Samen aanjagen van vernieuwing

Weerstand bieden tegen ransomware

Handreiking

Auteur(s): Mick Deben, Joost Gadellaa en Melvin Koelewijn
Versie: 1.0
Datum: 18 maart 2024

Versiebeheer

Versie	Datum	Auteur	Verwerking
1.0	18 maart 2024	Mick Deben, Joost Gadellaa, Melvin Koelewijn	Definitieve versie

Inhoudsopgave

1 Inleiding

Gijzelsoftware (ransomware) is nog steeds de grootste cyberdreiging en leidt wereldwijd tot zeer hoge impact. Maar wat kun je als instelling doen om te voorkomen dat je IT-infrastructuur en informatie gegijzeld worden door cybercriminelen? In deze anti-ransomware gids geven we praktische tips om ransomware besmettingen te voorkomen en te bestrijden wanneer dit onverhoopt toch het geval is.

Het door SURF gepubliceerde Cyberdreigingsbeeld 2023 onderkent dat ransomware momenteel de grootste cyberdreiging is voor de Nederlandse onderwijs- en onderzoeksector. In de eerdere gepubliceerde praktische vertaling van het cyberdreigingsbeeld hebben we al handelingsperspectief aangeboden voor de dreiging ransomware. In dit document gaan we een stap verder en zoomen we in op de dreiging ransomware en de maatregelen die je per fase van de aanvalsketen kunt nemen. Er is tegenwoordig sprake van viervoudige afpersing waarbij bij het uitblijven van betaling overgegaan wordt naar de volgende fase:

Stapsgewijs risico's verkleinen
Op de volgende pagina's hebben we aan de hand van de ransomware aanvalsketen een nadere toelichting en handelingsperspectief uitgewerkt. Hiermee kunnen instellingen stapsgewijs werken aan het verkleinen van de risico's op ransomware infecties.

Noot: de voorgestelde maatregelen in deze handreiking zijn voornamelijk technisch van aard, maar in het algemeen geldt dat instellingen risicomanagement moeten toepassen om de prioriteitstelling en kosteneffectiviteit van maatregelen te bepalen. Daarnaast is ook commitment en ondersteuning van (senior) management en effectieve governance noodzakelijk om de cyberweerbaarheid naar een hoger plan te kunnen brengen. Instellingen worden geadviseerd om een GAP-analyse uit te voeren om vast te stellen waar, en met welke prioriteit, zij verbetering kunnen aanbrengen. Ondanks dat deze handreiking met veel zorgvuldigheid is opgesteld bieden de gepresenteerde maatregelen geen garantie dat een instelling geheel veilig is voor ransomware infecties. Maar gezamenlijk dragen ze zeker bij aan het voorkomen, tijdig detecteren en het beperken van de impact daarvan.

Relatie met programma Cyberveiligheid en dienstverlening SURF
We sluiten dit document af met een tabel waarin we de relaties van de in dit document genoemde maatregelen met het SURFaudit Toetsingskader overzichtelijk in kaart brengen.

2 Ransomware en de betrokken actoren

Bij ransomware zijn verschillende (dreigings)actoren betrokken en het is nuttig om te begrijpen hoe deze actoren (samen)werken en wat hun aandeel in het proces is.

Ransomware

Ransomware dateert al van 1989, namelijk met "AIDS Trojan" virus, ook wel bekend als PC Cyborg. Dit virus werd verspreid via floppy disks en richtte zich op MS-DOS-computers. Zodra het virus was geïnstalleerd, versleutelde het bestanden op de harde schijf van de computer en toonde het een bericht waarin stond dat de gebruiker een 'licentievergoeding' moest betalen aan een postbus in Panama om de bestanden te herstellen. Ransomware is kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan.

Er zijn twee soorten ransomware: locker- en crypto ransomware. Locker ransomware is een type ransomware dat het apparaat van een slachtoffer volledig onbruikbaar maakt en crypto ransomware versleutelt (belangrijke) gegevens op een apparaat waardoor ze onleesbaar of onbruikbaar worden.

Ransomware is sterk toegenomen door de komst van cryptovaluta zoals Bitcoin. Deze digitale valuta maakt het voor cybercriminelen makkelijker en daarmee aantrekkelijker om geld te stelen en weg te sluizen dan via de traditionele bancaire infrastructuur. Daarnaast is de winstmarge zeer aantrekkelijk waardoor cybercriminelen eerder gemotiveerd zijn om zich hierin te mengen.

Slachtoffers

Slachtoffers zijn de organisaties of personen die aangevallen worden door de cybercriminelen met als doel het ontoegankelijk maken van IT-systemen en informatie, zodat zij vervolgens losgeld kunnen eisen.

Initial Access Brokers (IAB)

IAB's zijn actoren die via cyberaanvallen of omkoping initiële toegang tot netwerken en IT-systemen weten te verkrijgen en te behouden, om dat vervolgens te verhandelen. Dit zijn vaak ongerichte aanvallen aangezien het doel is om zoveel mogelijk toegang te verkrijgen tot apparaten, IT-systemen en netwerken van doelwitten om winst te kunnen maken. De IAB's onderzoeken vervolgens welke organisaties zij zijn binnengedrongen, wat hun omzet is, welke mate van toegang zij hebben verkregen en in welk(e) land(en) de organisatie gevestigd is. Dit is relevant omdat sommige Ransomwaregroepen bijvoorbeeld de Commonwealth of Independant States (CIS) zoals Rusland niet aanvallen om vervolging te voorkomen. Sommige IAB's werken voor specifieke ransomware groepen en sommigen opereren alleen. De initiële toegang wordt vaak op ondergrondse markten (fora op het Darkweb) te koop aangeboden.

```
sub_407760(v203, v204);
if ( sub_4CBDE0(&dword_4FFDC0, (int)"Russia", v205) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Ukraine", v16) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Armenia", v17) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Iran", v18) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Azerbaijan", v19) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Turkmenistan", v20) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Turkey", v21) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Georgia", v22) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Kazakhstan", v23) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Tajikistan", v24) != -1
  || sub_4CBDE0(&dword_4FFDC0, (int)"Uzbekistan", v25) != -1 )
{
  MessageBoxW(
    0,
    L"WARNING. Surtr does not run in this country, if you do it again you will be banned.",
    L"SurtrRansomware",
```

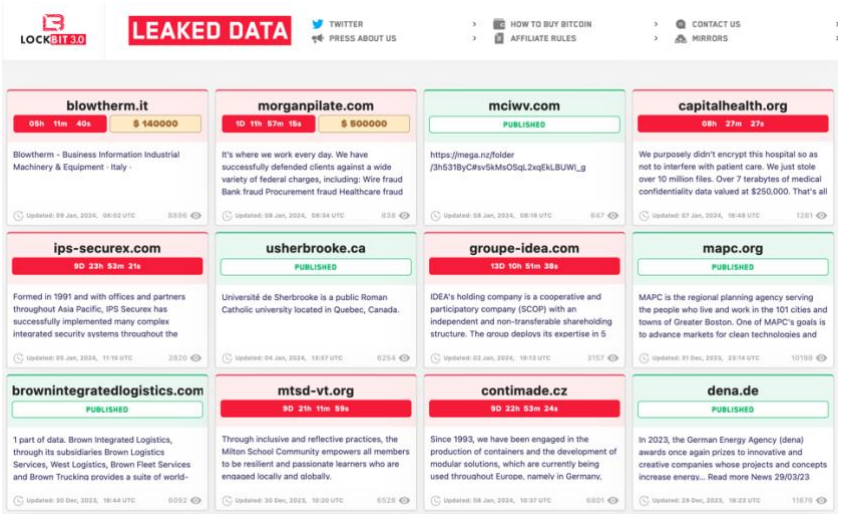
Voorbeeld uitsluiten van CIS-landen in ransomware code

Ransomware Affiliates

Ransomware Affiliates zijn de actoren die daadwerkelijk de IT-systemen en -infrastructuur binnendringen met als doel het met ransomware infecteren van zoveel mogelijk systemen en informatie om vervolgens doelwitten af te kunnen persen. Dit doen zij onder andere door initiële toegang te kopen van IAB's. Na het infecteren met ransomware krijgen doelwitten een bericht te zien met daarin de bevestiging dat systemen en informatie ontoegankelijk zijn gemaakt, en welk bedrag er betaald dient te worden voor het verkrijgen van een decryptiesleutel.

Ransomware Operators

Tot slot zijn er de Ransomware Operators en dat zijn de ontwikkelaars van de ransomware, de kwaadaardige code waarmee IT-systemen en informatie ontoegankelijk gemaakt worden. Zij zijn het brein achter de besmettingen en de Ransomware Affiliates moeten een deel van het losgeld afdragen aan de Operators (gemiddeld tussen de 20% en 30%). De ransomware operators zorgen er daarnaast voor dat er een platform is waarmee de onderhandelingen met slachtoffers kunnen plaatsvinden, betalingen kunnen plaatsvinden via cryptovaluta en een leksite waar (een deel van) de gestolen informatie gepubliceerd kan worden als (extra) drukmiddel. Er zijn meer dan honderd ransomware groepen bekend en het aantal ransomware infecties is in 2023 wederom sterk toegenomen. Indrukwekkende statistieken en meer informatie over deze groepen kun je bijvoorbeeld vinden op Ransomlook, Ransomware.live of Ransom-db.



Screenshot leksite van LockBit 3.0 (9 januari 2024)

3 Ransomware Kill Chain

De ransomware aanvalsketen (ook wel 'kill chain' genoemd) bestaat grofweg uit 5 stappen, klik op één van de fasen uit de aanvalsketen om direct naar de bijbehorende pagina's te navigeren. Het handelingsperspectief voor iedere fase van de aanvalsketen wordt uitgebreid behandeld en is onderverdeeld in ***preventie***, ***detectie*** en ***reactie***. Aanvullend daarop is in de bijlage de relatie met het SURFaudit Toetsingskader en de SURF Security Baseline gelegd.

4 Ransomware Kill Chain – Initiële toegang

1. Phishing

2. Remote Desktop Protocol

3. Credential stuffing/reuse

4. Derde partijen

5. Insider threats

6. Social engineering

Voor het verkrijgen van initiële toegang en het behouden van permanente toegang (persistence) worden hoofdzakelijk 6 manieren ingezet door IAB's en ransomware groepen. Voor initiële toegang wordt gebruik gemaakt van gecompromitteerde doorstuur infrastructuur (zoals botnets) om de oorsprong en identiteit van de aanvallers te verbergen. Op de volgende pagina's is ingezoomd op de maatregelen die je kunt treffen voor preventie, detectie en reactie.

Phishing aanvallen (T1566) in relatie tot ransomware leveren vaak niet de ransomware zelf af, maar zogenaamde payloads. Payloads stellen de aanvallers in staat om de omgeving te verkennen en bijvoorbeeld het binnenhalen van een loader (zoals Trickbot). Bijvoorbeeld het als bijlagen toevoegen van Microsoft Office macro's of (Java)script bestanden aan e-mails. Met een loader kunnen zij hands-on toetsenbord controle krijgen over een apparaat en vanuit die positie vervolgstappen bepalen.

Toegang tot een RDP-server is goud waard voor cybercriminelen omdat zij het netwerk hebben weten te infiltreren, de toegang kunnen verkopen of zelfs direct kunnen gebruiken om ransomware te installeren. Er zijn naast RDP ook andere oplossingen waar cybercriminelen in geïnteresseerd zijn om toegang op afstand te bewerkstellingen, zoals Citrix, TeamViewer, VNC of VPN-verbindingen (T1133).

Ransomware groepen vallen niet zozeer specifieke organisaties aan, maar bepaalde (kwetsbare) technologieën aan (T1190). Dit doen zij bijvoorbeeld via kwetsbaarheden scans of credential stuffing aanvallen waarbij uitgelekte en/of standaard wachtwoorden vanaf verschillende (gecompromitteerde) computers geprobeerd worden (T1110).

Derde partijen worden bijvoorbeeld misbruikt om getrojaniseerde software af te leveren, zoals met malware geïnfecteerde antivirussoftware of geïnfecteerde advertenties op websites (T1189 & T1195). Ook de toegang van derde partijen tot interne netwerken van doelwitten is aantrekkelijk voor ransomware groepen (T1199 & T1078).

Een dreiging die zijn oorsprong heeft binnen een organisatie wordt een insider threat genoemd. Bijvoorbeeld doordat medewerkers, oud-medewerkers en leveranciers bij informatie kunnen komen. Of doordat zij weten hoe zaken zijn beveiligd. Er is sprake van een insider threat als zo'n (oud-)medewerker of leverancier zijn positie misbruikt voor kwaadwillende activiteiten. IAB's en ransomware groepen bieden soms geld aan medewerkers voor toegang tot een bepaalde organisatie.

Social engineering is een verzamelnaam voor technieken waarbij geprobeerd wordt mensen onveilige handelingen te laten verrichten. Het bekendste voorbeeld daarvan is phishing, maar er zijn ook andere technieken die ingezet worden zoals vishing, QRishing, spearphishing, whaling en tailgating. Social engineering wordt niet apart behandeld aangezien dit samengevoegd is met phishing.

4.1 Phishing

PREVENTIE	DETECTIE	REACTIE
☐ Blokkeer macro's in Active Directory Group Policy Object (GPO) voor gebruikersgroepen die macro's niet nodig hebben ☐ Maak gebruik van blocklists en blokkeer veel misbruikte bestandsextensies ☐ Monitor de registratie en wijzigingen aan typosquat domeinen ☐ Implementeer phishing-bestendig MFA (Yubikey, passkeys) ☐ Implementeer de e-mail beveiligingsstandaarden (SPF, DKIM, DMARC, MTA-STS, etc.) en verifieer of deze correct geïmplementeerd zijn via de IV-metingen van SURF ☐ Implementeer (extended) endpoint protection & response op alle werkplekken en servers ☐ Stel in beleid en procedures vast dat intern nooit via links, QR-codes of bijlagen in e-mails gevraagd wordt om ergens in te loggen, oftewel, alle verzoeken die daar betrekking op hebben dienen gemeld en genegeerd te worden. ☐ Implementeer applicatie allowlisting ☐ Gebruik e-mail filtering SURFmailfilter ☐ Implementeer de Clear-Site-Data header om sessiecookies uit de lokale opslag te verwijderen (tegen infostealers) ☐ Schakel ActiveX in Office bestanden en het automatisch afspelen ('AutoPlay') uit	☐ Mails afkomstig van of links naar typosquat domeinen ☐ Monitor de registratie en het gebruik van typosquat domeinen ☐ Maak voor gebruikers duidelijk dat berichten afkomstig zijn van buiten de organisatie, van onbekende of look-a-like afzenders ☐ Gebruik van veel redirects via links ☐ Notificeer medewerkers en studenten over succesvolle inlogpogingen (van nieuwe locaties of apparaten) en wijzigingen aan het account (bijvoorbeeld wachtwoord gewijzigd) ☐ Implementeer URL (link) analyse zoals Microsoft Safelinks ☐ Monitor op door SURFcert gedeelde Indicators of Compromise (IoC) en Indicators of Attack (IoA) ☐ Controleer de eindbestemming van ontvangen (verkorte) links, bijvoorbeeld via Checkjelinkje ☐ Monitor databases met bekende phishing praktijken zoals bijvoorbeeld Phishtank	☐ Blokkeer tijdelijk accounts die (mogelijk) gecompromitteerd zijn of reset de credentials ☐ Maak gebruik van een sandbox voor het analyseren van bijlagen en het identificeren van IoC's (zie hieronder) ☐ Ga op zoek naar unieke identifiers die je kunt gebruiken om vergelijkbare berichten te blokkeren, bijvoorbeeld IP-adressen van de afzender, domeinnamen, URL's, e-mailadressen of unieke kenmerken in de body van het bericht (zoals een cryptocurrency wallet adres of dreigbericht) ☐ Blokkeer IOC's in DNS, firewalls en proxies (zowel inkomend als uitgaand) ☐ Meld het bericht als spam/phishing aan SURFcert ☐ Stel vast hoeveel personen een identiek of vergelijkbaar bericht hebben ontvangen (mail logs) en verwijder ze uit de mailboxen om incidenten te voorkomen ☐ Volg de adviezen van leveranciers en SURFcert op voor het bestrijden van specifieke phishing aanvallen ☐ Maak een melding van misbruik bij de registrar(s) en/of hostingpartijen om de domeinen en website(s) offline te laten halen en/of op een blocklist te laten plaatsen ☐ Behoed medewerkers en studenten voor phishing aanvallen, bijvoorbeeld via interne communicatiemiddelen zoals intranet, chat of SMS

4.2 Remote Desktop Protocol (RDP)

PREVENTIE	DETECTIE	REACTIE
☐ Overweeg om helemaal geen gebruik te maken van RDP, maar stel het niet direct bloot aan het internet als dat kan. Maak gebruik van een VPN met MFA of SSH met public key cryptografie ☐ Wijzig de standaard poort (3389) voor RDP zodat uit poortscans niet direct duidelijk is dat RDP gebruikt wordt ☐ Zorg ervoor dat alle RDP logging is geactiveerd ☐ Hanteer het least privilege principe voor RDP-accounts en evalueer ze regelmatig ☐ Dwing MFA af voor alle RDP-servers ☐ Limiteer de geografische IP-adressen die verbinding mogen maken met de RDP-servers ☐ Overweeg het blokkeren van toegang tot RDP door bekende ranges IP-adressen van VPN-providers ☐ Voorkom de top 10 misconfiguraties in netwerken (onder andere adequaat patchmanagement toepassen) ☐ Algemeen: verricht regelmatig geautomatiseerd kwetsbaarhedenscans (intern & extern) ☐ Algemeen: implementeer een coordinated vulnerability disclosure beleid ☐ Algemeen: Voer regelmatig pentesten of red/purple team oefeningen uit ☐ Algemeen: implementeer een web application firewall op publieke webservers	☐ Verricht regelmatig actieve en passieve scans op het eigen netwerk (intern en extern) om de aan het internet blootgestelde RDP-servers en overige (Remote Management) assets en services te identificeren ☐ Algemeen: zorg ervoor dat alle logging op een centrale plek verzameld, geanalyseerd en gecorreleerd wordt ☐ Monitor mislukte inlogpogingen op RDP-servers en beschouw gebeurtenissen van deze servers als hoge prioriteit in SIEM/SOC oplossingen (SURFsoc) ☐ Volg de kwetsbaarhedenmeldingen van SURFcert en overige bronnen nauwlettend om misbruik te voorkomen (bijv. door threat hunting IoC's, patchen of compenserende maatregelen) ☐ Implementeer een honeypot (fake attack surface)	☐ Blokkeer automatisch IP-adressen (tijdelijk) in de firewall bij meerdere mislukte inlogpogingen op RDP-servers ☐ Analyseer de logging op verdachte loginpogingen en stel vast of er sprake is van ongeautoriseerde toegang ☐ Blokkeer (tijdelijk) de toegang tot RDP-accounts wanneer er (vermeend) misbruik is gemaakt ☐ Blokkeer uitgaand verkeer in de firewall naar IP-adressen van het vermeende misbruik. Ransomware groepen maken gebruik van gecompromitteerde infrastructuur waardoor het effect hiervan beperkt kan zijn en continu veranderd ☐ Algemeen: overweeg het afsluiten van een retainer met een gespecialiseerde partij in incident response en forensics ☐ Algemeen: probeer de rootcause van incidenten te achterhalen en onmiddellijk op te lossen

4.3 Credential stuffing/reuse

PREVENTIE	DETECTIE	REACTIE
☐ Wijzig altijd standaard credentials en neem dit op in de change- en configuratie- procedures. Verifieer altijd of ze daadwerkelijk zijn aangepast ☐ Sta niet toe dat (uitgelekte en/of zwakke) wachtwoorden (her)gebruikt worden ☐ Stel een wachtwoordmanager met MFA beschikbaar om het gebruik van sterke en unieke logingegevens te stimuleren ☐ Maak daar waar mogelijk gebruik van SSO (SURFconext), passkeys en biometrie voor authenticatie ☐ Stel automatische lock-out policies in bij het meermaals falen van loginpogingen om het raden en proberen van wachtwoorden te dwarsbomen. Test of deze policies daadwerkelijk geïmplementeerd en effectief zijn ☐ Gebruik daar waar mogelijk MFA om de kans op succes van brute force en/of credential stuffing aanvallen te verkleinen ☐ Implementeer netwerkfiltering om het netwerkverkeer tussen bepaalde hosts, locaties, netwerken en netwerksegmenten te beperken (ook binnen segmenten) ☐ Implementeer conditionele toegang om het lastiger voor aanvallers te maken om ongeautoriseerd toegang te verkrijgen tot accounts vanaf onbekende apparaten en afwijkende locaties ☐ Algemeen: stel services alleen direct aan het internet bloot als dat noodzakelijk is	☐ Monitor op uitgelekte credentials voor domeinen in beheer van de instelling, bijvoorbeeld via HIBP en Darkweb monitoring ☐ Monitor applicatie- en systeem logs op hoge frequenties van falende loginpogingen. Dit kan een indicatie van een brute force of credential stuffing aanval zijn ☐ Monitor falende loginpogingen verspreid over meerdere accounts en systemen. Dit kan een indicatie van een brute force of credential stuffing aanval zijn ☐ Meldingen van medewerkers of studenten dat er succesvol is ingelogd op hun account(s) door iemand anders	☐ Isoleer de oorsprong van de aanval door bijvoorbeeld het apparaat te isoleren, het (lokale) IP-adres te blokkeren in de firewall of DNS-sinkholing toepassen ☐ Blokkeer tijdelijk accounts die (mogelijk) gecompromitteerd zijn of reset de credentials (let op: KRBTG service-account 2x resetten noodzakelijk) ☐ Analyseer logging om vast te stellen of en welke systemen en apparaten gecompromitteerd zijn

4.4 Derde partijen

PREVENTIE	DETECTIE	REACTIE
☐ Maak onderscheid tussen de verschillende beveiligingsniveaus binnen het IT-landschap voor geprivilegieerde toegang, waarbij in ieder geval een logisch onderscheid wordt gemaakt tussen endpoints, netwerktoegangslaag, netwerkkern, serverbeheerder en domeinbeheerder. ☐ Derde partijen die administratieve handelingen moeten verrichten in de IT-infrastructuur van de instelling dienen via jumpservers te authentiseren naar beveiligde zones ☐ Hanteer voor accounts gekoppeld aan derde partijen ook het least privilege principe en controleer dit regelmatig ☐ Dwing MFA af voor alle accounts gekoppeld aan derde partijen ☐ Beperk de toegang door derde partijen in de firewall door bijvoorbeeld het allowlisten van bepaalde IP-adressen of -ranges van de leverancier ☐ Blokkeer automatisch accounts gekoppeld aan derde partijen na inactiviteit van 45 dagen ☐ Zorg voor een actueel en volledig overzicht van cybersecurity contactgegevens van relevante derde partijen en zorg dat deze op verschillende plekken beschikbaar zijn ☐ Algemeen: voorkom veelvoorkomende kwetsbaarheden in websites en applicaties (OWASP top 10) en controleer dat regelmatig	☐ Controleer de integriteit van software(-updates) door het verifiëren van de hashes ☐ Monitor gefaalde en opvallende inlogpogingen (bijv. 's nachts of vanaf vreemde locaties) op accounts gekoppeld aan derde partijen ☐ Controleer regelmatig of er nieuwe accounts zijn aangemaakt of wijzigingen zijn aangebracht aan accounts gekoppeld aan derde partijen ☐ Volg de kwetsbaarhedenmeldingen van SURFcert en overige bronnen nauwlettend (bijv. door threat hunting IoC's, patchen of compenserende maatregelen)	☐ Neem direct contact op met de derde partijen waarvoor de accounts zijn bedoeld om misbruik te kunnen bevestigen of uitsluiten ☐ Blokkeer tijdelijk accounts die (mogelijk) gecompromitteerd zijn of reset de credentials ☐ Stel vast of er geldige sessies zijn en beëindig deze per direct ☐ Review alle (geprivilegieerde) handelingen van de accounts in kwestie van de afgelopen periode

4.5 Insider threats

PREVENTIE	DETECTIE	REACTIE
☐ Zorg ervoor dat accounts en handelingen altijd herleidbaar zijn naar unieke personen (onweerlegbaarheid/non-repudiation) ☐ Hanteer het least privilege principe en controleer dit regelmatig ☐ Hanteer het 4-ogen principe (functiescheiding) voor kritieke processen en -handelingen om te voorkomen dat één persoon veel schade kan aanrichten ☐ Informeer medewerkers dat het gebruik van hun accounts en de handelingen die zij verrichten (tijdelijk) worden opgeslagen en gemonitord en dat daar vragen over gesteld kunnen worden ☐ Trek direct alle toegangsrechten in zodra een medewerker vertrekt ☐ Houd medewerkers tevreden en realiseer een prettige organisatiecultuur (stress, werkdruk, secundaire arbeidsvoorwaarden, etc.) ☐ Implementeer Data Loss Prevention (DLP) ☐ Implementeer port-based Network Access Control (NAC) 802.1x ☐ Overweeg browser sandboxing ☐ Overweeg het dichtzetten van USB-poorten of het blokkeren van USB-opslag voor gebruikers die dit niet nodig hebben ☐ Overweeg browser extensies die de beveiliging bevorderen, zoals UBlock Origin en Ghostery	☐ Overweeg taakroulatie en verplicht dat medewerkers op vakantie gaan zodat anderen tijdelijk hun werkzaamheden over moeten nemen om potentieel misbruik te kunnen detecteren ☐ Het (geautomatiseerd) monitoren van logging ten behoeve van de detectie van anomalieën ☐ Monitor afwijkend gedrag ten opzichte van anderen, bijvoorbeeld 's nachts of in de weekenden ☐ Monitor en identificeer gebruikers die informatie opzoeken of manipuleren buiten hun reguliere permissies ☐ Stel alerts in voor grote hoeveelheden downloads, bestandsoverdrachten en andere vormen van exfiltratie ☐ Het downloaden of installeren van ongeautoriseerde software ☐ Het gebruik van TOR op managed apparaten ☐ Pogingen om beveiligingsmaatregelen te omzeilen ☐ Ongeautoriseerde wijzigingen aan bestanden en/of configuraties	☐ Betrek personeels- en juridische zaken bij het incident ☐ Direct blokkeren van de betrokken accounts en het beëindigen van alle lopende sessies totdat zekerheid is verkregen over de verrichte handelingen (misbruik of legitiem) ☐ Review alle (geprivilegieerde) handelingen van de persoon in kwestie van de afgelopen periode ☐ Neem apparatuur van de persoon in kwestie (tijdelijk) in beslag ☐ Het indien nodig veilig (laten) stellen van bewijslast ☐ Tref disciplinaire maatregelen volgens het beleid van de instelling ☐ Doe aangifte bij de politie bij vastgesteld misbruik

5 Ransomware Kill Chain – Verkenning & Lateraal bewegen

1. Verkenning

2. Permanente toegang

3. Escaleren van rechten

4. Lateraal bewegen

Zodra initiële toegang is verkregen wordt het netwerk verder verkend en wordt geprobeerd de toegang te verkrijgen die noodzakelijk is om de ransomware uit te rollen. Dit betekent onder andere het verkrijgen van initiële- en permanente toegang tot andere systemen binnen het netwerk. Ransomware actoren maken hierbij vaak gebruik van Cobalt Strike en 'Living of the Land (LotL)' tools[1], zoals net[2], ping[3], whoami[4], systeminfo[5], lsass[6] en WMIC[7].

De aanvallers proberen permanente toegang tot de IT-infrastructuur te behouden (persistence). Dit doen zij door bijvoorbeeld geplande taken (T1053) toe te voegen of opstartscripts te wijzigen (T1037). Voor de permanente toegang wordt gebruik gemaakt van Command & Control (C2) infrastructuur (TA0011). Door middel van beacons worden regelmatig signalen verzonden naar de C2 infrastructuur en kunnen de aanvallers bijvoorbeeld bestanden up- en downloaden (T1071.002).

Zodra de cybercriminelen hun toegang hebben weten te behouden, willen zij hun rechten escaleren om de ransomware op zoveel mogelijk systemen los te kunnen laten. Tools zoals Mimikatz voor het 'dumpen' van credentials uit het geheugen (lokaal escaleren van rechten) of BloodHound voor het bepalen van de kortste route naar de Domain Controller worden vaak gebruikt om het meest gunstige aanvalspad te kunnen bepalen.

Het gecompromitteerde systeem in combinatie met de lokaal geëscaleerde rechten worden misbruikt om andere systemen te benaderen (pivoting). Veelgebruikte tools voor het lateraal bewegen (horizontaal en verticaal) zijn: AdRecon, WMIC, MetaSploit, AdFind, Lazagne, Bloodhound, PowerSploit, Mimikatz, PSExec/, LOLBins, Advanced IP Scanner. GMER, ProcessHacker en TDSSKiller worden gebruikt om beveiligingsmaatregelen uit te schakelen. Remote control tools worden ook gebruikt zoals Remote Desktop Protocol (RDP), TeamViewer, AnyDesk, ScreenConnect, etc. De focus van laterale beweging ligt voornamelijk op servers (Linux, Windows, ESXi) en de domain controller.

[1] LotL-tools zijn tools die aanwezig zijn op besturingssystemen en daardoor minder opvallen dan wanneer er bijvoorbeeld tools van derde partijen gebruikt worden.

[2] Netwerkinstellingen van het systeem bekijken en bijwerken

[3] Bereikbaarheid van andere systemen testen

[4] Tonen van de gebruikersnaam van de huidige gebruiker op het systeem

[5] Toont informatie over de computer, systeem- en beveiligingsinstellingen

[6] Handhaaft beveiligingsbeleid op Windows systemen

[7] De command-line versie van Windows Management Instrumentation (WMI) dat wordt gebruikt om administratieve taken op Windows systemen uit te voeren, inclusief het uitvoeren van bestanden

5.1 Verkenning

PREVENTIE	DETECTIE	REACTIE
☐ Probeer normaal gedrag van LotL-tools te begrijpen/definiëren zodat afwijkend gedrag opvalt en (beter) gedetecteerd kan worden ☐ Sta geen communicatie tussen werkplekken toe ☐ Zorg ervoor dat onnodige poorten en services zijn uitgeschakeld of geblokkeerd om het verkenningsproces te bemoeilijken ☐ Implementeer een Network IDS/IPS ☐ Implementeer netwerksegmentatie (zie top 10 misconfiguraties in netwerken) ☐ Gebruik alleen SMB v3.1.1, implementeer SMB-signing, SMB over QUIC (TLS) en blokkeer onnodig SMB-verkeer ☐ Gebruik de *FileBlockExecutable* optie in Sysmon ☐ Ontwikkel en update regelmatig netwerk- en datastroom diagrammen t.b.v. threat modeling, bijvoorbeeld via OWASP Threat Dragon ☐ Maak verantwoord gebruik van PowerShell	☐ Monitor commando's, API-calls en nieuwe processen die gericht zijn op het enumereren van gedeelde netwerkschijven ☐ Host identificatie, poort- en servicescans vanaf interne IP-adressen / binnen een subnet ☐ Implementeer proces monitoring (parent-child relatie) om anomalieën te detecteren in processen ☐ Het gebruik van webshells (PHP, JSP, ASP, Python, PowerShell[8], etc.) voor command & control doeleinden ☐ Tunneling (bijv. RDP over HTTPS om detectie te vermijden) ☐ Uploaden van tools, scripts en bestanden via webshells, analyseer logging om vast te stellen of er vanaf externe IP-adressen bestanden worden geüpload ☐ Stel alerts in voor poortscans die vanaf interne IP-adressen uitgevoerd worden ☐ Stel alerts in voor het op ongebruikelijke wijze gebruiken van protocollen zoals SMB, RDP of SecureShell (SSH) ☐ Gebruik Sysmon ☐ Implementeer een honeypot (fake attack surface) ☐ SIEM/SOC alerts ☐ Kijk voor meer aanvullende detectie-mogelijkheden naar de adviezen van MITRE ATT&CK	☐ Isoleer machines die verkennings-activiteiten vertonen ☐ Wis alle gecompromitteerde systemen en bouw deze volledig opnieuw op (of vervang de hardware) om eventuele gemiste malware, webshells, etc. te elimineren

[8] Overweeg aanvullende logging: Module logging, Script-Block en Transscript logging

5.2 Permanente toegang

PREVENTIE	DETECTIE	REACTIE
☐ Implementeer een Endpoint Detection & Response oplossing, bij voorkeur met geautomatiseerd isoleren, op alle beheerde werkplekken en servers ☐ Hanteer een deny-by-default beleid in de firewall voor zowel inkomend als uitgaand netwerkverkeer ☐ Geef altijd prioriteit aan het patchen van systemen die direct aan het internet zijn blootgesteld ☐ Harden het gebruik van PowerShell via GPO's, verwijder het van machines die het niet nodig hebben, limiteer het gebruik tot beheerders, harden de beveiligings-instellingen en leg restricties op voor commando's ☐ Implementeer applicatie allowlisting, bijvoorbeeld via Windows Defender Application Control (WDAC) of AppLocker ☐ Implementeer DNS-filtering ☐ Implementeer webfiltering, bijvoorbeeld via een proxy	☐ Wijzigingen aan geplande taken (scheduled tasks) ☐ Wijzigingen aan services (creation, replacement) ☐ Wijzigingen aan registersleutels ☐ Wijzigingen aan (het laden van) Dynamic-link Library (DLL) bestanden ☐ Monitor (wijzigingen aan) Windows event logs, SMB logs, PowerShell logs, RDP logs en authenticatielogs ☐ Inspecteer netwerkschijven op vreemde bestanden ☐ Inspecteer de webserver logs voor verdacht inkomend en uitgaand verkeer en let op vreemde bestandsnamen (bijv. updates.php). Vergelijk de bestandsnamen en hun locatie met de golden images om afwijkingen vast te stellen ☐ SIEM/SOC alerts ☐ Monitor op het uitschakelen of deinstalleren van belangrijke applicaties zoals Endpoint Detection & Response (EDR) ☐ Server-side: kijk bij Sessions en bij Open Files en controleer verbonden systemen en gebruikers ☐ Kijk voor meer aanvullende detectie-mogelijkheden naar de adviezen van MITRE ATT&CK	☐ Isoleer indien mogelijk de geïnfecteerde systemen (bijvoorbeeld via EDR-oplossingen of koppel ze los van het netwerk) ☐ Verwijder de malware van de geïnfecteerde systemen ☐ Verwijder tijdelijk alle rechten van de bij het incident betrokken accounts ☐ Identificeer de IoC's en scan de rest van het netwerk daarop ☐ Wis alle geïnfecteerde systemen en bouw ze volledig opnieuw op of vervang de hardware ☐ Gebruik Linux Incident Response commando's ☐ Gebruik tools om een tijdlijn van de gebeurtenissen te maken zoals bijvoorbeeld Log2timeline

5.3 Lateraal bewegen

PREVENTIE	DETECTIE	REACTIE
☐ Implementeer netwerksegmentatie, een zero-trust architectuur en voorkom misconfiguraties in netwerken (zie de top 10 misconfiguraties in netwerken) ☐ Harden de (Entra) Active Directory en los beveiligingsproblemen op, bijvoorbeeld met Pingcastle of best practices voor het beveiligen van Active Directory ☐ Harden Microsoft Azure met behulp van de NBA policy template ☐ Los beveiligingsproblemen voor gedeelde netwerkschijven op (NFS open share scanner & SMB scanner) ☐ Implementeer Local Administrator Password Solution (LAPS) ☐ Implementeer Attack Surface Reduction (ASR) voor LSASS ☐ Implementeer Credential Guard voor Windows 10 en Server 2016 ☐ Schakel Windows Script Host (WSH) uit ☐ Log het verkeer tussen servers in dezelfde segmenten ☐ Gebruik een oplossing die weet wat normaal is voor het netwerk ☐ Gebruik aparte AD domeinen (forest/tree) voor verschillende beveiligingsniveaus ☐ Maak gebruik van de Protected Users AD groep om pass-the-hash aanvallen te bemoeilijken	☐ Het uitschakelen van virtuele machines ☐ Detectie van named pipes (bijv. postex_*, *-server, status_*) ☐ Zorg voor detectieregels (YARA/SIGMA[9]) voor veelgebruikte tools door aanvallers zoals AdFind, AdRecon, Mimikatz, etc. ☐ Implementeer een honeypot (vals aanvalsoppervlak) ☐ Maak gebruik van honeyfiles zoals Canarytokens ☐ Communicatie tussen endpoints ☐ Communicatie tussen servers ☐ SIEM/SOC alerts ☐ Kijk voor meer aanvullende detectie-mogelijkheden naar de adviezen van MITRE ATT&CK	☐ Isoleer indien mogelijk de geïnfecteerde systemen (bijvoorbeeld via EDR-oplossingen of koppel ze los van het netwerk) ☐ Verwijder de malware van de geïnfecteerde systemen ☐ Verwijder tijdelijk alle rechten van de bij het incident betrokken accounts ☐ Identificeer de IoC's en scan de rest van het netwerk daarop ☐ Wis alle geïnfecteerde systemen en bouw ze volledig opnieuw op of vervang de hardware

[9] Bijvoorbeeld via: https://valhalla.nextron-systems.com/ & https://github.com/SigmaHQ/sigma

5.4 Escaleren van rechten

PREVENTIE	DETECTIE	REACTIE
☐ Implementeer een Endpoint Detection & Response oplossing, bij voorkeur met geautomatiseerd isoleren, op alle beheerde werkplekken en servers ☐ Hanteer het least privilege principe ☐ Zie de top 10 misconfiguraties in netwerken ☐ Installeer geen extra software op domain controllers en verwijder software die niet nodig is ☐ Schakel onnodige services uit op domain controllers en andere servers en schakel de print spooler service uit op domain controllers ☐ Blokkeer internetconnectiviteit op de domain controllers (updates via WSUS) ☐ Overweeg op Windows servers extra Local Security Authority (LSA) beveiliging in te voeren	☐ Zorg voor detectieregels (YARA/SIGMA[10]) voor veelgebruikte tools door aanvallers zoals Mimikatz, Sysinternals, ProcDump, NTDSutil.exe, etc. ☐ EDR/SIEM/SOC alerts	☐ Isoleer indien mogelijk de geïnfecteerde systemen (bijvoorbeeld via EDR-oplossingen of koppel ze los van het netwerk) ☐ Verwijder de malware van de geïnfecteerde systemen ☐ Verwijder tijdelijk alle rechten van de bij het incident betrokken accounts ☐ Identificeer de IoC's en scan de rest van het netwerk daarop ☐ Wis alle geïnfecteerde systemen en bouw ze volledig opnieuw op of vervang de hardware

[10] Bijvoorbeeld via: https://valhalla.nextron-systems.com/ & https://github.com/SigmaHQ/sigma

6 Ransomware Kill Chain – Exfiltratie

Tijdens deze fase gaan de aanvallers op zoek naar gevoelige informatie van slachtoffers met als doel het stelen (exfiltreren) daarvan om als extra afpersingsmethode tegen de slachtoffers te kunnen gebruiken. Hierbij wordt gezocht aan de hand van bepaalde zoektermen en/of bestandstypen.

1. Vinden gevoelige informatie

Aanvallers vinden gevoelige informatie bijvoorbeeld door het enumereren van netwerkschijven en open shares (SMB/NFS) (T1021.002). Daarbij gaan ze opzoek naar specifieke informatie zoals financiële gegevens, klant- en medewerkersgegevens en projectgegevens (TA0009). Deze informatie heeft immers waarde voor het slachtoffer en kan daarom als extra drukmiddel gebruikt worden.

2. Exfiltreren gevoelige informatie

De aanvallers gebruiken verschillende tools om gevoelige informatie te stelen, zoals Rclone, WinSCP, StealBIT, MegaSYNC, 7-zip en legitieme clouddiensten zoals OneDrive, Google Drive of WeTransfer (TA0010). Rclone is met name populair omdat dit vaak gebruikt wordt door systeembeheerders en daarom geen alerts oplevert.

6.1 Vinden en exfiltreren van gevoelige informatie

PREVENTIE	DETECTIE	REACTIE
☐ Plaats Canary tokens op plekken met gevoelige informatie zodat beheerders een notificatie ontvangen zodra dergelijke bestanden worden geopend of bewerkt ☐ Implementeer Data Loss Prevention (DLP) ☐ Zie voorgaande pagina's	☐ Alerts van Canary tokens ☐ Alerts van honeypots ☐ Verkeer naar bekende C2 servers ☐ Aanwezigheid en/of gebruik van Rclone, Rsync, StealBIT, 7-zip, WinSCP of MEGAsync ☐ Gebruik van SFTP/FTP ☐ SIEM/SOC alerts ☐ Grote hoeveelheden informatie wordt gedownload of geüpload	☐ Blokkeer de toegang tot of isoleer de lekkende URI, -server, -machine via netwerkinfrastructuur ☐ Herstel informatie en systemen via backups ☐ Verifieer aan de hand van logging of en welke informatie is gestolen en waarnaartoe

7 Ransomware Kill Chain – Uitrollen

Nadat de aanvallers de gevoelige informatie hebben gestolen en de benodigde rechten hebben verkregen om de ransomware door het netwerk te verspreiden, start de voorbereiding voor het daadwerkelijk uitrollen van de ransomware.

1. Backups manipuleren

De eerste stap is dat aanvallers de backups vinden en die proberen te versleutelen of te vernietigen (T1490). Dit is dan ook de reden waarom het cruciaal is dat backups niet vanaf het interne netwerk toegankelijk en manipuleerbaar zijn, want als er geen backups zijn kan er ook geen herstel plaatsvinden.

2. Testen ransomware

Na het versleutelen of verwijderen van backups rollen de aanvallers de ransomware op een klein aantal systemen uit om vast te stellen of alles werkt naar behoren. Bijvoorbeeld dat andere machines geïnfecteerd kunnen raken, er geen security alerts afgaan of dat de ransomware code wordt geblokkeerd.

3. Ransomware uitrollen & afpersingsbericht

Nadat het testen van de ransomware succesvol is gebleken kan worden overgegaan tot het uitrollen van de ransomware in het netwerk (T1486). Aanvallers gebruiken hierbij verschillende tools, zoals .bat bestanden, PsExec scripts die via Server Message Block (SMB) andere machines infecteren, Group Policy Object (GPO) om de ransomware vanuit de domain controller te pushen naar systemen en System Center Configuration Manager (SCCM) of andere Remote Monitoring and Management (RMM) tools. Ook worden Shadow copies verwijderd om het snel kunnen herstellen van belangrijke bestanden te voorkomen. Zodra de ransomware succesvol is uitgerold krijgen de slachtoffers een afpersingsbericht (via printers) te zien waarin gevraagd wordt om losgeld te betalen met een deadline.

7.1 Backups manipuleren

PREVENTIE	DETECTIE	REACTIE
☐ Zorg ervoor dat backups op een andere locatie/infrastructuur en/of offline versleuteld worden opgeslagen om te voorkomen dat deze ook geïnfecteerd raken (3-2-1 regel) ☐ Zorg ervoor dat de integriteit van backups niet aangetast kan worden (immutable) ☐ Zorg ervoor dat de frequentie van backups in lijn is met de door de instelling vastgestelde beschikbaarheidseisen (RPO, RTO) ☐ Controleer automatisch of backups zijn geslaagd en controleer regelmatig of backups succesvol teruggeplaatst kunnen worden ☐ Ontwikkel en sla 'golden images' van kritieke servers veilig op. Golden images zijn geconfigureerde versies van het besturingssysteem inclusief alle geïnstalleerde applicaties op de betreffende server	☐ Verwijderen van shadow copies of shadow storage (bijvoorbeeld via bcdedit.exe, fsutilexe, vssadmin.exe, wbadmin.exe en wmic.exe) ☐ Verwijderen of versleutelen van backups ☐ Manipuleren of verwijderen van (backup) logs ☐ EDR alerts ☐ SIEM/SOC alerts	☐ Systemen, netwerken automatisch (SOAR) of handmatig isoleren (bijvoorbeeld via EDR-oplossingen of koppel ze los van het netwerk) ☐ Verwijder de malware van de geïnfecteerde systemen ☐ Verwijder tijdelijk alle rechten van de bij het incident betrokken accounts ☐ Identificeer de IoC's en scan de rest van het netwerk daarop

7.2 Testen ransomware

PREVENTIE	DETECTIE	REACTIE
☐ Zie voorgaande pagina's	☐ EDR, SIEM/SOC alerts ☐ Het uitschakelen van beveiligingssoftware zoals EDR op endpoints ☐ Gebruik SMB, SCCM, GPO of andere RMM-tools om ransomware te verspreiden naar andere systemen ☐ Ransomware notes op bureablad	☐ Systemen, netwerken automatisch (SOAR) of handmatig isoleren (bijvoorbeeld via EDR-oplossingen of koppel ze los van het netwerk) ☐ (Draadloze) netwerksegmenten loskoppelen van de rest en het internet (via netwerkapparatuur of kabels loskoppelen)

7.3 Ransomware uitrollen

PREVENTIE	DETECTIE	REACTIE
☐ Zie voorgaande pagina's	☐ Bestanden hebben een vreemde extensie gekregen zoals: .xyz, .abc, .locky, .locked, .encrypted, etc. ☐ Bestanden worden in een rap tempo gemanipuleerd (versleuteld) ☐ Het gebruik van scripts via de Domain Controller om beveiligingssoftware uit te schakelen, stoppen van services die encryptie van bestanden tegenhouden, het wissen van logs en het uitrollen van ransomware ☐ Het verwijderen van alle shadow copies (via vssadmin.exe, WMIC en PowerShell) ☐ Het verwijderen van Windows Event logs ☐ Portable Executables (PE) die het volgende gedrag vertonen: enumereren van lokale- en gedeelde (netwerk)schijven, het stoppen van beveiligingssoftware, het importeren public keys voor encryptie, het aanpassen van de bureablad achtergrond met een ransomware notitie ☐ EDR alerts ☐ SIEM/SOC alerts	☐ Schakel SURFcert direct in ☐ Schakel de retainer in (indien van toepassing) ☐ Identificeer de scope van de infectie met behulp van EDR- en threat hunting oplossingen (YARA/SIGMA/DFIR) ☐ Isoleer de bron van de ransomware infectie (initiële toegang/pivoting) of isoleer segmenten (via netwerk-apparatuur) ☐ Blokkeer in- en uitgaand C2 verkeer ☐ Blokkeer encryptieprocessen op basis van hun hash op andere systemen ☐ Blokkeer alle IP-adressen die (mogelijk) gebruikt worden door de aanvallers ☐ Blokkeer alle accounts die misbruikt worden ☐ Koppel gedeelde netwerkschijven los ☐ Koppel eventueel geïnfecteerde computers los van het netwerk om verdere verspreiding te voorkomen ☐ Wis alle geïnfecteerde systemen en bouw ze volledig opnieuw op of vervang de hardware ☐ Kijk op nomoreransom.org of er een decryptiesleutel beschikbaar is voor de variant van de ransomware-infectie. Verifieer of systemen daadwerkelijk schoon zijn voordat ze weer aan het netwerk worden verbonden ☐ Herstel bestanden en configuraties vanaf backups

8 Ransomware Kill Chain – Afpersing

Er is tegenwoordig sprake van viervoudige afpersing van slachtoffers die geïnfecteerd zijn geraakt met ransomware. Hieronder is nader toegelicht welke soorten afpersing worden toegepast.

1. Versleutelen informatie

De eerste afpersingsmethode is het versleutelen van informatie zodat slachtoffers er niet meer bij kunnen. Als slachtoffers een goede backup strategie hebben en bestanden en systemen daarmee kunnen herstellen hoeft er niet betaald te worden.

2. Publiceren gestolen informatie

De tweede afpersingsmethode omvat het (dreigen met het) publiceren of verkopen van gestolen informatie. Dit doen zij via leksites op het darkweb, vaak gepaard met een afteltimer en enkele voorbeelden van gestolen documenten of mappenstructuren. Daarmee bewijzen de aanvallers dat zij beschikken over gevoelige informatie van het slachtoffer. Zodra de gestolen informatie gepubliceerd wordt, kan iedereen deze inzien, downloaden, doorverkopen en misbruiken.

3. Uitvoeren aanvullende cyberaanvallen

De derde afpersingsmethode omvat het (dreigen met het) uitvoeren van aanvullende cyberaanvallen zoals DDoS-aanvallen, waardoor de continuïteit verstoord kan worden (T1498).

4. Afpersen of overtuigen van relaties van het slachtoffer

De vierde afpersingsmethode omvat het afpersen van klanten of relaties van het slachtoffer. Er zijn zelfs voorbeelden waarbij de aanvallers contact hebben opgenomen met verzekeringsmaatschappijen of toezichthouders om hen te informeren over het niet nakomen van (wettelijke) afspraken, zoals het tijdig melden van incidenten.

8.1 Afpersingstechnieken

PREVENTIE	DETECTIE	REACTIE
☐ Zorg voor anti-DDoS maatregelen voor kritieke netwerken en -bedrijfsmiddelen, bijvoorbeeld via SURF ☐ Laat ook verkeer naar externe leveranciers van websites via het SURF-netwerk lopen door middel van een proxy ☐ Zie de voorgaande pagina's	☐ Meldingen van SURFcert, SIEM/SOC ☐ Monitor leksites en Telegram kanalen van ransomware groepen, bijvoorbeeld via Ransomware.live of Cyber Threat Intelligence (CTI) platformen ☐ SURFcert detecteert DDoS-aanvallen op het SURF-netwerk en de door haar beheerde IT-infrastructuur	☐ Betaal nooit losgeld! ☐ Betrek de juiste stakeholders (senior management) voordat er actie wordt ondernomen ☐ Kijk op nomoreransom.org of er een decryptiesleutel beschikbaar is voor de ransomware waarmee de instelling is geïnfecteerd ☐ Schakel de verzekeringsmaatschappij in (indien van toepassing) ☐ Maak een melding bij de Autoriteit Persoonsgegevens (indien noodzakelijk) ☐ Doe aangifte bij de politie ☐ SURFcert mitigeert DDoS-aanvallen op de door haar beheerde IT-infrastructuur

Bijlage 1 Relatie met het SURFaudit Toetsingskader

De verwijzingen naar de SURF Security Baseline zijn al op de voorgaande pagina's verwerkt en daarom geen onderdeel van onderstaande tabel.

Ransomware Kill Chain	Technieken	SURFaudit Toetsingskader		
		Governance	Processen	Techniek
Initiële toegang	Phishing	GO.02 (1.2)	HR.06 (4.6), IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), SM.01 (11.1)	SM.12 (11.12)
	Remote Desktop Protocol	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), ID.03 (10.3), ID.05 (10.5), SM.01 (11.1)	SM.02 (11.2), SM.03 (11.3), SM.04 (11.4), SM.05 (11.5), SM.06 (11.6), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12)
	Credential stuffing/reuse	GO.02 (1.2)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3, SM.01 (11.1)	SM.02 (11.2), SM.03 (11.3), SM.04 (11.4), SM.06 (11.6), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12)
	Derde partijen	GO.02 (1.2)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), ID.01 (10.1), ID.03 (10.3), ID.05 (10.5), SM.01 (11.1), SC.01 (15.1), SC.02 (15.2), SC.03 (15.3), SC.04 (15.4)	SM.02 (11.2), SM.03 (11.3), SM.04 (11.4), SM.07 (11.7)
	Insider threats	GO.02 (1.2), OR.01 (2.1), OR.02 (2.2)	4.3, IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), ID.01 (10.1), ID.02 (10.2), ID.05 (10.5), SM.01 (11.1)	SM.04 (11.4), SM.11 (11.11)
Verkenning & laterale beweging	Verkenning	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), SM.01 (11.1)	SM.06 (11.6), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13)
	Permanente toegang	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), SM.01 (11.1)	SM.06 (11.6), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13)
	Escaleren van rechten	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), SM.01 (11.1)	SM.06 (11.6), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13)

Ransomware Kill Chain	Technieken	SURFaudit Toetsingskader		
		Governance	Processen	Techniek
	Lateraal bewegen	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), SM.01 (11.1)	SM.06 (11.6), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13)
Exfiltratie	Vinden gevoelige informatie	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), DM.03 (9.3), DM.05 (9.5), ID.01 (10.1), SM.01 (11.1), BC.03 (14.3)	SM.04 (11.4), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12)
	Exfiltreren gevoelige informatie	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), SM.01 (11.1)	SM.04 (11.4), SM.07 (11.7), SM.11 (11.11), SM.12 (11.12)
Uitrollen	Backups manipuleren	GO.02 (1.2), GO.04 (1.4)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), DM.03 (9.3), DM.04 (9.4), DM.06 (9.6), SM.01 (11.1)	SM.07 (11.7), SM.08 (11.8), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13), OP.02 (13.2)
	Testen ransomware	-	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), DM.06 (9.6)	SM.07 (11.7), SM.08 (11.8), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13), OP.02 (13.2)
	Ransomware uitrollen & afpersingsbericht	-	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), DM.06 (9.6)	SM.07 (11.7), SM.08 (11.8), SM.11 (11.11), SM.12 (11.12), SM.13 (11.13), OP.02 (13.2)
Afpersing	Versleutelen informatie	GO.02 (1.2)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), BC.01 (14.1), BC.05 (14.5), SC.04 (15.4)	SM.08 (11.8), SM.11 (11.11), SM.12 (11.12), OP.03 (13.3)
	Publiceren gestolen informatie	GO.02 (1.2)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), BC.05 (14.5)	SM.07 (11.7)
	Uitvoeren aanvullende cyberaanvallen	GO.02 (1.2)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), BC.05 (14.5)	SM.07 (11.7), SM.08 (11.8), SM.11 (11.11), SM.12 (11.12), OP.03 (13.3)
	Afpersen of overtuigen van relaties van het slachtoffer	GO.02 (1.2)	IM.01 (6.1), IM.02 (6.2), IM.03 (6.3), BC.05 (14.5)	-

Bijlage 2 Bronnen

- Blueprint for ransomware defense: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/blueprint-for-ransomware-defense_0523.pdf
- CISA stopransomware guide: https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf
- Incident Response Methodologies: https://github.com/certsocietegenerale/IRM
- Incidentresponsplan Ransomware: https://www.ncsc.nl/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware
- MITRE ATT&CK: https://attack.mitre.org/
- MITRE D3FEND: https://d3fend.mitre.org/
- NCSC factsheet ransomware: https://www.ncsc.nl/onderwerpen/ransomware/documenten/factsheets/2020/juni/30/factsheet-ransomware
- Nomoreransom: https://www.nomoreransom.org/nl/index.html
- Ransomware 2nd Edition: https://ransomware.org/wp-content/uploads/2023/07/Ransomware-2nd-Edition_Ebook.pdf
- Ransomware Control Matrix: https://www.rcxmatrix.org/
- Unified Kill Chain: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf