NORTHWAVE
Intelligent Security Operations

Onderzoek Valkenburg

Management Samenvatting

Versie: 1.0
Datum: April 13, 2021
Auteur: [redacted]

Versie	Datum	Reviewer	Titel	Handtekening
1.0	13-08-2020	[redacted]	Manager CERT	

1 Management Samenvatting

Op 9 Maart 2021 is Senzer slachtoffer geworden van een grootschalige cyberaanval waarbij een groot deel van het netwerk is versleuteld door aanvallers met behulp van gijzelsoftware. Omdat een groot deel van de organisatie afhankelijk is van dezelfde onderliggende IT-infrastructuur, viel het werk stil bij bijna alle divisies van Senzer. Daar bovenop kon Senzer geen betalingen uitvoeren met betrekking tot de bijstandsuitkering en de tijdelijke overbruggingsregeling zelfstandig ondernemers (Tozo).

Vanaf 9 Maart 2021 heeft Northwave Senzer bijgestaan in het herstellen van de IT-infrastructuur. Hierbij heeft Northwave in samenwerking met Senzer een plan gemaakt voor het veilig herstellen van de servers. Verder heeft Northwave ervoor gezorgd dat alle malafide software van alle systemen is gewist en onderzoek gedaan naar de oorzaak van de aanval.

Tijdens het onderzoek naar de bron van de infectie met gijzelsoftware zijn de onderstaande vragen beantwoord:

1. **Hoe zijn de aanvallers het netwerk van Senzer binnengedrongen?**

Northwave heeft verschillende hypotheses onderzocht met betrekking tot de bron van de infectie. Helaas was er geen bewijs beschikbaar dat direct naar de bron van de infectie wees. Het vroegste punt in de tijd waar sporen van de aanvaller zijn terug gevonden was op 27 Februari 2021 om 11:59:00 op systeem SRV-[redacted]. De aanvaller heeft op dat moment een achterdeur geplaatst welke een verbinding opzette met IP-adres "[redacted]". Deze activiteit vond plaats op systeem SRV-[redacted], wat een van de Citrix terminal servers was van Senzer.

De groep die verantwoordelijk was voor de aanval staat erom bekend dat ze gebruik maken van gerichte phishing e-mails en misbruik maken van publiekelijk bereikbare "remote desktop services" om zichzelf toegang te verschaffen tot netwerken[1]. Northwave heeft de e-mail omgeving van Senzer onderzocht, maar geen sporen gevonden die erop duiden dat de aanvaller toegang heeft gekregen tot het netwerk via een phishing e-mail.

Verder ondervond Senzer moeilijkheden in het gebruik van multi-factor authenticatie voor de Citrix terminal servers, en was Senzer bezig met een migratie van Citrix naar Windows Virtual Desktop. Gedurende dit proces waren de Citrix terminal servers kwetsbaar voor een brute-force aanval doordat multi-factor authenticatie uitstond. Kortom, de Citrix servers waren kwetsbaar voor deze aanvals-techniek, de aanvallers staan erom bekend dat ze dergelijke aanvallen uitvoeren, en de eerste (bekende) activiteit van de aanvaller vond plaats op een Citrix server. Op basis van voorgaande feiten verwacht Northwave dat

[1] https://www.secpod.com/blog/ryuk-ransomware/

de aanvaller zichzelf toegang heeft verschaft tot het netwerk van Senzer doormiddel van een brute-force aanval op de Citrix servers van Senzer rond 27 Februari 2021.

2. **Wat zijn de stappen die de aanvaller heeft gezet na het binnendringen van het netwerk van Senzer?**

Na het binnendringen van het netwerk rond 27 Februari 2021 heeft de aanvaller twee achterdeuren geplaatst op SRV-[redacted] op 27 Februari om 11:59 en 12:21. De volgende activiteit van de aanvaller vond plaats op 3 Maart 2021. De aanvaller begon op die datum met het plaatsen van achterdeuren op andere systemen binnen het netwerk, beginnende met SRV-[redacted] om 15:59. Vervolgens, op 4 Maart 2021, verplaatste de aanvaller zijn activiteit van SRV-[redacted] naar de domain controller van het netwerk, SRV-[redacted]

Op 8 Maart heeft de aanvaller om 22:29:35 een lijst van alle systemen op het netwerk uit de active-directory geëxporteerd op systeem SRV-[redacted] Vervolgens heeft de aanvaller om 22:36:22 een nieuwe folder gemaakt op SRV-[redacted] op de locatie “C:\Share$\”. Deze folder bevatte software die de aanvaller heeft gebruikt om gijzelsoftware uit te voeren op alle systemen binnen het netwerk, op basis van de lijst die de aanvaller eerder heeft geëxporteerd. De aanvaller is begonnen met het uitvoeren van gijzelsoftware op systemen op 9 Maart om 01:28:51. Gedurende de aanval heeft de aanvaller ook gepoogd om bewijsmateriaal te wissen door log bestanden te verwijderen. Dit is de aanvaller gelukt op 4 en 5 maart op SRV-[redacted]en op 8 Maart op ATL[redacted].

3. **Hebben de aanvallers gevoelige persoonsgegevens of vertrouwelijke informatie buitgemaakt?**

De analyse naar de bron van de infectie heeft geen enkel bewijs opgeleverd dat ernaar wijst dat er informatie is buitgemaakt door de aanvaller. Northwave heeft enkele verzoeken naar malafide websites gezien, echter was de hoeveelheid verkeer naar deze websites zo beperkt dat data exfiltratie naar deze websites onmogelijk was. Northwave heeft geen enkele andere indicatie van data exfiltratie gevonden op de systemen die onderzocht zijn. Bij andere incidenten die Northwave heeft onderzocht is er door deze groep geen informatie gestolen van hun doelwit. Verder staat deze groep er ook om bekend dat ze geen informatie stelen van hun doelwitten. Gebaseerd op deze informatie acht Northwave het hoogst onwaarschijnlijk dat er gevoelige persoonsgegevens of vertrouwelijke informatie is buitgemaakt door de aanvaller.

4. **Is de omgeving van Senzer nu beveiligd tegen soortgelijke aanvallen?**

Gedurende het incident heeft Senzer verschillende maatregelen genomen om de beveiliging van de omgeving naar een hoger niveau te tillen zodat de omgeving beter beveiligd is tegen aanvallen met gijzelsoftware. Onderdeel van deze maatregelen was het implementeren van een 24/7-bewakingsdienst op basis van Microsoft Defender for Endpoint. Deze dienst zorgt er onder andere voor dat eventuele achtergebleven software van de aanvallers wordt gedetecteerd. Verder heeft Senzer alle wachtwoorden

opnieuw ingesteld en multi-factor authenticatie ingesteld op alle applicaties die benaderbaar zijn vanaf het internet.

Voordat het incident plaatsvond was Senzer al bezig met het verbeteren van de beveiliging door te acteren op hun lange termijn cyber-beveiligings-plan. In essentie betekent dit dat de aanval niet plaats had kunnen vinden als de aanval enkele maanden later was geweest aangezien Senzer al bezig was om de kwetsbaarheden die de aanvaller heeft misbruikt te mitigeren. Verder heeft de backup procedure van Senzer ervoor gezorgd dat ze volledig hebben kunnen herstellen van de aanval, en heeft Senzer laten zien goed voorbereid te zijn op cyber gerelateerde incidenten en perfect gehandeld aan de hand van de incident response plannen die Senzer al paraat had.

Gedurende de herstelfase van het incident heeft Senzer veel punten van hun beveiligings-plan direct gerealiseerd. Dit was mogelijk doordat Senzer de voorbereidingen voor deze punten al voor de aanval gedaan had, wat het snel implementeren van extra mitigaties mogelijk maakte. Verder heeft Northwave nog enkele aanbevelingen gedaan om de beveiliging van Senzer nog beter te maken.