# Ransomware is here to stay: bescherm jezelf

.

Date: Juli 2017
Version: 1.0

Eshgro BV • Bereklauw 7 • 5831 PE Boxmeer • Postbus 61, 5830 AB Boxmeer • +31(0)485 - 47 61 93 • info@eshgro.com • www.eshgro.com
KVK 08191713 | BTW NL8205.54.820.B.01 | IBAN NL09 RABO 0113 9963 30 | BIC RABONL2U

Wat is ransomware nu eigenlijk en waarom kan het zo gevaarlijk zijn? In dit artikel geven we uitleg wat het is, wat wij doen om je te beschermen en wat je zelf kan doen om te voorkomen dat je systemen besmet raken.

## Inhoud

# Wat is ransomware

Traditioneel is ransomware een gerichte aanval. Dit betekent dat het slachtoffer vooraf is geselecteerd en de aanval specifiek is gericht op die individuele organisatie of dat netwerk. Kritische bronnen, zoals gegevens, worden gecodeerd en losgeld wordt gevraagd om een sleutel te krijgen voor het ontgrendelen van die gegevens.

# Een nieuwe generatie ransomware

In het voorjaar van 2017 kwam er een nieuwe variant: WannaCry. Deze variant voegde een nieuw element toe  aan ransomware bedreigingen. De makers combineerde voor het eerst de ransomware met een worm om de verspreiding te versnellen en de aanval uit te breiden. In de zomer van 2017 kwam er een volgende variant, die weer een element toevoegde: het herschrijven van het Master Boot Record (MBR)[1]. Dit versleutelde het besturingssysteem om extra kracht bij de bedreiging te zetten. De gevolgen van het niet voldoen aan het vereiste losgeld vergrootte daarmee de verliezen van niet alleen de bestanden, maar tot het verlies van het gehele systeem. Petya was geboren.

Deze vorm van malware[2] is iets waar de securityindustrie naar verwijst als een Ransomworm[3]. Deze varianten maken gebruik van een brede benadering en richten zich op elk apparaat dat ze kunnen vinden en waar de bijgevoegde worm gebruik van kan maken. De toevoeging van het wormgedeelte in deze nieuwe variant malware én de versleuteling van het besturingssysteem maakt van Petya een nieuwe generatie ransomware[4]. Het leverde wereldwijd veel ophef op. Deze ransomware en zijn varianten, GoldenEye, ExPetr en NotPetya, hebben veel impact op een scala van organisaties en vaak gericht op kritieke infrastructuren als energie- bank- en transportsystemen.

# Hoe werkt Petya?

Petya is ontworpen om te profiteren van zwakheden in Microsoft systemen. Het richt zich op dezelfde beveiligingslekken, die werden gebruikt tijdens de WannaCry aanval van mei 2017. Kaspersky Lab, een Russisch antivirusbedrijf, onthulde toen dat meer dan 98% van alle gedocumenteerde WannaCry-infecties plaatsvonden op computers die gebruik maakten van Windows 7. Op 60% daarvan draaiden de 64-bit editie.

Eén onderzoeker meldde dat de aanval begon met de verspreiding van een Excel document dat een bekende Microsoft Office zwakheid uitbuit, maar trok dat later terug. Later werd gemeld dat Petya zich verspreidt door de EternalBlue-exploit[5] en WMIC[6] . Het wormachtige gedrag dat deze malware laat zien wordt veroorzaakt door te zoeken naar SMB-servers[7]. Eén enkele besmette machine met de juiste rechten en toegang op het netwerk kan de infectie via WMI of PsExec onder alle andere computers verspreiden.

Zodra een kwetsbaar apparaat is gevonden, start Petya met de infectiecyclus. De malware wacht 10 tot 60 minuten met het herstarten van het systeem, waarna het de Master Boot Record overschrijft met de losgeldmelding. Het geeft de gebruiker dan een scherm, waarin staat: "Uw bestanden zijn niet meer toegankelijk, omdat ze gecodeerd zijn" en vraagt ongeveer $ 300 losgeld in de Bitcoin digitale valuta. De gebruiker wordt gevraagd te betalen voor een key die de bestanden en het systeem weer ontsleutelt. Gedreigd wordt dat uitzetten van de computer tot een volledig verlies van het systeem zal leiden.

Een andere antivirus softwareleverancier Bitdefender meldde dat de variant GoldenEye, net als Petya, de gehele harde schijf versleutelt en vervolgens de toegang tot de computer blokkeert. GoldenEye bood echter geen oplossing om de bestanden te ontsleutelen.

Later bleek ook bij Petya uiteindelijk losgeld niet het hoofddoel van de aanval te zijn. Hoewel op geïnfecteerde computers een melding wordt getoond, waarin om losgeld wordt gevraagd, lijkt het onwaarschijnlijk te zijn dat geld verdienen het hoofddoel van de verspreiders van Petya is geweest. Uit een analyse van de code bleek dat er helemaal geen bestanden worden versleuteld. In plaats daarvan wist Petya simpelweg delen van de schijf, waardoor hij onherstelbaar wordt beschadigd. Ook zei de aanvaller te willen communiceren via een e-mailadres, dat binnen enkele uren geblokkeerd werd. Daardoor is het ontgrendelen van bestanden na betaling van het losgeld überhaupt onmogelijk geworden.

Dit blokkeren van de harde schijf is een andere tactiek dan een aftelklok of het geleidelijk verwijderen van gegevensbestanden, waar andere versies van ransomware gebruik van maken.

Vanuit financieel oogpunt was WannaCry niet erg succesvol, omdat het voor zijn ontwikkelaars zeer weinig inkomsten genereerde. Dit kwam doordat onderzoekers snel een kill switch vonden, die de aanval uitschakelde. Petya is veel verfijnder, maar leek meer gericht op het creëren van chaos dan geld.

## Alleen patchen is niet voldoende

Vreemd genoeg gebruikte Petya, naast de Microsoft Office kwetsbaarheden, dezelfde aanvalsmethode als WannaCry. Daarbij werden de identieke Microsoft-kwetsbaarheden, die eerder door de Shadow Brokers (een groep hackers) werd ontdekt, gebruikt. Aangezien aanvullende aanvalstechnieken in deze uitbraak werden gebruikt, is patchen[8] alleen onvoldoende om deze infectie helemaal te stoppen. Dit betekent dat patchen gecombineerd moet worden met de juiste beveiligingsmaatregelen. Onze klanten werden tegen deze aanvallen beschermd, doordat ze werden gedetecteerd en geblokkeerd door onze IPS[9]- en NGFW[10]-oplossingen. Daarnaast hebben we binnen enkele uren na de ontdekking een nieuwe antivirushandtekening uitgereikt aan de firewalls om de eerste lijn van defensie te verbeteren.

# Ransomware blijft een risico

Naast deze nieuwe generatie ransomware is er een nieuwe ontwikkeling: ransomware op onlinediensten. Dit kan verschillende vormen aannemen. Er wordt bijvoorbeeld een Denial Of Service aanval (DDoS)[11] aanval op de onlinedienst gericht, waardoor deze niet beschikbaar is voor klanten en gebruikers. Vervolgens wordt losgeld geëist om de aanval uit te zetten.

## Wormen in IoT apparaten

Mirai, dat in augustus en september 2016 werd gelanceerd, was de grootste aanval op onlinediensten in de geschiedenis, deels omdat er honderdduizenden IoT-apparaten[12] werden gebruikt. In april 2017 heeft een nieuw Mirai-achtig IoT-botnet[13] genaamd Hajime gebruik gemaakt van IoT-apparaten om organisaties met een overweldigende DDoS-aanval plat te leggen. Hajime bleek een white hat bot[14] te zijn, die zich wel verspreidde, maar verder alleen een melding gaf over veiligheid en poorten sloot waar Mirai gebruik van maakte. Tot nu lijkt het dus op een actie om misbruik te voorkomen en IoT-apparaten beter te beveiligen. Maar ondertussen staat er een groot botnet netwerk klaar dat onder controle is van onbekenden, die dit netwerk alsnog voor allerlei aanvallen kan inzetten. Nieuwe botnets als deze bouwen voort op de code van Mirai, omdat deze code als open-source[15] gepubliceerd wordt op hacker fora. Hajime is een volgende generatie IoT-exploitatie. Het is cross platform en bevat een toolkit met geautomatiseerde taken, waaronder dynamische wachtwoordenlijsten die het updatable maken. Deze variant probeert het menselijk gedrag na te bootsen om minder op te vallen, zodat het onder de detectieradar kan blijven.

## Ransomware als dienst

Een interessante twist is de ontwikkeling van ransomware als een dienst (RaaS). Hiermee kunnen criminelen met minder technische kennis de ransomware-technologie gebruiken om hun eigen afpersingsbedrijf te starten in ruil voor winstdeling met de ontwikkelaars. Onlangs is de allereerste RaaS ransomware gericht op MacOS waargenomen, die tot nu toe grotendeels onder de radar van aanvallers is gebleven. Aangezien het profiel van Mac-gebruikers vaak zowel technici als bedrijfsleiders omvat, moet de komst van aanvallen die gericht zijn op deze apparaten niet verrassen.

De opkomst van ransomware, samen met een verrassende reeks varianten in 2016 en 2017, is dramatisch geweest. We volgen nu verschillende typen ransomware om op tijd en doeltreffend te kunnen handelen en onze klanten te beschermen voor nieuwe aanvallen en varianten van ransomware.

# Advies uit de securityindustrie

Uit de securityindustrie komen de volgende adviezen. Uiteraard gelden de meeste adviezen niet alleen voor het specifieke probleem van ransomware, maar zijn algemeen toepasbaar:

- Zorg voor een goede up-to-date IPS-systeem.
- Zorg voor een goede up-to-date antivirus-systeem.
- Zorg ervoor dat systemen voorzien zijn van de laatste (security) patches.
- Blokkeer botnet verkeer en de TOR[16] browser

# Wat doet Eshgro?

Wij bieden meerdere lagen van bescherming aan de online-desktop omgeving van onze klanten. Dat betekent dat wij:

- beschikken over een up-to-date IPS-systeem, dat bescherming biedt tegen alle bekende aanvallen. Dit wordt dynamisch geüpdatet, wanneer er nieuwe aanvallen bekend zijn.
- beschikken over een antivirus-systeem dat op de firewalls bescherming biedt tegen alle bekende malware. Dit wordt dynamisch geüpdatet, wanneer er nieuwe malwarevariaties bekend zijn.
- patchen de door ons beheerde systemen.
- blokkeren botnet en TOR-verkeer.
- blijven ons continue verbeteren, door nieuw verschafte inzichten in securitybeleid actief door te voeren.

# Wat kan ik zelf doen tegen ransomware?

Je kunt zelf ook zorgen voor het verhogen van jouw security en daarmee de kans op besmetting verkleinen. Wij beschermen zoveel mogelijk jouw online-desktopomgeving, maar hierbuiten heb je misschien ook een lokale infrastructuur en PC's die niet door ons worden beheerd.
Denk hierbij aan PC's en laptops, een lokale NAS, maar ook jouw internetverbinding met een bijbehorende firewall. Dit geldt op kantoor, maar ook bij jouw thuis. Ook voor al deze apparatuur geldt:

- Zorg voor een goede en up-to-date antivirus op PC's en eventueel IPS (op de firewall).
- Zorg voor up-to-date patching van alle systemen.
- De juiste firewall rules: zet niet alles open, maar alleen wat nodig is om te kunnen werken.

Tot slot, maar misschien nog wel het belangrijkste: zorg voor een goede 'awareness' bij alle medewerkers. De meeste malware komt op de systemen door op een link te klikken of een bijlage in een e-mail te openen. Zorg dat er geen zip-bestanden worden geopend en vraag medewerkers grote bestanden te ontvangen via services als DossierBox.

# Woordenlijst

1. Master Boot Record (MBR): De MBR is de allereerste sector van een harde schijf of een ander digitaal opslagmedium waarmee een pc opgestart kan worden.
2. Malware / Virussen: Een computervirus is een vorm van schadelijke software (malware). In ernstige gevallen kunnen virussen binnenin de computer schade aanrichten, bijvoorbeeld door het wissen en verspreiden van gevoelige gegevens. In zeer ernstige gevallen kan de gebruiker zelfs de totale controle over de computer verliezen.
3. Worm: Een computerworm is een zichzelf vermenigvuldigend computerprogramma. Via een netwerk worden kopieën doorgestuurd zonder tussenkomst van een gebruiker.
4. Randsomware: Letterlijk vertaald betekent ransom: losgeld. Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te `bevrijden`.
5. EternalBlue: Het zogenoemde EternalBlue-lek werd oorspronkelijk gevonden door de Amerikaanse inlichtingendienst NSA en onder de pet gehouden. Nadat een groep hackers de hacksoftware van de NSA wist te stelen, maakte de NSA melding van het lek bij Microsoft. In een recente update is het probleem verholpen, maar computers die de update nog niet hebben ontvangen zijn nog kwetsbaar.
6. WMIC: WMIC (Windows Management Instrumentation Command-line) breidt WMI uit voor gebruik vanuit meerdere commando-interfaces en door batch scripts.
7. SMB-servers: netwerkschijven op fileservers, op een Netwerk of USB-disk.
8. Patchen: het updaten van software en besturingssystemen.
9. IPS: Dit staat voor Intrusion Prevention System. Het betreft een systeem dat ongeautoriseerde toegang tot een computernetwerk of computer kan blokkeren.
10. NGFW: Een volgende generatie firewall (NextGenFirewall) is een geïntegreerd netwerksecurityplatform dat deel uitmaakt van de derde generatie firewalltechnologie. Hierbij wordt een traditionele firewall gecombineerd met andere functies voor het filteren van netwerkverkeerr, zoals een firewall voor toepassingen met behulp van in-line deep packet inspectie (DPI ) en een inbraakpreventiesysteem (IPS).
11. DDoS: (Distributed) Denial-of-service-aanvallen (dos-aanvallen) zijn pogingen om een computer, computernetwerk of dienst onbeschikbaar te maken voor de bedoelde gebruiker.
12. IoT: Internet of Things, denk b.v. aan slimme thermostaten, zonnepanelen of Webcamera's.
13. Botnet: Botnet is een collectie van softwarerobots of bots, die automatisch en zelfstandig opereren. Botnets worden vaak gebruikt door malware en ransomware voor updates en opdrachten. Maar ook voor verspreiden van spam of distributed-computing.
14. White hat: dit beschrijft een hacker (of cracker), die een beveiligingszwakheid in een computersysteem of netwerk identificeert, maar in plaats daar misbruik van te maken, stelt het de zwakte bloot op een manier waarmee de eigenaars van het systeem de oplossing kunnen maken, voordat het door anderen kan worden gebruikt (zoals black hat hackers).
15. Open source: computerprogrammatuur waarvan de broncode wordt vrijgegeven. Dit geeft gebruikers de mogelijkheid om de software te bestuderen, aan te passen en te verbeteren.
16. TOR: Tor (afgeleid van de oorspronkelijke projectnaam The Onion Router) is een open netwerk voor anonieme communicatie, gebaseerd op een techniek genaamd onion routing. Onion routing is een technologie ontwikkeld in 1995 door het United States Naval Research Laboratory. Het netwerk is een van de systemen die Edward

Snowden gebruikte om geclassificeerde documenten openbaar te maken. Het Tor-netwerk is bedoeld om te voorkomen dat anderen door analyse van het berichtenverkeer kunnen achterhalen wat de herkomst en bestemming van berichten is. Tegenwoordig wordt dit vaak gebruikt voor illegale praktijken op het internet.