Ransomware

Bescherming en preventie

CERT.be

TLP: WHITE

10 september 2019

CERT.be
The Federal Cyber Emergency Team

CENTRE FOR
CYBER SECURITY
BELGIUM

Inhoudstafel

1 RANSOMWARE

1.1 Wat is ransomware ?

Ransomware is kwaadaardige software (malware) die de gegevens van de gebruikers versleutelt met de bedoeling om hun gegevens later terug te sturen in ruil voor losgeld. In extreme gevallen blokkeert de ransomware de toegang tot het informaticasysteem door ook gegevens te versleutelen die essentieel zijn voor de goede werking van het systeem.

Ransomware is geen nieuw fenomeen, maar de dreiging is de laatste jaren exponentieel gegroeid.

Daarnaast is de werkwijze van cybercriminelen veranderd. Criminelen zijn van doelwit veranderd: ze zijn overgestapt van een groot aantal geïnfecteerde gebruikers met weinig losgeld naar minder doelwitten die wel hoge sommen losgeld kunnen betalen.

Gezien het destructieve karakter van ransomware-software is het vaak moeilijk om de logbestanden te herstellen en te achterhalen wat er werkelijk gebeurd is. Hackers kunnen intellectueel eigendom hebben gestolen maar ook ransomware hebben ingezet om hun echte bedoelingen te verbergen.

Er zijn verschillende categorieën van ransomware:

Locker — de toegang tot het informaticasysteem is geblokkeerd. Het slachtoffer kan het informaticasysteem niet meer gebruiken totdat hij of zij het losgeld heeft betaald.

Cryptor — een cryptor, ook bekend als cryptoware, versleutelt de bestanden op het systeem en het informaticanetwerk met behulp van gesofisticeerde versleutelingsalgoritmen. Meer geavanceerde soorten ransomware kunnen bovenop het lokale informaticasysteem ook de harde schijven, databanken, back-ups, cloudgegevens en USB-sleutels versleutelen.

bitcoin

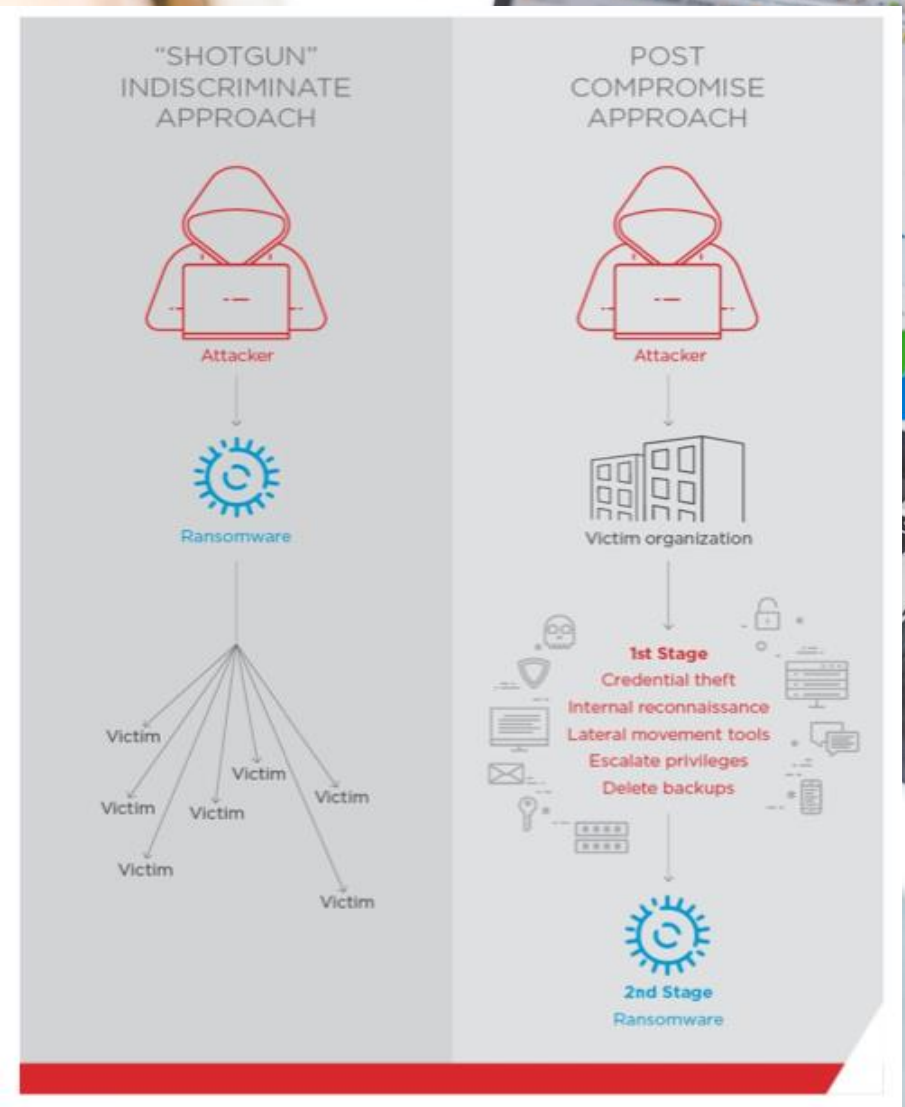
Ransomware blokkeert de toegang tot het informaticasysteem of versleutelt de gegevens, waardoor deze onbruikbaar worden. De situatie zal zogezegd weer normaal worden na betaling van het losgeld (ransom). In de meeste gevallen kan het slachtoffer het losgeld alleen in cryptovaluta zoals Bitcoin betalen.

1.2 Hoeveel bedraagt het losgeld ?

Er is een groot verschil tussen een opportunistische ransomware-aanval en een gerichte aanval. Ook zal men aan een individu doorgaans minder losgeld vragen dan aan een bedrijf.

Bij een opportunistische aanval wordt geprobeerd om een aanzienlijk aantal slachtoffers te besmetten en zal meestal het equivalent van een paar honderd of een paar duizend euro worden geëist.

Bij een gerichte en zorgvuldig voorbereide aanval door een groep cybercriminelen kan het losgeld tot in de honderdduizenden euro's oplopen. We hebben de laatste tijd een aanzienlijke toename van dergelijke aanvallen gezien[1].



[1] Fireye – Case Studies : Ransomwaredeployed post-compromise

1.3 Is ransomware een toenemende dreiging?

CERT.be heeft een stijgende trend waargenomen voor alles wat ransomware betreft. Cybercriminelen gebruiken ransomware om grote sommen geld af te persen van grote bedrijven, die hun favoriete nieuwe doelwitten zijn. Ook al houden de aanvallen op dergelijke doelen een risico op blootstelling in, de winst is toch groter dan de risico's.

Mensen met slechte bedoelingen die eerder geïnteresseerd zijn in gevoelige informatie gebruiken ook ransomware om hun sporen uit te wissen. In sommige gevallen is het zelfs niet meer mogelijk om de gegevens te herstellen, aangezien de ransomware eigenlijk het software-equivalent van een wiper (harde-schijfwisser) is.

1.4. Wat zijn de infectievectoren ?

Cybercriminelen worden steeds creatiever in hun aanvalstechnieken. De volgende lijst is dus niet exhaustief, maar geeft een goede indicatie:

1.4.1 Oorspronkelijke vectoren

(Spear) Phishing: het slachtoffer krijgt 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 een website te surfen. Veel slachtoffers downloaden en installeren de ransomware zonder het te beseffen. Het is belangrijk dat de gebruikers van een informaticasysteem kwaadaardige e-mails herkennen en ze bij ontvangst onmiddellijk verwijderen.

Geïnfecteerde webpagina: het raadplegen van een geïnfecteerde webpagina kan ertoe leiden dat er ransomware wordt gedownload en geïnstalleerd. Up-to-date antivirussoftware en antiransomware software kan de gebruiker tegen deze dreiging beschermen door de activiteit van het proces dat verantwoordelijk is voor het coderen van de gegevens te detecteren.

1.4.2 Nieuwe trends

Cybercriminelen hebben een sterke interesse ontwikkeld in de snelle winst die het fenomeen ransomware oplevert.

Sommige groepen cybercriminelen hebben zich gespecialiseerd in het verkrijgen van toegang tot netwerken om deze vervolgens te verkopen aan andere groepen die op hun beurt gespecialiseerd zijn in het exploiteren van toegangen om intellectueel eigendom te stelen en/of voor andere lucratieve doeleinden, waaronder het installeren van ransomware.

We zien vaak dat dat deze groepen misbruik maken van **een Remote Desktop Protocol (RDP)-toegang**, die ze ofwel door **brute-force** hebben verkregen ofwel **gekocht hebben van een derde partij**, die het doelwit eerder heeft gecompromitteerd.

We houden uiteraard altijd rekening met de gebruikelijke vectoren zoals phishing. Het voordeel van de toegang via RDP is vooral de discretie die deze biedt: het is gemakkelijker om op te gaan in het netwerkgebruik door gebruik te maken van de bestaande credentials.

2 PREVENTIE

Er bestaat geen wondermiddel dat bescherming biedt tegen ransomware. Aangezien het doel van criminele groepen die ransomware verspreiden financieel gewin is, is het aan te raden om uw netwerk te beschermen met een in depth-verdedigingssysteem, zodat hackers meer moeite hebben met het uitvoeren van hun ransomware-aanval.

Hackers zullen de potentiële winst analyseren en opgeven als de aanval waarschijnlijk meer tijd in beslag zal nemen in verhouding tot het losgeld dat ze kunnen krijgen.

Daarnaast zijn cyberverdedigingen tegen ransomware ook doeltreffend tegen andere dreigingen.

2.1 Back-ups

- Back-ups zijn essentieel om de bestanden te herstellen na een incident met ransomware. Een back-up maken van alle vitale bestanden en systemen is een van de beste manieren om u tegen ransomware te verdedigen. Als u moet beslissen over het aantal potentieel haalbare back-ups, evalueer dan welke informatie het meest kritiek is voor uw bedrijf.
- Alle gegevens kunnen worden hersteld tot het moment van de laatste back-up. De back-upbestanden moeten worden getest om er zeker van te zijn dat de gegevens volledig en niet-corrupt zijn. Deze analyse is essentieel!
- Pas de regel van drie toe: 2 verschillende dragers op 1 locatie en 1 drager op een andere locatie. Een van deze back-up moet de "offline" kopie zijn.
- Beperk het aantal gebruikers dat toegang heeft tot uw back-up. Hoe minder, hoe beter.
- De logs moeten ook een integraal onderdeel zijn van uw back-upstrategie (SIEM etc.).

2.2 Updates

- Hoewel het uitvoeren van updates op uw systemen een aanval niet voorkomt, zal dit het voor hackers toch aanzienlijk moeilijker maken om malware te verspreiden op basis van een recente kwetsbaarheid.

- De meeste software die door bedrijven wordt gebruikt, wordt regelmatig bijgewerkt door de maker van de software. Deze updates kunnen patches bevatten om de software beter te beschermen tegen nieuwe dreigingen.

- Elk bedrijf moet een medewerker aanwijzen om de software bij te werken. Door het aantal mensen dat betrokken is bij het updaten van het systeem te verminderen, wordt het aantal potentiële aanvalsvectoren voor cybercriminelen verminderd.

- De maandelijkse updates zijn een must en het is goed om een stapsgewijze aanpak (testfase en vervolgens ingebruikname) te implementeren.

- U moet ook over een inventaris van uw assets beschikken: een duidelijk overzicht van wat er op uw netwerk aanwezig is.

2.3 Bescherming van het Remote Desktop Protocol

- Evalueer of het nodig is om RDP open te hebben op de systemen en, zo ja, beperk de verbindingen dan tot specifieke en betrouwbare hosts.

- Zorg ervoor dat de cloudomgevingen voldoen aan de beste praktijken die door de cloudaanbieder zijn gedefinieerd. Zodra de configuratie van de cloudomgeving is voltooid, zorg er dan voor dat de RDP-poorten niet zijn ingeschakeld, tenzij dit noodzakelijk is voor professionele doeleinden.

- Plaats elk systeem met een open RDP-poort achter een firewall en vraag de gebruikers om een VPN te gebruiken via een firewall.

- Controleer regelmatig of de RDP 3389-poort niet open staat voor het publiek op het internet.

- Gebruik veilige wachtwoorden en implementeer een beleid voor accountvergrendeling om u te beschermen tegen brute-force-aanvallen.

2.4 Sensibiliseringsprocedures

- Neem het proces voor incident response door: u moet een volledig proces voor incident-response uitwerken dat ook omvat hoe infecties door ransomware worden beheerd. Dit proces moet ook beschrijven hoe incidenten worden geprioriteerd, geregistreerd, beheerd, gecorrigeerd, opgelost en, indien nodig, gerapporteerd aan een leidinggevende. Denk ook aan de externe communicatie.

- Stel een kwalitatief hoogstaand cybersecurity-opleidings- en sensibiliseringsprogramma op.

- Voer regelmatig phishingtests uit en sensibiliseer de medewerkers. Maak gebruikers bewust van het belang om niet op alles en nog wat te klikken en leer hen hoe ze spam- en phishingmails kunnen herkennen.
- Leid uw informaticapersoneel op een permanente basis op.

2.5 Actief toezicht

- Houd toezicht op de gecompromitteerde identificatiegegevens.
- Houd toezicht op de ongebruikelijke activiteiten in de Domain Name System (DNS)-logs.
- Verbeter de zichtbaarheid van de veiligheidsincidenten: implementeer een SIEM.
- Voer een intrusiedetectie/intrusiepreventiesysteem (“Intrusion Detection System/Intrusion Prevention System - IDS/IPS”) in.
- Herken het basisgedrag van het netwerk: weet wat normaal is voor uw netwerk.
- Zorg ervoor dat de gebruikerstoegangscontrole (“User Access Control” - UAC) is ingeschakeld op Windows.

2.6 Bescherming van het netwerk

- Segmenteer uw netwerk goed.

2.7 Beheer van de rechten

- Beperk de administratieve rechten en het delen ervan.
- Gebruik veilige, complexe wachtwoorden.
- Houd toezicht op de gecompromitteerde identificatiegegevens.
- Houd toezicht op de identificatiegegevens: elke werknemer, aannemer of persoon met toegang tot de systemen is een potentieel kwetsbaar punt voor mensen met slechte bedoelingen. Personeelswisselingen, gebrek aan wachtwoordupdates en ongepaste beperkingen zijn allemaal potentiële vectoren die een kwaadwillig persoon kan misbruiken om een informaticasysteem te compromitteren.
- Schakel het besturingssysteem in om de bestandsextensies weer te geven.
- Schakel automatisch afspelen ("AutoPlay") uit.

- Blokkeer de USB-opslag.
- Installeer advertentieblokkeringssoftware op de netwerkperimeter.
- Installeer een dreigingsinformatiesysteem.

2.8 Bescherming van e-mails

- Verbeter de veiligheid van de e-mails met DMARC, SPF en DKIM.

2.9 Bescherming van de toestellen van medewerkers

- Zorg ervoor dat de antivirussoftware en antiransomware software up-to-date zijn en dat alle functies zijn ingeschakeld.
- Schakel ActiveX in Office-bestanden uit.
- Uw pc moet zo geconfigureerd zijn dat uitvoerbare bestanden niet vanuit de volgende mappen kunnen worden geopend: Appdata, LocalAppData, Temp, ProgramData, Desktop. Voer testen uit vooraleer u in productie gaat.
- Installeer Windows AppLocker: Application Whitelist.
- Schakel de macro's in Office-bestanden uit.
- Installeer de laatste Windows-updates.

3 SLACHTOFFER VAN RANSOMWARE ?

3.1 Hoe een informaticasysteem herstellen ?

Zodra de ransomware de bestanden gecodeerd heeft, is de meest betrouwbare oplossing om ze te herstellen met behulp van een back-up en niet om het losgeld te betalen.

Indien mogelijk moet het geïnfecteerde systeem worden geïsoleerd van het netwerk om te vermijden dat de ransomware zich verder verspreidt.

Als het niet mogelijk is om de bestanden door middel van een back-up te herstellen, is het raadzaam om na te gaan of er een ontcijferingstool bestaat, bijvoorbeeld op de website van het "No More Ransom"[2]-project, een initiatief van de politiediensten en de privésector.

Momenteel bestaat er (nog) geen oplossing voor alle types ransomware. In dit geval wordt het slachtoffer geadviseerd om de versleutelde bestanden te bewaren, aangezien de website *nomoreransom.org* regelmatig wordt bijgewerkt met nieuwe ontcijferingstools. Wat vandaag niet ontcijferd kan worden, kan dat morgen misschien wel.

Wat moet je doen in geval van besmetting door ransomware?

1. Verwijder het geïnfecteerde informaticasysteem uit het computernetwerk.
2. Meld de infectie bij de lokale politie en CERT.be (cert@cert.be).
3. Verwijder de ransomware uit het geïnfecteerde computersysteem. Het systeem wordt indien nodig volledig opnieuw geïnstalleerd.
4. Herstel het computersysteem met behulp van de back-up.

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

3.2 Betalen of niet ?

Het wordt niet aanbevolen om het losgeld te betalen, vooral omdat dit geen oplossing voor het probleem garandeert.

De kans is ook groot dat er bij de ontcijfering tal van problemen opduiken. De ontcijferingssoftware die door de hackers wordt geleverd, heeft vaak veel minder aandacht gekregen dan de coderingssoftware waardoor de gegevens in het slechtste geval niet meer te herstellen zijn!

Als het losgeld wordt betaald, moedigt dit cybercriminelen bovendien aan om ransomware te gebruiken, aangezien het een winstgevende business is. Cybercriminelen zullen hun activiteiten bijgevolg voortzetten en nieuwe manieren zoeken om de systemen te exploiteren, met als gevolg meer infecties, meer slachtoffers en meer geld op hun rekeningen.

De slachtoffers die losgeld hebben betaald, hebben aangegeven dat er na deze eerste betaling een hoger bedrag van hen werd geëist. In sommige gevallen werden de slachtoffers na een tijdje opnieuw door dezelfde ransomware getroffen.

3.3 Hoe een infectie signaleren ?

Een slachtoffer van ransomware kan op elk moment een klacht indienen bij de lokale politie en het incident melden bij CERT.be via cert@cert.be. In geval van een melding of klacht wordt aanbevolen de volgende informatie te verstrekken: type gegevensdrager, besturingssysteem, besmettingswijze, naam van de ransomware, betaalmethode en, indien mogelijk, screenshots van het geïnfecteerde informaticasysteem. Het indienen van een klacht en/of het melden van het incident leidt niet altijd tot een oplossing voor de ransomware-infectie, maar draagt bij aan de (internationale) bestrijding van deze vorm van cybercriminaliteit.

4 CONTACT

The Federal Cyber Emergency Team
Rue de la Loi 16
1000 Bruxelles

Le Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles