Whitepaper

Ransomware

CYBERVEILIG NEDERLAND

Inhoudsopgave

Inleiding

De missie van Cyberveilig Nederland is om de weerbaarheid van Nederlandse organisaties te vergroten. Cybersecurity wordt nog vaak wordt gezien als een ‘ver van mijn bed show’, waar het management zich niet in hoeft te verdiepen. Een kostenpost in plaats van een investering. Cybercriminaliteit treft echter steeds meer organisaties en herstellen van een cyberincident is vele malen duurder dan vooraf investeren. Via een serie whitepapers willen we, gericht op de doelgroep CISO en security verantwoordelijke, bewustwording, inzicht én handelingsperspectief bieden voor veelvoorkomende schadelijke cyber-manifestaties. Dat doen we in samenwerking met het NCSC, de Nationale Politie, andere stakeholders en verschillende van onze leden met specifieke kennis en ervaring over dit onderwerp.

Ransomware of gijzelsoftware is op dit moment de meest voorkomende en meest lucratieve vorm van cybercrime wereldwijd. Aanvallen vinden op een continue basis plaats en de gevraagde losgelden lopen geregeld in miljoenen euro’s. Het afpersen van organisaties levert criminele groeperingen honderden miljoenen op. Het veroorzaakt bij de slachtoffers grote schade en werkt maatschappelijk ontwrichtend.

Met dit whitepaper willen we inzicht verschaffen zodat organisaties:

- meer bewustwording krijgen over deze vorm van aanvallen;
- zich er beter tegen beveiligen;
- snel en adequaat handelen wanneer ze slachtoffer zijn;
- aanknopingspunten hebben voor het opwerpen van barrières.

Dit whitepaper is bedoeld als top-level document. We beschrijven het fenomeen, de fases van de aanval, de actoren en geven een aanzet tot de acties die u kunt ondernemen om zich te wapenen tegen ransomware.

Volgende whitepapers zullen zich meer verdiepen in andere aspecten van ransomware zoals varianten, enabling factoren als crypto-currency en de rollen van de verschillende dadergroepen en hoe slachtoffers daarmee te maken krijgen.

Wat is ransomware?

De naam ransomware is een samenvoeging van de woorden ransom (losgeld) en software. De aanvallers gijzelen data van het slachtoffer en gebruiken drukmiddelen om het slachtoffer over te halen te betalen. Die gijzeling bestaat vaak uit het versleutelen van de gegevens[1] van het slachtoffer en het uploaden van data naar de actor, waar het als aanvullend pressiemiddel wordt gebruikt om betaling van losgeld te bewerkstelligen. In sommige gevallen slaan daders de encryptie stap over en gaan direct over tot uploaden.

Een ransomware-aanval schaadt niet alleen de beschikbaarheid van gegevens, maar ook steeds vaker de vertrouwelijkheid – de aanvaller dreigt gestolen informatie te publiceren. Daarnaast is ook de integriteit van de data in gevaar: er zijn immers onbekenden in het systeem van het slachtoffer geweest die overal aan konden komen.
Ransomware is op dit moment de meest voorkomende en meest lucratieve vorm van cybercrime wereldwijd[2]. Het heeft meer en meer impact op de economische en nationale veiligheid van Nederland[3]. Volgens de betrokken leden van Cyberveilig Nederland betreft het merendeel van de cyberincidenten momenteel ransomware. Rond de 90% van incident respons capaciteiten binnen Nederlandse informatiebeveiligingssector wordt in 2021 ingezet bij organisaties die slachtoffer zijn geworden van een ransomware-aanval.

Voorbeelden van recente Nederlandse ransomware-aanvallen zijn die van Hof van Twente (december 2020)[4], Senzer (maart 2021)[5] en de Mandemakers Groep (juni 2021)[6].

[1] Harde schijven, locale IT systemin, cloud opslag, databases, back-ups, USB-sticks: over het algemeen proberen de aanvallers zoveel mogelijk te versleutelen of vernietigen (back-ups, virtuele systemen).
[2] New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion| McAfee Press Release
Cybercrime cost the world over $1 trillion in 2020 | ITProPortal
Cybercrime Could Cost the World $10.5 Trillion Annually by 2025 (entrepreneur.com)
2021 Ransomware Statistics, Data, & Trends | PurpleSec
Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021 (cybersecurityventures.com)
[3] Cybersecuritybeeld Nederland, https://www.rijksoverheid.nl/documenten/rapporten/2021/06/28/cybersecuritybeeld-nederland-2021 Hoofdstuk 4
[4] https://www.hofvantwente.nl/actueel/veelgestelde-vragen-cyberaanvalhack-gemeentehuis
[5] https://www.security.nl/posting/693921/Helmonds+werkbedrijf+Senzer+getroffen+door+inbraak+op+netwerk
[6] https://nos.nl/artikel/2387348-mandemakers-groep-getroffen-door-cyberaanval-hackers-eisen-losgeld

Hoe werkt ransomware?

Elke cyberaanval bestaat uit verschillende fases, met elk hun eigen acties en technieken. We gebruiken hier een vereenvoudigde vorm van de Unified Kill Chain[7] om de meest voorkomende varianten van ransomware te ontleden.

FASE	IN	DOOR	UIT
OMSCHRIJVING	Alle acties tot en met het succesvol binnendringen van de omgeving	Alle acties om zich binnen de omgeving te bewegen	Alle acties om het uiteindelijke doel te bereiken
VOORBEELDEN	1. Phishing 2. Configuratie-fouten 3. Kwetsbaarheden	1. Verhogen van rechten 2. Laterale beweging 3. Verkennen gevoelige informatie; financiën	1. Wegsluizen van informatie 2. Versleutelen van bestanden 3. Financiële afhandeling

Tabel 1 - Fases en acties in een ransomware-aanval

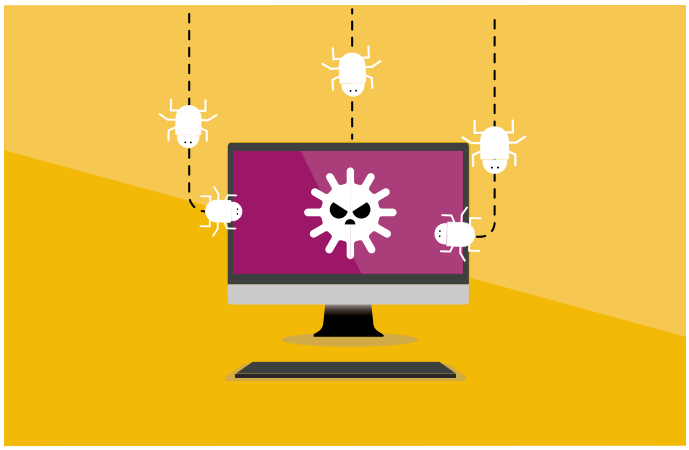
IN
De IN fase is niet specifiek voor ransomware. In deze fase proberen de aanvallers het systeem binnen te dringen. Dit heet de initial foothold.

Eenmaal binnen worden achterdeurtjes in de omgeving van het slachtoffer ingebouwd zodat de aanvallers voor langere tijd binnen kunnen blijven. Tussen de initial foothold en de daadwerkelijke aanval kunnen maanden zitten.

In de IN-fase blijkt het opportunisme van de aanvaller. Voorbeelden:
- Actueel nieuws zoals COVID wordt aangegrepen om phishing e-mails te versturen;
- Zodra kwetsbaarheden in gangbare programma's bekend worden proberen de aanvallers deze te misbruiken;
- Ontwikkelingen als remote werken zetten de aanvallers ertoe aan zich hierop te concentreren.

Een recent voorbeeld is de ransomware aanval op Bakker Logistiek. Zij werden getroffen door ransomware doordat een kwetsbaarheid in Microsoft Exchange gebruikt is door cybercriminelen om hun systemen binnen te komen en het netwerk plat te leggen[9].

DOOR
In de DOOR fase proberen de aanvallers toegang te krijgen tot de voor hen aanval relevante delen van het netwerk. Hier zijn verschillende tools voor, maar er komt ook vaak handwerk bij kijken. De aanvallers proberen verkregen gebruikersrechten te verhogen om meer toegang te forceren, en maken zijwaartse bewegingen in het netwerk (lateral movement) om van de ene computer naar de andere te springen.



[7] https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf
[8] Zie de verklarende woordenlijst bij dit whitepaper voor een korte beschrijving van de hier gebruikte terminologie.
[9] https://blog.malwarebytes.com/awareness/2021/04/ransomware-disrupts-food-supply-chain-exchange-exploitation-suspected/

De DOOR fase is grotendeels generiek, maar professionele ransomware groeperingen gebruiken deze fase echter ook om te onderzoeken hoeveel losgeld (ransom) ze kunnen vragen en/of welke drukmiddelen ze kunnen inzetten.

UIT

De UIT fase is voor elk type aanval verschillend. Voor ransomware aanvallen bestaat deze fase uit twee stappen:

- Het aanrichten van schade bij het slachtoffer: bestanden versleutelen, backup vernietigen, gegevens stelen. Een DDoS aanval starten, het lekken naar de pers, etc. wordt dan vaak nog gebruikt als extra motivatie om te betalen;
- Het afpersen van het slachtoffer (extortion): de criminelen bieden het slachtoffer de mogelijkheid om tegen betaling van een fors bedrag de schade “ongedaan” te maken. De schade en het afpersen zijn nauw met elkaar verbonden en dienen gezamenlijk één doel: zo veel mogelijk geld verdienen.

Vormen

In de praktijk komen we de volgende vormen van afpersing tegen:

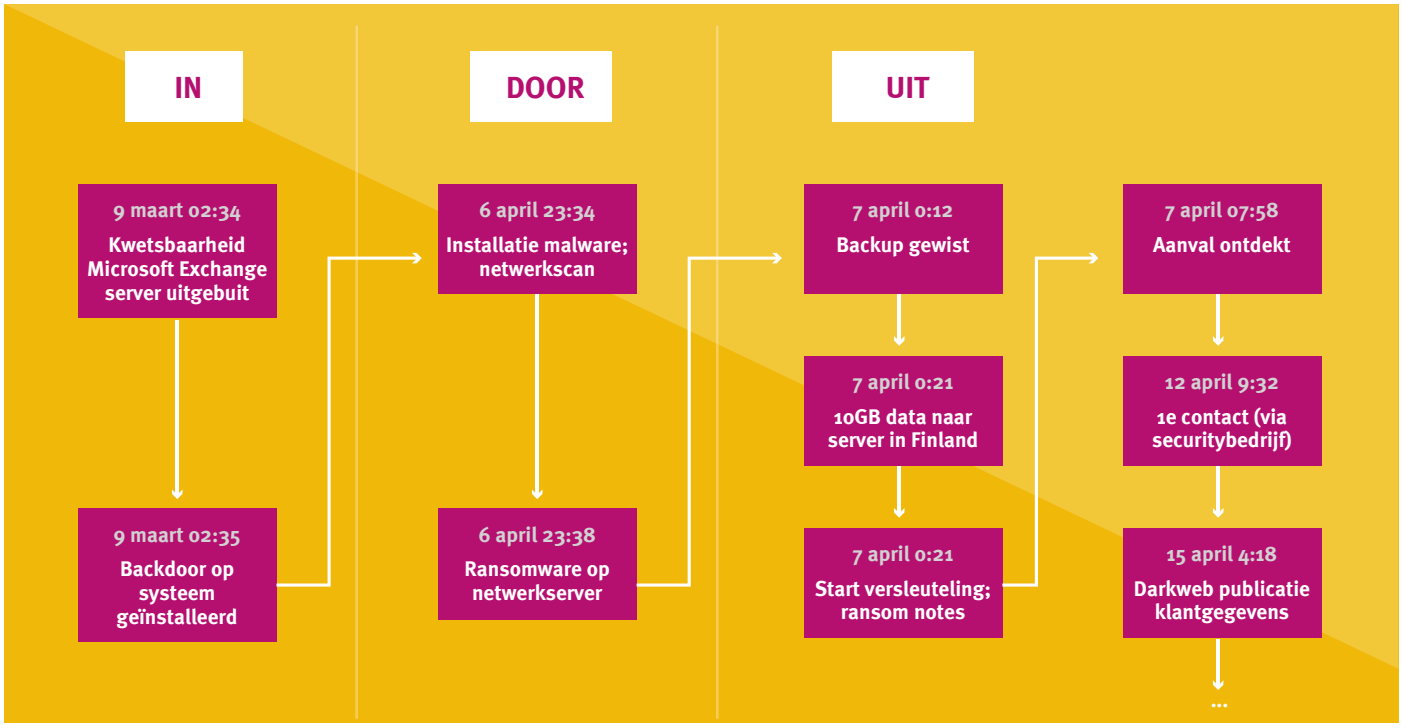
- **Single extortion:** bestanden of systemen van het slachtoffer zijn versleuteld; de sleutel wordt tegen betaling aangeboden;
- **Double extortion:** naast versleuteling worden gevoelige gegevens van het slachtoffer buitgemaakt, betaling moet voorkomen dat ze gelekt worden;
- **Triple extortion:** naast het slachtoffer worden ook diens klanten, partners of andere derde partijen afgeperst.

In 2020 werd Visser Precision, een bedrijf dat precisieonderdelen maakt voor onder andere Tesla, Boeing en Lockheed Martin, getroffen door DoppelPaymer ransomware[10]. De bestanden van Visser Precision werden daarbij op slot gezet en vertrouwelijke informatie werd gestolen. DoppelPaymer publiceerde vertrouwelijkheidsovereenkomsten met klanten van Visser Precision om zo de druk op te voeren.

In 2018/2019 werd Vastaamo, een Fins centrum voor geestelijke gezondheidszorg gehackt en werden alle (oud)patiëntgegevens gestolen. In 2020 benaderden de aanvallers de individuele patiënten met de dreiging dat hun gegevens gepubliceerd zouden worden tenzij ze betaalden.[11]

Voorbeeld

Het onderstaande gefingeerde voorbeeld geeft aan hoe de mijlpalen van een geslaagde ransomware-aanval eruit kunnen zien.



Figuur 1 - Mijlpalen van een geslaagde ransomware-aanval (gefingeerd voorbeeld)

[10] https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/
[11] https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/

Evolutie van ransomware

Het fenomeen ransomware heeft het afgelopen decennium een snelle ontwikkeling doorgemaakt. Rond 2011 verscheen de zogenaamde politie-ransomware, waarin de aanvallers op goed geluk computers op slot zetten en een politielogo toonden met de mededeling dat er kinderporno was gevonden. De “boete” kon online betaald worden met behulp van anonieme digitale betaalmiddelen. De PC was echter eenvoudig te herstellen omdat de bestanden niet daadwerkelijk versleuteld waren.

In de tussentijd zijn de aanvallers op vrijwel alle aspecten geprofessionaliseerd naar goed georganiseerde misdaadgroeperingen.

ASPECT	10 JAAR GELEDEN	NU
KWALITEIT	Slecht	Zeer professioneel
VORM	Opportunistische aanvallen op eindgebruikers	Volwassen criminele markt met gerichte en ongerichte aanvallen op organisaties van elke grootte
BETROUWBAARHEID	Niet reageren op betaling	Hoogwaardige service bij betaling
DRUKMIDDELEN	Social Engineering / single extortion	Double en triple extortion
BEDRAGEN	Enkele tientjes per slachtoffer	Tot tientallen miljoenen per slachtoffer
ACTOREN	Amateurs	Ransomware as a service; gespecialiseerde samenwerkende groeperingen

Tabel 2 - Professionalisering van ransomware

De ontwikkeling van ransomware-aanvallen is nog niet afgelopen. Momenteel is er bij de aanvallers bijvoorbeeld toenemende aandacht voor supply chain aanvallen, met name via IT-leveranciers.

Begin juli 2021 werd bekend dat 800 tot 1500 organisaties tegelijkertijd waren getroffen door REvil ransomware. De organisaties konden besmet worden door een kritieke fout in het remote monitoring en management softwarepakket VSA van IT leverancier Kaseya[12].

Sectoren

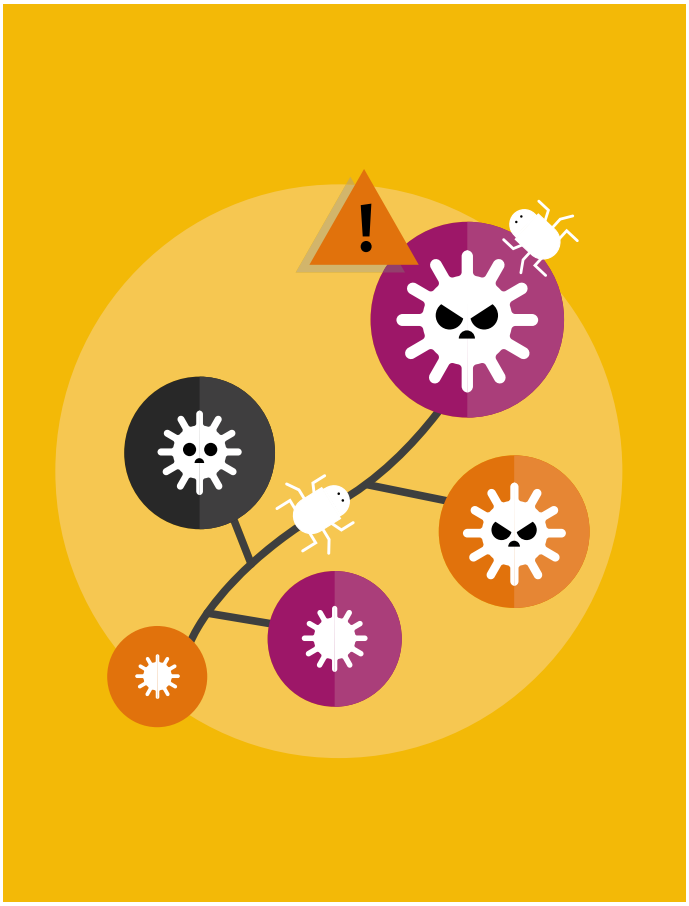
Er lijkt sprake te zijn van trends in de doelwitten van ransomware-groeperingen. Ze proberen sectoren te treffen waar de verwachte opbrengst het hoogst is, alhoewel er ook groeperingen bestaan, zoals DarkSide, die zich beroepen op een soort van ethische code, waarin staat welke sectoren niet getarget mogen worden. Desondanks blijven sectoren als ziekenhuizen en gemeentes een gewild aanvalsdoel. Volgens de voormalige REvil-ransomware groepering zijn binnenkort hightech land- en tuinbouw aan de beurt[13] . Over het geheel genomen is er echter geen sector aan te wijzen die intrinsiek interessanter is voor de aanvallers dan andere sectoren[14].

[12] https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/
[13] https://www.youtube.com/watch?v=nlxMS6K5Cdk
[14] De meningen verschillen hierover. Sommige cybersecurity rapporten noemen de overheid en financiële sector als duidelijke targets, terwijl anderen juist retail en industrie noemen. Vanuit de leden van Cyberveilig Nederland komt geen specifieke sector naar voren als bovengemiddeld vatbaar voor een ransomware aanval.

Professionaliteit
De professionaliteit van ransomware groeperingen blijft toenemen. Ze verfijnen hun methodieken om tot een maximale opbrengst te komen: meer of minder losgeld eisen, wel of niet onderhandelen, wel of niet persoonlijk contact, wel of niet de pers opzoeken, etc.
Sommige experts verwachten dat ransomware binnenkort ook voor geopolitieke doeleinden zal worden ingezet[15]. Gijzeling wordt al eeuwenlang gebruikt als politiek wapen. Ransomware voegt daar simpelweg een nieuwe variant aan toe.

Al deze ontwikkelingen betekenen overigens niet dat 'oude' vormen van ransomware verdwijnen. Naast gerichte aanvallen is er bijvoorbeeld nog steeds sprake van een groot aantal ongerichte aanvallen, waar met name het MKB steeds vaker slachtoffer van wordt.

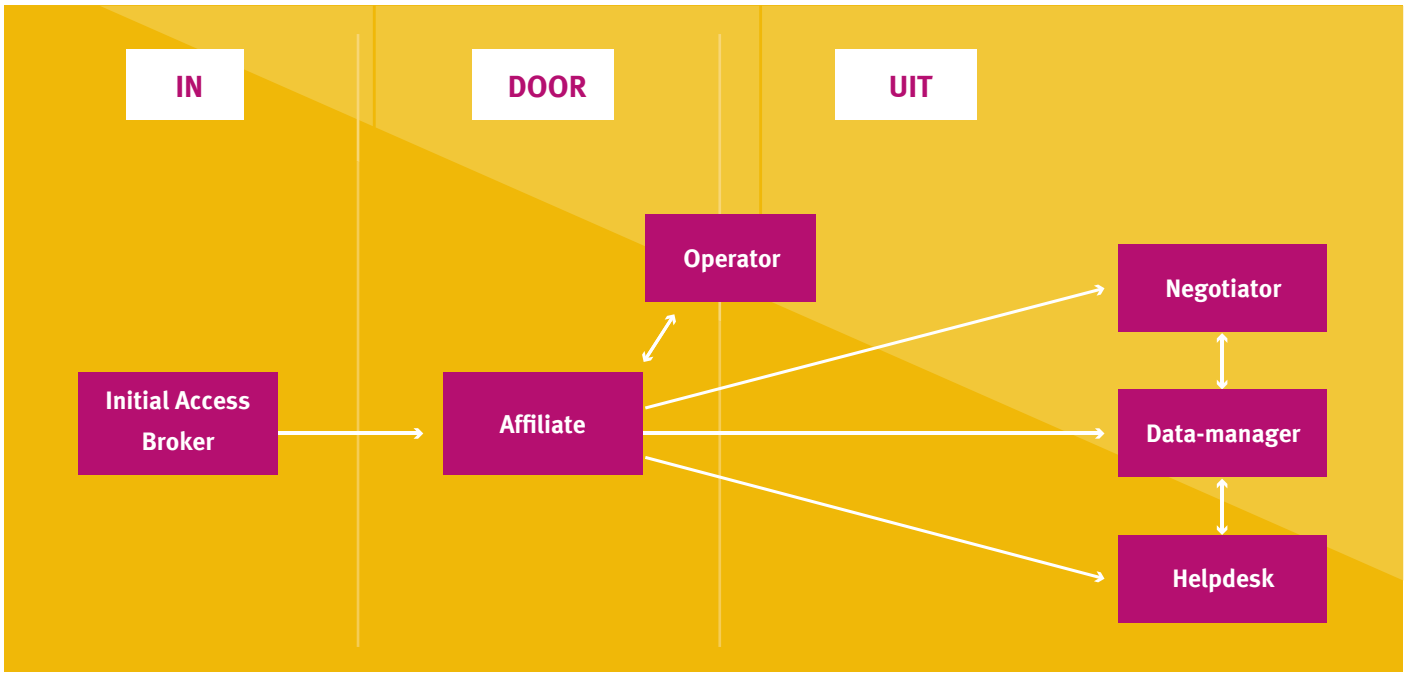
Groei
Tenslotte is sprake van een snelle groei van het fenomeen. Volgens Bitdefender is het aantal ransomware verslagen wereldwijd in 2020 met 715% gegroeid ten opzichte van 2019[16]. Blockchain-analyse firma Chainalysis zag in 2020 een verviervoudiging van via cryptocurrency (Bitcoin en andere digitale munten) betaald losgeld ten opzichte van 2019[17].



[15] https://www.politico.com/news/magazine/2021/07/08/ransomware-game-theory-geopolitics-cyber-attack-498625
[16] https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf pag 14
[17] https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

De aanvallers

De snelle groei van het ransomware fenomeen is deels te danken aan de professionalisering en specialisatie van de aanvallers. Er is vaak sprake van een keten van goed gerunde criminele bedrijven, waarbij een affiliate (gelieerde) afnemer is van verschillende diensten in een ransomware keten. Dit gebeurt in wisselende samenstelling, net naar gelang wat op dat moment het beste uitkomt. We noemen dit Ransomware as a Service (RaaS). Deze samenwerking kan als volgt gemodelleerd worden:



Figuur 2 - Samenwerkende criminele organisaties in een ransomware-aanval

1. **De initial access broker verkoopt toegang tot netwerken.** Deze toegang verkrijgt hij vaak met behulp van de standaardmethoden uit de IN fase van de cyberaanval. Vervolgens zal hij proberen om een achterdeur in het netwerk aan te brengen zodat zijn klanten ook later nog binnen kunnen komen;
2. **De affiliate voert de daadwerkelijke aanval uit.** Hij brengt het netwerk in kaart, besmet de computers, sluist gegevens weg en maakt de back-up onklaar;
3. **De operator beheert de ransomware.** Zodra de affiliate het netwerk gehackt heeft zorgt deze groep voor de versleuteling;
4. **De negotiator onderhandelt namens de affiliate met de slachtoffers.** De negotiator moet bekend staan als betrouwbaar om de transactie een betere kans van slagen te geven;
5. **De data-manager voert het technisch beheer van de databases uit** om slachtoffers na betaling hun sleutel terug te kunnen geven, maar publiceert ook gevoelige data om het slachtoffer verder onder druk te zetten;
6. **De helpdesk ondersteunt slachtoffers**, bijvoorbeeld met het ontsleutelen. Helpdesks zijn vaak 24/7 beschikbaar en spreken goed Engels.

Dit model kan verder worden uitgebreid. Zo worden er bijvoorbeeld aan de achterkant nog gespecialiseerde witwassers ingehuurd. In individuele gevallen zijn de rollen uit dit model samengevoegd of juist opgesplitst.

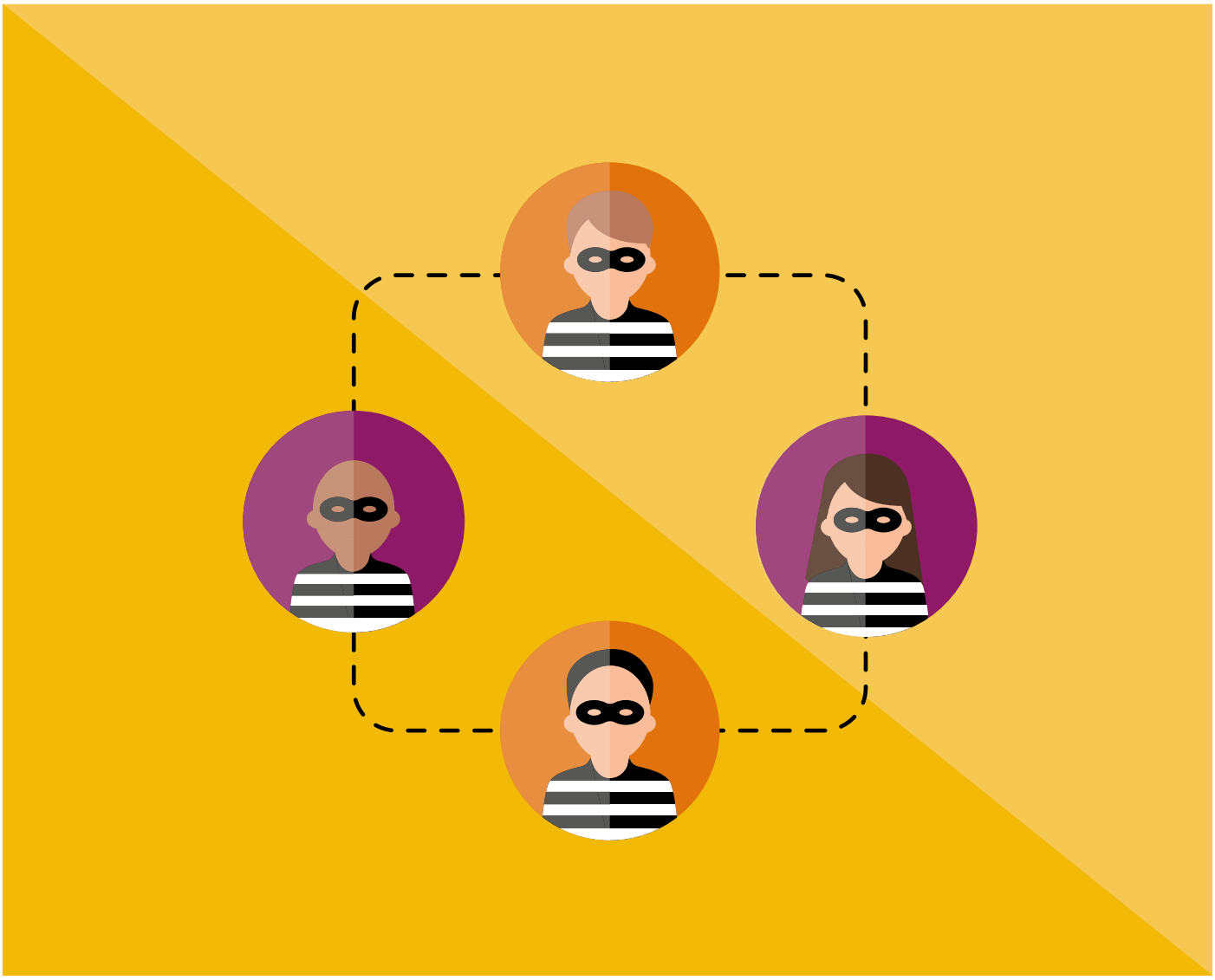
De REvil[18] ransomware groep biedt niet alleen de ransomware (operator) aan maar verzorgt ook de volledige afhandeling van de aanval (negotiator, data-manager, helpdesk)

Het verkrijgen van toegang tot netwerken (initial access broker) en de aanval zelf worden aan de affiliate overgelaten. Deze affiliate verdient ongeveer 70% van de opbrengst in ruil voor het uitvoeren van de meest arbeidsintensieve fase van de aanval.

De REvil groep werkt met verschillende affiliates samen en verdient naar eigen zeggen meer dan 100 miljoen dollar per jaar. In maart 2021 eiste de groep een losgeld van $50 miljoen van computerfabrikant Acer.

Herkomst

Attributie is niet eenvoudig in de huidige malware-wereld. Toch lijkt een onevenredig groot aantal ransomware-groeperingen uit de voormalig Sovjet landen te komen. Deze groeperingen werken in de regel ook alleen samen met partijen uit deze landen. De taal spreken is niet voldoende, potentiële partners worden gescreend op kennis van lokale politieke en sociale issues. Omdat Rusland geen criminelen uitlevert en alleen onderzoek doet naar criminaliteit met Russische slachtoffers heeft een aantal ransomware-pakketten code ingebouwd om computers waarop de taalinstelling op Russisch staat te ontzien.



[18] Ook bekend onder de namen Sodinokibi en Sodin.

De kosten van ransomware

In het Cybersecuritybeeld Nederland 2021 wordt gesteld dat ransomware tot onomkeerbare schade leidt.[19] De Nationale Politie constateert dat in Nederland zowel de geëiste als de uitbetaalde bedragen inmiddels geregeld in de miljoenen euro's lopen.

De Nederlandse overheid adviseert om geen losgeld te betalen, vooral omdat dit geen oplossing voor het probleem garandeert. De kans is groot dat er bij de ontsleuteling tal van problemen opduiken. Daarnaast houdt het betalen van losgeld een ecosysteem in stand: het moedigt cybercriminelen aan om ransomware te gebruiken aangezien het een winstgevende business is.

Kosten voor het slachtoffer

De gemiddelde losgeldeis bedroeg volgens ransomware incident response organisatie Coveware in het 4e kwartaal van 2020 $220.298, met een mediaan van $78.398 (het verschil kan verklaard worden door een klein aantal zeer hoge losgeldeisen)[20]. Dit is, ongeacht of het slachtoffer betaalt, slechts een deel van de kosten. Het slachtoffer moet rekening houden met reputatieschade, een mogelijk onveilige werksituatie, het doorbetalen van mensen en apparatuur en natuurlijk de investeringen om het netwerk weer op te bouwen en te beveiligen. Coveware stelt dat de gemiddelde downtime van slachtoffers (Q4, 2020) 23 dagen is.

Naar draagkracht

Ransomware groeperingen willen hun opbrengst maximaliseren, en proberen daarom het losgeld 'naar draagkracht' te eisen. Ze investeren tijd om de financiële situatie van het slachtoffer goed in te kunnen schatten. Dit varieert van bedrijfsinformatie opzoeken op sites als zoominfo.com tot het stelen en bestuderen van financiële informatie uit het netwerk van hun slachtoffer. Bij bedrijven ligt de losgeldeis vaak tussen de 0,4% en 2% van de jaaromzet. Bij overheidsinstellingen zullen ransomware groeperingen eerder kijken naar de maatschappelijke verantwoordelijkheden van het slachtoffer en de eis daarop aanpassen. Ook de inschatting van de impact van het stilstaan van de bedrijfsprocessen van het slachtoffer speelt mee in de keuze van het losgeldbedrag.

Fysieke gevolgen

De gevolgen van ransomware-aanvallen beperken zich niet tot het cyberdomein en ook niet tot het slachtoffer, maar kunnen verstrekkende gevolgen hebben in de fysieke wereld. Een ransomware-aanval op transportbedrijf Bakker Logistiek in april 2021 zorgde voor lege schappen in de supermarkten omdat er geen kaas meer geleverd kon worden[21]. De ransomware-aanval op het Amerikaanse oliepijpleidingsysteem Colonial Pipeline in mei 2021 leidde ondanks een prompt betalen van de 75 bitcoin ($4,4 miljoen) losgeld tot het stilleggen van de pijplijn met als gevolg een tijdelijk sterke prijsstijging van brandstof in de Verenigde Staten[22].

[19] https://www.rijksoverheid.nl/documenten/rapporten/2021/06/28/cybersecuritybeeld-nederland-2021 pag 19.
[20] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[21] https://nos.nl/artikel/2376425-kaas-hack-opgelost-ging-om-gijzelsoftware
[22] https://nos.nl/artikel/2380207-stilleggen-oliepijplijn-vs-veroorzaakt-door-gijzelsoftware-van-darkside

Een ransomware aanval voorkomen

Er is niet één maatregel die ransomware voorkomt. De aanpak tegen ransomware bestaat uit een samenspel van maatregelen die een geslaagde aanval proberen te voorkomen en de gevolgen van een geslaagde aanval proberen te beperken. Maatregelen die tegelijkertijd ook bescherming bieden tegen andere vormen van digitale aanvallen. Dit vraagt om een weldoordachte risicomanagement-strategie die mee kan evolueren met de ontwikkelingen in ransomware.

De maatregelen die moeten worden getroffen dienen zich niet te beperken tot de IN fase van de aanval (het binnendringen van het netwerk), maar ook de DOOR en de UIT fase mee te nemen. Daarnaast is het belangrijk om te beseffen dat cybersecurity geen puur technisch domein is. In de driedeling mens, organisatie en techniek zijn de eerste twee minstens even belangrijk als de laatste. En daarnaast behoeft naast de digitale beveiliging ook de fysieke beveiliging de aandacht.

Maatregelen

Het voert te ver om in dit whitepaper alle maatregelen uit te werken. We beperken ons hier tot een aantal maatregelen die als voorbeeld moeten dienen van de mogelijkheden. Voor de toepassing van een aantal (technische) maatregelen verwijzen we naar het Factsheet Ransomware van het NCSC[23].

- **Awareness training:** het trainen van de medewerkers om zo bijvoorbeeld het risico op succesvolle phishing te verkleinen;
- **Wachtwoordbeleid:** wachtwoordzinnen en multifactor-authenticatie (het aanmelden met meer dan alleen een wachtwoord) invoeren om wachtwoorden raden of het succesvol aanmelden met een gestolen wachtwoord tegen te gaan;
- **Patch management:** een vaste systematiek om alle hard- en software binnen de organisatie up-to-date te houden om aanvallen op verouderde versies tegen te gaan;
- **End point detection & response:** geautomatiseerde analyse van en reactie op alle activiteiten op servers en clients om verdachte activiteiten direct te stoppen;
- Een **positieve securitycultuur** opbouwen waarin melden wordt beloond in plaats van afgestraft. Zo worden medewerkers een extra beschermlaag;
- **Kritieke processen en informatie in kaart** brengen en beheren om de beveiliging te kunnen concentreren daar waar deze het belangrijkst is;
- **Netwerksegmentatie en access control:** delen van het netwerk die niet met elkaar verbonden hoeven te zijn loskoppelen. Medewerkers alleen die rechten geven die ze voor hun werk nodig hebben. Dit maakt het lastiger om het hele netwerk te besmetten;
- **Netwerkmonitoring:** logging en analyse van het netwerkverkeer zodat afwijkende activiteiten snel worden gesignaleerd en erop gereageerd kan worden;
- **Training crisisscenario's:** voldoende personeel dat kan omgaan met crises zodat de continuïteit van de organisatie niet in gevaar komt bij een aanval;
- **Incident response plan:** het van tevoren opstellen van procedures, acties en contacten om de schade te beperken bij een geslaagde aanval;
- **Offline backup:** minimaal één niet-overschrijfbare kopie op een gescheiden locatie, zodat deze niet onklaar kan worden gemaakt.

[23] Deze maatregelen zijn: 1. Bescherm tegen phishing. 2. Organiseer vulnerability & patch management; netwerk segmentering. 3. Beperk de mogelijkheden van code-execution. 4. Filter webbrowser verkeer. 5. Beperk USB-gebruik. Het Factsheet Ransomware is te vinden op https://www.ncsc.nl/documenten/factsheets/2020/juni/30/factsheet-ransomware

	IN	DOOR	UIT
MENS	Awareness training	Positieve securitycultuur	Training crisis-scenario's
ORGANISATIE	Wachtwoordenbeleid; Patch management	Kritieke processen beheren	Incident Response plan
TECHNIEK	End point detection & response	Netwerksegmentatie; access control; Netwerk monitoring	Offline back-up

Tabel 3 - Voorbeeldmaatregelen afgezet tegen de IN, DOOR en UIT fase van de aanval

Voldoen de maatregelen?
De maatregelen die worden geïmplementeerd zullen ook getest moeten worden. Dit kan in vele vormen. Te denken valt aan assessments, penetratietests en red team oefeningen[24]. Maar soms is het ook niet moeilijker dan controleren of de back-up inderdaad bruikbaar is om de data terug te zetten.

Meer lezen over maatregelen?
Het NCSC heeft diverse kennisproducten die helpen met het vergroten van de weerbaarheid tegen cyberaanvallen. Deze vindt u hier https://www.ncsc.nl/documenten.

Basismaatregelen
https://www.ncsc.nl/onderwerpen/basismaatregelen
Deze basismaatregelen zou elke organisatie moeten treffen om cyberaanvallen tegen te gaan.

Ransomware
https://www.ncsc.nl/documenten/factsheets/2020/juni/30/factsheet-ransomware
Meer advies over hoe een ransomware-aanval te voorkomen en wat te doen als uw organisatie geraakt wordt.

Bereid u voor op Zero Trust
https://www.ncsc.nl/actueel/nieuws/2021/augustus/18/publicatie-factsheet-bereid-u-voor-op-zero-trust
Zero Trust is een beveiligingsmodel met een set ontwerp-principes dat aanvallen en datalekken helpt te voorkomen.

[24] Cyberveilig Nederland heeft een buyers guide security testen ontwikkeld. Dit document vormt een hulpmiddel waarmee inzicht wordt geboden in wat de verschillende security testen inhouden en hoe ze zich tot elkaar verhouden. https://cyberveiligNederland.nl/upload/userfiles/files/CVNL_Buyersguide_Security_Testen_final2.pdf

Wat te doen bij een ransomware-aanval

Professionele hulp
Ondanks alle maatregelen kan elke organisatie geraakt worden door een ransomware-aanval. Wat dan? Het is belangrijk om te beseffen dat het specialistische kennis vergt om met zo'n aanval om te gaan. Het is dan ook aan te raden om zo snel mogelijk de hulp van een professionele security-organisatie in te roepen. Zij hebben ervaring met dit soort aanvallen en kunnen slachtoffers bijstaan in alle acties die ze moeten ondernemen.

Mitigatie
Het mitigeren van de aanval – ondersteund door specialisten – kent vier fases:

- **Analyse:** wat is de aard, reikwijdte en impact van de aanval;
- **Containment** (inperking): maatregelen die ervoor zorgdragen dat de aanval zich niet verder over het netwerk verspreidt, zoals systemen isoleren (maar niet uitzetten);
- **Eradication** (eliminatie): maatregelen die de dreiging volledig van het netwerk verwijderen, zoals het analyseren van de systemen om malware te verwijderen en de toegang van de aanvallers af te sluiten;
- **Recovery** (herstel): maatregelen die de functionaliteit van het netwerk herstellen, zoals het terugzetten van backups.

Grijp het incident vooral aan om het securityniveau te verhogen, zodat een soortgelijke aanval niet nogmaals zal plaatsvinden.

Communicatie
Zowel tijdens als na een ransomware-aanval kan een heldere communicatie, intern én extern, veel verschil maken. Een vooraf opgesteld communicatieplan zorgt dat in de paniek van het moment geen partijen worden vergeten.

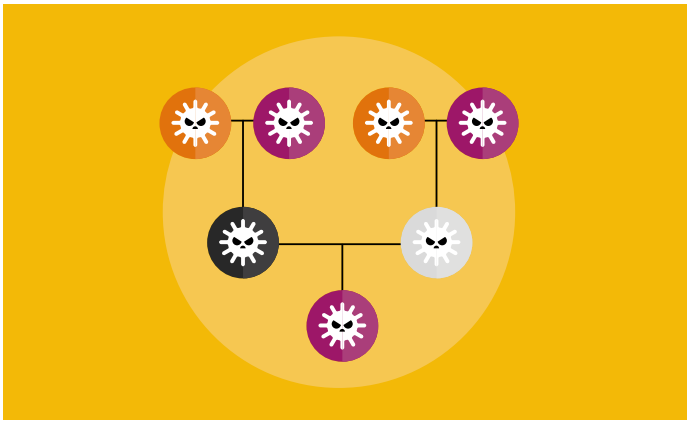
- Medewerkers: dienen te weten waar ze aan toe zijn. Kunnen ze werken, welke acties worden van hen verwacht;
- Stakeholders, ketenpartners, afnemers: moeten weten wat ze kunnen verwachten;
- Juridisch: een ransomware-aanval kan verstrekkende juridische gevolgen hebben. Zorg voor juridische ondersteuning;
- Autoriteit Persoonsgegevens: moet ingelicht worden als er (persoons)data is geupload of ontvreemd. Ga ervan uit dat een ransomware-aanval een datalek inhoudt;
- De pers: kan met vragen komen: hoe gaan deze beantwoord worden;
- De politie: het is aan te raden om melding te maken van de aanval en, eventueel op een later moment, aangifte te doen.

Tenslotte: deel als alles achter de rug is uw kennis en ervaringen met anderen. Alleen gezamenlijk kunnen we Nederland weerbaarder maken.

BIJLAGE: Ransomwarefamilies

Gezien de grote bedragen die met ransomware worden verdiend is het opmerkelijk dat er maar een betrekkelijk klein aantal ransomware-families is. Het succes van deze families in termen van aantallen aanvallen en totaal verkregen losgeld wisselt sterk door de tijd. Ransomware-groeperingen kunnen van de ene op de andere dag verdwijnen, zoals Maze in 2019 of REvil in 2021. Ze komen dan vaak later onder een andere naam weer terug.

Ransomware incident response organisatie Coveware houdt per kwartaal de top 10 van ransomware-families bij. Gebaseerd op hun gegevens van Q1 2021[25] volgt hier een kort overzicht van een aantal bekende malware-families.



NAAM[26]	% MARKT IN Q1 2021	GEMIDDELD (BETAALD) LOSGELD [27]	VOORBEELDEN VAN SLACHTOFFERS [28]
REVIL / SODINOKIBI	14,2	$124.418	Kaseya, Acer, Quanta
CONTI / IOCP	10,2	$849.581	Volkswagen groep, ITxx (een Belgisch IT bedrijf)
LOCKBIT	7,5	$69.625	Koninklijke Reesink, Kopter (een Zwitserse helicoptermaker)
CLOP	7,1	Onbekend. Weinig slachtoffers, losgeld in de miljoenen	Bombardier, Shell, Universiteit Maastricht
EGREGOR	5,3	$700.000	Randstad uitzendbureau, Barnes & Noble boekhandel, DAX ziekenhuis (Frankrijk)

Tabel 4 - Top 5 ransomware-families

- **REvil** – Triple extortion - Tot op heden de hoogste losgeld-eis, laten zich betalen in de cryptovaluta Monero. Slachtoffers: Kaseya, Acer, Quanta, etc. Toen Apple toeleverancier Quanta weigerde te betalen begon de groep met het lekken van Apple blauwdrukken en probeerden zo Apple onder druk te zetten om te betalen. In juli 2021 plotseling verdwenen;
- **Conti** – Double extortion - biedt naast de sleutel ook een securityrapport zodat slachtoffers hun kwetsbaarheden kunnen patchen;
- **Lockbit** – Double extortion. Vergaande automatisering van de DOOR en UIT fase voor een snellere besmetting en minder menselijk handelen door de aanvallers;
- **Clop** – Double extortion, maar ook data diefstal en afpersing zonder versleuteling van files, gebruik van o-day kwetsbaarheden – biedt slachtoffers een complete pentestrapportage. In juni 2021 werden in Oekraïne 6 verdachte bendeleden gearresteerd;
- **Egregor** – Double extortion – na een gezamenlijk Frans en Oekraïens politieonderzoek werden in februari 2021 meerdere personen aangehouden die achter de ransomware zouden zitten.

[25] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[26] Veel ransomware-families staan bekend onder verschillende benamingen
[27] Gegevens per juni 2021, volgens Coveware
[28] Bron o.a. DarkTracer Intelligence Report on Ransomware Gangs on de Darkweb: https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3

BIJLAGE: Woordenlijst

Cybersecurity gebruikt een groot aantal specifieke begrippen. Hoewel we in dit document hebben geprobeerd het jargon beperkt te houden vonden we toch dat we in een aantal gevallen wel de naamgeving uit de sector moesten gebruiken om aan te sluiten bij andere publicaties. We geven hier een verklarende woordenlijst. Deze is opgesteld op basis van het Cybersecurity Woordenboek[29].

BEGRIP	BETEKENIS
ACHTERDEUR	Een manier om via een ongewone omweg in een digitaal systeem te komen. Iemand heeft die omweg vaak met opzet gemaakt, en op zo'n manier dat anderen die niet kunnen zien.
AFFILIATE	Een aan een ransomwaregroep gelieerde criminele groepering. Affiliates huren de software en de expertise van de ransomwaregroep.
AWARENESS	Bewustwording. Wat de medewerkers weten over de risico's die ze lopen en introduceren, en wat ze daaraan kunnen doen.
CONFIGURATIEFOUT	Een foutieve instelling van hardware of software voor het gewenste doel.
CRYPTOVALUTA	Digitaal ruilmiddel. Een bekende cryptovaluta is de bitcoin.
KWETSBAARHEID	Fout in een digitaal systeem waardoor een aanvaller in het systeem kan komen. De aanvaller kan vervolgens bij informatie of toepassingen in het systeem komen, terwijl hij dat niet mag. Of de aanvaller zorgt ervoor dat de gebruiker niet meer bij deze informatie kan komen. Of de toepassing niet meer kan gebruiken.
LATERAL MOVEMENT	Technieken die aanvallers gebruiken om geleidelijk door een netwerk te bewegen. Terwijl ze door het netwerk bewegen, zoeken ze naar informatie.
MALWARE	Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse malicious software.
ONTSLEUTELEN	Versleutelde informatie leesbaar maken. Bijvoorbeeld een versleuteld tekstbestand of netwerkverkeer. Om te kunnen ontsleutelen moet men weten welke versleutelmethode is gebruikt en beschikken over de sleutel.
PHISHING	Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inlog-gegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.
RAAS / RANSOMWARE AS A SERVICE	Het tegen betaling aanbieden van het gebruik van ransomware plus ondersteuning aan klanten.
RECHTEN	Afbakening van wat een gebruiker of systeem wel of niet mag doen.
SOCIAL ENGINEERING	Als een aanvaller iemand misleidt door bijvoorbeeld in te spelen op nieuwsgierigheid of behulpzaamheid. Op deze manier probeert de aanvaller bijvoorbeeld aan informatie te komen om in een digitaal systeem in te breken.
VERSLEUTELEN	Informatie (bijvoorbeeld een tekstbestand of netwerkverkeer) onbegrijpelijk maken voor anderen. De informatie wordt onleesbaar gemaakt en kan alleen met behulp van de juiste sleutel weer leesbaar gemaakt worden.

[29] cyberveilignederland.nl/woordenboek

Colofon

Dit is een uitgave van Cyberveilig Nederland. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Cyberveilig Nederland kan daarvoor niet aansprakelijk worden gesteld.

De definities van de begrippen die zijn opgenomen in dit document komen uit de tweede druk van het Cybersecurity Woordenboek (ISBN 9789083026411).

Eerste uitgave: augustus 2021

Meer informatie over de activiteiten van Cyberveilig Nederland vindt u op cyberveilignederland.nl

Contactgegevens
E-mail: info@cyberveilignederland.nl
Telefoon: 088 - 118 25 10

Dit whitepaper is mede mogelijk gemaakt door

Eindredactie
Peter Zinn
Liesbeth Holterman

COOLER MEDIA
THE EXPLANATION COMPANY

CYBERVEILIG NEDERLAND