# Cyberaanvallen van ziekenhuizen door UNC1878 groep met Ryuk-ransomware


**Ransomware-aanvallen met het Ryuk-virus van ziekenhuizen leidt in de Verenigde Staten de laatste 24 uur tot verhitte gemoederen. Op 26 oktober liet het cybersecuritybedrijf Hold Security via haar topman Alex Holden weten dat leden een Oost-Europese, waarschijnlijk Russische, hackersgroep met de codenaam UNC1878 drieste plannen hadden. Het bedrijf onderschepte onderlinge communicatie over plannen om ransomware bij meer dan 400 ziekenhuizen in de VS te installeren. Daarbij gebruik makend van het Ryuk-virus. Het vehikel is een phishing-email.** Over dit ramsomware-virus publiceerde ik op 6 oktober 2020, toen dit virus een ziekenhuisketen met 250 vestigingen trof. Alex Holden deelde de informatie o.a. met cybersecurity-journalist Brian Krebs op 27 oktober. Die publiceerde er op 28 oktober over. Inmiddels verscheen een gemeenschappelijk statement van 15 pagina's afkomstig van de FBI, het Homeland security Department en het U.S. Department of Health and Human Services. Daarin beschrijft men het mechanisme van de aanvallen.

## Modus operandi

In het statement gaat men uitgebreid in op aanvallen met het Trickbotvirus of Trickbot-achtigen als "carrier', die erna het Ryuk-virus als "payload" naar binnen helpen. Om eenmaal binnen zijdelings zich door het netwerk te bewegen maakt het virus gebruik van software-tools als PowerShell, Windows Management Instrumentation (WMI) en Remote Desktop Protocol (RDP). De binnendringers maken ook gebruik van normaal verkrijgbare open-sourcetools zoals Bloodhound. Als het Ryuk-virus ter

plekke is gebruikt het een AES-256, een sterke computerversleutelingstechniek om bestanden te versleutelen en een RSA(een asymmetrisch versleutelingsalgoritme) om de genoemde AES-sleutel ook nog te versleutelen. Ook zorgen de aanvallers via het virus ervoor dat een batch-file actief wordt die alle backup-bestanden en schaduwbestanden probeert te vernietigen. Dat doet men om te voorkomen dat het slachtoffer kan proberen de aanval te boven te komen door backups terug te zetten. Tot overmaat van ramp probeert men beveiligingssoftware af te sluiten of te de-installeren.

## Contact met aanvallers

Om contact met de aanvallers mogelijk te maken teneinde losgeldbetaling en ontsleuteling mogelijk te maken plaatsen de aanvaller een RyukReadMe-bestand op het aangedane systeem. Daarin staan dan één of twee email-adressen om met het end-to-end-versleutelde Protonmail-programma die contact met de aanvallers mogelijk maken. Eerdere versies van het virus zorgden direct voor een bericht met het benodigde losgeld-bedrag. Recente versies laten de slachtoffers alleen weten om welk bedrag het gaat als ze contact opnemen. Overigens maakt het virus tijdens de kwaadwillende activiteiten gebruik van een kwetsbaarheid in systemen die bekend staat als CVE-2020-1472, een kwetsbare Netlogon-procedure.

## Snel reageren noodzakelijk

Terwijl het bij cyberaanvallen nog weleens één of meerdere dagen duurt voor na binnendringen er onherroepelijke dingen gebeuren, ligt het voor de recente Ryuk-aanvallen anders. Na besmetting van een systeem kan in **vijf uur** na binnendringen het aangevallen systeem al volledig gecompromitteerd zijn. Een tijdslijn ziet u in deze publicatie op The DFIR Report van 18 oktober 2020. Adequaat handelen gedurende 24/7 uur is na het signaleren van ongewone activiteiten daarom een must. Backups buiten de bronsystemen bewaren is uiteraard een eerste

vereiste voor goed herstel.

## Github-lijst

Inmiddels is op het ontwikkelingsplatform GitHub een lijst beschikbaar met zogenaamde UNC1878-indicatoren. Dat zijn kenmerken die aan die hackersgroep te koppelen zijn, zoals gebruikte websites en beveiligingscertificaten. Het is in ieder geval iets om mee te starten. Op YouTube is sinds 28 oktober 2020 een ruim 58 minuten durende videopresentatie en discussie te vinden van de *SANS Computer Forensics Training Community over de Ryuk-malware*. Voor mij te hoog gegrepen maar voor kenners ongetwijfeld interessant.

## Nederland voortuin van de VS

Op cyber-gebied is Nederland in veel gevallen de voortuin, maar ook de proeftuin van de VS. We hebben hier een zeer goede internet-infrastructuur. Er staan veel grote datacentra, een zeer belangrijk knooppunt van het internet en we hebben een bevolking en bedrijfsleven waarin de digitale ontwikkelingen ver doorgedrongen zijn. Ziekenhuizen en andere zorginstellingen zijn verregaand geautomatiseerd. **Het is niet de vraag òf in Nederland een groep als UNC1878 met het Ryuk-malwarevirus een keer gaat toeslaan, maar wanneer.** Iedereen die in de zorg actief is dient alert te zijn van zorgmedewerkers die op phishing-email moeten letten tot cybersecurity-medewerkers. Een adequaat en alert update-beleid van software is van belang zodat kwetsbaarheden in software niet uitgebuit kunnen worden door aanvallers.