Maastricht University

Reactie Universiteit Maastricht op rapport FOX-IT

05-02-2020

Inleiding

De Universiteit Maastricht werd op 23 december 2019 het slachtoffer van een aanval door cybercriminelen. In de vroege nacht van 24 december 2019 heeft de Universiteit Maastricht contact opgenomen met Fox-IT BV. Fox-IT heeft vanaf die dag ondersteuning geboden op het gebied van crisismanagement, het in kaart brengen van de toedracht van de aanval, alsmede forensisch onderzoek en advisering in het herstelproces van de systemen.

Fox-IT heeft op 5 februari 2020 het rapport *Project Fontana* opgeleverd, de naam die het bedrijf aan het onderzoek heeft gegeven.

Het gaat daarbij om de feitelijke weergave van bevindingen en aanbevelingen op basis van forensisch onderzoek van het technische landschap.

Feiten kennen echter altijd een context. De Universiteit Maastricht kijkt daarom niet alleen vanuit technisch maar ook vanuit de context van de eigen organisatie naar de cyberaanval. In onze ogen is dat nodig om een zo compleet mogelijk antwoord te krijgen op de vraag of de universiteit zich afdoende heeft gewapend tegen digitale kwetsbaarheden.

Vandaar dat de universiteit bij een aantal bevindingen en aanbevelingen in het rapport een aanvulling, toelichting of kanttekening plaatst, zonder iets af te willen doen aan de feitelijkheid. En waar de UM op sommige punten zelf nog (aanvullend) antwoord op specifieke vragen zoekt, zal in de nabije toekomst (intern) onderzoek daar meer helderheid over dienen te verschaffen.

De Universiteit Maastricht wil door openbaarmaking van het rapport, deze reactie en de resultaten van vervolgonderzoek haar aandeel leveren in vergroting van digitale veiligheid.

In de steeds intensievere strijd tegen cyberonveiligheid beschouwt de UM dit als haar maatschappelijke plicht.

Ransomware-aanval

Sinds de cyberaanval op 23 december 2019 is de UM volop bezig geweest om enerzijds de schade te herstellen en anderzijds zo snel mogelijk onderwijs en onderzoek weer mogelijk te maken. Dit was de absolute inzet en focus van het Crisis Management Team (CMT), dat de UM meteen in het leven heeft geroepen. In de loop van de tijd zijn de werkzaamheden van het CMT verschoven van het wegwerken van de directe verstoringen naar het weer opbouwen van de dienstverlening aan studenten, wetenschappers en medewerkers. Over het verloop daarvan is open, transparant en zoveel als mogelijk in detail gerapporteerd via de (dagelijkse) updates op de website van de universiteit.

Tijdens de aanval is een deel van onze technische infrastructuur geraakt. Die infrastructuur bestaat uit 1.647 Linux en Windows-servers en 7.307 werkplekken. De aanval heeft zich uiteindelijk gericht op 267 servers van het Windows-domein. De aanvaller heeft zich gefocust op het versleutelen van gegevensbestanden in het Windowsdomein. Daarbij is van een beperkt aantal systemen ook de back-up getroffen.

Conclusie en opvolging

De Universiteit Maastricht omarmt het rapport van Fox-IT. Het geeft op basis van forensisch onderzoek aan hoe de cybercriminelen een deel van de data van de UM gegijzeld hebben. Maar gezien de scope en de tijdsduur van het onderzoek is een verdiepingsslag verstandig en nodig. Nog niet alles is precies uitgezocht. De UM is om die reden een intern onderzoek gestart.

Aan de hand van de nu voorliggende adviezen uit het rapport en van de toekomstige bevindingen uit het eigen interne onderzoek, kan de UM haar beveiligingsbeleid toetsen en bepalen welke al bestaande plannen aangepast en/of uitgebreid dienen te worden.

Geleerde lessen

Op basis van het Fox-IT rapport, aangevuld met eigen inzichten, kan de UM nu al een aantal 'geleerde lessen' aangeven. Lessen die betrekking hebben op de cyberveiligheid in het algemeen en de cyberaanval van december in het bijzonder:

1. **Betere 'awareness' en afhandeling van (meldingen van) 'phishing-mails'**

We weten uit onderzoek dat ongeveer 20% van de gebruikers zogenaamde 'phishing-mails' opent. Door sterker in te zetten op 'bewustwordings-campagnes' wil de universiteit het aantal succesvolle kwaadwillende inbraakpogingen terugbrengen. Zodra er een 'phishing-mail' binnenkomt bij gebruikers, willen we dat zij dit melden bij de Service Desk. De medewerkers van deze desk willen we via scholing en met tools beter in staat stellen om de juiste acties te ondernemen.

Dankzij intern onderzoek weten we van deze specifieke aanval inmiddels dat er meerdere varianten van 'phishing-mails' zijn verstuurd en dat enkele meldingen van deze mails bij onze Service Desk zijn binnengekomen. Echter: omdat de aanvaller meerdere mails met vrijwel vergelijkbare links had verstuurd, heeft één variant onvoldoende opvolging gehad. We onderzoeken nu hoe we dit in de toekomst kunnen voorkomen.

2. **Technische maatregelen**

De UM wil ervoor zorgen dat aanvallers, áls ze onverhoopt toch 'binnen komen', niet verder kunnen komen op onze infrastructuur. Daarvoor zijn de volgende acties noodzakelijk:

- Het accuraat updaten van de software.

  Het IT-landschap bestaat uit een grote hoeveelheid software, die de afgelopen jaren steeds complexer is geworden. Daarmee is het aantal fouten en foutjes dat in die software zit ook behoorlijk toegenomen. Leveranciers ontdekken doorlopend onvolkomenheden in hun software en leveren updates, die gebruikers dienen te installeren. Om een beeld te schetsen: de UM krijgt ongeveer 100.000 updates per jaar binnen, die allemaal verwerkt dienen te worden op 1.647 servers en 7.307 werkstations.

  Met die updates worden onveilige 'achterdeurtjes' in software gedicht. De aanvallers hebben bij de UM misbruik gemaakt van dergelijke achterdeurtjes. In één geval is ook door Fox-IT niet vastgesteld hoe de aanvallers precies zijn binnengekomen.

  In een ander geval lijkt het erop dat er een zogenaamde 'patch' niet geïnstalleerd was, omdat bij een update naar een nieuwe versie van de software iets niet goed is gegaan.

  Nader onderzoek is dus ook hier nodig.

- Het verbeteren van de segmentering van het Windows-domein.

  Tot nu toe werd binnen het Windows-domein van de UM het domein administrator account met bijbehorende rechten ook gebruikt voor beheer en onderhoudswerkzaamheden op gewone servers. Dit is in strijd met het bestaande beleid. Hierdoor was het makkelijker voor criminelen om via malware zeggenschap over het domein te bemachtigen en daarmee kwaadwillende acties uit te voeren, zoals het installeren van malware en ransomware. In de toekomst zullen we daarom nauwer toezien op het gebruik van de domain administrator accounts en het gebruik ervan beperken voor onderhoud aan het domein en de domein controllers. Ook zullen we de rechtenstructuur binnen het Windows-domein verder verfijnen.

  Het netwerk van de UM is gesegmenteerd in zogenaamde V-LAN's. Deze zijn relatief open met elkaar verbonden om de openheid van het netwerk te garanderen en ook decentraal beheer en gebruik van UM-infrastructuren te faciliteren. Inmiddels weten we dat een striktere segmentering van het netwerk de verplaatsing van malware door het netwerk had kunnen bemoeilijken. Reden voor de UM om de segmentering van het UM-netwerk opnieuw te bezien.

- Het inrichten van 24/7 monitoring door middel van een SIEM en/of SOC.

  De cyberaanval heeft geleerd dat de UM signalen van afwijkend gedrag die in de logbestanden terecht komen beter moet filteren. Per seconde worden 30.000 inbraakpogingen geblokkeerd en per dag worden 1400 malware aanvallen gestopt. Daarnaast komen nog eens duizenden signalen per dag binnen in diverse logbestanden.

  We moeten ervoor zorgen dat belangrijke signalen sneller zichtbaar worden voor onze beheerders. Daarvoor willen we een 7 x 24 uurs SIEM (Security Information and Event Management) alsmede een Security Operations Center (SOC) inrichten, ook in samenspraak met de collega-universiteiten. Een SOC is een team met als vaste en enige taak om de cyberdreigingen in de gaten te houden, de instelling te adviseren over veiligheid, feitelijke dreigingen te detecteren en in te grijpen als dat nodig is.

De UM was overigens al van plan om een dergelijk SOC in januari 2020 te beginnen.

Zoals in het rapport van Fox-IT staat aangegeven, is verder per direct gestart met zowel end-point monitoring als uitbreiding van netwerk-sensoren.

- Configuration Management Data Base.

  Bij het herstellen van de schade is relatief veel werk gestoken in het helder krijgen van de impact van de aanval op de IT-infrastructuur. Er was onvoldoende inzicht in het aantal actieve en niet meer actieve computer- en serversystemen in het UM-domein. Om hier adequaat zicht op te krijgen, wil de UM de 'computer inventaris' (Configuration Management Data Base) in kaart brengen.

3. Dubbele back-ups

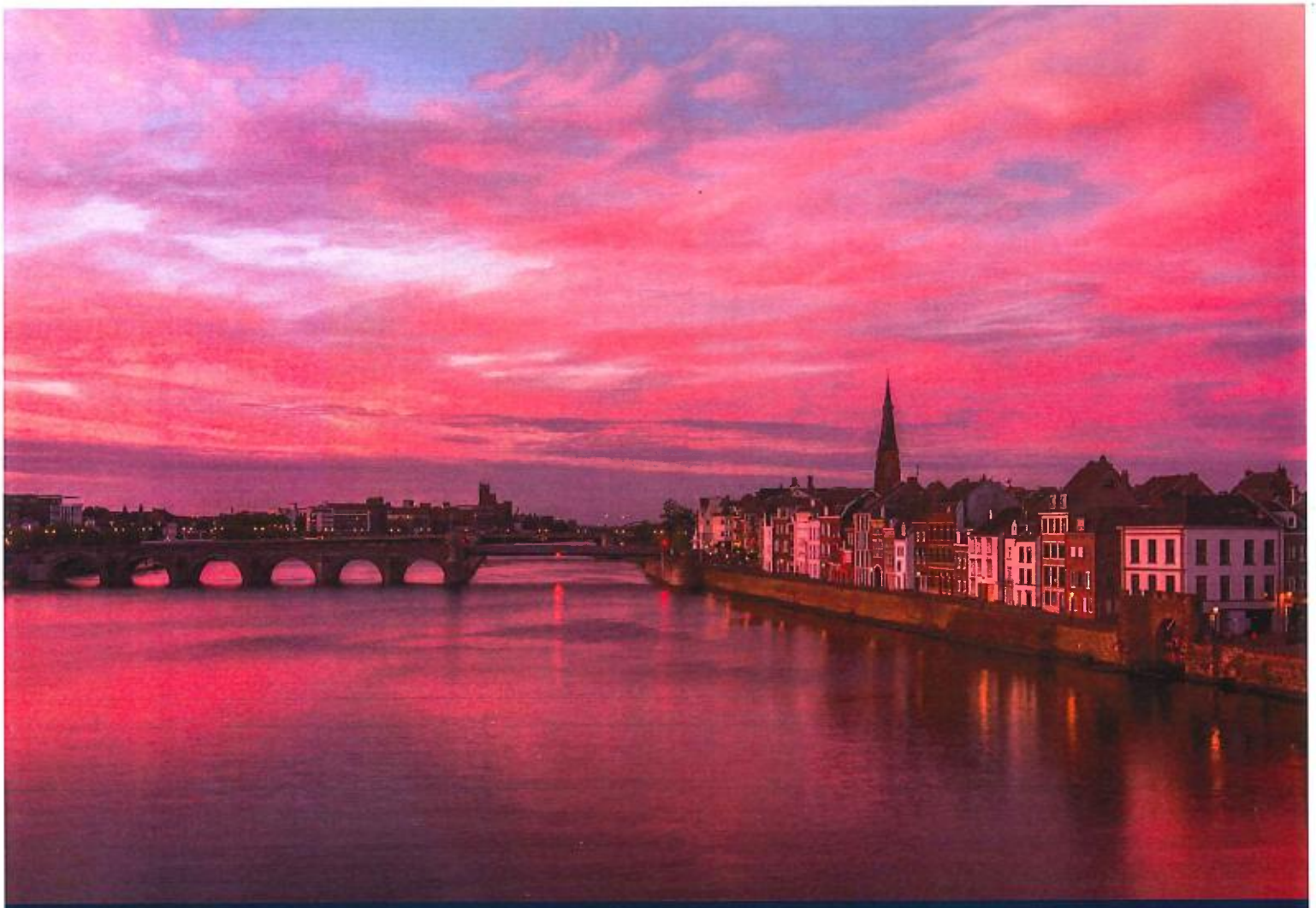
Als cyberaanvallers onverhoopt toch schade weten aan te richten, wil de UM beter in staat zijn de schade zelf te herstellen met back-ups. Tot nu toe koos de UM ervoor om back-ups vooral te gebruiken om bijvoorbeeld bij een storing of uitval zo snel mogelijk weer te kunnen beschikken over een werkende omgeving. Hier zijn diverse technieken voor. Het meest gebruikt is het aanleggen van zogeheten *'snapshots'* verdeeld over meerdere locaties. Deze techniek vraagt erom dat deze 'snapshots' online staan, afhankelijk van de gekozen oplossing of fabrikant.

De cyberaanvaller wist van een paar kritische systemen deze online back-ups te versleutelen. Dat moet in de toekomst voorkomen worden. Daarom moeten er naast online back-ups óók offline back-ups komen, zodat het scenario van totale uitval kan worden voorkomen. Inmiddels hebben we voor elk cruciaal systeem offline én online back-ups gemaakt.

Overigens dienen gebruikers er rekening mee te houden dat - ook al zijn er back-ups – het opnieuw installeren van servers altijd extra tijd en inspanning kost. Dat is onvermijdelijk om de gehele configuratie weer op de juiste manier werkend te krijgen.

Vervolgonderzoek data

Het rapport van Fox-IT beveelt aan een vervolgonderzoek in te stellen naar eventuele 'extractie' van onderzoeks- en persoonsgegevens. Weliswaar zijn tijdens het onderzoek op dat vlak geen sporen gevonden, maar de UM voelt het als haar nadrukkelijke verantwoordelijkheid om hier nader onderzoek naar te laten doen. De universiteit zal Fox-IT opdracht geven om aanvullend forensisch onderzoek te verrichten naar een aantal belangrijke databestanden die representatief zijn voor onderwijs, onderzoek en bedrijfsvoering. Daarnaast gaat de UM ook zelf voor een aantal databestanden nader onderzoek verrichten.



Maastricht University

CLASSIFICATIE
PUBLIC

Spoedondersteuning Project Fontana

Onderwerp	Ondersteuning bij ransomware
Datum	5 februari 2020
Projectnummer	190346
Opdrachtgever	Universiteit Maastricht
Auteurs	Mattijs Dijkstra & Maarten van Dantzig
Versie	3.0
Status	Definitief
Pagina's	38

FOX IT
part of nccgroup

DOCUMENTCLASSIFICATIE

Dit document is geclassificeerd als PUBLIC. De informatie die in dit document en bijbehorende bijlagen gepubliceerd is, is alleen bedoeld voor de geadresseerde(n). Het gebruik van het document door een andere partij dan de geadresseerde(n) is niet toegestaan, tenzij deze partij hiertoe expliciet geautoriseerd is door een geadresseerde. De informatie in dit document is PUBLIC van aard en valt onder de bepalingen van een geheimhoudingsverklaring of -plicht.

Indien u het voorliggende document foutief heeft ontvangen en/of geen toestemming heeft tot inzage van het document, verzoekt Fox-IT u om het document direct te sluiten en te retourneren aan Fox-IT.

Enig misbruik van dit document of de informatie in het document is niet toegestaan. Fox-IT aanvaardt geen aansprakelijkheid voor enig ongeautoriseerd gebruik of misbruik van voorliggend document door een derde partij of schade ontstaan door de inhoud van het document.

Fox-IT B.V.
Olof Palmestraat 6
2616 LM Delft
Postbus 638
2600 AP Delft
Nederland

T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
fox@fox-it.com
www.fox-it.com

Copyright © 2020 Fox-IT B.V.
Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier, zonder voorafgaande schriftelijke toestemming van Fox-IT B.V.

Handelsmerk
Fox-IT en het logo van Fox-IT zijn handelsmerken van Fox-IT B.V.
Alle andere in dit document opgenomen handelsmerken zijn eigendom van de genoemde organisaties.

Documentbeheer

Projectnaam	Fontana
Projectnummer	190346
Opdrachtgever	Universiteit Maastricht
Onderwerp	Ondersteuning bij ransomware
Datum	5 februari 2020
Versie	3.0
Status	Definitief
Auteurs	Mattijs Dijkstra & Maarten van Dantzig

Deze versie vervangt alle voorgaande versies van dit document.

Distributielijst

Versie	Datum	Verspreidingsvorm	Naam/functie/opmerking
1.0	30-1-2020	PDF via de Fox-IT Clientportal	
2.0	3-2-2020	PDF via de Fox-IT Clientportal	
3.0	3-2-2020	PDF via de Fox-IT Clientportal	

Reviews

Versie	Datum	Door	Functie
0.1	27-1-2020	*Geredigeerd*	Sr. Forensic IT Expert
0.2	28-1-2020	Wouter Janssen	Sr. Forensic IT Expert
0.3	29-1-2020	Christian Prickaerts	Director Managed Services
0.4	29-1-2020	Vera Schönfeldt	Manager Legal
2.0	04-02-2020	Erik de Jong & Frank Groenewegen	Chief Research Officer & Chief Security Expert

Wijzigingen

Versie	Datum	Door	Opmerkingen
0.1	27-1-2020	Mattijs Dijkstra & Maarten van Dantzig	Initiële versie
0.2	27-1-2020	Mattijs Dijkstra & Maarten van Dantzig	Review verwerkt
0.3	28-1-2020	Mattijs Dijkstra & Maarten van Dantzig	Review verwerkt
0.4	29-1-2020	Mattijs Dijkstra & Maarten van Dantzig	Review verwerkt
1.0	30-1-2020	Mattijs Dijkstra	Definitief gemaakt
2.0	03-02-2020	Mattijs Dijkstra	Feedback opdrachtgever verwerkt
3.0	04-02-2020	Mattijs Dijkstra	Feedback opdrachtgever verwerkt

Gerelateerde documenten

Versie	Datum	Omschrijving	Opmerkingen
1.0	27-1-2020	Fontana_Timeline.xlsx	Apart aangeleverd

Managementsamenvatting

Op 24 december 2019 heeft Universiteit Maastricht (hierna: Opdrachtgever) contact opgenomen met Fox-IT B.V. (hierna: Fox-IT) aangaande een ransomware-aanval op haar infrastructuur. Deze aanval had ertoe geleid dat zeer kritieke systemen voor de bedrijfsvoering van Opdrachtgever waren versleuteld. Onder deze systemen vallen de e-mailservers, bestandsservers met onderzoeks- en bedrijfsvoering gegevens, en een aantal back-up servers. Tijdens het incident heeft Fox-IT ondersteuning geboden op het gebied van crisismanagement, en digitaal forensisch onderzoek uitgevoerd.

Fox-IT heeft vastgesteld dat de aanvaller initieel toegang heeft verkregen tot het netwerk van Opdrachtgever door middel van twee phishing e-mails. Deze twee e-mails zijn op 15 en 16 oktober 2019 op twee werkstations geopend, waarmee de aanvaller toegang heeft verkregen tot de systemen.

Van 16 oktober 2019 tot en met 23 december 2019 heeft de aanvaller meerdere servers gecompromitteerd. De aanvaller is er op 21 november 2019 in geslaagd om, via een server met ontbrekende beveiligingsupdates, volledige rechten te verkrijgen binnen de infrastructuur van Opdrachtgever. Uiteindelijk is op 23 december 2019 door de aanvaller op 267 Windows servers de zogenaamde Clop-ransomware uitgerold. Na zorgvuldige analyse van de mogelijkheden is op 30 december 2019 aan Fox-IT door Opdrachtgever medegedeeld dat zij hadden besloten om de losgeldsom te betalen.

Tijdens het onderzoek zijn sporen aangetroffen die aantonen dat de aanvaller data heeft verzameld aangaande de topologie van het netwerk, gebruikersnamen en wachtwoorden van meerdere accounts, en andere netwerkarchitectuur informatie. Fox-IT heeft binnen de scope van het onderzoek geen sporen aangetroffen die wijzen op het verzamelen van andersoortige data. Additioneel forensisch onderzoek op kritieke systemen, ook wel aangeduid als kroonjuwelen, zou hier meer inzicht in kunnen bieden.

Op basis van het onderzoek heeft Fox-IT verschillende aanbevelingen geformuleerd welke kunnen worden ingedeeld in de categorieën preventie, detectie, en respons:

- Verbeter processen omtrent vulnerability en patch management.
- Breng meer segmentatie aan binnen de netwerk architectuur en gebruikersrechten.
- Implementeer of verbeter netwerk- en logmonitoring.
- Oefen planmatig met verschillende crisis scenario's en verbeter de opgestelde plannen waar nodig.

Tot slot adviseert Fox-IT om de implementatie van bovenstaande aanbevelingen kritisch te (laten) toetsen.

Inhoudsopgave

1	**Inleiding**	**6**
1.1	Achtergrond	6
1.2	Doelstellingen	6
1.3	Leeswijzer	6
2	**Universiteit Maastricht**	**8**
3	**Bewijsmateriaal**	**9**
3.1	Log-data	9
3.2	Systeemdata	9
3.3	Netwerkdata	10
3.4	Overige data	10
4	**Aanpak onderzoek**	**11**
4.1	CERT organisatie	11
4.2	Scope	12
4.3	Uitrol detectie en response mogelijkheden	12
4.4	Forensisch onderzoek	13
4.5	Mitigatie en herstel	14
5	**Bevindingen uit het onderzoek**	**16**
5.1	Initiële compromittatie	16
5.2	Verspreiding binnen het netwerk	17
5.3	Voorbereiden en uitrollen van ransomware	19
5.4	Detectie van aanvallersactiviteit	24
5.5	Tijdlijn van belangrijke gebeurtenissen	25
5.6	Over de aanvaller	26
5.7	Gecompromitteerde systemen en accounts	26
5.8	Kroonjuwelen	28
6	**Conclusies**	**29**
7	**Aanbevelingen**	**30**
7.1	Preventie	30
7.2	Detectie	32
7.3	Response	33
7.4	Vervolgonderzoek	34
Appendix A		**35**
A.1	Verklarende woordenlijst	35
A.2	Gecompromitteerde systemen	36

1 Inleiding

Deze rapportage beschrijft de uitkomst van het digitaal forensisch onderzoek genaamd project Fontana. Dit onderzoek is uitgevoerd in de periode van 24 december 2019 tot 29 januari 2020.

1.1 Achtergrond

In de nacht van 23 op 24 december 2019 hebben twee medewerkers van het IT security team van Universiteit Maastricht (hierna: Opdrachtgever) contact opgenomen met het Computer Emergency Response Team (CERT) noodnummer van Fox-IT inzake een cyber-incident. Op dat moment waren verschillende servers onbereikbaar vanwege een ransomware-aanval op de infrastructuur van Opdrachtgever. Rond het middaguur heeft vervolgens een uitgebreide telefonische intake plaatsgevonden met Opdrachtgever waaruit snel duidelijk werd dat ondersteuning op locatie gewenst was. Vervolgens is Fox-IT op 24 december 2019 om 16:00 uur op de locatie van het ICT kantoor van Opdrachtgever gearriveerd om te assisteren in het incident response proces. De werkzaamheden in de eerste fase van het incident waren voornamelijk gericht op het ondersteunen van crisismanagement processen, en het in kaart brengen van de toedracht van de aanval door middel van digitaal forensisch onderzoek.

1.2 Doelstellingen

Opdrachtgever heeft Fox-IT verzocht een onderzoek uit te voeren met daarbij als doelstellig om de volgende onderzoeksvragen te beantwoorden:

- Wat is de toedracht van het incident?
- Wat is de oorzaak van het incident?
- Wat is de omvang van het incident?
- Welke data is benaderd door de aanvaller?
- Zijn gegevens ingezien of ontvreemd van door Opdrachtgever geïdentificeerde kroonjuwelen?

Aanvullend heeft Fox-IT, in overleg met Opdrachtgever, de volgende doelstellingen aangedragen om mee te nemen binnen het onderzoek:

- adviseren bij het inrichten en opstarten van de crisisorganisatie;
- advies geven in het kader van benodigde mitigatie- en herstelmaatregelen.

1.3 Leeswijzer

De datums en tijden in dit document geven de datum en tijd weer in de gecoördineerde wereldtijd (UTC).

Dit hoofdstuk beschrijft de achtergrondinformatie en doelstellingen die ten grondslag liggen aan het onderzoek. Hoofdstuk 2 beschrijft de organisatie van Opdrachtgever op basis van zowel het type organisatie als de infrastructuur. Hoofdstuk 3 beschrijft het onderzochte bewijsmateriaal. Hoofdstuk 4 beschrijft de aanpak van het onderzoek. De onderzoekbevindingen zijn beschreven in hoofdstuk 5 en hoofdstuk 6 beschrijft de daarop gebaseerde conclusies. Tot slot zijn in hoofdstuk 7 aanbevelingen beschreven die volgen uit de observaties gedurende het project.

Bijlage A.1 bevat een verklarende woordenlijst voor technische termen. In bijlage A.2 is een overzicht terug te vinden van alle door Fox-IT geïdentificeerde gecompromitteerde systemen.

2 Universiteit Maastricht

Dit hoofdstuk beschrijft op hoog abstractieniveau de infrastructuur van Opdrachtgever. Denk hierbij aan het aantal systemen in het netwerk, kern functionaliteit en het mandaat aangaande beheer van de systemen.

Infrastructuur

Universiteit Maastricht (UM) is een publieke organisatie met 4.500 werknemers, 18.000 studenten en 70.000 alumni. De IT-infrastructuur van de UM bestaat uit een verscheidenheid aan servers en werkstations welke niet allen direct onder het mandaat vallen van de centrale IT-beheer organisatie, het zogenaamde ICT Service Centre (ICTS). Bij het ICTS kunnen studenten, werknemers en gasten terecht voor ICT gerelateerde zaken.

Centraal/Decentraal

Een gedeelte van de IT-infrastructuur van UM wordt centraal beheerd door ICTS. Hoeveel werkplekken en servers dit precies zijn is Fox-IT ten tijde van het onderzoek niet duidelijk geworden. Er is ook een gedeelte van de IT-infrastructuur dat buiten het mandaat van ICTS valt maar wel onderdeel uitmaakt van het centrale netwerk. Dit deel wordt decentraal beheerd door de betreffende bedrijfseenheden zelf. Het verschilt per faculteit, per server en per werkstation of deze toegang hebben tot het centrale Windows domein van UM. De naam van het domein is `UNIMAAS`.

VDI

Naast vaste werkstations in de vorm van desktops en laptops maken werknemers van de UM ook gebruik van virtuele werkplekken. Zowel op de vaste als op de virtuele werkplekken kan met persoonlijke inloggegevens worden ingelogd. De virtuele werkstations maken gebruik van Virtual Desktop Infrastructure (VDI) waarbij sprake is van desktopvirtualisatie in het datacenter. Deze VDI omgeving is bereikbaar via zogenaamde thin-clients en de lokale browsers. In de VDI omgeving draait een golden image van het besturingssysteem op een server in plaats van op het lokale werkstation, waarbij een stuk virtueel geheugen van de server wordt gereserveerd voor elke gebruiker. Dit stelt de ICTS-afdeling in staat om de VDI-omgeving centraal te beheren, terwijl het voor werknemers en studenten mogelijk is op afstand te werken op virtuele werkplekken.

3 Bewijsmateriaal

Fox-IT heeft een aantal bewijsstukken veiliggesteld en onderzocht. Dit hoofdstuk geeft een hoog-over omschrijving van dit materiaal.

3.1 Log-data

Gedurende het onderzoek heeft Fox-IT log-data veiliggesteld. In dit geval betreft het specifiek Splunk log-data. Opdrachtgever stuurt vanuit verschillende bronnen data door naar het Splunk-systeem. De data van de verschillende bronnen is door Fox-IT veiliggesteld op het Splunk-systeem. Tabel 1 bevat de lijst van veiliggestelde log-data.

Tabel 1 - Veiliggestelde log-data

ID	Naam	Bron	Veiliggesteld op	Omschrijving
IEV3	DNS verzoeken	Splunk	30-12-2019	Alle DNS-verzoeken sept/okt/nov/dec 2019 naar domein: `drm_server13-login-microsoftonline`
IEV14	UM	Splunk	20-01-2020	Windows Event Log en netlogon-logbestanden van Domain Controller UM-
IEV15	UM-FS	Splunk	14-01-2020	Windows Event Log logbestanden van MUSL-share op UM-FS

3.2 Systeemdata

Fox-IT heeft data veiliggesteld van verschillende systemen in het netwerk van Opdrachtgever. Hieronder vallen disk-images, geheugen-images en diverse type data die is veiliggesteld van live systemen. Tabel 2 bevat de lijst van veiliggestelde systeemdata.

Tabel 2 - Veiliggestelde systeemdata

ID	Systeemnaam	Type data	Veiliggesteld op	Omschrijving
IEV1	321	Disk en geheugen image	30-12-2019	Disk image en geheugen image van 321
IEV3	UM-	Geheugen image	30-12-2019	Geheugen image van server UM-
IEV4 IEV10	316 systemen	Acquire data	02-01-2020 14-01-2020	Verzameling van forensische artefacten van 316 systemen
IEV5	WS	Disk image	06-01-2020	Disk image van werkstation WS
IEV7	UM-	Disk image	02-01-2020	Disk image systeempartitie van Domain Controller UM-
IEV9	UM	Disk image	03-02-2020	Disk image van 2 servers
IEV11	UM	Disk image	09-01-2020	Disk image van CORSA UM
IEV12	UM-	Disk image	10-01-2020	Disk image van Syllabus server UM-DE

ID	Systeemnaam	Type data	Veiliggesteld op	Omschrijving
IEV17	15 systemen	Acquire data	20-01-2020	Verzameling van forensische artefacten van verschillende servers
IEV20	UB	Disk image	21-01-2020	Disk images van twee servers

3.3 Netwerkdata

Opdrachtgever registreert zelf op enkele firewalls aan de buitenkant van het netwerk metadata van alle verbindingen in zogenaamde flow logging. Fox-IT heeft deze data veiliggesteld om hier verder onderzoek op te kunnen verrichten. Tabel 3 bevat de omschrijving van de veiliggestelde netwerkdata.

Tabel 3 - Veiliggestelde netwerkdata

ID	Type data	Bron	Veiliggesteld op	Omschrijving
IEV13	Flowlogs	Firewall Opdrachtgever	14-01-2020	Metadata van netwerkverkeer tussen 2019-07-03 en 2019-12-25

3.4 Overige data

Fox-IT heeft nog overig materiaal veiliggesteld dat relevant is voor het onderzoek. Hieronder vallen mailboxen, database-bestanden en versleutelde bestanden. Tabel 4 bevat de lijst van overige veiliggestelde data.

Tabel 4 - Overige veiliggestelde data

ID	Veiliggesteld op	Omschrijving
IEV2	2019-12-30	Disk image eerste infectie virtueel werkstation
IEV3	2019-12-30	Versleutelde bestanden
IEV8	2020-01-03	SDBbot malware en bijbehorende registersleutels
IEV16	2020-01-14	EPO databases
IEV18	2020-01-21	Mailboxen accounts ********en ********

4 Aanpak onderzoek

Dit hoofdstuk beschrijft allereerst het opzetten van de CERT-organisatie. Vervolgens worden de scope en de aanpak van het onderzoek besproken. Tot slot volgen daaruit een aantal concrete mitigatiestappen welke door Fox-IT geadviseerd zijn uit te voeren.

4.1 CERT organisatie

Op 24 december 2019 zijn de incident response experts van Fox-IT op locatie gearriveerd bij Opdrachtgever in Maastricht. Zoals besproken in hoofdstuk 1.2 was één van de doelstellingen het adviseren bij het inrichten en opstarten van de crisisorganisatie. Fox-IT is daarom begonnen met assisteren van het Crisis Management Team (CMT) bij het inrichten van de crisisorganisatie. Dit bestond in eerste instantie uit het bij elkaar krijgen van de juiste disciplines. Om efficiënt te werk te kunnen gaan ten tijde van een incident is het namelijk van belang een multidisciplinair crisisteam samen te stellen. Dit concept staat weergegeven in Figuur 1.
Ten eerste heeft Fox-IT benadrukt dat het tijdig aanhaken van een communicatie-expert prioriteit had. Aangezien het incident publiekelijk bekend was ten tijde van het opstarten van de crisisorganisatie. Dit was tevens van belang omdat transparantie in de aard zit van een publieke organisatie als die van Opdrachtgever. Mocht deze positie niet intern vervuld kunnen worden was het advies een externe partij aan te haken om deze communicatie te verzorgen.

Ten tweede heeft Fox-IT geadviseerd de inhoud van zowel interne als externe berichtgeving af te stemmen met de juridische afdeling van Opdrachtgever.

Ten derde heeft Fox-IT geadviseerd zowel business als IT en IT security deel te laten nemen aan het dagelijkse crisis management team (CMT) overleg. Dit was in het belang van het bepalen van de impact van te nemen besluiten. In dit geval was de noodzaak voor een deelnemer van HR minder hoog, omdat de impact op de bedrijfsvoering tijdens de vakantiedagen minder groot werd geacht. Op basis van het type incident werd verder de kans dat het incident voortkwam uit een dreiging vanuit binnen de organisatie als laag ingeschat.

De werkzaamheden waren in de eerste dagen ingedeeld in drie sporen en drie teams: organisatie, onderzoek en herstel. Opdrachtgever heeft voornamelijk invulling gegeven aan het organisatie- en het herstelteam. Het onderzoeksteam bestond uit een combinatie van experts van Fox-IT en werknemers van Opdrachtgever. Ten behoeve van zowel het in scope brengen van de compromittatie als het uitvoeren van root cause onderzoek is op grote schaal forensisch bewijsmateriaal veiliggesteld.



Figuur 1 – Crisisteam

4.2 Scope

Om de initiële scope van het onderzoek te bepalen heeft Fox-IT een inventarisatie gemaakt van gecompromitteerde systemen en accounts. Een systeem werd gezien als gecompromitteerd als er handmatige aanvalleractiviteit op heeft plaatsgevonden, of wanneer er sporen zijn aangetroffen van malware. Een account wordt gezien als gecompromitteerd indien op basis van forensisch sporen onderzoek is vastgesteld dat het door de aanvaller is gebruikt. In totaal heeft Fox-IT vijf accounts en 269 Windows systemen geïdentificeerd als gecompromitteerd (van in totaal 1.647 servers en 7.307 werkplekken). Naast Windows systemen heeft Opdrachtgever Linux en OS X systemen binnen de infrastructuur welke niet zijn geraakt door de aanval. Een overzicht van gecompromitteerde accounts en systemen is terug te vinden in respectievelijk Tabel 9 en de tabel in Appendix A.2.

4.3 Uitrol detectie en response mogelijkheden

Gedurende de incident response fase heeft Fox-IT in samenwerking met Opdrachtgever verschillende detectie- en response-middelen ingezet. Dit gaf meer zichtbaarheid van activiteit in het netwerk en de mogelijkheid real-time te kunnen reageren op aanvalleractiviteit.

4.3.1 Inzet Fox-IT sensoren

Door de inzet van netwerksensoren heeft Fox-IT de mogelijkheid voor live detectie en analyse van malafide of anderzijds verdacht netwerkverkeer. Naast detectie op basis van detectieregels, registreren de sensoren alle metadata van het gemonitorde netwerk. Dit is cruciaal voor response doeleinden om eventueel malafide verkeer op een later tijdstip te kunnen onderzoeken.
Live detectie door middel van netwerksensoren assisteert het onderzoeksteam verder bij in het in kaart brengen van regulier en malafide netwerkverkeer. Bij Opdrachtgever zijn op twee strategisch gekozen plaatsen in het netwerk netwerksensoren geplaatst. Op de eerste locatie wordt al het inkomende en uitgaande internetverkeer gemonitord door twee sensoren. Op de tweede locatie monitort één sensor het interne netwerkverkeer binnen het `UNIMAAS` domein.
Door middel van netwerkdetectie op dit niveau is het mogelijk om zowel de pogingen van een aanvaller tot binnentreden als ook het lateraal bewegen door het netwerk te detecteren. Een overzicht van de geplaatste netwerksensoren is terug te vinden in Tabel 5.

Tabel 5 - Netwerksensoren

Sensor naam	Actief	Locatie	Dekking
UM-1	24-12-2019	Universiteitssingel 50 - Maastricht	Internet verkeer
UM-2			
UM-3	24-12-2019	Grote Looierstraat 17 - Maastricht	Intern verkeer

4.3.2 Inzet Carbon Black

Tijdens de incident response fase heeft Fox-IT in samenwerking met Opdrachtgever de detectie- en response-tool Carbon Black Response (CB) uitgerold op Windows systemen binnen het netwerk van Opdrachtgever. Op 25 december 2019 heeft Fox-IT de organisatie Carbon Black benaderd om de uitrol van de software te starten. Vervolgens is binnen een tijdsbestek van vier weken Carbon Black uitgerold op 8.873 systemen. Door op deze manier zichtbaarheid van activiteit op systemen en in het netwerk van Opdrachtgever te creëren, kunnen onregelmatigheden centraal worden gedetecteerd.
De focus voor CB-installatie lag in eerste instantie op gecompromitteerde Windows servers, gevolgd door installatie op de rest van de Windows servers binnen het netwerk. De aanvaller richtte zich namelijk voornamelijk op Windows Servers. Secundair is CB uitgerold op Windows werkstations om nieuwe infecties te kunnen detecteren. Als laatste zijn de VDI-systemen voorzien van CB. Uiteindelijk was het doel een CB-dekkingsgraad van meer dan 90% van alle systemen in het netwerk van Opdrachtgever te realiseren.

Een compleet overzicht van de actieve CB-sensoren is terug te vinden in onderstaande Tabel 6. Ten tijde van schrijven van deze rapportage heeft Opdrachtgever aan Fox-IT laten weten een dekkingsgraad van 94% te hebben gerealiseerd.

Tabel 6 - Carbon Black sensoren

Datum	Servers	Werkstations	VDI	Totaal
27-12-2019	96	0	0	96
28-12-2019	218	21	0	239
31-12-2019	469	21	0	490
03-01-2020	732	306	0	1.038
14-01-2020	408	4.621	2.839	7.868
24-01-2020	411	4.901	3.561	8.873

4.4 Forensisch onderzoek

Opdrachtgever heeft besloten in de eerste fase van het onderzoek prioriteit te willen geven aan het spoedig herstellen van de bedrijfsvoering. Om de mogelijkheid te houden voor het later uitvoeren van delen van een forensisch sporen onderzoek heeft Fox-IT geadviseerd in deze eerste fase wel al onderzoeksmateriaal veilig te stellen. Wanneer dit niet tijdig zou zijn gebeurd, zouden waardevolle forensische sporen namelijk verloren kunnen gaan.

Voor het veiligstellen van forensisch onderzoeksmateriaal is hoofdzakelijk gebruik gemaakt van Dissect Acquire. Deze door Fox-IT ontwikkelde software kopieert van een Windows systeem die bestanden die de meest relevante forensische sporen bevatten. Deze bestanden worden weggeschreven als zip-bestand via het netwerk naar een machine welke enkel voor dit onderzoek wordt gebruikt.

Bestanden zijn vanaf deze netwerklocatie geüpload naar Fox-IT's forensische lab voor analyse. Eveneens zijn disk images en logbestanden verzameld. Het verzamelen van dergelijk onderzoeksmateriaal zorgt ervoor dat analyse van historische activiteit op een systeem mogelijk is en assisteert daarmee bij het op grote schaal identificeren van gecompromitteerde systemen. Fox-IT heeft Opdrachtgever de Dissect Acquire programmatuur ter beschikking gesteld en daarbij relevante instructies aangeleverd voor het inzetten van de software.

Op het moment van schrijven is van 324 systemen Acquire-data veiliggesteld. De data is geanalyseerd op basis van de bij Fox-IT bekende "indicators of compromise" (IOCs), oftewel sporen van compromittatie. Op momenten dat tijdens het onderzoek nieuwe IOCs gevonden werden, zijn de reeds geanalyseerde systemen opnieuw gecontroleerd op deze nieuwe IOCs. Het analyseren van de data heeft geholpen het pad van de aanvaller inzichtelijk te maken en de scope van de compromittatie in kaart te brengen.

De IOCs zijn in overleg met Opdrachtgever eveneens gedeeld met de relevante instanties en partnerorganisaties om ook hen in staat te stellen zich te beschermen tegen deze aanvaller.

4.5 Mitigatie en herstel

Hoewel de primaire focus van Fox-IT het uitvoeren van onderzoek en het assisteren in de crisisorganisatie was, heeft Fox-IT, waar mogelijk, Opdrachtgever voorzien van advies op het gebied van mitigatie. Allereerst heeft Fox-IT geadviseerd om een mitigatieteam in te richten. Het is van belang dat de leden van dit team zich optimaal kunnen concentreren op hun takenpakket. De leden laten zich weliswaar leiden door bevindingen uit het onderzoeksteam maar houden zelf de focus op de mitigatie en het buitensluiten van de aanvaller.

Binnen het takenpakket van het mitigatieteam vallen verschillende werkzaamheden, waaronder het verwijderen van de malware, het identificeren en opnieuw installeren van kritieke systemen en het vaststellen van de volgorde van herstelmaatregelen. Opdrachtgever heeft het doel uitgesproken de herstelmaatregelen zo uit te voeren dat organisatie-kritieke systemen begin januari weer live zijn. Vanuit technisch perspectief heeft Fox-IT het mitigatie-team ondersteund door besmette systemen te identificeren. Aanvullend heeft Fox-IT inhoudelijk advies gegeven over de daadwerkelijke invulling van het takenpakket van het mitigatieteam.
Opdrachtgever heeft tijdens het incident, in de periode tussen 24 december 2019 en 1 januari 2020, de volgende mitigatiestappen ondernomen. Waar overleg met Fox-IT heeft plaatsgevonden is dit aangegeven bij de specifieke stap.

- Op 24 december heeft Opdrachtgever verbindingen zowel van als naar het internet dichtgezet. Deze actie had als gewenst resultaat dat de aanvaller het netwerk niet langer kon benaderen en dat geïnfecteerde systemen niet langer naar buiten konden communiceren. Het op een dergelijke manier isoleren van het netwerk heeft Opdrachtgever de ruimte verschaft om te onderzoeken wat de scope van het incident was.
- Ten behoeve van de door te voeren herstelmaatregelen was het noodzakelijk dat een aantal systemen van beheerders weer internet-toegang kregen. Om te borgen dat dit geen aanvullende veiligheidsrisico's met zich mee zou brengen is door Opdrachtgever besloten om op 26 december bepaalde systemen op basis van IP-adres weer toegang te geven tot zowel het interne netwerk als het internet. Dit is op advies van Fox-IT pas doorgevoerd ná het blokkeren van IP-adressen uit de set van bekende IOCs op de centrale firewalls, en nadat er sprake was van netwerkmonitoring.

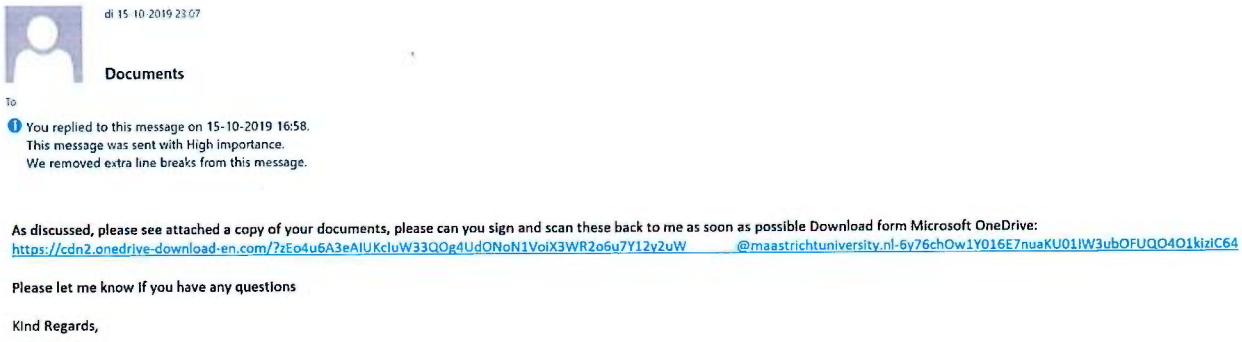
- Fox-IT heeft geadviseerd netwerktoegang te limiteren vanaf het Eduroam studenten WiFi netwerk naar het interne netwerk. Dit is op advies van Fox-IT pas doorgevoerd nadat er op dit segment van het netwerk voldoende netwerkmonitoring was gerealiseerd.
- Fox-IT heeft geadviseerd actief te monitoren op basis van firewall meldingen op IOCs door middel van e-mailnotificaties en daarbij een escalatie pad voor het melden van incidenten in te richten. Dit escalatie pad is getest door middel van een simulatie.
- Fox-IT heeft geadviseerd om een wachtwoord-reset verplicht te stellen voor alle accounts binnen het UNIMAAS domein van Opdrachtgever, met daarbij primair de focus op de administrator- en service-accounts.
- Fox-IT heeft een stappenplan opgesteld voor het omgaan met door de aanvaller besmette systemen, ter input voor het team verantwoordelijk voor het terug live brengen van deze systemen.
- Fox-IT heeft geadviseerd een lijst te maken met de zogenaamde kroonjuwelen van de organisatie om de prioriteit te kunnen bepalen van herstelmaatregelen.
- Fox-IT heeft geadviseerd om schone en opgeschoonde systemen die weer live gebracht (zouden) gaan worden te voorzien van CB omwille van de zichtbaarheid van eventuele activiteit van de aanvaller. Fox-IT heeft tot slot geadviseerd om monitoring door middel van CB en netwerksensoren te implementeren zodat het netwerkverkeer op basis van geïdentificeerde en generieke IOCs kan worden gecontroleerd en zo de integriteit van het netwerk kan worden geborgd.

5 Bevindingen uit het onderzoek

Dit hoofdstuk beschrijft de belangrijkste bevindingen uit het Fontana onderzoek met de daarbij horende relevante forensische sporen. De volledige tijdlijn met daarin alle aangetroffen forensische sporen van aanvallersactiviteit is apart bijgevoegd in het Excel-document `Fontana_Timeline.xlsx`.
De tijdlijn en de inhoud van dit hoofdstuk beschrijft op chronologische volgorde de (gevolgen van de) stappen zoals die zijn gezet door de aanvaller, en dus niet in de volgorde waarop de sporen zijn aangetroffen.

5.1 Initiële compromittatie

Op 15 oktober 2019 om 14:06:31[1] is op het e-mailadres `********@maastrichtunversity.nl` een phishing e-mail met als onderwerp `Documents` ontvangen.



di 15-10-2019 23:07

Documents

To

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
https://cdn2.onedrive-download-en.com/?zEo4u6A3eAIUKcluW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW @maastrichtuniversity.nl-6y76chOw1Y016E7nuaKU01IW3ubOFUQO4O1kiziC64

Please let me know if you have any questions

Kind Regards,

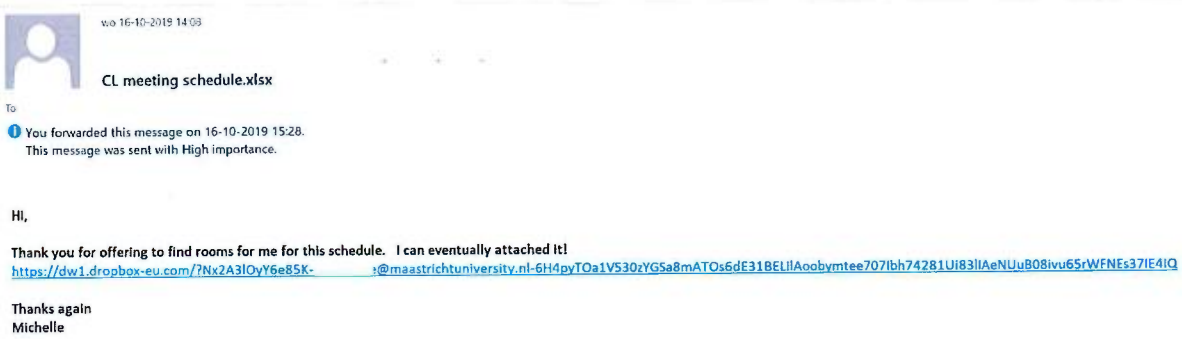
Figuur 2 – Phishing e-mail ontvangen op 15 oktober 2019

De link in de phishing e-mail leidde naar een Excel document, dat op 15 oktober 2019 om 14:55:27 onder het gebruikersaccount ******** op werkstation is geopend. In het Excel document bevond zich een macro. Deze macro heeft van een externe server met domeinnaam `windows-en-us-update.com` en IP-adres `185.225.17.99`, de zogenaamde SDBBot malware opgehaald, en uitgevoerd op het werkstation

Op 16 oktober 2019 om 09:07:51[2] heeft het e-mailadres `********maastrichtuniversity.nl` en vijf andere e-mailadressen van Opdrachtgever een phishing e-mail ontvangen met als onderwerp `CL meeting schedule.xls`. De vijf overige e-mailadressen staan vermeld in de volledige timeline.

[1] Deze datum en dit tijdstip is gebaseerd op de ontvangstdatum van de mailserver van Opdrachtgever. De datum en het tijdstip bovenaan Figuur 2 zijn afhankelijk van de tijdsinstellingen van het systeem waarvandaan de e-mail verstuurd is.

[2] Deze datum en dit tijdstip is gebaseerd op ontvangstdatum van de mailserver van Opdrachtgever. De datum en het tijdstip bovenaan Figuur 3 zijn afhankelijk van de tijdsinstellingen van het systeem waarvandaan de e-mail verstuurd is..


wo 16-10-2019 14:08

CL meeting schedule.xlsx

To

You forwarded this message on 16-10-2019 15:28.
This message was sent with High importance.

Hi,

Thank you for offering to find rooms for me for this schedule. I can eventually attached it!
https://dw1.dropbox-eu.com/?Nx2A3lOyY6e85K- :@maastrichtuniversity.nl-6H4pyTOa1V530zYGSa8mATOs6dE31BELIlAoobymtee707Ibh74281Ui83lIAeNUuB08ivu65rWFNEs37IE4IQ

Thanks again
Michelle

Figuur 3 - Phishing e-mail ontvangen op 16 oktober

De link in deze phishing e-mail leidde de gebruiker van account ********, op 16 oktober 2019 om 12:52:28, naar een soortgelijk Excel-document. De gebruiker van account ********maakte op dit moment gebruik van een virtueel werkstation dat draaide op server . Op dit systeem haalde de macro de SDBBot malware binnen vanaf een externe server met domeinnaam `windows-afx-update.com` en IP-adres `185.212.128.146`. Vervolgens is de malware uitgevoerd op het systeem.

Op beide systemen communiceerde de SDBBot malware vervolgens elke 15 minuten met een externe server met de domeinnaam `drm-server13-login-microsoftonline.com` en IP-adres `195.123.242.250`. Bovendien registreerde SDBBot zichzelf op beide systemen in het Windows systeemregister, waardoor de malware ook na het opnieuw opstarten van de systemen weer actief werd.

Via de infecties op de twee systemen van bovenstaande gebruikers heeft de aanvaller de eerste toegang verkregen tot het netwerk van Opdrachtgever.

5.2 Verspreiding binnen het netwerk

In de periode van 16 oktober 2019 tot en met 23 december 2019 is de aanvaller op meerdere dagen actief geweest. Vanaf de initieel gecompromitteerde werkstations heeft de aanvaller zichzelf toegang verschaft tot de rest van het netwerk van Opdrachtgever. Deze paragraaf beschrijft de belangrijkste gebeurtenissen gedurende deze periode.

5.2.1 Eerste handmatige activiteit van de aanvaller

Op 16 oktober 2019 om 19:35:03 werd op het virtuele werkstation dat in gebruik is bij de gebruiker van account ******** via de SDBBot malware een andere type malware gestart, namelijk Meterpreter[3]. Deze malware wordt primair ingezet door aanvallers om handmatig met de systemen van slachtoffers te interacteren. Dit is dan ook de eerste indicatie dat de aanvaller handmatig, via de virtuele desktop van account ********, het netwerk van Opdrachtgever heeft benaderd.

[3] Meterpreter is de zogenaamde payload van de penetratie testing software Metasploit (https://www.metasploit.com/)

5.2.2 Aanvaller krijgt toegang tot servers en verkent het netwerk

Op 17 oktober 2019 heeft de aanvaller de eerste servers binnen het netwerk van Opdrachtgever gecompromitteerd. De aanvaller heeft de Meterpreter malware om 17:33:22 op de server en om 17:40:33 op de server gestart. Hoewel uit de beperkte forensiscne sporen op deze twee systemen niet blijkt hoe de aanvaller dit heeft gedaan, is het mogelijk dat hier de zogenaamde EternalBlue exploit voor is gebruikt. Beiden servers draaiden namelijk nog op het niet langer door Microsoft ondersteunde besturingssysteem Windows Server 2003 R2, waar de MS17-010[4] patch niet op is geïnstalleerd. Deze patch zou de kwetsbaarheid die EternalBlue misbruikt hebben verholpen. Met de EternalBlue exploit kan een aanvaller vanaf een ander systeem in het netwerk toegang krijgen tot doel-systeem en malware uitvoeren met het lokale SYSTEM account.

De Meterpreter malware is op 20 oktober 2019 om 19:00:33 ook op de server gestart, en diezelfde dag om 19:02:45 ook op de server. De server draaide op het besturingssysteem Windows Server 2012 R2 en was ook kwetsbaar voor de EternalBlue exploit. De UM-erver is niet kwetsbaar voor de EternalBlue exploit, uit forensisch onderzoek blijkt niet hoe de aanvaller de Meterpreter malware op dit systeem heeft kunnen starten.

Op de vier hierboven genoemde servers is de Meterpeter malware gestart onder het lokale Windows account SYSTEM. Met dit account had de aanvaller lokale administrator-rechten op de servers. Nadat de aanvaller administrator-rechten heeft bemachtigd op meerdere servers binnen het netwerk van Opdrachtgever is deze teruggevallen op de twee initieel gecompromitteerde werkstations om vanuit daar het netwerk verder te verkennen. Op 24 oktober 2019 vanaf 11:38:50 maakte de aanvaller op werkstation ., dat in gebruik is bij de gebruiker van account ********, gebruik van PowerSploit[5]. Het betreft een verzameling van PowerShell-scripts dat oorspronkelijk is bedoeld om de beveiliging van een netwerk te testen, maar ook voor malafide doelen wordt ingezet. Met deze PowerShell-scripts heeft de aanvaller het interne netwerk gescand en geprobeerd om ook kwetsbaarheden te vinden op het werkstation zelf.

Op 24 oktober 2019 om 15:17:57 heeft de aanvaller PingCastle[6] gebruikt op het virtuele werkstation van account ********. Met PingCastle kon de aanvaller (grafisch) in beeld brengen hoe de Active Directory-structuur van Opdrachtgever is geconfigureerd, om eventuele zwakheden vervolgens uit te kunnen buiten.

> *Uit de manier waarop de aanvaller zich door het netwerk van Opdrachtgever beweegt, blijkt specifiek binnen het Windows domein UNIMAAS in beperkte mate sprake te zijn van netwerksegmentering.*

5.2.3 Aanvaller verkrijgt domain admin rechten

Op 21 november 2019 om 11:34:57 was de aanvaller weer actief op de virtuele desktop van account ********, vanaf waar om 13:06:22, een verbinding is opgezet naar server . Om 13:07:46 lukt het de aanvaller om de Meterpreter malware op de server uit te voeren met

[4] https://www.microsoft.com/en-us/download/details.aspx?id=55248

[5] https://github.com/PowerShellMafia/PowerSploit

[6] https://www.pingcastle.com/

het lokale Windows account SYSTEM. Met dit account heeft de aanvaller administrator-rechten op de server.

Zoals eerder beschreven kan Fox-IT aan de hand van forensisch onderzoek niet exact vaststellen hoe de aanvaller exact de heeft gecompromitteerd, maar blijkt uit het onderzoek wel dat ook op 21 november 2019 niet de meest recente Windows patches waren geïnstalleerd[7]. Hierdoor was de server onder andere kwetsbaar voor de EternalBlue exploit.

Ongeveer 10 minuten na het compromitteren van de server, om 13:19:53, heeft de aanvaller ingelogd op één van de Domain Controllers, UM van Opdrachtgever. De aanvaller maakte hiervoor gebruik van het account Administrator.UNIMAAS, een account met domein administrator rechten. De aanvaller had met dit account volledige beheerrechten binnen het UNIMAAS domein.

Hoewel Fox-IT geen forensische sporen heeft aangetroffen die aantonen hoe de aanvaller toegang heeft gekregen tot het Administrator.UNIMAAS account, is het aannemelijk dat de inloggegevens van dit account in het geheugen stonden van de eerder gecompromitteerde server. Het Administrator.UNIMAAS account heeft namelijk een gebruikersfolder op de server, wat een indicatie is dat het account in het verleden is ingelogd op deze server.

Met de inloggegevens van het Administrator.UNIMAAS account en toegang tot de Domain Controller had de aanvaller toegang tot het account met de hoogste rechten en toegang tot het systeem met de hoogste rechten binnen het netwerk van Opdrachtgever. De aanvaller heeft vervolgens zowel Cobalt Strike[8] als Meterpreter gebruikt op UM , onder andere om de software PingCastle uit te kunnen voeren.

Op 19 december 2019 om 14:49:25 heeft de aanvaller op deze Domain Controller (UM-) ook de software AdFind[9] gebruikt. Het gaat om een combinatie van verschillende Active Directory tools die gebruikt is om een overzicht te maken van de verschillende processen en services die op servers en werkstations binnen het Windows netwerk van Opdrachtgever draaien.

> *Doordat de aanvaller de inloggegevens van account Administrator.UNIMAAS heeft weten te verkrijgen, had de aanvaller toegang tot zowel het systeem met de hoogste rechten (Domain Controller) als de gebruiker met de hoogste rechten (Domein Administrator rechten) binnen het netwerk van Opdrachtgever.*

5.3 Voorbereiden en uitrollen van ransomware

Met toegangsrechten tot het gehele Windows domein van Opdrachtgever in bereik is de aanvaller op 23 december 2019 om 17:53:52 gestart met de voorbereiding van de laatste fase van de aanval: de uitrol van de ransomware.

---

[7] Op 2 december 2019 wordt op het systeem Windows update KB4525243 geïnstalleerd door Opdrachtgever, waardoor de server niet meer kwetsbaar is voor EternalBlue

[8] Een commercieel software pakket voor het uitvoeren van penetratie testen, vergelijkbaar met Metasploit (https://www.cobaltstrike.com/)

[9] http://www.joeware.net/freetools/tools/adfind/

Om deze aanval zo gecontroleerd mogelijk uit te voeren heeft de aanvaller gebruik gemaakt van software met de bestandsnaam `sage.exe`. Deze software heeft de aanvaller ondersteund bij het uitrollen van de ransomware binnen het netwerk van Opdrachtgever. Het bestand `sage.exe` is op 23 december 2019 vanaf 17:53:52 op vier systemen geplaatst: `02` `04`, `89` en `17`. Op één server, `04`, werd de software gedetecteerd en verwijderd door de McAfee antivirus software.
De aanvaller heeft vervolgens met het lokale administrator account `admin` de McAfee antivirus software verwijderd van de server, en heeft `sage.exe` vervolgens opnieuw op de server geplaatst. Vervolgens heeft de aanvaller ook de McAfee antivirus software van de servers `02` en `17` verwijderd.

Uiteindelijk heeft de aanvaller gebruik gemaakt van drie servers, `02`, `04` en `17`, om de ransomware aanval te starten. Daarvoor is op deze drie servers `sage.exe` in de `C:\Users\Public\Music\` folder geplaatst. Vervolgens heeft de aanvaller tijdens het opstarten van `sage.exe` bepaalde argumenten meegegeven, zoals de naam en het pad van de daadwerkelijke ransomware en andere instellingen die worden gebruikt om deze ransomware te starten. Zodra `sage.exe` wordt uitgevoerd, draait deze onder de Windows service genaamd `Winsysstrinsag`.

Op 23 december 2019 om 18:26:51 is vanaf de drie hierboven genoemde systemen de ransomware aanval op het volledige Windows netwerk van Opdrachtgever gestart. Hiervoor heeft de aanvaller het domein administrator account gebruikt om via `sage.exe` de ransomware, met de bestandsnaam `swaqp.exe`, te starten op alle Windows servers die onderdeel uitmaken van het `UNIMAAS` domein. Hierbij is gebruik gemaakt van een service met de naam `psxexesvc`[10]. De aanvaller maakte tevens gebruik van `sage.exe` om op alle systemen, voor het starten van de ransomware, Windows Defender uit te schakelen.

Omstreeks 18:52:34 heeft op minimaal 267 servers de ransomware zijn schade aangericht door alle bestanden[11] te versleutelen. Onder de getroffen systemen bevinden zich zeer kritieke systemen voor de bedrijfsvoering van Opdrachtgever zoals de Domain Controllers, Exchange servers, File servers met onderzoek- en bedrijfsvoering gegevens en een aantal van de back-up servers. Op deze back-up servers stonden mogelijk kopieën van (een gedeelte van) de op de andere servers versleutelde data. Van deze back-up server is een overzicht terug te vinden in Tabel 7.

Tabel 7 - Lijst van back-up systemen

Hostname	Omschrijving	Versleuteld op
ICTS	DPM (Exchange omgeving)	23-12-2019 18:31:25
ICTS	DPM (Exchange omgeving)	23-12-2019 18:31:59
ICTS-	DPM (Exchange omgeving)	23-12-2019 18:47:33
ICTS-	DPM (Exchange omgeving)	23-12-2019 18:31:25
ICTS-	DataProtector (Fysieke machines, SAP)	23-12-2019 18:47:59
ICTS	DataProtector (Fysieke machines, SAP)	23-12-2019 18:30:01
ICTS-	Veeam (Virtuele servers)	23-12-2019 18:47:40
ICTS-	Veeam (Virtuele servers)	23-12-2019 18:34:42
ICTS-	Veeam (Virtuele servers)	23-12-2019 18:47:33
ICTS-	Veeam (Virtuele servers)	23-12-2019 18:47:33

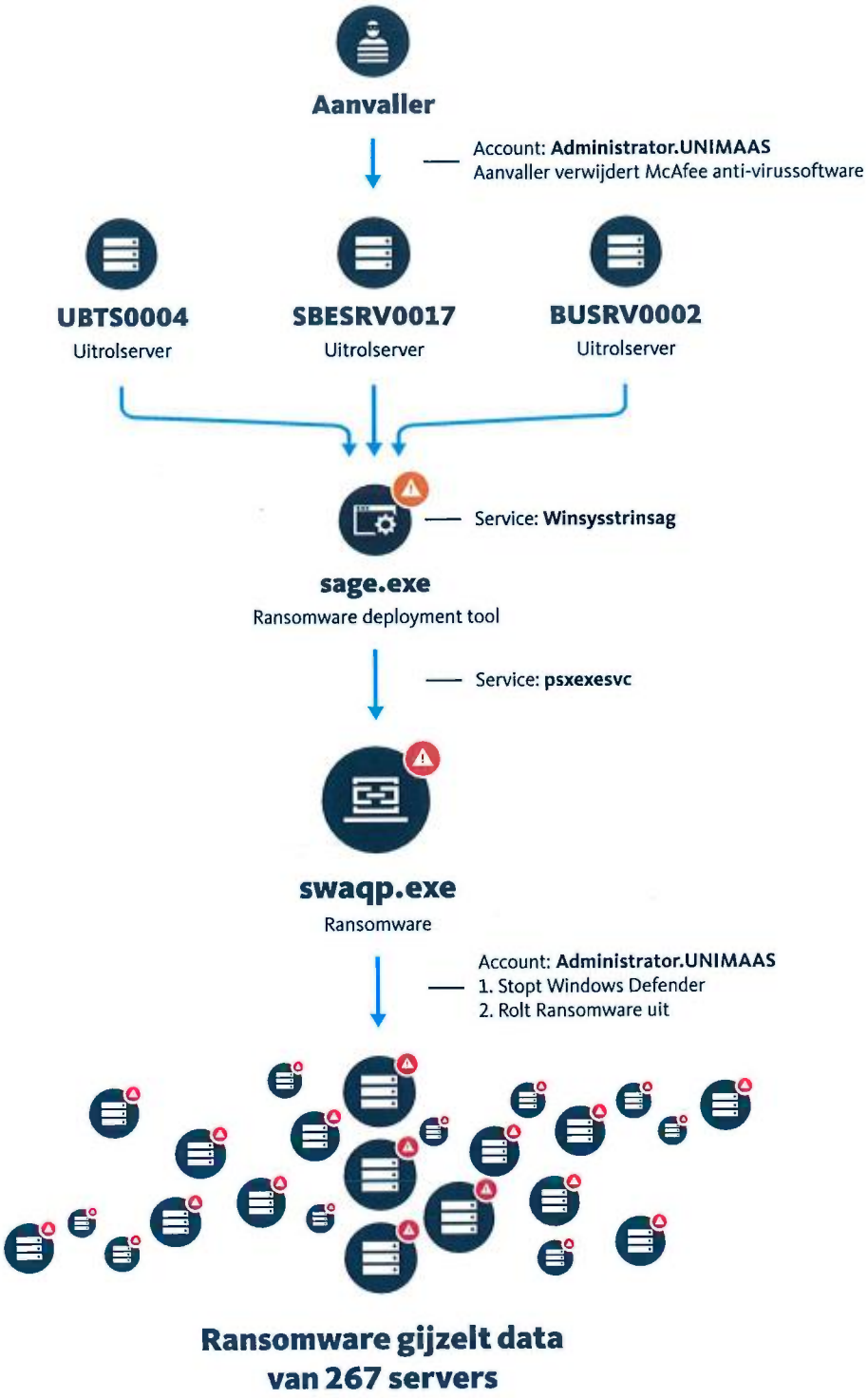
[10] De aanvaller heeft hier een service naam gebruikt die lijkt op die van de legitieme Windows beheer software PsExec

[11] De ransomware heeft geen bestanden versleuteld die impact zouden kunnen hebben op het functioneren van het Windows besturingssysteem

Hostname	Omschrijving	Versleuteld op
ICTS-	Veeam (Virtuele servers)	23-12-2019 18:47:37
ICTS-	Veeam (Virtuele servers)	23-12-2019 18:47:37

Doordat back-up servers onderdeel waren van het UNIMAAS domein en er verder op netwerkniveau geen segmentatie is aangebracht heeft de aanvaller meerdere back-ups kunnen versleutelen.

Figuur 4 is een (op hoofdlijnen) grafische weergave van de in dit hoofdstuk beschreven ransomware uitrol.



Figuur 4 - Uitrol van de ransomware

5.3.1 Over de ransomware

De ransomware die de aanvaller heeft gebruikt is de zogenaamde Clop[12] ransomware. Deze ransomware versleutelt bestanden door middel van het RC4 encryptie algoritme. De RC4 sleutel wordt per bestand willekeurig gegenereerd en wordt vervolgens weer versleuteld met een RSA-1024 bits publieke sleutel. Alleen de aanvaller heeft de bijbehorende geheime sleutel. Aan bestandsnamen van bestanden die zijn versleuteld door de ransomware wordt bovendien `.CIop` (hoofdletter 'i') aan de bestandsnaam toegevoegd. In elke folder waarin de ransomware bestanden versleutelt, wordt tevens een instructie geplaatst die is gericht aan het slachtoffer. In dit bestand met de naam `CIopReadMe.txt` (hoofdletter 'i') was bij Opdrachtgever de volgende tekst terug te vinden:

```
*-*ALL FILES ON EACH HOST IN THE NETWORK HAVE BEEN ENCRYPTED WITH A STRONG ALGORITHM*-*

-Backups were either encrypted or deleted or backup disks were formatted.
-Shadow copies also removed, so F8 or any other methods may damage encrypted data but not
recover.
-If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 3-5 encrypted files
-(Less than 6 Mb each, non-archived and your files should not contain valuable information
-(Databases, backups, large excel sheets, etc.)).
-You will receive decrypted samples.

-MESSAGE THIS INFORMATION TO COMPANY'S CEO, UNLOCKING OF 1 COMPUTER ONLY IS IMPOSSIBLE, ONLY
WHOLE NETWORK.
-ATTENTION-
-Your warranty - decrypted samples.
-Do not rename encrypted files.
-Do not try to decrypt your data using third party software.
-We don`t need your files and your information.

:::CONTACT EMAIL:::

AND

or


NOTHING PERSONAL IS A BUSINESS
PLEASE DO NOT USE GMAIL, MAIL DOES NOT REACH OR GETS INTO THE SPAM FOLDER.
PLEASE CHECK SPAM FOLDER!!! CLOP^_-
```

[12] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/

5.4 Detectie van aanvallersactiviteit

Dit hoofdstuk beschrijft de verschillende momenten waarop activiteit van de aanvaller is gedetecteerd. Het gaat om detectie door detectiemaatregelen die bij Opdrachtgever al aanwezig in het netwerk waren voordat de aanval op de avond van 23 december aan het licht kwam. Hoewel de meldingen uit deze detectiemaatregelen grotendeels naar een centrale log-server worden gestuurd, wordt er door Opdrachtgever niet proactief naar deze meldingen gekeken of op geacteerd. Dit heeft onder andere bijgedragen aan het feit dat de aanvaller zijn activiteit kon voortzetten.

5.4.1 24 oktober 2019

Op 24 oktober 2019 heeft de aanvaller vanaf 11:38:50 gebruik gemaakt van PowerSploit op het systeem dat in gebruik was door account ********. Met deze PowerShell scripts heeft de aanvaller het interne netwerk gescand en geprobeerd om ook kwetsbaarheden te vinden op . Gedurende deze activiteit op systeem heeft Windows Defender om 11:41:25 één van de PowerShell scripts, PowerView, gedetecteerd en verwijderd met de volgende omschrijving[13]:

```
Threat_Name="HackTool:PowerShell/PowerView.A" Severity_ID="4" Severity_Name="High"
```

5.4.2 19 december 2019

Op 19 december 2019 was de aanvaller vanaf 14:44:58 op meerdere systemen van Opdrachtgever actief. Op één van deze servers, 04, heeft de aanvaller vanaf 16:35:11 zowel Cobalt Strike als Mimikatz uitgevoerd met het account admin.

Op dit systeem draaide McAfee Enterprise Endpoint Security dat voor het scannen en detecteren van potentieel kwaadaardige scripts in de zogenaamde Observer mode stond ingesteld. Deze instelling komt overeen met de standaard-instelling van deze programmatuur. Dit wil zeggen dat de software wel kwaadaardige scripts detecteert en logt naar de Windows Event Log logbestanden, maar deze niet blokkeert. In dit logbestand is te zien dat de McAfee anti-virus software tot drie keer toe, binnen korte tijd, heeft gedetecteerd dat de aanvaller Cobalt Strike opstart. Een voorbeeld van een dergelijke registratie:

```
'admin ran C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe. The
Trojan named CobaltStrike!4A9074C4D0EE was detected but wasn't blocked because AMSI was set
to Observe mode."
```

Ook is in de Windows Event Log logbestanden te zien dat de aanvaller tot negen keer toe, binnen korte tijd, Mimikatz heeft opgestart. Een voorbeeld van een dergelijke registratie:

```
admin ran C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe. The
Trojan named PS/Mimikatz.c!D45F343464D8 was detected but wasn't blocked because AMSI was set
to Observe mode."
```

5.4.3 23 december 2019

Zoals beschreven in hoofdstuk 5.3 is de aanvaller op 23 december 2019 gestart met de voorbereiding van de ransomware aanval. Tijdens deze voorbereiding heeft de McAfee antivirus software om 17:55:46

[13] De complete log-regel kan terug worden gevonden in de volledige timeline

op de server UBTS0004 de ransomware deployment software sage.exe gedetecteerd en verwijderd. Dit heeft een Windows event log entry gegenereerd, met daarin de volgende detectie:

```
NT AUTHORITY\\SYSTEM ran C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe,
which attempted to access C:\\Users\\Public\\Music\\sage.exe. The Trojan named Generic
Trojan.ip was detected and deleted.
```

5.5 Tijdlijn van belangrijke gebeurtenissen

Dit hoofdstuk beschrijft op grote lijnen de belangrijke gebeurtenissen welke uit het onderzoek naar voren zijn gekomen. Een compleet overzicht van de tot nu toe bekende gebeurtenissen is te vinden in het bijgevoegde Excel document Fontana_Timeline.xlsx.

Tabel 8 - Tijdlijn van belangrijke gebeurtenissen

Tijd	Bron	Hostname	Beschrijving
15-10-2019 16:56:03	Netwerk logs		Eerste SDBbot-infectie op werkstation van account ********
16-10-2019 12:52:28	Netwerk logs	60	Tweede SDBBot-infectie op werkstation van account ********
16-10-2019 19:35:03	Netwerk logs	60	Eerste handmatige aanvallersactiviteit, op het werkstation van account *********
17-10-2019 17:33:22	Netwerk logs	54	Eerste compromittatie van een server
24-10-2019 11:41:25	Event logs		Windows Defender detecteert en verwijdert Powerview malware
21-11-2019 13:06:22	Event logs	UM	Aanvaller compromitteert de server en verkrijgt hier toegang tot een account met domein administrator rechten
21-11-2019 13:19:59	Event logs	UM-	Aanvaller logt in op een Domain Controller met account met domein administrator rechten
19-12-2019 16:35:11	Event logs	04	McAfee antivirus software detecteert meerdere keren aanvallersactiviteit
23-12-2019 17:53:52	Event logs, MFT	17, 04, 02, 89	Aanvaller start voorbereiding ransomware uitrol
23-12-2019 17:55:46	Event logs	04	McAfee antivirus software detecteert en verwijdert ransomware deployment tool
23-12-2019 18:26:51	MFT, AppCompat, Event logs, USNJRNL, Shimcache	267 servers	Aanvaller start uitrol van ransomware
23-12-2019 18:52:34	MFT, AppCompat, Event logs, USNJRNL, Shimcache	267 servers	Grootste deel van Windows servers Opdrachtgever is versleuteld door ransomware
23-12-2019 18:55:35	Event logs	04	Laatste activiteit van aanvaller op systeem van Opdrachtgever

Tijd	Bron	Hostname	Beschrijving
24-12-2019 00:35	Telefonisch	-	Opdrachtgever neemt contact op met Fox-IT
30-12-2019 13:50:26	E-mail	-	Opdrachtgever ontvangt decryptie sleutel van aanvaller

5.6 Over de aanvaller

In het kader van Threat Intelligence vergaart Fox-IT al jaren informatie over criminelen die vanuit een financieel oogmerk opereren, en daarvoor organisaties wereldwijd compromitteren. De modus operandi van de groepering achter deze specifieke aanval komt overen met een criminele groepering die al een lange historie heeft, en terug gaat tot tenminste 2014. Publiek wordt de groep vaak gerefereerd als "TA505", als wel "GraceRAT", genoemd naar één van de tools die gebruikt werd door de groep. Historisch heeft Fox-IT de groep ook gerefereerd als "Dridex-RAT-groep", aangezien de groep samenwerkte met de "Dridex" groep en veelvuldig gebruikt maakte van zogenaamde "Remote Administration Tools".

In de recente historie, sinds februari 2019, is de groep begonnen met het gebruik van de ransomware (Clop) gericht op organisaties die gebruik maken van een Microsoft Windows domein. Uit data van Fox-IT blijkt dat de groep al meer dan 150 slachtoffers heeft gemaakt in 2019. Bij al deze slachtoffers gaat de groep op hoofdlijnen hetzelfde te werk:

1) infecteren van één of meerdere systemen door middel van wijdverspreide phishing e-mails;
2) identificeren van organisatie;
3) lateraal bewegen binnen het netwerk;
4) verwijderen of versleutelen van back-ups;
5) uitrollen van ransomware op zo veel mogelijk systemen;
6) eisen van losgeld per e-mail (de hoogte van het geëiste bedrag is afhankelijk van de grootte van de organisatie).

Eerder in de periode van 2014 tot en met 2017 is de groep veelal betrokken geweest bij aanvallen op slachtoffers in de financiële sector, zowel in West-Europa als wel de Verenigde Staten.

In de periode van 2017 tot begin 2019 is de groep voornamelijk betrokken geweest bij aanvallen op financiële instellingen waarbij vaak creditcard uitgeef-systemen het doelwit waren, De buitgemaakte data werd daarna doorverkocht via verschillende creditcard-shops. De financiële instellingen waren hoofdzakelijk gelokaliseerd in Zuid- en Centraal Amerika, Afrika en Centraal- en Zuidoost Azië waarbij tientallen banken slachtoffer zijn geworden van aanvallen op hun netwerk. Deze aanvallen waren niet exclusief in deze periode; pogingen om slachtoffers in de financiële sector te compromitteren vinden nog steeds plaats.

5.7 Gecompromitteerde systemen en accounts

In onderstaande Tabel 9 zijn de hostnames van systemen genoemd in volgorde waarop deze door de aanvaller zijn gecompromitteerd. Ook is bij de activiteit genoemd op basis waarvan een systeem als gecompromitteerd wordt beschouwd door Fox-IT.

Systemen die zijn besmet met de ransomware worden door Fox-IT ook beschouwd als gecompromitteerd. Voor de leesbaarheid is Tabel 9 een beknopte lijst geworden. Een volledig overzicht van alle gecompromitteerde systemen is te vinden in Appendix A.2.

Tabel 9 - Gecompromitteerde systemen

Datum / tijd	Hostname	Activiteit
15-10-2019 14:56:03		SDBBot, PowerSploit
16-10-2019 12:52:28	Virtueel werkstation op	SDBBot, PingCastle, Cobalt Strike, Meterpreter
17-10-2019 17:33:22	54	Meterpreter
17-10-2019 17:40:33	50	Meterpreter
20-10-2019 19:00:33	56	Meterpreter
20-10-2019 19:02:45	49	Meterpreter
21-11-2019 13:14:49	05	Cobalt Strike
21-11-2019 13:19:53		Cobalt Strike, AdFind
19-12-2019 16:34:34	02	sage.exe
19-12-2019 16:35:03	04	Cobalt Strike, Mimikatz, sage.exe
19-12-2019 16:35:45		Cobalt Strike
19-12-2019 16:36:09		Cobalt Strike
19-12-2019 16:36:12	um-	Cobalt Strike
19-12-2019 16:36:32	17	Cobalt Strike, sage.exe
19-12-2019 16:36:32	UM-	Cobalt Strike
19-12-2019 16:37:06	UM-	Cobalt Strike, sage.exe
23-12-2019 04:16:57	UM-	Cobalt Strike, Invoke-WssBpaScan
23-12-2019 16:36:35	ICTS-	Cobalt Strike

Los van gecompromitteerde systemen heeft Fox-IT ook accounts geïdentificeerd die door de aanvaller zijn gebruikt en derhalve beschouwd dienen te worden als gecompromitteerd. Een overzicht van deze accounts is terug te vinden in Tabel 10. Hoewel dit de accounts zijn waarvan Fox-IT tijdens het onderzoek heeft bevestigd dat deze zijn gebruikt door de aanvaller, had de aanvaller in feite toegang tot alle accounts in het UNIMAAS domein: de aanvaller heeft immers op 21 november 2019 om 13:19:53 domein administrator rechten verkregen.

Tabel 10 - Gecompromitteerde accounts

Datum / tijd	Accountnaam	Omschrijving
15-10-2019 14:55:27	********	Gebruikersaccount ********
16-10-2019 12:52:28	********	Gebruikersaccount ********
21-11-2019 13:19:53	Administrator.UNIMAAS	Account met domein administrator rechten
20-10-2019 19:02:45	Administrator	Lokaal administrator account van UM-DB11049
19-12-2019 16:35:15	admin	Administrator account van één van de beheerders van het UNIMAAS domein

5.8 Kroonjuwelen

Opdrachtgever heeft benadrukt specifiek geïnteresseerd te zijn in mogelijke aanvallersactiviteit op een aantal systemen die worden beschouwd als kritiek voor de bedrijfsvoering (hierna: kroonjuwelen). Opdrachtgever heeft omwille van efficiënte allocatie van onderzoeksmiddelen een selectie van kroonjuwelen aangedragen waar direct aandacht voor diende te zijn vanuit onderzoeksperspectief:

- CORSA (bestaande uit systemen UM- en UM-
- MUSL-share (bestaande uit systeem UM-
- Maastricht studie (bestaande uit systemen UM- en UM-

Van de kroonjuwelen CORSA en MUSL-share heeft Fox-IT Acquire data ontvangen die door Opdrachtgever is verzameld. Op basis van de voor Fox-IT bekende IOCs zijn er, anders dan de ransomware die de bestanden op de servers hebben versleuteld, geen sporen van aanvallersactiviteit gevonden. Het onderzoek op deze twee kroonjuwelen heeft zich dus echter beperkt tot de bekende IOCs, en bovendien tot de beperkte informatie die door Fox-IT Acquire zijn verzameld. Fox-IT adviseert een vollediger onderzoek uit te voeren op alle servers van de beide kroonjuwelen om een vollediger beeld te kunnen schetsen.

Van het derde kroonjuweel, de Maastricht studie, kan vanwege de omvang van de data op de te onderzoeken servers, vanuit Opdrachtgever geen forensische data aangeleverd worden. Het advies van Fox-IT is om op locatie bij Opdrachtgever een forensisch onderzoek op dit derde kroonjuweel uit te laten voeren.

6 Conclusies

Op basis van de bevindingen uit het uitgevoerde onderzoek trekt Fox-IT de volgende conclusies:

1 Wat is de toedracht van het incident?
De aanvaller heeft toegang verkregen tot het netwerk van Opdrachtgever door middel van twee phishing e-mails die geopend werden op twee werkstations die verbonden waren met het netwerk van Opdrachtgever. In de phishing e-mails bevond zich een link naar een Excel document waarin zich een macro bevond die malware heeft geïnstalleerd op de twee werkstations. Via de malware-infecties op deze twee systemen heeft de aanvaller de eerste toegang verkregen tot het netwerk van Opdrachtgever. Van daaruit heeft de aanvaller zich lateraal door het netwerk bewogen.

2 Wat is de oorzaak van het incident?
Door een combinatie van ontbrekende belangrijke beveiligingsupdates, beperkte segmentatie binnen het netwerk en het niet opvolgen van verschillende alarmsignalen, was de aanvaller in staat ongestoord door het netwerk te bewegen. Vervolgens kon ransomware worden uitgerold naar belangrijke servers van Opdrachtgever. Een combinatie van niet adequaat oppakken van alarmsignalen en onveilige netwerk- en systeemconfiguraties liggen ten grondslag aan het incident.

3 Wat is de omvang van het incident?
In totaal zijn in het onderzoek 269 Microsoft Windows systemen, voornamelijk centraal beheerde servers, geïdentificeerd als geraakt door de aanval. Onder de getroffen systemen bevinden zich voor de bedrijfsvoering van Opdrachtgever zeer kritieke systemen zoals de Domain Controllers, Exchange servers, File servers met onderzoeksgegevens en een aantal back-up servers.

4 Welke data is benaderd door de aanvaller?
Uit het forensische onderzoek naar de activiteit van de aanvaller blijkt dat de aanvaller als primaire focus het breed uitrollen van ransomware had. Hiervoor is de aanvaller handmatig actief geweest op 18 servers met een vijftal accounts. Zo is het netwerk verkend, zijn gebruikersnamen en wachtwoorden van accounts met hoge rechten verkregen en is vervolgens ransomware uitgerold.

Fox-IT heeft op basis van de beschikbare onderzoek data, en binnen de temporele kadering geen activiteit van de aanvaller geobserveerd, anders dan het verzamelen van data aangaande de topologie van het netwerk, gebruikersnamen en wachtwoorden en aanvullende data ten dienste van het realiseren van bovenstaand beschreven primaire focus.

5 Zijn gegevens ingezien of ontvreemd van door Opdrachtgever geïdentificeerde kroonjuwelen?
Wat betreft de kroonjuwelen kan, technisch gezien, op het moment van schrijven gelet op de scope van het onderzoek niet met een grote mate van waarschijnlijk worden vastgesteld of data daarvan is ingezien, ontvreemd, of anderszins is verwerkt door de aanvaller. Op basis van de beschikbare onderzoeksgegevens is in ieder geval aanvallersactiviteit waargenomen op drie van de vijf servers die zijn aangewezen als kroonjuweel. Derhalve adviseert Fox-IT vervolgonderzoek uit te voeren op de kroonjuwelen om met een grotere waarschijnlijkheid uitspraken te kunnen doen over de activiteit van de aanvaller op deze systemen en de gevolgen daarvan voor Opdrachtgever.

7 Aanbevelingen

Dit hoofdstuk bevat aanbevelingen verdeeld over twee categorieën. De eerste subsectie bevat aanbevelingen gebaseerd op bevindingen vanuit het onderzoek. De aanbevelingen kunnen bijdragen aan een hoger beveiligingsniveau waarmee de kans op vergelijkbare incidenten in de toekomst zal worden verkleind. Het risicomitigatie-hoofdstuk is onderverdeeld in drie categorieën; Preventie, Detectie en Response. De tweede subsectie bevat aanbevelingen voor vervolgonderzoek.

7.1 Preventie

Train security awareness van medewerkers

Fox-IT heeft tijdens het onderzoek waargenomen dat de initiële compromittatie heeft plaatsgevonden via een phishing e-mail.

De mens is veelal de zwakste schakel in de cyber security keten. Mensen zijn zich onbewust van het risico wanneer ze onbetrouwbare websites bezoeken, klikken op links in ongevraagde e-mails of niet geverifieerde software uitvoeren op hun systeem. Het niveau van security awareness kan verhoogd worden door middel van het organiseren van periodieke awareness sessies of door een online awareness cursus. Het niveau van awareness dient periodiek beproefd te worden met bijvoorbeeld een phishing test.
Eveneens is het van belang van de reeds aanwezige open communicatie-cultuur gebruik te maken, zodat melding kan worden gemaakt van het (onbedoeld) genereren van een security incident (bijvoorbeeld na te klikken op een phishing link). Security awareness bij de ontvangende partij van een dergelijke melding, zou er aan kunnen bijdragen dat deze meldingen worden opgevolgd en adequaat geadresseerd.

Fox-IT raadt aan om een security awareness programma in te richten waar trainingen een onderdeel van zijn. Ook raadt Fox-IT aan om, waar dit nog niet is gebeurd, werknemers en studenten van richtlijnen te voorzien betreffende bijvoorbeeld het maken van sterke wachtwoorden, en wat te doen bij het vermoeden van een security incident.

Voer geen beheer werkzaamheden met domein administrator accounts uit

Tijdens het onderzoek is gebleken dat beheerwerkzaamheden zijn verricht met domein administrator accounts. Hierdoor was het wachtwoord mogelijk aanwezig in het geheugen van een gecompromitteerd systeem.

Domein administrator accounts dienen niet gebruikt te worden voor beheerwerkzaamheden anders dan op een domein controller. Wanneer een beheerder onderhoud moet verrichten aan een server dient deze hiervoor zijn eigen beheeraccount te gebruiken met zo min mogelijk rechten. Wanneer het domein administrator account wordt gebruikt voor onderhoud aan standaard servers, wordt het aanvalsoppervlak vergroot. Zo bestaat de kans dat het wachtwoord van dit account in bijvoorbeeld het geheugen van deze server terug te vinden is.

Om deze reden adviseert Fox-IT zo min mogelijk beheerwerkzaamheden uit te voeren met domein administrator accounts. Probeer zo veel mogelijk het principe van “least privilege” toe te passen.

Macro's

Op basis van het onderzoek kan met hoge waarschijnlijkheid worden vastgesteld dat de initiële compromittatie heeft plaatsgevonden middels macro's in een Excel document.

Macro's in Officedocumenten worden vaak gebruikt als aanvalsmethode om een systeem te compromitteren (bijvoorbeeld door middel van phishing). Het advies is daarom om het gebruik van macro's niet toe te staan. Als het gebruik van macro's essentieel is voor de bedrijfsvoering is het advies alleen digitaal getekende macro's toe te staan. Dit zorgt ervoor dat ongetekende macro's, met mogelijk kwaadaardige inhoud, niet geopend en uitgevoerd kunnen worden.

Fox-IT adviseert het gebruik van (ongetekende) macro's niet toe te staan.

Beschermde gebruikers groep

Tijdens het onderzoek is duidelijk geworden dat de aanvaller onder andere Mimikatz heeft gebruikt om inloggegevens buit te maken, waarmee de aanvaller verhoogde privileges kon verkrijgen binnen het netwerk.

Het concept van een 'beschermde gebruikersgroep' is geïntroduceerd[14] in Windows Server 2012 R2 en kan worden gebruikt om in te perken welke privileges de leden van de Active Directory beschermde gebruikersgroep krijgen toegekend. Op deze manier segmentatie van rechten in te regelen zijn deze gebruikers beter beschermd tegen bijvoorbeeld een pass-the-hash-attack[15]. De primaire functie van de beschermde gebruikersgroep is het beschermen tegen misbruik van inloggegevens van gebruikers wanneer deze inloggen op een systeem.

Het advies is om accounts met hogere privileges toe te voegen aan deze beschermde gebruikersgroep.

Houd besturingssystemen up to date

Tijdens het onderzoek is duidelijk geworden dat de aanvaller zich onder andere lateraal door het netwerk heeft kunnen bewegen door het gebruiken van de zogenaamde EternalBlue exploit. Deze exploit maakt misbruik van een lek in een netwerkprotocol van het Windows besturingssysteem. Microsoft heeft hiervoor een update beschikbaar gesteld (MS10-017) voor alle versies van Windows.

Het advies is om regelmatig de meest recente software-updates te installeren voor besturingssystemen, en om niet-ondersteunde installaties te upgraden naar een wel ondersteunde versie. Daarnaast is het advies om een procedure op te stellen, of waar deze al aanwezig is te verbeteren, waarin enerzijds het updateproces wordt geborgd, en anderzijds een verificatie plaatsvindt of een update al dan niet correct is geïnstalleerd. Dit proces zou kunnen worden vereenvoudigd door bijvoorbeeld een centraal gemanagede update faciliteit in te richten zoals Microsoft WSUS of SCCM.

Fox-IT adviseert om besturingssystemen en applicaties te voorzien van de meest recente software updates en om procesmatig te borgen dat dit structureel correct gebeurt.

---

[14] Voor meer informatie zie ook: hxxps://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

[15] Een hacking techniek waarbij een aanvaller authenticeert tegen een server door gebruik te maken van de wachtoord hash in plaats van de het gebruikersnaam en het wachtwoord.

Opgesomd adviseert Fox-IT op basis van het onderzoek om; geen beheerwerkzaamheden te verrichten met domein administrator accounts; het gebruik van ongetekende Macro's niet toe te staan; een beschermde gebruikersgroep in te richten; systemen & software up-to-date te houden; en security awareness van werknemers en studenten te verhogen.

7.2 Detectie

Netwerkmonitoring

Fox-IT heeft tijdens het onderzoek vastgesteld dat er in geen netwerkmonitoring is geïmplementeerd door Opdrachtgever voorafgaand aan en ten tijde van het incident.

Het continu monitoren van het netwerkverkeer waarbij de focus ligt op het detecteren van potentieel kwaadaardige activiteit, kan ervoor zorgen dat een aanval niet leidt tot een grootschalig security incident. Hierbij kan gebruik worden gemaakt van een groot aantal indicatoren die bij de aanwezigheid van malware op het netwerk een incident zouden veroorzaken.

Fox-IT adviseert om netwerkmonitoring voor zowel het interne, als uitgaande verkeer te implementeren.

Monitor logbestanden voor anomalieën

Tijdens het onderzoek is duidelijk geworden dat sommige systemen al weken of maanden gecompromitteerd waren voordat dit werd gedetecteerd.

Logbestanden kunnen worden gemonitord op sporen van afwijkend gedrag. Logregistraties kunnen bijvoorbeeld worden gemonitord op pieken in activiteit of activiteiten bestempeld als 'hoog risico'. Denk bij deze laatstgenoemde categorie aan specifieke zoekopdrachten naar complete databases, of (ongewone) loginactiviteiten op kritieke systemen waarbij gebruik wordt gemakt van accounts met hoge rechten. Aanvullend brengt dit de mogelijkheid met zich mee tot het doen van analyse nadat een incident heeft plaatsgevonden. Er is een grote verscheidenheid aan oplossingen beschikbaar voor een dergelijke inrichting van logmonitoring, vaak beschreven als SIEM (Security Information and Event Management).

Organisaties hebben vaak meerdere apparaten en applicaties in gebruik die security gerelateerde meldingen kunnen genereren, meestal in de vorm van log-data. Het gaat bijvoorbeeld om data uit een IPS (Intrusion Prevention System), Windows audit logs, antivirus-oplossingen en firewalls. Het monitoren van deze meldingen zorgt voor een significante toename van de kans op tijdige detectie van kwaadaardige activiteit binnen het netwerk. Het vereist echter wel een bepaalde mate van kennis op het gebied van technologie, expertise en processen om deze monitoring adequaat in te kunnen regelen en uitvoeren.

Opgesomd adviseert Fox-IT op basis van het onderzoek om netwerk- en logmonitoring te implementeren.

7.3 Response

Een centraal beheerde Configuration Management Database

Tijdens het onderzoek is duidelijk geworden dat Opdrachtgever geen compleet overzicht had van alle systemen en back-ups in haar IT-infrastructuur. De complexiteit van zowel centraal als decentraal gemanagede systemen zou deels ondervangen kunnen worden door een centraal beheerde Configuration Management Database (CMDB) voor de hele organisatie.

Het hebben van een up-to-date CMDB is essentieel zowel tijdens incident response activiteiten, als voor monitoring. Incident response leunt in grote mate op de beschikbare CMDB-informatie gedurende een onderzoek naar een mogelijke compromittatie. In een dergelijke database is informatie terug te vinden over de systeem status, de eigenaar, de functie en andere relevante netwerkinformatie.

Derhalve adviseert Fox-IT om een complete en accurate CMDB bij te houden, om een significante reductie in response tijd, en een toename in de efficiency van het response team te bewerkstelligen.

Incident response plan

Fox-IT heeft waargenomen dat Opdrachtgever tijdens het incident niet de beschikking had over een incident response plan voor dit soort calamiteiten.

Gedurende een crisissituatie zijn er veel acties die uitgevoerd moeten worden en resources die beschikbaar gesteld moeten worden. Een incident response plan helpt bij het plannen van deze benodigdheden. Een incident response plan zorgt ervoor dat er sneller op incidenten gereageerd wordt en dat de effectiviteit van incident response wordt verhoogd. Een doordacht plan bevat allocatie van menselijke resources en definitie van de crisisorganisatie en processen.

Fox-IT raadt aan om een incident response plan op te stellen, te onderhouden en periodiek te (laten) toetsen.

Data recovery plan

Tijdens het onderzoek heeft Fox-IT geobserveerd dat er geen kant-en-klaar data recovery plan voor handen was, en dat er ten tijde van het incident geen beschikking was over offline back-ups.

Het oefenen van crisissituaties zorgt ervoor dat het handelen tijdens een daadwerkelijke crisis gestroomlijnder verloopt. Dit is ook het geval voor een cybercrisis. Door een data recovery plan op te stellen, waarin zowel temporeel als op basis van prioriteit een indeling wordt gemaakt voor het herstel van (kritieke) systemen kan de business continuïteit efficiënter gerealiseerd worden. Een dergelijk plan dient periodiek getoetst en geoefend te worden, als mede up-to-date te zijn op basis van veranderingen in het netwerk of gebruik van systemen en applicaties. Denk hierbij aan het daadwerkelijk oefenen met het terugzetten van back-ups om vast te kunnen stellen of deze back-ups vervolgens naar behoren werken en de bedrijfsvoering hervat kan worden binnen acceptabele termijn.

Fox-IT adviseert om een data recovery plan op te stellen, waar offline back-ups onderdeel van zijn, en dit plan periodiek te (laten) toetsen op volledigheid en werkbaarheid.

Opgesomd adviseert Fox-IT op basis van het onderzoek om centraal een CMDB te beheren, een incident response plan op te stellen en een data recovery plan op te stellen; en om deze plannen te oefenen..

7.4 Vervolgonderzoek

Op basis van het onderzoek zijn 267 Windows servers geïdentificeerd als gecompromitteerd. Om vast te kunnen stellen wat de aanvaller op deze servers voor handmatige activiteiten heeft verricht raadt Fox-IT aanvullend onderzoek aan.

Omwille van temporele beperkingen is tijdens zowel de incident response fase als tijdens de root cause analyse door Opdrachtgever besloten het onderzoek naar data-extractie in eerste instantie te beperken tot de kroonjuwelen CORSA (UM- , MUSL-share (UM-) en de Maastricht studie (UM- en UM-I). Wat betreft de UM- en de UM- zijn binnen de door Acquire verzamelde data geen sporen van data-extractie aangetroffen. Fox-IT kan niet uitsluiten dat een dergelijke data-extractie van de data op deze kroonjuwelen niet heeft plaatsgevonden. Enerzijds is geen volledig onderzoek op de systemen uitgevoerd, en anderzijds kan data-extractie hebben plaatsgevonden vanuit andere bronnen zoals de (decentrale) servers of de mailboxen van individuen.

Om met een grotere waarschijnlijkheid uitspraken te kunnen doen over data-extractie adviseert Fox-IT om een breder forensisch onderzoek uit te voeren door middel van bijvoorbeeld e-Discovery op e-mail en een grondig forensisch onderzoek op (disk images van) de servers UM en de UM

Voor wat betreft het laatste kroonjuweel, de Maastricht studie, kan Fox-IT geen uitspraken doen over data-extractie, omdat zoals eerder besproken in hoofdstuk 0 het OS van de servers het niet mogelijk maakt de Dissect Acquire software te gebruiken. Ten tweede is de dataset te substantieel om via het Evidence Portal een kopie van aan te kunnen leveren bij het Fox-IT Lab. Derhalve is het advies wat betreft het derde kroonjuweel om op locatie forensisch sporen onderzoek te laten verrichten op de twee servers UM en UM-

Appendix A

In de onderstaande tabel is een lijst met begrippen gebruikt in dit document.

A.1 Verklarende woordenlijst

Term	Uitleg
Active Directory	Microsoft product dat bestaat uit een combinatie van services die draaien op een Windows server om permissies te managen, en te organiseren welke gebruikers, en wat voor systemen op welke manier toegang krijgen tot het netwerk.
Command & Control server	Systemen gebruikt om op afstand geïnfecteerde systemen te besturen. Command & Control (C&C) servers zijn in staat om commando's te versturen naar geïnfecteerde systemen (het botnet) en de resultaten daarvan te ontvangen.
Cobalt Strike	Een hacking framework.
Dissect Acquire	Dissect Acquire is een forensische software ontwikkeld door Fox-IT. Het is een uitvoerbaar bestand dat van een groot aantal systemen relevante data op kan halen ten behoeve van triage van het systeem op basis van IOCs. De software kan eveneens het verzamelde bewijsmateriaal op efficiënte wijze scannen voor de aanwezigheid van IOCs.
Domain controller	Op Microsoft Servers is een domain controller (DC) een server computer welke reageert op security authenticatie verzoeken (inloggen, permissies verifiëren, etc.) binnen een Windows domein.
EternalBlue	EternalBlue is een exploit voor Windows systemen waarbij gebruik wordt gemaakt van een fout in de implementatie van het SMB Protocol (CVE-2017-0144), dat gebruikt wordt om in Microsoft Windows bestandsuitwisseling tussen meerdere computers mogelijk te maken.
Golden Image	Een centraal beheerde image van een systeem dat gebruikt wordt voor de uitrol van nieuwe systemen, zoals virtuele desktops.
Indicator of compromise	Een Indicator Of Compromise (IOC) is een spoor, waargenomen op bijvoorbeeld een netwerk of in een besturingssysteem, dat blijk kan geven van een ongeoorloofde of kwaadwillende digitale handeling. Typische IOC's zijn virusdefinities, IP-adressen, MD5-hashes van malwarebestanden en URL's van (schadelijke) domeinnamen.
Malware	Software ingezet met een kwaadaardig doel. Het woord malware is afkomstig van het Engelse Malicious Software, afgekort malware.
Metasploit	Een hacking framework.
Meterpreter	Meterpreter is een onderdeel van Metasploit en wordt gebruikt voor interactie met een gecompromiteerd system.
Mimikatz	Een programma dat gebruikt wordt voor het extraheren van wachtwoorden, wachtwoordhashes, PIN codes en Kerberos tickets uit het geheugen van een Windows systeem.
Network Lateral Movement	Ook wel bekend als "lateral movement", verwijst naar een combinatie van technieken gebruikt door aanvallers om pro-actief door het network te bewegen terwijl zij op zoek zijn naar relevante data. Het bemachtigen daarvan is uiteindelijk het doel van de aanval.
PsExec	Een gratis software van Microsoft welke kan worden gebruikt om op afstand programma's uit te voeren op een ander systeem. Het wordt gebruikt door zowel IT administrators als aanvallers.
Ransomware	Ransomware is een type malafide software waarmee toegang tot bestanden en/of systemen kan worden geblokkeerd totdat een losgeldsom wordt betaald.
SCCM	System Center Configuration Manger is een systeem management software product, ontwikkeld door Microsoft ten einde het managen van grote groepen systemen gebaseerd op Windows NT, Windows Embedded, MacOS (OS X), Linux of UNIX, als mede Windows telefoons, Symbian, iOS en Android Mobile OS.

SDBBot	Malware welke wordt gebruikt door de threat actor TA505/Grace RAT voor het initieel toegang krijgen totj slachtoffers
Security Information and Event Management (SIEM)	Een SIEM-product of dienst kan informatie binnen de ICT-infrastructuur die een relatie heeft met informatiebeveiliging verzamelen en analyseren. Op basis van deze analyses kunnen kwetsbaarheden ontdekt worden en kunnen aanvallen of verdacht gedrag in een vroeg stadium worden gesignaleerd.
Splunk	Software-oplossing waarmee logbestanden kunnen worden doorzocht, monitoring kan worden ingeregeld en analyse op grote datasets mogelijk is via een web-interface.
Thin-client	Een computer met relatief zwakke eigen rekenkracht evenals zonder of beperkte eigen opslag. Het leeuwendeel van de capaciteit wordt virtueel gebruikt vanaf een server.

A.2 Gecompromitteerde systemen

Onderstaande tabel is een lijst met alle door Fox-IT geïdentificeerde gecompromitteerde systemen binnen het UNIMAAS domein van Opdrachtgever.

Hostname	Hostname	Hostname	Hostname	Hostname
IAM-	UB	UM	UM	UM
IAM-	UB	UM	UM	ICTS
UM-	UB	UM	UM	UM
IAM-	UB	UM	UM	UB
UM-	UB	UM	UM	UM
UB	UM-	UM-	UM	SBE
UM-	UM	UM	UM	SBE
UM-	UM-	UM	UM	SBE
ICTS-	UM-	UM	UM	UM
UM-	UM-	UM	UM-	FD-
ICTS-	UM-	UM	UM-	UM
UB	UM	UM	UM	UM
UM-	UM	UM	UM-	UM
SBE	UM-	UM	UM-	ICTS
UM-	UM	UM	UM	FD-
SBE	UM	UM	UM	UM
ICTS	UM	UM	UM	UM
UM-	UM	UM	UM-	UM-
UM-	UM	UM-	SBE	SSC-
UM-	UM	UM-	SBE	UM-
UM	UM-	UM	SBE	ICTS
UM-	UM	UM	SBE	UM
UM-	UM	UM	SBE	UM
FD-	UM	UM	SBE	UM
FD-	UM	UM-	SBE	UM
FD-	UM	UM-	SBE	UB
FD	UM	UM	SBE	UM
FD-	UM	UM	SBE	UM
FIN-	UM	UM-	SBE	UB
ICTS-	UM	UM-	SBE	UM

ICTS	UM	UM	SBE	FHML
ICTS	UM	UM	SBE	FHML
ICTS	UM	UM	SBE	FHML
ICTS	UM	UM	SBE	FDR
ICTS	UM	UM	SBE	FDP
ICTS	UM	UM	SBE	FPN
ICTS	UM	UM	SBE	FPN
ICTS	UM	UM	ICTS	BU
ICTS	UM	UM	UM	FHML
ICTS	UM	UM	SBE	FHML
ICTS	UM	UM	FDP	ICTS
ICTS	UM	UM	UM	ICTS
ICTS	UM	UM	UM	ICTS
ICTS	UM	UM	UM	SBE
ICTS	UM	UM	UM	SBE
ICTS	UM	UM	ICTS	SBE
ICTS	UM	UM	ICTS	SVM
ICTS	UM	UM	UM	UB
ICTS	UM	UM	UM	UM
ICTS	UM	UM	UM	UM
SSC	UM	UM	UM	UM
UB	UM	UM	UM	UM
UB	UM	UM	UM	FA
UB	UM	UM	ICTS	

Fox-IT

Fox-IT voorkomt, onderzoekt en beperkt de meest serieuze dreigingen door cyberaanvallen, datalekken of fraude met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. In zijn aanpak combineert het bedrijf slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. Fox-IT ontwikkelt producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

Bezoek onze website voor meer informatie over Fox-IT en onze partners.

CLASSIFICATIE
PUBLIC

FOX IT
part of nccgroup

fox-it.com

Fox-IT
Olof Palmestraat 6, Delft
Postbus 638, 2600 AP Delft
Nederland

T +31 (0)15 284 7999
F +31 (0)15 284 7990
fox@fox-it.com