware.
- Wees zeker dat de kwaadaardige software niet aanwezig is op de back-up zelf.
- Test regelmatig het terugplaatsen van de back-up.

Update alle software steeds zo spoedig mogelijk om te voorkomen dat cybercriminelen misbruik kunnen maken van software kwetsbaarheden in het informaticasysteem.

Gebruik antivirus software om een extra beschermingslaag toe te voegen aan het informaticasysteem.

> **Preventie** is de beste strategie om zichzelf te beschermen tegen de gevaren van ransomware.

Geavanceerd:

Stel een lijst van vertrouwde programma's in om te voorkomen dat de gebruiker van een informaticasysteem ongewenste programma's uitvoert. Hiervoor kan de applicatie “AppLocker” van Microsoft gebruikt worden.

Pas de macro instellingen van Microsoft Office aan om te voorkomen dat een onbetrouwbare programmacode uitgevoerd wordt.

Gebruik het account met administrator rechten enkel wanneer het nodig is, bijvoorbeeld om een applicatie te installeren. Indien de administrator rechten niet nodig zijn tijdens een werksessie, werk dan met een account zonder administrator rechten.

Pas de browserinstellingen aan om Flash, Java, advertenties en andere ongewenste toepassingen te blokkeren.

[1] https://www.safeonweb.be/nl/tips/phishing-herkennen

Meer preventieve maatregelen kan je vinden op: http://www.thewindowsclub.com/prevent-ransomware-windows

3 SLACHTOFFER VAN RANSOMWARE?

Hoe kan men een informaticasysteem herstellen

Eenmaal ransomware de bestanden versleuteld heeft is de meest betrouwbare oplossing een back-up terug te plaatsen en niet over te gaan tot de betaling van het losgeld.

Het is noodzakelijk het getroffen systeem, indien mogelijk, los te koppelen van het netwerk om verdere verspreiding van de ransomware te vermijden.

Indien het niet mogelijk is om een back-up terug te plaatsen, is het aan te raden om na te gaan of er een decryptietool beschikbaar is. Dit kan bijvoorbeeld nagegaan worden op de website van het No More Ransom project[2], een initiatief van politiediensten en de private sector.

Voor vele ransomware versies is er momenteel (nog) geen oplossing beschikbaar. In dit geval krijgen de slachtoffers de raad om de versleutelde bestanden bij te houden omdat de website, nomoreransom.org, op regelmatige basis wordt aangevuld met nieuwe decryptietools. Wat vandaag nog niet kan worden gedecrypteerd, is morgen misschien wel mogelijk.

Wat te doen in geval van een ransomware infectie?

1. Haal het geïnfecteerde informaticasysteem van het informaticanetwerk.
2. Rapporteer de besmetting aan de lokale politie en CERT.be.
3. Verwijder de ransomware van het geïnfecteerde informaticasysteem. Indien nodig wordt het systeem volledig opnieuw geïnstalleerd.
4. Plaats de back-up terug op het informaticasysteem.

[2] https://www.nomoreransom.org

Betalingen

Het betalen van losgeld wordt meestal afgeraden. Er is geen enkele garantie dat na betaling de versleutelde bestanden opnieuw toegankelijk worden. De betaling gebeurt immers aan (onbetrouwbare) cybercriminelen. Betalen impliceert tevens het steunen van een criminele organisatie waardoor cybercriminelen een drijfveer hebben om hun illegale activiteiten verder te zetten. Na een eventuele betaling is het ook nooit zeker dat het informaticasysteem terug veilig is.

Slachtoffers die het losgeld betaald hebben geven aan dat ze na de initiële betaling gevraagd worden om opnieuw een hoger bedrag over te maken. In sommige gevallen worden de slachtoffers na verloop van tijd opnieuw slachtoffer van dezelfde ransomware.

Rapporteer een besmetting

Een slachtoffer van ransomware kan steeds aangifte doen bij de lokale politie en ook het incident melden bij CERT.be. Bij aangifte of melding is het aan te raden volgende informatie te verschaffen: soort gegevensdrager, besturingssysteem, infectiewijze, naam van de ransomware, betalingswijze en indien mogelijk screenshots van het geïnfecteerde informaticasysteem. Aangifte en / of melding van het incident biedt niet noodzakelijk een oplossing voor de ransomware infectie maar het helpt in de (internationale) strijd tegen deze vorm van cybercriminaliteit.

4 CONTACT INFORMATIE

The Federal Cyber Emergency Team
Wetstraat 16
1000 Brussel
M: info@cert.be

Het Centrum Voor Cybersecurity België
Wetstraat 16
1000 Brussel
Tel: +32 (0) 2 501 05 63
M: info@ccb.belgium.be