HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

Red Mudnester: Rapportage

PUBLIEK

HUNT & HACKETT

Hunt & Hackett BV

Kranenburgweg 147

2583 ER Den Haag

Nederland

Telefoon +31 (0)70 222 0000

Mail: info@huntandhackett.com

Web: www.huntandhackett.com

KvK: 78688841

In deze rapportage is informatie die door publicatie een bedreiging kan vormen voor de (digitale) veiligheid van de Gemeente Buren, en/of voor personen werkzaam bij of voor de Gemeente Buren, dan wel in belang van het opsporingsonderzoek geanonimiseerd. Omwille van de leesbaarheid is dergelijke informatie vervangen voor afkortingen tussen blokhaken, en voorzien van een getal wanneer de afkorting in kwestie vaker voorkomt. Relevante getallen in de tekst zijn vervangen voor [X].

Voorbeeld: Een gebruikersnaam is vervangen voor [GN1].

Document management

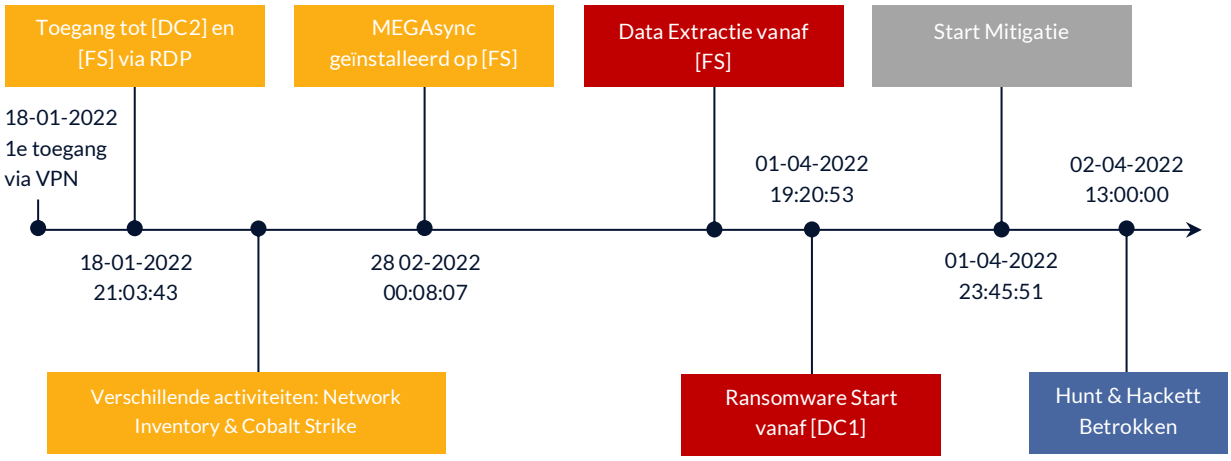
Projectnaam	Red Mudnester
Offerte nr.	8462027184
Klant	Gemeente Buren
Contactpersoon	Michiel van Dalen
Onderwerp	Incident response n.a.v. ransomware incident
Datum	28/06/2022
Versie	Publiek
Status	Definitief
Auteurs	Mattijs Dijkstra & Zawadi Done
Gerelateerde documenten	20220402_Hardening_Guidelines_Buren.pdf 20220403_Big_bang_Playbook_Red Mudnester_v1.pdf

Management Samenvatting

Op 2 april 2022 heeft [WN] namens Gemeente Buren (hierna: 'de gemeente') contact opgenomen met Hunt & Hackett via de 24/7 Incident Response Hotline inzake een ransomware-aanval op de gemeente. Tijdens deze aanval waren op dat moment 12 systemen versleuteld geraakt, waardoor de dienstverlening van de gemeente stil was komen te liggen. Op dat moment is Hunt & Hackett gevraagd om te ondersteunen bij het incident. In de eerste fase van het incident heeft de focus vanuit de gemeente voornamelijk gelegen op mitigatie en herstel, om de impact voor de burger zoveel mogelijk te minimaliseren. Vervolgens is forensisch sporenonderzoek verricht op het beschikbare onderzoeksmateriaal om de *root cause* van het incident vast te stellen. Dit rapport beschrijft de bevindingen van dat onderzoek.

Bevindingen

De scope van het onderzoek is beperkt gebleven tot het domein [DOM1]. Alle systemen getroffen door de ransomware vielen binnen dit domein. Op basis van het forensisch sporenonderzoek kan op hoofdlijnen de tijdlijn als volgt worden ingevuld:



De eerste toegang tot het netwerk van de gemeente is verkregen door een legitiem VPN-account te misbruiken. Het is op basis van het beschikbare onderzoeksmateriaal echter niet vast te stellen hoe de aanvaller aan de inloggegevens is gekomen van dit account[1]. Uit de onderzochte logging blijkt dat de aanvaller door middel van het *Remote Desktop Protocol* (RDP) verbinding heeft gemaakt met het de *Domain Controller* (DC) en de bestandserver [FS]. Op de DC heeft de aanvaller een administrator account gecompromitteerd met de hoogste rechten, mogelijk door middel van een (offline) *brute force* aanval. Daarnaast heeft de aanvaller op zowel de DC als op de bestandserver meerdere programma's geïnstalleerd om aanvullende informatie over de netwerkinfrastructuur te verzamelen, alsmede ten behoeve van data-extractie. Gedurende een periode van ongeveer een maand is het programma MEGAsync actief geweest op de bestandserver, waarmee de aanvaller grote hoeveelheden data heeft kunnen exfiltreren naar een extern MEGAsync IP-adres.

Hunt & Hackett heeft op 3 april 2022 vastgesteld dat de aanvaller bekend staat als de [TA], waarvan bekend is dat ze gebruik maken van drievoudige afpersing. Deze afpersingsmethode begint met het versleutelen van

[1] De gemeente heeft aangegeven de inloggegevens van dit account niet te beheren. Hoe het mogelijk is geweest dat de aanvaller op 18 januari 2022 in één keer inlogt met het account is niet vast te stellen op basis van het beschikbare onderzoeksmateriaal.

bestanden en systemen en vragen om een losgeld som (eerste methode, zoals ook waargenomen bij de gemeente). Vervolgens wordt bij een drievoudige afpersing een DDoS aanval gelanceerd die tegen betaling stopgezet kan worden (de tweede methode), om tot slot het slachtoffer af te persen met een data-lek, wanneer er niet betaald wordt (derde methode). Om die reden is na de ransomware-aanval door de gemeente op advies van Hunt & Hackett direct (aanvullende) DDoS protectie ingeregeld. De impact van de eerste twee methoden kon adequaat worden gemitigeerd, voor zover bekend heeft een DDoS aanval niet plaatsgevonden. Helaas gold dit niet voor de derde methode waarbij de [TA] een deel (126 GB) van de geclaimde beschikbare data (5 TB) heeft gepubliceerd. Op het moment dat het incident voor de Gemeente Buren zichtbaar werd was het kwaad daarmee al geschied. Welke informatie er precies is ontvreemd en gepubliceerd valt buiten de scope van dit onderzoek. Dit is onderdeel van een onderzoek uitgevoerd door Hoffmann.

Conclusies

Ondanks het feit dat de IT Security team van de gemeente erin is geslaagd om kort na het constateren van de ransomware-aanval direct actie te nemen in de vorm van recovery maatregelen en daarmee de verstorende impact op de organisatie grotendeels heeft weten te voorkomen, heeft het handelen niet kunnen voorkomen dat er een grote hoeveelheid data is ontvreemd door de [TA]. Dit komt mede doordat de uitrol van ransomware de laatste stap vormt in het proces van de aanvalsgroep en de data reeds daarvoor al was geëxfiltreerd zonder dat dit is opgemerkt.

Mitigatie & Aanbevelingen

De recovery van de versleutelde systemen is snel verlopen. Dit was mogelijk door de wijze waarop de gemeente haar back-up strategie heeft ingeregeld (middels offline tapes), in combinatie met het adequate handelen van het IT Security team. Daardoor konden getroffen machines en daarmee de dienstverlening voor de burger relatief snel hersteld worden. In dat opzicht was *Incident Readiness* goed ingeregeld. Wat echter voor verbetering vatbaar is, is; het *hardenen* van systemen (preventie), het loggen van security relevante informatie en het verkrijgen van 24x7 zichtbaarheid op de IT-omgeving (detectie en respons). Dat is van belang om indicaties en mogelijke sporen van aanvallen in een vroeg stadium te kunnen opmerken. Om die reden is gedurende het incident *endpoint* monitoring uitgerold op alle systemen. Dit geeft direct (maar ook slechts gedeeltelijk[2]) zichtbaarheid op de IT-omgeving en heeft het IT Security team op advies van Hunt & Hackett daarnaast ook meerdere mitigerende maatregelen geïmplementeerd lopende het sporenonderzoek.
Het onderzoek naar de *root cause* van de aanval heeft geresulteerd in een mitigatieplan om de geïnfecteerde machines te identificeren, op te ruimen en de aanvallers uit het netwerk te houden. Een volledig overzicht van de mitigerende maatregelen ten aanzien van Firewall, werkstations, servers en Windows *hardening*, is aangeleverd vanuit Hunt & Hackett aan het IT Security team. De belangrijkste maatregelen zijn hieronder opgesomd:

- Het implementeren van detectie en response mechanismen op zowel *endpoint*, als netwerkniveau;
- Het implementeren van Multi Factor authenticatie op ten minste VPN, email en beheer accounts;
- Het verhogen van de weerbaarheid van de netwerk infrastructuur;
- Het verbeteren van het wachtwoordbeleid, en de processen rondom veilig systeembeheer.

Naast het opschonen en verwijderen van de aanvallers uit het netwerk, bevat dit rapport aanbevelingen voor [CAT1], [CAT2] en [CAT3] om de weerbaarheid en het beveiligingsniveau van het netwerk van de gemeente verder te verhogen.

---

[2] Voor volledige zichtbaarheid op het MITRE ATT&CK aanvalspad is naast *endpoint* detectie ook security log & telemetrie informatie monitoring benodigd idealiter aangevuld met netwerk detectie en *honeypots*.

Inhoudsopgave

1. Introductie

Deze rapportage beschrijft de resultaten van het onderzoek met de codenaam 'Red Mudnester' zoals uitgevoerd door Hunt & Hackett in de periode van zaterdag 2 april 2022 tot woensdag 4 mei 2022.

1.1 Achtergrond

Op 2 april 2022, heeft [WN], namens de gemeente Buren (hierna: 'de gemeente'), contact opgenomen met Hunt & Hackett via de 24/7 *Incident Response Hotline* naar aanleiding van een ransomware-aanval. De desbetreffende aanval zou hebben plaatsgevonden middels [TA] ransomware. Het uitrollen van de ransomware begon op vrijdag 1 april 2022 rond 19:20 en heeft in totaal 12 systemen versleuteld, waaronder een aantal bedrijfskritieke systemen. De gemeente was voorafgaand aan het contact met Hunt & Hackett reeds begonnen met het '*containen*' en 'mitigeren' van het incident en zodoende begonnen met opruimen en herstellen van de getroffen systemen. Dit met als doel om zo snel mogelijk weer de bedrijfsvoering te kunnen herstellen die stillag door de uitrol van de ransomware. De gemeente huisvest ongeveer 27.000 inwoners en meerdere bedrijven en organisaties. Derhalve was de prioriteit voor de gemeente om de getroffen systemen voor maandag 4 april 2022 weer hersteld te hebben. Om die reden heeft het IT-security team van de gemeente gedurende het weekend hieraan doorgewerkt. Tijdens het eerste gesprek is Hunt & Hackett door de gemeente gevraagd om direct ondersteuning te verlenen.

1.2 Onderzoeksvragen

De gemeente heeft Hunt & Hackett gevraagd om onderzoek te doen, en onderstaande vragen te beantwoorden:

- Wat is er gebeurd?
- Hoe heeft dit incident kunnen plaatsvinden?
- Wat is de omvang van het incident?
- Tot welke data en systemen is toegang geweest door de aanvallers?
- Hoe kan het incident worden gemitigeerd?

In aanvulling op bovenstaande, heeft Hunt & Hackett ten aanzien van de organisatie in samenspraak met de gemeente gedurende het verloop van het onderzoek de volgende doelen of vragen toegevoegd:

- Het opzetten, dan wel uitbreiden van de crisisorganisatie;
- Het geven van mitigatie advies om dergelijke incidenten in de toekomst te voorkomen.

1.3 Leeswijzer

Het hiernavolgende hoofdstuk, hoofdstuk 2 beschrijft het onderzoek, de toegepaste methodologieën, evenals het proces en de scope. Hoofdstuk 3 beschrijft de bevindingen die zijn voortgekomen uit het uitgevoerde onderzoek. Hoofdstuk 4 geeft inzicht in welke stappen van de aanval gedetecteerd hadden kunnen worden. Hoofdstuk 5 beschrijft de conclusies en het laatste hoofdstuk (6) geeft een overzicht van de [CAT1], [CAT2] en [CAT3] aanbevelingen.

2. Onderzoek

Dit hoofdstuk beschrijft het onderzoek zoals uitgevoerd door Hunt & Hackett en het verzamelde bewijsmateriaal waarop de bevindingen zijn gebaseerd. Paragraaf 2.1 beschrijft het *incident response* proces. Paragraaf 2.2 geeft inzicht in de scope van het onderzoek. Paragraaf 2.3 beschrijft de onderzoeksmethodologie. Tot slot, is in paragraaf 2.4 het ontvangen onderzoeksmateriaal uiteengezet.

Alle tijden in dit rapport zijn in *Universal Coordinated Time* (UTC), tenzij anders vermeld.

2.1 Proces

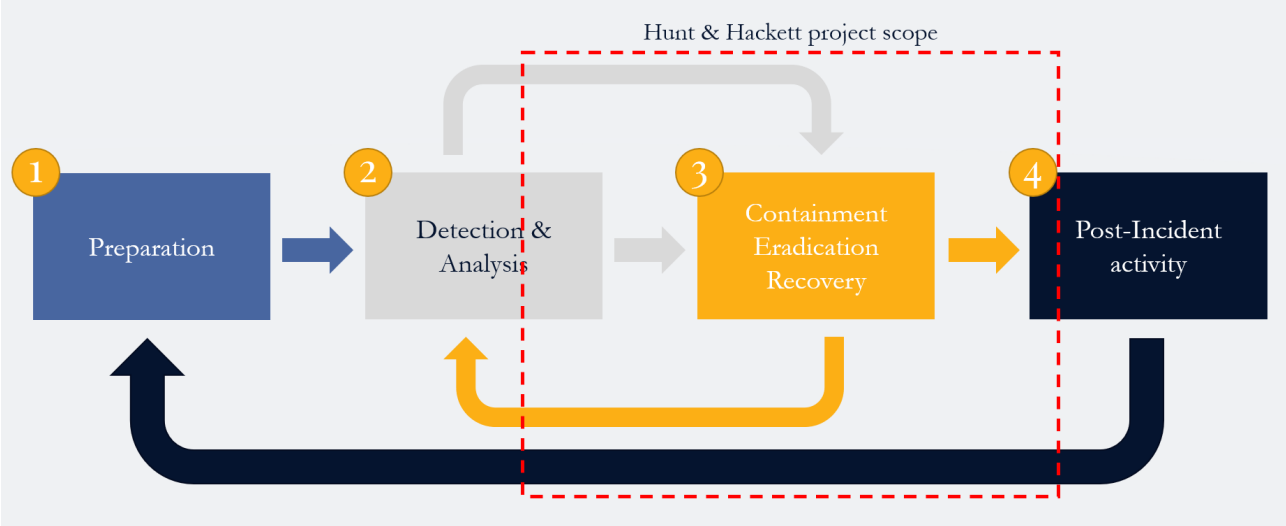
Het incident response proces is een iteratief proces wat kan worden verdeeld in vier fasen, zoals te zien is in *Figuur* 1. Hierbij betreft de eerste stap het voorbereidingsproces die veelal plaatsvinden ter voorbereiding op een eventueel incident. Zie onderstaand een korte beschrijving per fase van het incident response proces:

1. **[Preparation]**: het voorbereiden van onder meer de vereiste processen, procedures, technologie en mensen om een beveiligingsincident zo efficiënt en effectief mogelijk security logging in te richten om sporen van (mogelijke) aanvallen te kunnen analyseren, veelal aangevuld met het vroegtijdig te kunnen detecteren om bredere organisatie-impact te voorkomen;

2. **[Detection & Analysis]**: omvat het monitoren op potentiële aanvalsvectoren, het zoeken naar tekenen van een incident, en de analyse hiervan op het moment dat een incident wordt vastgesteld;

3. **[Containment, Eradication, and Recovery]**: betreft het opstellen van een *containment*-strategie, het identificeren van systemen die betrokken zijn bij het incident, het verwijderen van de aanvaller uit het netwerk en het hebben van een plan voor herstel op het moment dat een incident heeft plaatsgevonden;

4. **[Post-Incident Activity]**: het vaststellen van de geleerde lessen en het hebben van een plan ter voorkoming van toekomstige incidenten, die weer meer genomen worden in de voorbereidende fase.



***Figuur* 1** - Incident response proces

Tijdens dit project is Hunt & Hackett gevraagd om (delen van) stap twee, drie en vier van het *incident response* proces te coördineren en te focussen op het coördineren van zowel de verschillende procesmatige, als ook onderzoek stappen ten behoeve van het crisismanagement en het forensisch sporenonderzoek. Grofweg kunnen twee fasen onderscheiden worden ten aanzien van het incident. De eerste fase heeft zich voornamelijk gefocust op het herstel van de bedrijfsvoering en de tweede fase op het (verder) uitvoeren van forensisch onderzoek om inzicht te krijgen in wat precies is gebeurd. In eerste instantie was de scope van Hunt & Hackett beperkt tot de eerste fase. Het mandaat voor de tweede fase is, kort na publicatie van 126 GB aan data door de aanvaller, aan Hunt & Hackett gegeven. De beide fasen van het *incident response* proces zijn op hoofdlijnen hierna uiteengezet en terug te vinden in *Tabel 1*.

Fase	Activiteit

Fase 1 - Containment & recovery: Op specifiek verzoek van de gemeente heeft de eerste twee weken van het incident de focus primair gelegen op herstel en mitigatie, om op die manier de impact voor de burger ten aanzien van de bedrijfsvoering zo veel mogelijk te minimaliseren.	• **[Coördinatie]:** afstemming over het reguliere verloop van het incident en advisering over het herstellen van de bedrijfsvoering en het gecontroleerd weer beschikbaar maken van de diensten;
	• **[Detectie]:** om zicht te krijgen op eventuele aanvallersactiviteit in het netwerk van de gemeente en daarmee ook controle over de omgeving alvorens de bedrijfsvoering weer beschikbaar te maken, is de *Endpoint Detection & Response* (EDR) software, genaamd VMWare Carbon Black uitgerold. Naast dat deze EDR-software gebruikt kan worden voor detectie van aanvallersactiviteit, kan het ook gebruikt worden om snel te kunnen reageren en (nieuwe) aanvallersactiviteit te mitigeren. Gedurende de *containment & recovery* fase (evenals de periode hierna) is actief gemonitord op aanvallersactiviteit;
	• **[Onderzoek]:** omdat de focus voor de gemeente lag op het herstellen van de bedrijfsvoering heeft verder gedurende deze fase beperkt onderzoek plaats kunnen vinden en is de focus vanuit onderzoeksperspectief primair geweest op het *real-time* monitoren van aanvallersactiviteit en een initieel basaal onderzoek naar sporen middels VMWare Carbon Black;
	• **[Data preservatie]:** daar waar dit nog mogelijk was, is de gemeente geadviseerd om relevante data apart te zetten ten behoeve van eventueel toekomstig onderzoek;
	• **[Containment]:** Hunt & Hackett heeft als onderdeel van stap drie van het *incident response* proces, in het eerste weekend na plaatsvinden van het incident (2 april 2022 en 3 april 2022) input geleverd voor de *containment*-strategie, zoals te lezen is in:
	  ○ `20220402_Hardening_Guidelines_Buren.pdf`;
	  ○ `20220403_Big_bang_Playbook_Red Mudnester_v1.pdf`.

Fase	Activiteit
Fase 2 - Root cause analyse: Nadat de gemeente de bedrijfsvoering heeft kunnen herstellen en de eerste mitigatiemaatregelen door heeft kunnen voeren is Hunt & Hackett gevraagd om de *root cause* in kaart te brengen.	Een root cause analyse is enerzijds noodzakelijk voor het vaststellen van het aanvalspad, zodat op basis van de bevindingen, gerichte mitigerende maatregelen getroffen kunnen worden ten einde de aanvaller buiten te sluiten. Anderzijds is het van belang het aanvalspad in kaart te brengen om verantwoording af te kunnen leggen aan belanghebbenden en autoriteiten over de oorsprong van de aanval. Tot slot helpt een *root cause* analyse de organisatie lering te trekken van het incident en zichzelf op basis van de onderzoeksbevindingen de weerbaarheid van de organisatie te verbeteren, ten einde dergelijke incidenten in de toekomst te voorkomen.

Tabel 1 - Overzicht van verschillende incident fasen.

2.2 Scope

Het server landschap van de gemeente bestaat uit [X] fysieke en [X] virtuele servers. Daarnaast wordt gebruik gemaakt van [X] fysieke, en ongeveer [X] virtuele werkstations binnen het `[DOM1]` domein. De virtuele werkstations worden gefaciliteerd via een *Virtual Desktop Infrastructure* (VDI) welke binnen het `[DOM1]` domein valt. De werkstations zijn in eerste instantie buiten de scope van het onderzoek gelaten omdat geen werkstations door de ransomware aanval waren getroffen. Dergelijke systemen vielen echter wel binnen de scope wanneer uit het onderzoek, zijnde *real-time incident* monitoring en de *root cause* analyse, duidelijk zou worden dat er aanvalleractiviteit van of naar werkstations heeft plaatsgevonden. Wel is er direct in fase 1, aanvullend op de verschillende virtuele en fysieke servers en op alle werkstations VMWare Carbon Black geïnstalleerd. De scope van het onderzoek omvat systemen waarvan de gemeente heeft aangegeven dat ze vertrouwelijke en/of bedrijfskritieke informatie bevatten zodat deze systemen op verzoek van de gemeente met prioriteit hersteld konden worden. Daarnaast omvat de scope de systemen waarop de aanvaller actief is geweest. Het vaststellen op welke systemen de aanvaller actief is geweest, heeft plaatsgevonden door:

1. Te bepalen in hoeverre sporen van de ransomware aanwezig waren op een systeem;
2. Wanneer uit het forensisch sporenonderzoek of de *real-time* monitoring naar voren kwam dat een aanvaller (handmatig) interactie heeft (gehad) met een bepaald systeem.

Vanuit de gemeente heeft de focus gedurende de eerste twee weken van het incident nadrukkelijk gelegen op herstel en mitigatie. Toen de eerste impact van de versleuteling van systemen was gemitigeerd is de focus verschoven naar het in kaart brengen van de *root cause*. Desalniettemin is in de laatste fase van dit onderzoek de scope op basis van overwegingen aangaande budget, prioriteiten en bijbehorende risico indicatie beperkt gebleven tot de systemen binnen het `[DOM1]` domein welk zijn geïdentificeerd als gecompromitteerd op basis van de ten tijde van schrijven bekende IOCs. Er is geen volledige scan verricht van alle systemen binnen de omgeving van de gemeente. Wel worden alle systemen 24x7 actief gemonitord op Indicators of Compromise (IOC) gerelateerd aan het incident middels Carbon Black.

2.3 Methodologie

De aanpak voor het onderzoek is in te delen in twee onderzoeksporen, waarvan de eerste '*real-time*' monitoring van de servers en werkstations betreft en het tweede spoor kan worden gezien als het uitvoeren van een *root cause* analyse:

- **[Onderzoekspoor 1 – *real-time* monitoring]:** door middel van *endpoint* monitoring met Carbon Black is *real-time* gekeken naar potentiële sporen van compromitatie, of (pogingen tot) *intrusie*. Dit heeft plaatsgevonden vanaf 2 april 2022;
- **[Onderzoekspoor 2 – *root cause* analyse]:** het tweede spoor bestaat uit het actief '*hunten*' naar sporen van compromitatie, waarbij van bronnen en systemen binnen de scope van het onderzoek onderzoeksdata is opgehaald, om vervolgens binnen deze dataset te bepalen of historische sporen van compromitatie aanwezig zijn.

In sub paragraaf 2.3.1 is onderzoekspoor 1 in detail beschreven en in sub paragraaf 2.3.2 onderzoekspoor 2. Opgemerkt zij dat tussen beide sporen een wisselwerking bestaat. Wanneer binnen spoor 2 zaken werden aangetroffen die kenmerkend zijn voor aanvallersactiviteit, ook wel IOC's genoemd, is deze toegevoegd aan de *real-time* monitoring uit spoor 1. Hetzelfde geldt andersom; voor het eventueel observeren van aanvallers gerelateerde activiteiten binnen spoor 1, zijn deze IOC's gebruikt om verder onderzoek te doen binnen spoor 2.

2.3.1 Onderzoekspoor 1 – Real-time monitoring

Door Carbon Black sensoren te installeren op de zowel de fysieke als de (virtuele) werkstations en servers, is zichtbaarheid gecreëerd in potentiële (aanvaller) activiteit op de zogeheten *endpoints* in scope van het onderzoek. De kernelementen van een succesvolle *Endpoint Detection & Response* (EDR) oplossing zijn samen te vatten in de onderstaande drie punten:

- Beschermen tegen bekende en onbekende aanvallen. Hierbij wordt bij voorkeur gekeken naar gedragingen op de *endpoints* en naar afwijkingen van wat normaal gedrag op systemen is;
- Loggen van telemetrie over activiteit en (security) *events* op de *endpoints*;
- *Response* capaciteit zodat op afstand onderzoek kan worden gedaan of ingegrepen kan worden, bijvoorbeeld door een *endpoint* te isoleren (in quarantaine zetten).

Het aantal actieve sensoren is ten tijde van schrijven van dit rapport, is in totaal [X] *endpoints*. Verder dient opgemerkt te worden dat de fysieke werkstations van het [DOM2] domein op aangeven van de gemeente buiten de scope van Carbon Black zijn gelaten. Er was er geen directe aanleiding om de werkstations binnen het [DOM2] domein mee te nemen, omdat gedurende het onderzoek geen aanvalleractiviteit van of naar deze systemen is waargenomen en er geen encryptie van systemen binnen dit domein heeft plaatsgevonden. Daarnaast was het binnen de beschikbare tijd en op basis van de prioriteiten zoals gesteld door de gemeente niet haalbaar om alle werkstations mee te nemen. Wel zijn de virtuele werkstations voorzien van Carbon Black.

2.3.2 Onderzoekspoor 2 – Root cause analyse

Voor het sporenonderzoek naar de *root cause* zijn door de gemeente verschillende zaken aangeleverd. Dit is verder uitgewerkt in paragraaf 2.4. Na het ontvangen van het (onderzoeks)materiaal is hierop verdere analyse uitgevoerd door Hunt & Hackett.

De meest relevant databronnen van de Windows systemen zijn met gebruik van software die forensisch onderzoek faciliteert, omgezet naar tijdlijnen van de systemen. Hierin staat wanneer er welke activiteiten hebben plaatsgevonden op de systemen in chronologische volgorde. Voor de firewall logboeken was dit niet nodig, omdat deze al in dergelijke volgorde stonden.

2.4 Onderzoeksmateriaal

Gedurende het onderzoek is onderzoeksmateriaal verzameld en de ontvangen data geanalyseerd. Het onderzoeksmateriaal en/of de data zijn weergeven in *Tabel 2*.

Materiaal	Beschrijving
End point detection & response	Omdat na het contact met gemeente bleek dat het om een actieve aanvaller ging, is op 2 april 2022 besloten om *Endpoint Detection & Response* tool Carbon Black in te zetten. Deze tool heeft Hunt & Hackett in staat gesteld om gegevens van de systemen te verzamelen en te bewaren en om te reageren op een mogelijke escalatie van het incident, wanneer de aanvaller zou besluiten zijn activiteiten uit te breiden.
Firewall logboeken	De logboeken van de firewall zijn opgevraagd om de mogelijke verbindingen die de aanvaller gemaakt heeft te onderzoeken. De logboeken van de firewall bevatten ook de VPN-authenticatielogs waardoor de analyse mogelijk was van het identificeren van potentieel gecompromitteerde accounts die zouden kunnen worden gebruikt om op afstand verbinding met het netwerk te maken.
Forensische *Packages*	De systemen die geraakt zijn door de ransomware aanval, zijn geïdentificeerd en hiervan is een kopie gemaakt van de meest relevant databronnen op de systemen ten behoeve van het forensische onderzoek. Zie ook BIJLAGE 1: Overzicht Forensische Packages voor een volledig overzicht.
MSRT-logs	De gemeente heeft in het eerste weekend na het plaatsvinden van de ransomware-aanval op eigen initiatief de *Malicious Software Removal Tool* (MSRT) van Microsoft uitgevoerd voor het vinden van potentiële kwaadaardige software. De logs van onder meer de volgende systemen zijn aangeleverd aan Hunt & Hackett: `[BEH]`, `[DC1]`, `[FS]`, `[BACK]` en `[MAIL1]` & `[MAIL2]`. Als gevolg van het gebruik van deze tool zijn waardevolle forensische sporen, hoogstwaarschijnlijk gerelateerd aan de aanval, verwijderd voordat deze veilig gesteld, en geanalyseerd konden worden.

Tabel 2 – Overzicht van het veiliggestelde onderzoeksmateriaal

3. Bevindingen

Dit hoofdstuk beschrijft de bevindingen op basis van het onderzoek zoals uitgevoerd door Hunt & Hackett. Paragraaf 3.1 geeft een overzicht van de sleutelmomenten in de aanval. Paragraaf 3.2 beschrijft de aanval ten opzichte van het MITRE ATT&CK *framework*. Tot slot, beschrijft paragraaf 3.3 de attributie van de aanval.

3.1 Tijdlijn van sleutelmomenten

De tijdlijn zoals weergegeven in de hiernavolgende tabel (*Tabel 3*) geeft een overzicht van de sleutelmomenten in de aanval, waar deze zijn aangetroffen, op welk systeem, en vervolgens gekoppeld aan een MITRE ATT&CK Tactiek. Het MITRE ATT&CK[3] *framework* betreft database met daarin tactieken en technieken van dreigingsactoren, welke tijdens onderzoeken zijn geobserveerd. Het *framework* helpt te begrijpen en te documenten wat de aanvalspaden zijn per fase van een aanval.

Het mappen van sporen van een aanval met het framework, helpt aan de ene kant om hoog over een goed begrip te krijgen van wat heeft plaatsgevonden tijdens een aanval. Daarnaast helpt het ook om een overzicht te krijgen van de bestaande hiaten in de aanvalsketen, wat vervolgens weer richting geeft aan eventuele aanvullende onderzoekstappen. Verder helpt het begrijpen van de kwaadaardige activiteiten die hebben plaatsgevonden, bij het definiëren van mitigerende en preventieve stappen, om te voorkomen dat een incident nogmaals op een soortgelijke manier kan plaatsvinden. Eventuele gaten in de tijdlijn kunnen worden verklaard omdat er geen relevante bevindingen waren in die periode, of omdat er geen onderzoeksmateriaal beschikbaar was.

Tijd	Bron	Systeem	Beschrijving	MITRE ID
18-01-2022 18:35	VPN log	10.[X].[X].[X]	Succesvolle login op (`10.[X].[X].[X]`) VPN IP vanaf `91.[X].[X].[X]` (Zie ook 'BIJLAGE 4: ') met account [`gebruikersnaam @domeinnaam`]	T1133
18-01-2022 18:36	EVTX	[DC2]	RDP connectie naar Domain Controller (DC) vanaf `10.[X].[X].[X]`	T1133
18-01-2022 18:57	EVTX	[DC2]	SMB br*ute force* aanval op de Domain Controller ([`DC`]) vanaf `10.[X].[X].[X]`	T1190

[3] https://attack.mitre.org/

Tijd	Bron	Systeem	Beschrijving	MITRE ID
18-01-2022 18:57	EVTX	[DC1]	*Brute force* aanval op het lokaal `[GN1]` account voor [DC] vanaf `10.[X].[X].[X]`	T1078.002 T1110
18-01-2022 19:59	MRT Logs	[DC1]	Cobalt Strike is gestart onder de naam `spools.exe`. Cobalt Strike is offensief security *framework* dat kan worden gebruikt voor penetratietesten, maar ook door aanvallers met malafide doeleinden.	T1588.002
18-01-2022 19:55	EVTX	[DC1]	Succesvolle RDP Logon met lokaal `[GN1]` account en wachtwoord `[Geredigeerd]` op Domain Controller	T1078.002
18-01-2022 20:04	Shimcache	[DC1]	Netwerk scanning tool `'Total Network Inventory'` (TNI) aangetroffen op de DC. Deze software kan worden gebruikt om informatie te verzamelen over onder andere accounts, systemen en het AD zelf.	T1588.002
18-01-2022 20:05	EVTX	[DC1]	Niet succesvolle poging tot aanpassen McAfee *Common Management Agent files* instellingen	T1562.001
18-01-2022 20:06	EVTX	[DC1]	McAfee detecteert uitvoeren van Cobalt Strike en TNI vanuit de temp folder. Dit wordt echter niet geblokkeerd of op gereageerd.	T1074.001
18-01-2022 20:16	MFT	[DC1]	Aanvaller heeft door middel van TNI op basis van de geobserveerde *ouput* files, informatie verzamelt over Active Directory (AD) van de gemeente, waaronder zeer waarschijnlijk over het `[GN2]` account, servers en (VDI) werkplekken	
18-01-2022 21:02	Register	[FS]	Toegang tot *Fileshare* [FS] met account `[GN2]`	T1021.001

Tijd	Bron	Systeem	Beschrijving	MITRE ID
19-01-2022 13:53	Register	[FS]	Aanvaller opent de H: schijf van de *FileShare* [FS]	
14-02-2022 08:55	Register	[FS]	Aanvaller opent de F: schijf van de *FileShare* [FS]	
16-02-2022 09:49	Register	[FS]	Aanvaller opent de G: schijf van de *FileShare* [FS]	
28-02-2022 00:08	Register	[FS]	Het programma `MEGAsync.exe` wordt door de aanvaller geïnstalleerd op de [FS]	T1567.002
03-03-2022 10:30	Register	[FS]	Aanvaller opent de schijf U: van de *FileShare* [FS]	T1083
04-03-2022 23:50	EVTX	[DC2]	Eerste observatie gebruik `[GN3]` Domain Admin account door aanvaller	
01-04-2022 19:06	WebCache	[FS]	Het programma `PCHunter` is door de aanvaller gedownload. Dit kan worden gebruikt om malware op te sporen.	
01-04-2022 19:15	EVTX	[FS]	Meerdere services gestopt: waaronder Volume Shadow Copies en Application Experience	T1070 T1489
01-04-2022 19:20	EVTX	[DC1]	Ransomware `bu.exe` en `buren_cryptor.exe` uitgevoerd door middel van de *scheduled task* met de naam '\crypt!'	T1486

Tabel 3 - Tijdlijn van sleutelmomenten.

3.2 MITRE ATT&CK fases

MITRE ATT&CK is een database met daarin tactieken en technieken gebruikt door *threat actors* op basis van observaties van uitgevoerde aanvallen. Het MITRE ATT&CK *framework* helpt het aanvalspad per fase inzichtelijk te maken en te documenteren, zoals hieronder zichtbaar. Daarnaast kan monitoring op dusdanige manier worden ingeregeld of verbeterd op basis van de bevindingen, zodanig dat de acties van de aanvallen gedurende de meeste van deze fases kan worden gedetecteerd.

MITRE ATT&CK Tactiek	Bevindingen	Detectie mogelijkheden
Reconnaissance: De aanvaller probeert informatie te verzamelen om toekomstige operaties te plannen.	Er zijn geen bevindingen gerelateerd aan de verkenningsfase van de aanval.	N/A
Resource development: De aanvaller ontwikkelt tools of scripts die kunnen worden gebruikt tijdens de aanval.	Er zijn geen bevindingen gerelateerd aan de ontwikkelingsfase van de aanval.	N/A
Initial Access: De aanvaller probeert toegang te krijgen tot uw netwerk.	Via een legitiem VPN-account heeft de aanvaller initieel toegang verkregen tot het netwerk door in te loggen op de VPN vanaf een Russisch IP. Het wachtwoord van dit account was willekeurig gegenereerd door KeePass, en bestond uit 14 karakters afwisselend hoofdletters, kleine letters, cijfers en speciale karakters. Dit is van voldoende complexiteit en lengte om een succesvolle uitkomst van een *brute force* aanval minder waarschijnlijk te maken. Het is een mogelijkheid dat dit wachtwoord is gelekt, of op een andere manier door een aanvaller is buitgemaakt op een systeem buiten de omgeving van de gemeente.	[1] Login vanaf ongebruikelijke locatie [2] Login vanaf blocklist locaties (bijvoorbeeld Rusland en/of China).

Execution: De aanvaller probeert kwaadaardige code uit te voeren.	In het Windows Security logbestand van de [DC1] is een brute force aanval terug te vinden op het [GN1] account. Ondanks dat deze in eerste instantie niet lijkt te slagen, is op een later moment in de tijdlijn een succesvolle *logon* te zien via RDP van dit account. Daarnaast zijn sporen aangetroffen in de EVTX van de [DC1], van het gebruik van Cobalt Strike door Microsoft Safety Scanner. Echter door de mitigerende handelingen uitgevoerd door de gemeente is het niet precies meer te herleiden op wat voor manier Cobalt Strike is gebruikt door de aanvaller.	[3] RDP-login (over het netwerk) vanaf een ongebruikelijke locatie (bijvoorbeeld buiten *allowlist*, of niet vanaf de *jumphost*). [4] Detectie van offensieve tool Cobalt Strike op *endpoints*.
Persistence: De aanvaller probeert toegang tot het netwerk te houden.	Mogelijk is het wachtwoord [Geredigeerd] van het [GN1] account door middel van een (offline) *brute force* aanval buitgemaakt. Dit wachtwoord lijkt sterk, maar is dat in feite niet. Dat het is buitgemaakt, staat vast. De aanvaller had hierdoor een extra account, met in dit geval verhoogde rechten, waarmee toegang tot het netwerk en systemen mogelijk werd behouden.	[5] Netwerk gebaseerde *logins* van het *administrator* account.
Privilege Escalation: De aanvaller probeert rechten op een hoger niveau te verkrijgen.	Op basis van het beschikbare log-materiaal is niet vast te stellen wanneer de rechten van het door een leverancier gebruikte [GN3] account zijn gewijzigd. Wel is bekend dat dit account op 18 januari 2022 geen lid was van de *Domain Admin* (DA) groep, maar dit ten tijde van de aanval op 1 april 2022 wel het geval was.	[6] Wijziging van groep lidmaatschap, in het bijzonder met verhoogde rechten

Defense Evasion: De aanvaller probeert te voorkomen dat hij wordt gedetecteerd.	In logboeken van de [DC1] is te zien dat de aanvaller probeert om detectieregels van McAfee AV aan te passen. Dit doet de aanvaller mogelijk omdat McAfee AV het gebruik van de TNI-tool detecteert. De tool `PCHunter` wordt door de aanvaller geïnstalleerd voorafgaand aan de ransomware uitrol. `PCHunter` is een *toolkit* met toegang tot honderden instellingen, waaronder kernels en kernelmodules, processen, netwerk, opstarten en nog veel meer. Het is ontworpen om malware, inclusief rootkits, op te sporen en te verwijderen, maar kan door aanvallers worden gebruikt om eigen sporen te vinden, en verwijderen.	[7] Installatie en uitvoer van bekend aanvaller gerelateerde software (TNI, PCHunter, MegaSync, Cobalt Strike, etc). Op een systeem waar dit niet hoort te gebeuren. [10] Uitzetten van services verwant aan back-ups van data (Volume Shadow Service, Application Experience, File Server Storage Reports Manager, Microsoft Software Shadow Copy Provider)
Credential Access: De aanvaller probeert accountnamen en wachtwoorden te stelen.	Na gebruik van de TNI-tool heeft de aanvaller toegang tot informatie over het AD, servers, (VDI) werkplekken en vermoedelijk het `[GN2]` account. Met dit account wordt vervolgens via RDP ingelogd op de `[DC1]`.	[8] Detectie van verschillende technieken om accountinformatie te bemachtigen (TNI, scanning, etc.)
Discovery: De aanvaller probeert uw netwerk te verkennen.	De aanvaller maakt gebruik van de tool `Total Network Inventory` (TNI). Deze tool kan worden gebruikt om alle systemen in het netwerk te scannen en een overzicht te maken van accounts, systemen en gebruikte software. Daarnaast is door de aanvaller meerdere andere bekende software gebruikt voor malafide doeleinden.	[7] Installatie en uitvoer van bekend dubieuze software (TNI, PCHunter, MEGASync, Cobalt Strike, etc)

Lateral Movement: De aanvaller probeert zich door uw omgeving te verplaatsen.	Door gebruik te maken van het *Remote Desktop Protocol* (RDP) was de aanvaller in staat om lateraal door het netwerk te bewegen van onder andere de DC naar de bestandsserver. Op die systemen heeft de aanvaller vervolgens toegang gehad tot alle opgeslagen bestanden.	[3] RDP-login van ongebruikelijke locatie (bijvoorbeeld buiten de *allowlist*).
Collection: De aanvaller probeert gegevens te verzamelen die van belang zijn voor hun doel.	De aanvaller maakt gebruik van de tool `Total Network Inventory` (TNI). Deze tool kan worden gebruikt om alle systemen in het netwerk te scannen en een overzicht te maken van accounts, systemen en gebruikte software. Hiermee is hoogstwaarschijnlijk informatie verzameld gerelateerd aan de netwerk infrastructuur.	[7] Installatie en uitvoer van bekend dubieuze software (TNI, PCHunter, MegaSync, etc.)
Command and Control: De aanvaller probeert te communiceren met gecompromitteerde systemen.	De aanvaller gebruikt het VPN-account `[gebruikersnaam@domein]` en andere verzamelde (DA) accounts (zie *Tabel 14*) om via RDP naar systemen te verbinden. Door mitigerende maatregelen uitgevoerd door de gemeente zijn sporen gerelateerd aan Cobalt Strike verwijderd. Wel zijn in de logbestanden sporen gevonden die duiden op de uitvoer van het *framework*.	[1] Login van ongebruikelijke locatie [2] Login van blocklist locaties (bijvoorbeeld Rusland en/of China).
Exfiltration: De aanvaller probeert gegevens te stelen.	De aanvaller heeft op het systeem `[FS]` een programma geïnstalleerd genaamd MEGAsync. Dit programma is gedurende een maand op verschillende momenten actief, en is zeer waarschijnlijk gebruikt om een kopie van de bestanden op de `[FS]` te exfiltreren naar een extern `MEGAsync` IP-adres.	[9] (Grote) afwijkingen in verkeersstromen. [7] Installatie en uitvoer van bekende dubieuze software (TNI, PCHunter, MEAGsync, Cobalt Strike, etc.)

Impact: De tegenstander probeert de systemen en gegevens te manipuleren, te onderbreken of te vernietigen.	Uiteindelijk wordt vanaf de [DC1] tot twee keer toe het ransomware proces gestart. In eerste instantie gebruikt de aanvaller `bu.exe`, maar waarna ook `buren_cryptor.exe` actief is geweest. Met deze software is het de aanvaller gelukt om in totaal 12 systemen te versleutelen. Zie BIJLAGE 2: Overzicht gecompromitteerde systemen	[11] Detectie van verdacht proces dat verdachte (encryptie) activiteit uitvoert.

Tabel 4 - Overzicht van aanvallersactiviteit op basis van het MITRE ATT&CK framework.

3.3 Attributie

Op basis van het onderzoek en verzamelde bewijsstukken is het zeer aannemelijk dat de aanval is uitgevoerd met de zogenaamde [TA] ransomware.

[TA] is een ransomwaregroep die als eerst is geobserveerd in oktober 2019 en opereert volgens het Ransomware-as-a-Service (RaaS) model[4]. In deze constructie houdt [TA] zich bezig met het ontwikkelen van de ransomware, maar maken ze eveneens gebruiken van affiliaties om doelwitten binnen te dringen en hun ransomware te verspreiden. [TA] claimt onderdeel te zijn van het Maze ransomware kartel[5], een groep van ransomware-families, waaronder Maze zelf, LockBit en Ragnar Locker. Binnen het kartel worden bijvoorbeeld tactieken, infrastructuur en slachtofferdata gedeeld en wordt een deel van de winst geïnvesteerd in het verder ontwikkelen specifieke tooling waaronder de ransomware zelf. Opgemerkt zij dat op het moment van schrijven onduidelijk is of desbetreffende kartel nog bestaat. Maze zou zijn gestopt met ransomware terwijl Lockbit en Ragnar Locker nog actief zijn.

[TA] (en affiliates) is één van de eerste RAAS groepen die zogenaamde *triple extortion*[6] technieken gebruikt. Hierbij wordt de data niet alleen versleuteld (1), maar wordt er ook gedreigd om de data te lekken (2) en om een DDoS aanval uit te voeren (3) wanneer een organisatie weigert te betalen. Inmiddels heeft [TA] al verantwoordelijkheid voor meer dan dertig aanvallen geclaimd, aldus de leaksite waarop ze de gestolen data van slachtoffers publiceren die niet willen betalen. In de praktijk zal het aantal succesvolle aanvallen significant hoger liggen, gezien het feit dat mogelijk niet alle aanvallen succesvol zijn en organisaties in veel gevallen het losgeld betalen, waardoor de desbetreffende organisatienaam niet op de leaksite van [TA] terecht komt.

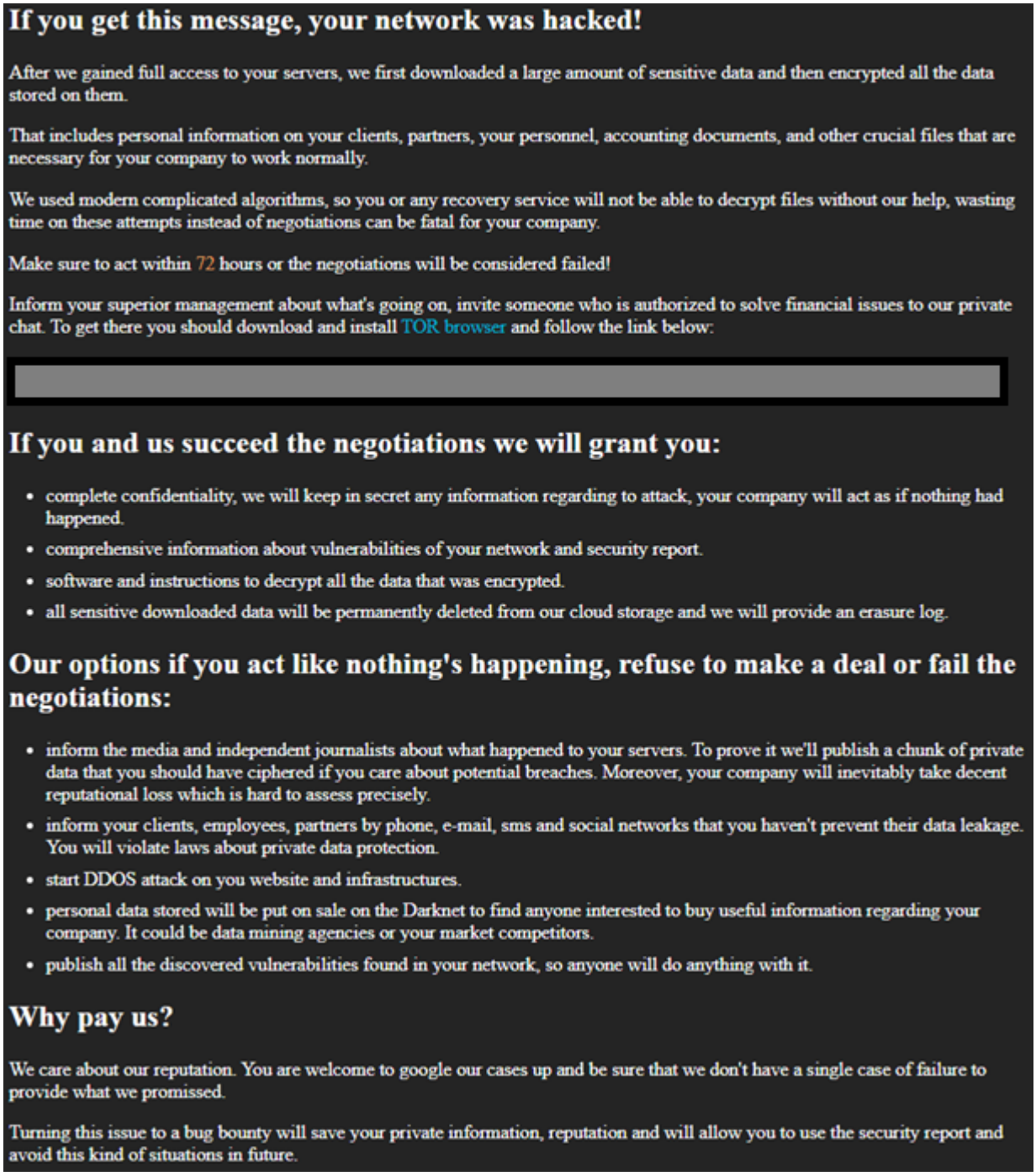
De *ransom note* (*Figuur 2*), aangetroffen op de systemen van gemeente, vertonen gelijkenissen met andere publiek gedeelde *ransom notes* van [TA]. In de *ransom note* '`YOUR_FILES_ARE_ENCRYPTED.HTML`' die op het systeem wordt geplaatst na het versleutelen van een systeem, wordt benoemd dat het netwerk gehackt is en dat de problemen opgelost kunnen worden door naar de een URL te *browsen* voor de 'supportwebsite', waarmee het slachtoffer in contact kan treden met de aanvaller. Desbetreffende *ransom note* is weergegeven in *Figuur 2*. In het

4 [URL]

5 [URL]

6 [URL]

figuur is een grijs blok geplaatst over de URL waarnaar verwezen wordt, om te voorkomen dat de lezer eventueel zelfstandig naar deze pagina toe gaat waar contact gezocht kan wordt met aanvaller namens gemeente. Desgewenst kan deze separaat aangeleverd worden.



If you get this message, your network was hacked!

After we gained full access to your servers, we first downloaded a large amount of sensitive data and then encrypted all the data stored on them.

That includes personal information on your clients, partners, your personnel, accounting documents, and other crucial files that are necessary for your company to work normally.

We used modern complicated algorithms, so you or any recovery service will not be able to decrypt files without our help, wasting time on these attempts instead of negotiations can be fatal for your company.

Make sure to act within 72 hours or the negotiations will be considered failed!

Inform your superior management about what's going on, invite someone who is authorized to solve financial issues to our private chat. To get there you should download and install TOR browser and follow the link below:

If you and us succeed the negotiations we will grant you:

- complete confidentiality, we will keep in secret any information regarding to attack, your company will act as if nothing had happened.
- comprehensive information about vulnerabilities of your network and security report.
- software and instructions to decrypt all the data that was encrypted.
- all sensitive downloaded data will be permanently deleted from our cloud storage and we will provide an erasure log.

Our options if you act like nothing's happening, refuse to make a deal or fail the negotiations:

- inform the media and independent journalists about what happened to your servers. To prove it we'll publish a chunk of private data that you should have ciphered if you care about potential breaches. Moreover, your company will inevitably take decent reputational loss which is hard to assess precisely.
- inform your clients, employees, partners by phone, e-mail, sms and social networks that you haven't prevent their data leakage. You will violate laws about private data protection.
- start DDOS attack on you website and infrastructures.
- personal data stored will be put on sale on the Darknet to find anyone interested to buy useful information regarding your company. It could be data mining agencies or your market competitors.
- publish all the discovered vulnerabilities found in your network, so anyone will do anything with it.

Why pay us?

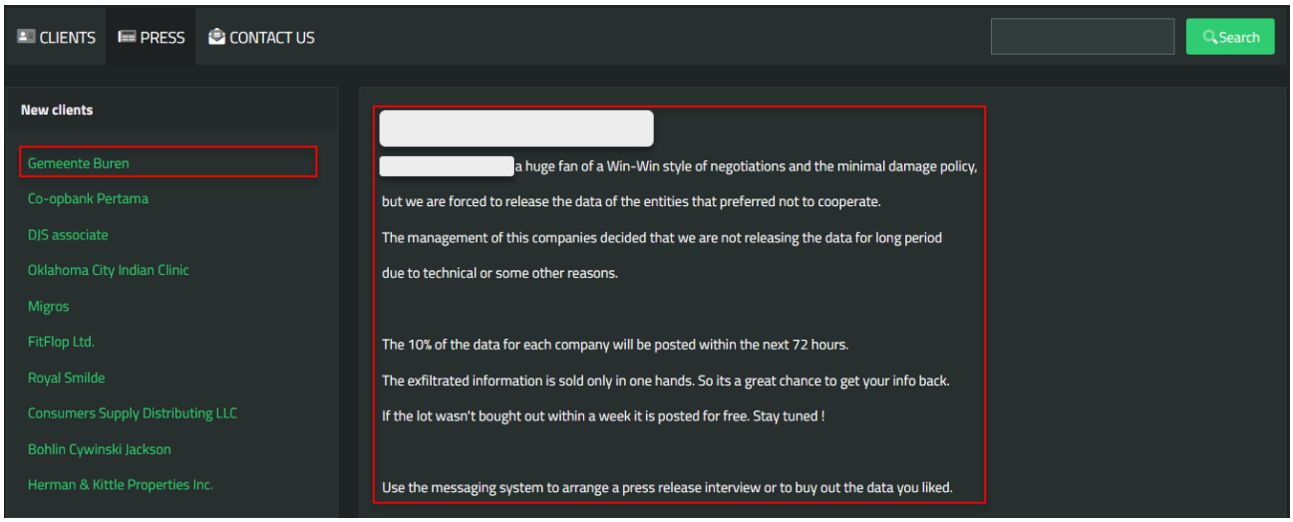
We care about our reputation. You are welcome to google our cases up and be sure that we don't have a single case of failure to provide what we promissed.

Turning this issue to a bug bounty will save your private information, reputation and will allow you to use the security report and avoid this kind of situations in future.

Figuur 2 - Ransomnote [TA], aangetroffen op systemen gemeente.

De overeenkomstige stijl van de ransom note en de URL zijn eerder waargenomen in een publiek artikel[7] van een [TA] ransomware aanval.

Tot slot vermeldt een andere website[8] (de 'leak website') van [TA], ook de naam van [TA], zoals in rood geaccentueerd in *Figuur 3*. Tevens is links in het figuur ook een verwijzing te zien naar de pagina met vermelding van Gemeente Buren, met wanneer met hierop doorklikt, de hyperlinks naar de geëxfiltreerde data (of tenminste een gedeelte hiervan). De *sample* is door Hunt & Hackett gedownload om te verifiëren dat het daadwerkelijk om data van de gemeente ging. Vervolgens is de dataset aangeleverd aan Hoffman voor inhoudelijk onderzoek.



Figuur 3 – [TA] pagina.

7 [URL]

8 [URL]

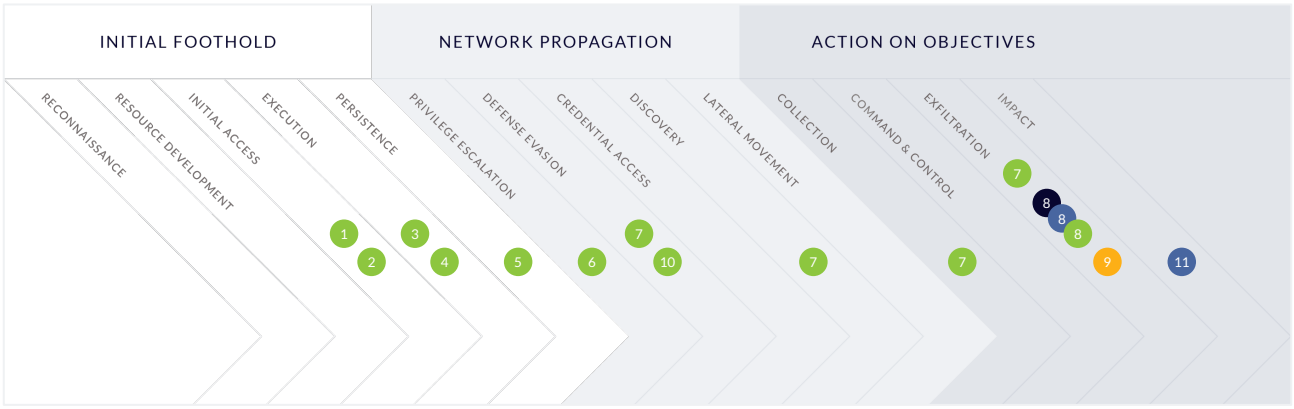
4. In welke mate was de aanval te detecteerbaar geweest?

Met een hoger beveiligingsniveau was de aanval aanzienlijk moeilijker geweest om succesvol uit te voeren. Echter, de ervaring leert ook dat gemotiveerde aanvallers bijna altijd wel een *point-of-entry* vinden waarmee de *initial access* kan worden verkregen. Wat er daarna gebeurt hangt in hoge mate af van de mate waarin een organisatie in staat is om de aanval vroegtijdig te detecteren. Om te zien in welke mate deze aanval detecteerbaar was, is op basis van de gebruikte MITRE ATT&CK tactieken bepaald in hoeverre de in paragraaf 3.2 uiteengezette MITRE-fases te detecteren waren geweest voor de gemeente Buren. In *Figuur* 4 zijn de aanvalsstappen geplot op de Hunt & Hackett detectie-matrix, met daarin een categorisering naar de mogelijkheden voor (het soort) detectie.

***Figuur* 4 –** Detectiematrix waarin de aanval is geplot op het MITRE ATT&CK framework

Op basis van deze matrix kan worden geconcludeerd dat, met name in de beginfase van de aanval, een groot gedeelte van de aanvalsstappen vrij goed te detecteren was geweest met adequaat ingerichte monitoring. Een aantal specifieke stappen in de aanval, waaronder de date exfiltratie en de uitrol van ransomware waren te detecteren geweest op basis van gedragingen (*behaviour anomaly* detectie).

Uit de volgordelijkheid van de fasen van de aanval zoals uiteengezet in het MITRE ATT&CK *framework* zien de mogelijkheden tot detectie eruit zoals weergegeven in *Figuur 5*. Hieruit is op te maken dat de aanval tot aan de laatste aanvalsstappen relatief gemakkelijk te detecteren waren en daarmee de impact op de organisatie ook relatief goed te voorkomen was geweest. De laatste aanvalsstappen (exfiltratie & impact) waren vergen geavanceerdere vormen van detectie om opgemerkt te worden. Het detecteren van, en daarmee reageren op, de geobserveerde aanvalsstappen was *overall* relatief eenvoudig geweest met hoogwaardige *Security Operations Centre* (SOC) of *Managed Detection and Response* (MDR)-service.



Figuur 5 - Detectie mogelijkheden over het verloop van de aanval

5. Conclusies

Op basis van een analyse van het verzamelde onderzoeksmateriaal heeft Hunt & Hackett de onderzoeksvragen zoals gesteld in paragraaf0als volgt kunnen beantwoorden.

Wat is er gebeurd?
De gemeente Buren slachtoffer is geworden van [TA] ransomware. De eerste geobserveerde sporen van de aanval dateren van 18 januari 2022, toen de aanvaller toegang verkreeg tot het netwerk door het VPN-account [gebruikersnaam@domein] te misbruiken. In de periode die volgde is de aanvaller lateraal door het netwerk bewogen, hoofdzakelijk door middel van het *Remote Desktop Protocol* (RDP). Daarnaast heeft de aanvaller met onder andere de software Total Network Inventory aanvullende data gerelateerd aan de netwerkinfrastructuur verzameld. Op 28 februari 2022 heeft de aanvaller de software MEGAsync geïnstalleerd op de bestandserver [FS], van waar data extractie heeft plaatsgevonden naar een extern IP-adres. Vervolgens heeft de aanvaller vanaf een *Domain Controller* (DC) door middel van ransomware 12 systemen versleuteld. Een overzicht van de 12 systemen is terug te vinden in BIJLAGE 2: Overzicht gecompromitteerde systemen. Nadat de initiële impact van de ransomware aanval was gemitigeerd door het IT-security team, is op 14 april 2022 door de aanvaller 126GB van de ontvreemde data online aangeboden.

Hoe heeft dit incident kunnen plaatsvinden?
Op basis van de eerste geobserveerde sporen is het waarschijnlijk dat vanaf het externe IP-adres 91.[X].[X].[X] de aanvaller met het VPN account [gebruikersnaam@domein] toegang heeft verkregen tot het netwerk van de gemeente. Het is onduidelijk waar de aanvaller de inloggegevens van dit account heeft weten te bemachtigen. Door middel van het RDP heeft de aanvaller in verbinding kunnen maken met het systeem [DC2], mogelijk door het lokaal administrator account, een account met de hoogste rechten, te compromitteren met een *brute force* aanval. Ten eerste was wachtwoord van dit administrator account niet voldoende complex om een dergelijke aanval onmogelijk te maken. Ten tweede was het wachtwoordbeleid niet dusdanig ingericht dat dergelijke wachtwoorden met enige regelmatig werden gewijzigd. Als derde en laatste waren accounts met verhoogde rechten, en de VPN-accounts niet beveiligd met een tweede factor. Met het VPN-account account heeft de aanvaller vanaf in ieder geval het interne VPN IP 10.[X].[X].[X] meerdere systemen binnen het netwerk benaderd en informatie verzameld gerelateerd aan de netwerkinfrastructuur. Dit heeft wel antivirus meldingen gegenereerd, maar hier is geen opvolging aan gegeven. Een van de belangrijkste systemen die is benaderd, is de bestandserver [FS]. Omdat er geen proces is ingericht om adequaat om te gaan met meldingen uit detectiemechanismen zoals antivirus, is het mogelijk geweest voor de aanvaller om ongemerkt door het netwerk te bewegen en grote hoeveelheden informatie van de organisatie te kunnen exfiltreren.

Wat is de omvang van het incident?
In BIJLAGE 2: Overzicht gecompromitteerde systemen is een overzicht terug te vinden van de systemen welke door de aanvaller zijn gecompromitteerd. In totaal is tot 15 van de 100 servers binnen het [DOM1] domein toegang geweest door de aanvaller en zijn er 12 systemen versleuteld met ransomware. Geen van de werkstations fysiek of virtueel zijn versleuteld met de [TA] ransomware. Daarnaast heeft de aanvaller tijdens de aanval misbruik gemaakt van meerdere accounts, waaronder de accounts [GN1], [GN2], [GN3], en [gebruikersnaam@domein]. Echter, omdat de aanvaller met een account met de hoogste rechten, toegang heeft gehad tot de DC moeten alle accounts binnen het [DOM1] domein worden beschouwd als gecompromitteerd. Daarnaast moet de data op de [FS] waaronder tekstbestanden, certificaten en alle overige informatie als gecompromitteerd worden beschouwd. De aanval is voor zover bekend beperkt gebleven tot het [DOM1] domein. Omdat binnen het domein [DOM2] geen ransomware is aangetroffen, of er handmatige aanvaller

activiteit is aangetroffen richting of vanuit het domein [DOM2], is dit domein buiten de scope van het onderzoek gelaten. Wel is binnen de VDI-omgeving van dit laatstgenoemde domein Carbon Black uitgerold.

Tot welke data en systemen is toegang geweest door de aanvallers?
De aanvaller heeft tenminste toegang gehad tot informatie gerelateerd aan de infrastructuur en alle bestanden op het systeem [FS]. Dit betreft in ieder geval officebestanden, wachtwoord hashes, certificaten en *private keys*, Welke data precies op deze bestandserver aanwezig was ten tijde van de aanval valt buiten de scope van dit onderzoek. Op de bestandserver is in de periode van 28 februari 2022 tot en met 31 maart 2022 het programma MEGAsync actief geweest waarmee data extractie heeft plaatsgevonden naar een extern MEGAsync IP-adres. Daarnaast is het technisch mogelijk geweest voor de aanvaller om toegang te verkrijgen tot de mailserver [MAIL1] en [MAIL2] omdat deze versleuteld zijn geweest door de ransomware. Op de mailservers zijn echter op basis van de ten tijde van het onderzoek bekende IOCs, geen handmatige aanvaller activiteiten aangetroffen.

Hoe kan het incident worden gemitigeerd?
De directe impact van de ransomware aanval kon worden gemitigeerd doordat de back-up processen op dusdanige wijze is geïmplementeerd dat het mogelijk is geweest voor het IT Security team om met een verlies van 24 uur aan data de getroffen systemen te herstellen. In de periode van 1 april 2022 tot 4 april 2022 zijn de getroffen systemen hersteld vanuit back-up tapes. Daarna heeft het IT-security team van de gemeente op advies van Hunt & Hackett verschillende, aanvullende mitigerende maatregelen geïmplementeerd, waaronder de implementatie van Multi Factor Authenticatie (MFA) op VPN, email en beheeraccounts en het dichtzetten van RDP waar mogelijk. Een volledig overzicht van de geadviseerde mitigerende maatregelen kan worden teruggevonden in het document 20220402_Hardening_Guidelines_Buren.pdf.
Van de actor is bekend dat deze doet aan zogenaamde *triple extortion*. Een van de manieren van afpersen is het lanceren van een DDoS aanval. Voordat een dergelijke aanval plaats heeft kunnen vinden, is in samenwerking met een serviceleverancier van de gemeente DDoS bescherming ingeregeld. Tot slot is op alle virtuele werkstaions binnen zowel het [DOM1] domein en het [DOM2] domein VMWare Black Endpoint Detectie en Respons (EDR) geïnstalleerd. Dit is eveneens gedaan op de servers en fysieke werkstations binnen het [DOM1] domein. Door middel van VMWare Carbon Black worden de *endpoints* 24/7 gemonitord op aanvaller activiteit.

Ondanks het feit dat de IT Security team van de gemeente Buren erin is geslaagd om kort na het constateren van de ransomware-aanval direct actie te nemen in de vorm van recovery maatregelen en daarmee de verstorende impact op de organisatie grotendeels heeft weten te voorkomen, heeft het handelen niet kunnen voorkomen dat een grote hoeveelheid data is ontvreemd door de [TA]. Dit komt mede doordat de uitrol van ransomware de laatste stap vormt in het proces van de aanvaller en de data reeds daarvoor al was geëxfiltreerd zonder dat dit is opgemerkt. Het aspect van datadiefstal is niet meer te mitigeren.

6. Aanbevelingen

Het onderzoek naar de *root cause* van het incident heeft geresulteerd in een onmiddellijk mitigatieplan dat is uitgevoerd om de geïnfecteerde machines te identificeren, op te ruimen en de aanvallers uit het netwerk te houden. Voor een volledig overzicht van de geadviseerde mitigerende maatregelen ten aanzien van Firewall, werkstation, server en Windows *hardening*, kan het document `20220402_Hardening_Guidelines_Buren.pdf` worden geraadpleegd.

Voor [CAT2] en [CAT3] beveelt Hunt & Hackett aan om de algehele beveiliging van de organisatie te verbeteren. De aanbevelingen die in dit hoofdstuk worden beschreven, moeten dienen te worden gewogen en indien van toepassing, te worden doorgevoerd. Hierbij moet rekening gehouden worden dat deze aanbevelingen niet de [CAT1] aanbevelingen bevatten die al in het mitigatieplan zijn verwerkt.

6.1 [CAT1]

A/ Managed Detection & Response
Op basis van de bevindingen in Hoofdstuk 3 is inzichtelijk geworden welke verschillende tools, technieken en procedures door de aanvaller zijn gebruikt. Voor bijna alle fasen van de aanval geldt dat de geobserveerde aanvalsstappen detecteerbaar waren geweest als *endpoint, log en network* monitoring op de juiste manier waren geïmplementeerd. Bijvoorbeeld door middel van een externe partij.
Het is daarom, gegeven het dreigingsbeeld en de huidige risicoblootstelling, aan te bevelen om prioriteit te geven aan de implementatie van dergelijke monitoring. Daarnaast is monitoring relevant omdat dit element de meeste impact heeft in het verlagen van het huidige risiconiveau. Dit zou ervoor zorgen dat snel zicht ontstaat op de digitale omgeving en er direct een actieve verdediging wordt geïmplementeerd om de gemeente in staat te stellen incidenten vroegtijdig te detecteren en daar direct op te kunnen acteren.
Daarnaast is het op advies om op zeer korte termijn in ieder geval de hiernavolgende drie punten ten aanzien van *logging* in te regelen, zoals omschreven in *Tabel 5*.

Actie	Instructies
1. Gedetailleerde logging	Configureer een GPO waarmee de volgende instellingen technisch worden afgedwongen. • Schakel gedetailleerde logging in op alle werkstations en servers • De instellingen zijn te vinden onder: Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration
2. Aanzetten audit process	In deze zelfde GPO van '1. Gedetailleerde logging', schakel de volgende instellingen in: • Computer Configuration → Administrative Templates → System → Audit Process Creation ***(Include command line in process creation event)***
3. Blokkeren PowerShell scripts	Zet PowerShell script block logging aan: • Instructies zijn uitgewerkt op de volgende pagina: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.1

Tabel 5 - Instructies voor inregelen van logging.

B/ Multi-factor authenticatie

De aanvaller heeft in kunnen loggen op de VPN met legitieme inloggegevens. Waar deze inloggegevens zijn buitgemaakt is op basis van het beschikbare onderzoeksmateriaal niet vast te stellen. Wanneer dergelijke accounts gebruik maken van authenticatie mechanismen zonder een tweede factor kan, wanneer de inloggegevens uitlekken of op een andere manier bemachtigd worden, een kwaadwillende deze misbruiken om toegang te krijgen tot het netwerk. Op basis van de observatie en het daarbij behorende risico adviseert Hunt & Hackett om tenminste alle accounts voor extern benaderbare services, zoals VPN, en email te voorzien van extra authenticatiemechanisme. Wanneer inloggegevens van dergelijke accounts lekken of door een aanvaller buitgemaakt worden, zijn deze gegevens niet door een aanvaller te gebruiken wanneer MFA is geïmplementeerd.

C/ Wachtwoord complexiteit

Tijdens de aanval is het mogelijk geweest voor de aanvaller om een wachtwoord te *brute forcen*. Dat het mogelijk is om een wachtwoord op die manier te bemachtigen komt omdat het wachtwoord niet voldoende complexiteit heeft om dit tegen te gaan. Met wachtwoorden van een lagere (of voorspelbare) complexiteit is het voor een aanvaller mogelijk om variaties hierop, al dan niet geautomatiseerd, te raden.

Op basis van bovenstaande observaties adviseert Hunt & Hackett om na te gaan in hoeverre het huidige wachtwoordbeleid afdoende is gegeven het geldende dreigingslandschap voor de gemeente en risicobereidheid. Denk hierbij aan een wachtwoordbeleid dat bijvoorbeeld op dusdanige wijze is ingeregeld dat technisch afgedwongen strengere voorwaarden gelden voor accounts met hogere rechten. Hiervoor kan gebruik gemaakt worden van wat Windows definieert als '*finegrained passwordpolicies*' voor accounts die in het AD staan. Met deze *policies* kan een onderscheid worden gemaakt tussen serviceaccounts en generieke gebruikersaccounts. Een sterk wachtwoord dient uniek en minstens 12 karakters of langer te zijn. Daarnaast dient het wachtwoord te zijn opgebouwd uit willekeurig gekozen leestekens en cijfers. Hierbij kan gebruik worden gemaakt van een wachtwoordmanager (die gebruik maakt van tweede factor authenticatie) voor het op een veilige manier opslaan van deze wachtwoorden, om te voorkomen dat deze bijvoorbeeld in leesbare tekstdocumenten worden opgeslagen.

6.2 [CAT2]

De aanbevelingen in deze paragraaf zijn van toepassing voor [CAT2] en hebben betrekking op gebruikers en wachtwoord, evenals op host- en protocolverharding.

A/ Gebruikers & Wachtwoorden

De acties en instructies rondom het verbeteren van beveiliging met betrekking tot gebruikers en wachtwoorden is verder uitgewerkt in de hiernavolgende tabel (*Tabel 6*)

Actie	Instructies
Configureer unieke lokale beheerderswachtwoorden	• Alle werkstations en servers moeten worden geconfigureerd met unieke en sterke wachtwoorden voor het lokale beheerdersaccount. • Richtlijnen zijn te vinden op de volgende URL: https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772

Actie	Instructies
Gebruik van domeinbeheerdersaccounts beperken	• Domeinbeheerdersaccount en vergelijkbare verhoogde-rechten accounts mogen alleen worden gebruikt als dit absoluut noodzakelijk is. Het aantal accounts met hoge privileges moet tot het absolute minimum worden teruggebracht.
Schakel MFA in voor accounts met verhoogde rechten	• In aanvulling op de aanbeveling over MFA voor extern benaderbare services, is het advies om dit ook in te regelen voor accounts met verhoogde rechten Schakel MFA in op alle beheerinterfaces • Voor alle administratieve interfaces zoals Exchange ECP, VPN, enz. moet MFA zijn ingeschakeld.
Inactieve accounts bekijken en verwijderen	• Bekijk alle actieve directory-, firewall-, VPN- en andere soorten gebruikersaccounts en verwijder alle accounts die gedurende een lange periode inactief zijn geweest. Verwijder bijvoorbeeld alle accounts die de afgelopen 6 maanden geen activiteit hebben vertoond.

Interactieve aanmeldingen voor serviceaccounts weigeren	• Maak een GPO die het volgende blokkeert:
	  ○ Lokaal aanmelden weigeren
	  ○ Aanmelding via RDP weigeren
	• Richtlijn is te vinden op de volgende URL: http://paulasitblog.blogspot.com/2017/01/deny-interactive-logon-for-service.html

Tabel 6 - Overzicht acties en instructies voor gebruikersnamen en wachtwoorden.

B/ Veilig systeem beheer

Tijdens het onderzoek is duidelijk geworden dat systeembeheerders gebruik maken van gepersonaliseerde beheer accounts. Echter, niet van toegewezen beheer werkstations, of van specifieke beheer infrastructuur zoals *jumphosts*. Door middel van een *jumphost* is het mogelijk om vanaf een extra beveiligde server beheerwerkzaamheden te verrichten. Daarnaast maakt het inzichtelijk wie, wanneer welke werkzaamheden heeft verricht en vanaf welk systeem. Een dergelijke server is weliswaar in gebruik, echter ten tijde van schrijven nog niet voorzien van voldoende *hardening* maatregelen. Derhalve is het advies van Hunt & Hackett om de reeds in gebruik zijnde beheer server verder te hardenen, en de processen en het beleid rondom systeembeheer te verbeteren en op een veiligere wijze vorm te geven.

C/ Protocol hardening

Tijdens de beginfase van de aanval heeft de aanvaller onder andere gebruik gemaakt van SMB. Op basis van deze observatie is het advies van Hunt & Hackett om *legacy* protocollen uit te schakelen waar mogelijk. Protocollen zoals SMBv1, LLMNR, NBNS dienen waar mogelijk te worden uitgeschakeld. Richtlijnen om dit inhoudelijk te implementeren kunnen hier worden gevonden:

- http://woshub.com/how-to-disable-netbios-over-tcpip-and-llmnr-using-gpo/
- https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

6.3 [CAT3]

De hiernavolgende aanbevelingen zijn van toepassing in [CAT3].

A/ Security assessment
De aanbevelingen in dit document komen direct voort uit de observaties met betrekking tot het incident en betreffen daarmee geen breder securityadvies, al zullen zaken als *hardening* en security monitoring daar wel sterk aan bijdragen. Om er zeker van te zijn dat de huidige staat van de digitale beveiliging afdoende bescherming biedt tegen ransomware aanvallen, en andere dreigingen vanuit het dreigingslandschap, adviseert Hunt & Hackett om een security assessment te doen of laten uitvoeren. Op basis van een dergelijke gap analyse zou duidelijk moeten worden in hoeverre de organisatie beschermd is tegen de dreigingen uit het voor de organisatie van toepassing zijnde dreigingslandschap, en waar er nog gaten in de verdediging zitten. Het doel van een dergelijke analyse is om tot concrete adviezen te komen waarmee de weerbaarheid van de organisatie verder kan worden verhoogd. Het is raadzaam om deze assessment pas uit te laten voeren als de [CAT1] en [CAT2] maatregelen zijn geïmplementeerd.

BIJLAGE 1: Overzicht Forensische *Packages*

Van de systemen weergegeven in *Tabel 7* zijn van de meest relevante databronnen op de systemen Forensische *packages* gemaakt.

Scope	Naam	Type
Veiliggesteld binnen de scope van het onderzoek	[Geredigeerd]	Domain Controller
	[Geredigeerd]	Domain Controller
	[Geredigeerd]	Domain Controller
	[Geredigeerd]	Domain Controller
	[Geredigeerd]	Fileserver
	[Geredigeerd]	Mail-server
	[Geredigeerd]	Onbekend
Veiliggesteld binnen initiële scope van het onderzoek	[Geredigeerd]	Beheer server
	[Geredigeerd]	Test server DMS
	[Geredigeerd]	OCR tooling
	[Geredigeerd]	Makelaar server

Tabel 7 - Veiliggestelde systemen

BIJLAGE 2: Overzicht gecompromitteerde systemen

Op de systemen weergeven in *Tabel* 8 zijn op aangeven van de gemeente versleutelde bestanden aangetroffen, of is aanvaller activiteit geobserveerd.

Naam	Type
[Geredigeerd]	Domain Controller
[Geredigeerd]	Domain Controller
[Geredigeerd]	Domain Controller
[Geredigeerd]	Read Only Domain Controller
[Geredigeerd]	Exchange Mailbox server
[Geredigeerd]	Exchange Mailbox server
[Geredigeerd]	Veeam backup server (Fysiek)
[Geredigeerd]	Ouder beheer server
[Geredigeerd]	Fileserver (9,2TB)
[Geredigeerd]	Document managementsysteem (Prod)
[Geredigeerd]	ESB
[Geredigeerd]	Kofax scanner naar het DMS (OCR)
[Geredigeerd]	Kofax scanner naar het DMS (OCR)
[Geredigeerd]	Document managementsysteem (Test)
[Geredigeerd]	Onbekend systeem, de gemeente heeft geen informatie kunnen aanleveren over de oorsprong of functie.

***Tabel* 8 -** Overzicht systemen met versleutelde bestanden

BIJLAGE 3: Indicators of compromise overzicht

Deze bijlage geeft een overzicht van de belangrijkste *indicators of compromise* die tijdens het project zijn waargenomen.

Domeinnamen & IP-adressen	**Beschrijving**
10.[X].[X].[X]	Intern IP-adres VPN, toegewezen aan aanvaller
10. [X].[X].[X]	Intern IP-adres VPN, toegewezen aan aanvaller
91. [X].[X].[X]	Gebruikt IP adres door aanvaller om in te loggen op de VPN service.
66. [X].[X].[X]	MEGASync
[URL]	MEGASync

***Tabel 9** - Indicators of compromise* domeinnamen en IP-adressen

Bestanden	**Beschrijving**
bu.exe	[TA] ransomware
buren_cryptor.exe	[TA] ransomware
spools.exe	Cobalt Strike
tni.exe	Total Network Inventory
MEGAsync.exe	MEGASync
MEGAupdater.exe	MEGASync

***Tabel 10** - Indicators of compromise* bestanden

Hashes	**Beschrijving**
899b02fa31b29c67437b67bff8959d8dee288d9d	sha1 - bu.exe, buren_cryptor.exe
d92522dcaec6a3d22a1b05d8f5c9ebae08ec74da	sha1 - MEGAsync.exe
4e7578c638d480da1c3b3b3b54f46b153717981d	sha1 - MEGAupdater.exe

***Tabel 11** - Indicators of compromise hashes*

Scheduled Tasks	**Beschrijving**
MEGAsync Update	MEGASync update taak
\crypt!	Verantwoordelijk voor de uitvoer van [TA] ransomware

Tabel 12 - Indicators of compromise Scheduled Tasks

Mappen	**Beschrijving**
C:\tmp	Gebruikt voor het distribueren van de ransomware met de `Scheduled Task` *\crypt!*
C:\Windows\Temp	Gebruikt voor het opslaan van `Cobalt Strike` en `Total Network Inventory die` gedetecteerd zijn door Mcafee Anti Virus
C:\users\[GN2]\Desktop	Vanaf deze locatie zijn `MEGAsync`, `PCHunter` en `bu.exe` en `buren_cryptor.exe` uitgevoerd

Tabel 13 - Indicators of compromise mappen

Accounts	**Type account**	**Beschrijving**
[gebruikersnaam@domein]	VPN-account	Gebruikt voor initiële toegang
[GN1]	Domain Admin	Gebruikt voor laterale bewegingen en uitvoer ransomware
[GN2]	Domain Admin	Gebruikt voor laterale bewegingen en data extractie
[GN3]	Domain Admin	Gebruikt voor laterale bewegingen

Tabel 14 - Indicators of compromise accounts

BIJLAGE 4: WHOIS-informatie

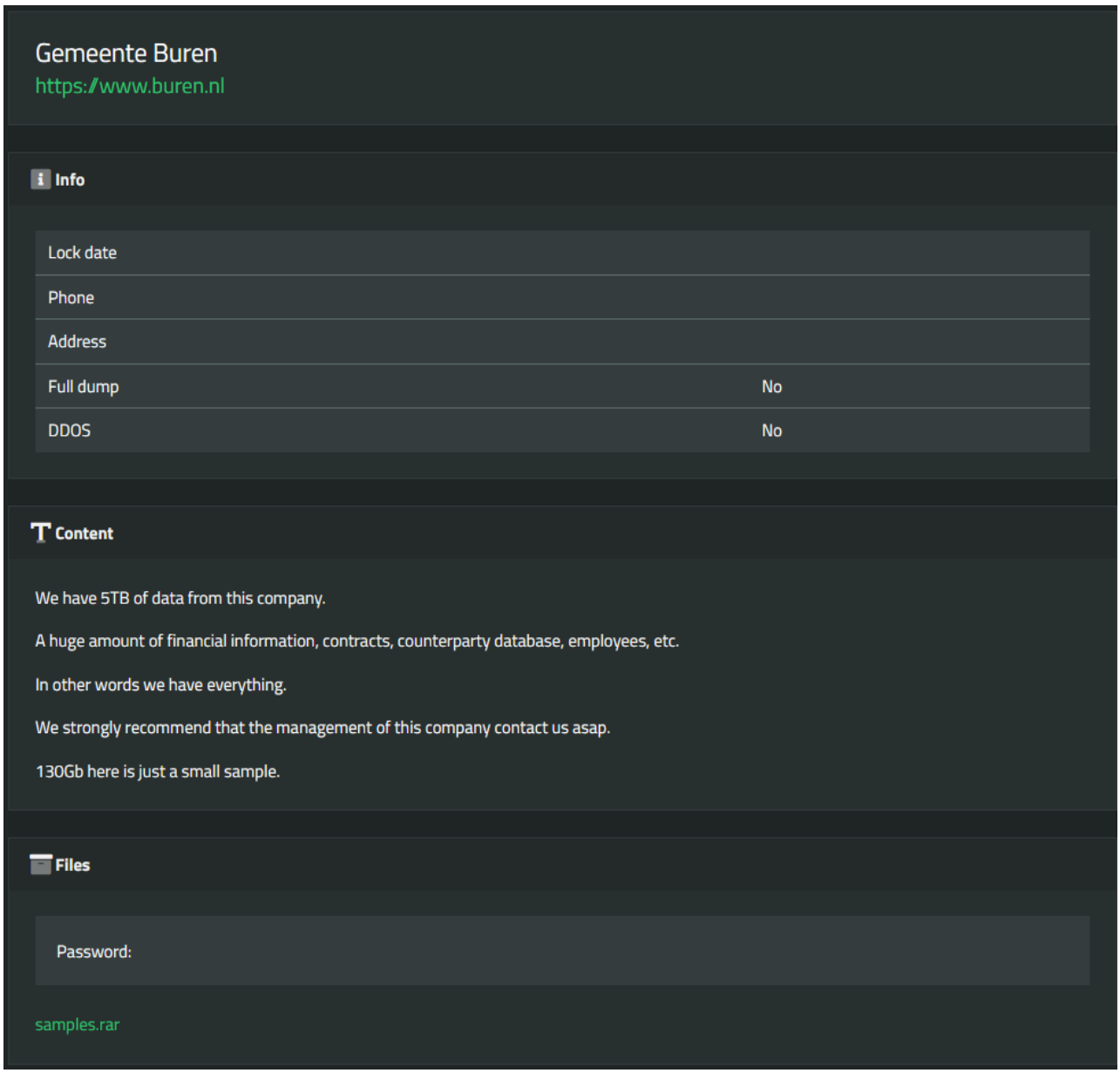
In *Tabel 15* staat een overzicht van de WHOIS-informatie uit de RIPE Database van het IP-adres `91.[X].[X].[X]`. Dit IP-adres is door de aanvaller meermaals gebruikt om op de VPN in te loggen.

Naam	Beschrijving
Abuse contact	[Geredigeerd]
Netwerk	91.[X].[X].[X]/24
Netwerknaam	[Geredigeerd]
Land code	RU
Organisatie	[Geredigeerd]
Organisatie naam	[Geredigeerd]
Organisatie beschrijving	[Geredigeerd]
Organisatie adres	[Geredigeerd]
Organisatie e-mail	[Geredigeerd]

Tabel 15 - Whois informatie 91.[X].[X].[X]

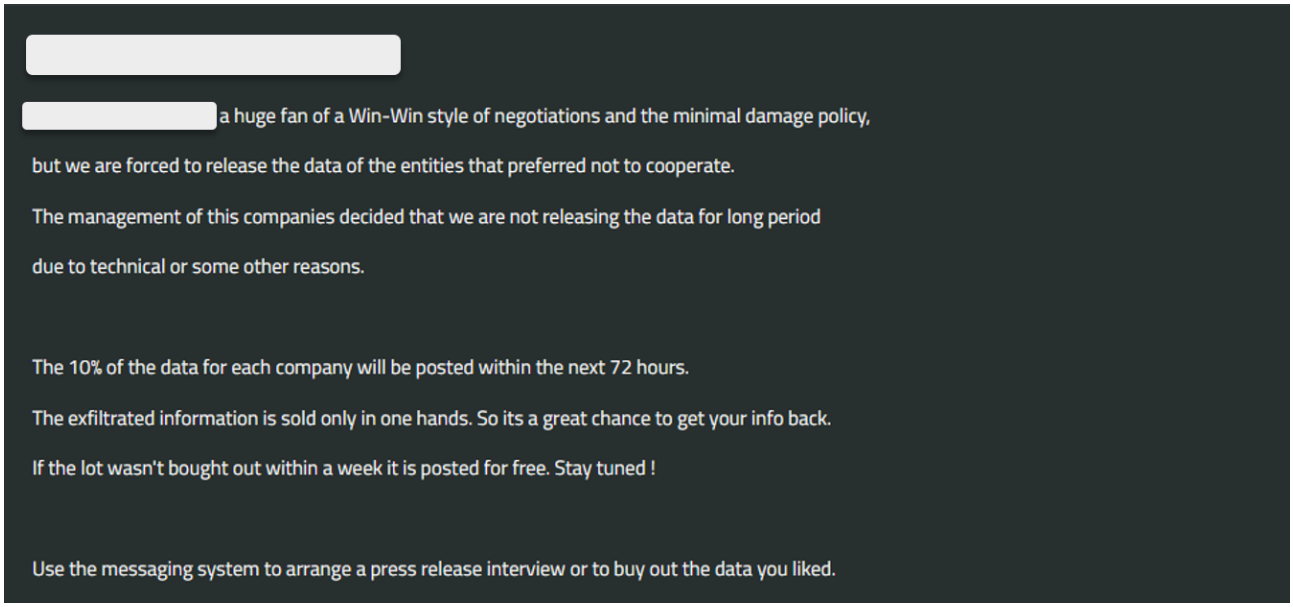
BIJLAGE 5: Screenshot [TA] leak

Onderstaand screenshot is genomen op 14 april 2022. De afbeelding laat zien dat op de *leak* website van de [TA] een data sample aangeboden wordt van de gemeente. De afbeelding geeft eveneens weer dat de groep beweert meer dan de sample in bezit te hebben. Deze hoeveelheid komt overeen met de beschreven schijfruimte op de bestandserver [FS]. De totale schijfgrootte van deze bestandserver is 6.4 TB waarvan ongeveer 5 TB gebruikt is.



Figuur 6 - [TA] *leak* website mededeling

In *Figuur 7* is een screenshot van de pers pagina opgenomen. De afbeelding laat zien op welke wijze de groep [TA] te werk gaat wat betreft het lekken van data van entiteiten, die volgens hen niet meewerken.



Figuur 7 - [TA] *leak* website pers pagina

BIJLAGE 6: Afkortingen Publiekversie

Deze bijlage geeft een overzicht van de afkortingen zoals deze zijn gebruikt in de publieke versie van de rapportage.

Term	Afkorting
Domain Controller	[DC0-9]
Mailserver	[MAIL0-9]
Bestandserver	[FS]
IP-adres	10.[X].[X].[X]
Gebruikersnaam Intern	[GN0-9]
Gebruikersnaam Extern	[gebruikersnaam@domein]
URL	[URL]
Threat Actor	[TA]
Werknemer	[WN]
Categorie	[CAT0-9]

Tabel 16 - *Afkortingen publiekversie*