Pim's heilige uurtje

Datum:
15 februari 2022
Document nummer:
2022/002/DOC-CY

Inleiding

De specialisten hebben uitgelegd wat ze precies gezien hebben in de SIGINT hit en wat dat betekent voor het incident bij Electron B.V.. Vanwege de potentieel grote impact van dit incident heeft de AIVD een incident-response team naar Electron B.V. gestuurd. Dit team is teruggekomen met waardevolle informatie van de systemen in het Electron kantoornetwerk. Hopelijk zit er voldoende informatie in om een goed beeld te kunnen vormen van wat er exact gebeurd is.

Windows event logs worden in het Electron kantoornetwerk centraal verzameld op een WEC server. De logging is opgezet aan de hand van https://github.com/JSCU-NL/logging-essentials . Van deze server hebben we de eventlogs gekregen omstreeks het tijdstip van de initiële infectie. Electron B.V. SOC heeft ook full-pcap capture draaien met een retentietijd van 10 dagen. Daarvan hebben we een snapshot gekregen van het verkeer omstreeks het moment van infectie.

Challenge

Binaries

3 vlaggen

We hebben twee implant binaries[1] veilig weten te stellen bij Electron B.V.. Ze zaten op twee verschillende systemen en lijken variaties te zijn voor Windows en Linux.

Vragen:

- Hoe ziet het communicatieprotocol van de implant eruit?
- Welke crypto algorithmen worden gebruikt en welke sleutels en instellingen horen daarbij?

1 De tasks in de binaries zijn aangepast in situaties waar het gaat om code-execution of connecties. De code-execution functies zijn verwijderd en alle connecties en/of scans gaan altijd naar 127.0.0.1. De netwerkcommunicatie van de implant is volledig intact, maar communicatie vindt enkel plaats naar pannenkoekenpalazzo.local. Pannenkoekenpalazzo.nl reageert niet op de implants.

- Welke functionaliteiten biedt de implant voor de operator?
- Wat is de interne naam van de implant-suite?

Logs & PCAP

1 vlag

We willen graag weten:

- Hoe heeft ZUURKOOL zijn initial access verkregen?
- Op welk ander systeem, naast de initial access server, heeft ZUURKOOL toegang verkregen?
- Welke commando's heeft ZUURKOOL op welk systeem en op welk tijdstip uitgevoerd?
- Welke mogelijkheden had ZUURKOOL om credentials voor dat systeem te bemachtigen?

Vergeet in je write-up niet om aan te geven waar je welk stukje informatie vandaan hebt gehaald.