Rapport: Afschaling onderzoek ZUURKOOL

Datum:
4 februari 2021
Documentnummer:
2021/00362/DOC-CY

Inleiding

Begin juni 2018 is de [redacted] een onderzoek begonnen naar APT Cautious Raven (hierna: ZUURKOOL) nadat deze groep een incident heeft veroorzaakt in [redacted]. Contact met collega-dienst [redacted] heeft de dreiging duidelijk gemaakt, ook richting Nederland. In de periode 2018-2020 hebben er meerdere incidenten plaatsgevonden waar ZUURKOOL bij betrokken was.

Slachtofferprofiel

- Ministerie van Buitenlandse Zaken van [redacted] (2018), [redacted] (2020-2019) en [redacted] (2020);
- Ministerie van Defensie van [redacted] (2019);
- [redacted], Inc. (2018);
- [redacted] B.V. (2020);
- Ministerie [redacted] (2019).

Reden voor afschaling

Laatst waargenomen activiteit van actor ZUURKOOL vond plaats op 3 mei 2020 tijdens het incident bij [redacted] B.V.. Hierbij is de actor gedetecteerd 3 uur na het verkrijgen van een foothold binnen het netwerk. Vervolgens is het incident eenvoudig opgelost en de actor verwijderd van het netwerk. Actor deactiveerde vervolgens alle bekende infrastructuur. Een uitgebreid rapport over dit incident en de afhandeling is te vinden onder dossiernummer 2020/42004/DOS-CY. Hierna is er geen nieuwe infrastructuur meer gevonden, ook in OSINT rapportages is het stil over deze actor.

Geautomatiseerde detecties voor ZUURKOOL gerelateerde activiteit, gebaseerd op het huidige kennisniveau zullen actief blijven tot tenminste augustus 2022. Het onderzoek kan weer opgebouwd worden indien daar aanleiding toe ontstaat, bijv.: nieuwe slachtoffers binnen ons aandachtsgebied, OSINT rapportages over nieuwe relevante campagnes, etc.

Suricata

```
alert tcp any any -> any any (content: "GET"; content: "Mozilla/5.0
(Windows NT 10.0\; Win64\; x64\; rv:42.0) Gecko/20100101 Firefox/42.0";
content: "Cookies: PHPSESSID="; pcre: "/PHPSESSID=[a-z0-9]{32}/"; msg:
"[ZUURKOOL]: ROOKWORST backdoor implant: beacon"; sid:7328; rev:2;
reference:url,2020/00325/DOC-CY; classtype:trojan-activity;)
```

```
alert tcp any any -> any any (content: "POST"; content: "Mozilla/5.0
(Windows NT 10.0\; Win64\; x64\; rv:42.0) Gecko/20100101 Firefox/42.0";
content: "Content-Type: text/plain"; content: "Cookies: PHPSESSID="; pcre:
"/PHPSESSID=[a-z0-9]{32}/"; content: "data="; pcre: "/data=[A-Za-z0-9_\-\=]
+/" msg: "[ZUURKOOL]: ROOKWORST backdoor implant: results beacon";
sid:7329; rev:2; reference:url,2020/00325/DOC-CY; classtype:trojan-
activity;)
```