Samen aanjagen van vernieuwing

# Handreiking Identificeren Infecties

## Een zoektocht naar de bron van infectiemeldingen

Auteur(s): SURF, MBO Digitaal
Versie: 1.1
Datum: 4 februari 2025
Kenmerk: Handreiking Identificeren Infecties

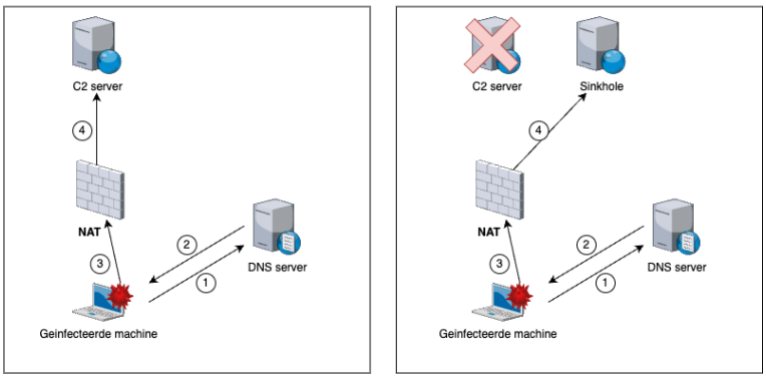
# Inhoudsopgave

# 1 Inleiding

Meldingen van mogelijke malware infecties of indicatoren van ander potentieel risicovol gedrag kunnen voortkomen uit verschillende bronnen. Deze handreiking richt zich specifiek op meldingen die zijn ontstaan vanuit de analyse van netwerkverkeer aan de rand van of buiten de instelling. Dit zowel actueel (near realtime) als historisch (achteraf terugzoeken), of op meldingen die voortkomen uit analyse van de data welke is gewonnen bij onderzoeken naar botnets, sinkholes en honeypots. Deze informatie komt via internationale handhaving vaak terecht bij providers en (nationale) CSIRTS, zoals SURFcert.

## 1.1 Uitdaging

Het grote nadeel van infectiemeldingen op basis van de bovengenoemde bronnen is dat voor de melder de bron van de infectie gelijkstaat aan een publiek IP-adres toebehorend aan de betrokken instelling. De uitdaging bij de behandeling van deze meldingen zit voornamelijk in het vinden van het daadwerkelijk geïnfecteerde systeem binnen het netwerk van de organisatie, dit verergerd in omgevingen waar veel gebruik gemaakt wordt van Bring-your-own-device (BYOD). Deze systemen zijn vaak vluchtiger in de logs omdat ze in en uit de instelling bewegen.




Deze handreiking bevat informatie over mogelijke bronnen die kunnen leiden tot het vinden van het daadwerkelijk geinfecteerde systeem, en hoe de informatie van deze bronnen geinterpreteerd kan worden. Er worden ook potentiele queries in SPL (Splunk) en KQL (Sentinel) gegeven die kunnen worden aangepast naar de omgeving van de instelling.

## 1.2 Benodigde informatie voor onderzoek

Een melding van buiten de organisatie moet tenminste aan één (bron IP), maar bij voorkeur meerdere van de volgende kenmerken bevatten  om onderzocht te kunnen worden:

- Tijdstip;
- Bron IP;
- Doel IP;
- Domein.

Bij het vermelden van een tijdstip is het belangrijk om rekening te houden met tijdzones en settings. Als de melder een andere tijdzone gebruikt of als verschillende logs binnen het netwerk uiteenlopende tijdinstellingen hanteren, moet hier zorgvuldig aandacht aan worden besteed!

# 2 Infecties opsporen

Voor het opsporen van het geïnfecteerde systeem kan gebruik gemaakt worden van verschillende bronnen/informatiesystemen binnen de instelling. Afhankelijk van hoe deze zijn geconfigureerd ten aanzien van data retentie en/of logging kan het zijn dat meerdere van deze bronnen ingezet kunnen worden om het systeem te identificeren. Op het moment dat de te doorzoeken informatie met een IP-adres terugkomt en niet een hostname, dan is het aan te raden om NAC/Switch logging te doorzoeken wat op het moment (tijdstip) van het event de bijbehorende hostname was en niet te vertrouwen op wat ten tijde van het onderzoek de hostname is.

## 2.1 Startpunt

De initiële melding bevat altijd een bron IP (ook wel source IP). Als een melding deze niet bevat was de melding nooit uitgekomen bij de instelling, omdat men dan niet had kunnen bepalen vanuit welk netwerk/organisatie de geïnfecteerde machine verbond.

Dit bron IP kan gebruikt worden als startpunt voor het onderzoek omdat het iets zegt over de publieke interface waar de infectie over communiceerde. Op basis van dit IP-adres kan de instelling meestal 2 dingen bepalen:

- Welk soort systemen communiceren over dit publiek IP-adres
- Welke maatregelen worden gebruikt (en door welke logging dus moet worden gezocht).

## 2.2 Firewall (en netwerksensoren)

Wanneer de firewall logs worden bewaard is dit een bron van data die (deels) kan helpen bij het opsporen van de geïnfecteerde machine. Firewall logging bevat (mits juist geconfigureerd) altijd de volgende informatie over het verkeer wat over de Firewall loopt:

- Bron IP en poort;
- Doel IP en poort;
- Protocol.

Recente Firewalls (ook wel NGFW's) bevatten vaak ook additionele functionaliteiten waar bijvoorbeeld proxy, ssl-inspectie, webfiltering, dns-logging en bevatten daardoor ook:

- Domeinen.

Hieronder volgen voorbeelden van queries voor SPL en KQL. De groene gedeelten moeten waarschijnlijk vervangen worden voor waarden die passen bij de instelling. Afhankelijk van de gebruikte firewall vendor kan het in enkele gevallen voorkomen dat ook de veldnamen anders zijn.

SPL:

```
index=firewall sourcetype=traffic
| search (dest_domain="*example.com*" OR dest_ip="203.0.113.5")
| stats count by src_ip dest_ip dest_domain dest_port protocol
```

KQL

```
FirewallData
| where DestinationDomain contains "example.com" or DestinationIP ==
"203.0.113.5"  // Zoeken op domein of IP-adres
| summarize count() by SourceIP, DestinationIP, DestinationDomain,
DestinationPort, Protocol
```

## 2.3 Domain Name System (DNS)

DNS kan ook worden ingezet als middel om de bron van een infectie op te sporen. Veel malware is namelijk sterk afhankelijk van DNS-verzoeken voor communicatie met command-and-control (C2)-servers en, in mindere mate, voor het exfiltreren van gegevens. DNS kan een waardevolle bron van informatie zijn wanneer de initiële melding een domein bevat. Omwille van performance is DNS vaak hiërarchisch uitgevoerd, het kan zijn dat DNS data uit verschillende bronnen komt.

SPL:

```
index=DNS sourcetype=requests
| search query="*example.com*"
| stats count by src_ip, client, query, _time
```

KQL

```
DnsEvents
| where QueryName contains "example.com"
| project TimeGenerated, SourceIP, Client, QueryName, QueryType,
ResponseCode, DnsResponse, DestinationIP
```

## 2.4 Endpoint Detection & Response (EDR)

EDR-systemen bevatten enorm veel telemetrie over systemen die onder controle staan van de instelling. Vaak bevatten ze geen informatie over systemen die door werknemers en/of studenten van de instellingen zelf onder beheer staan (BYOD).

De verscheidenheid van EDR-oplossingen is zeer groot en niet alle EDR-systemen sturen alle beschikbare telemetrie 1 op 1 door naar een centraal SIEM. Het kan zijn dat er gebruik gemaakt moet worden van een specifieke portal bedoelt voor de configuratie en/of het inzien van de logs van EDR. De verschillen tussen EDR-telemetrie kun je hier zien.

Omdat de combinatie MDE (Microsoft Defender for Endpoint) met Sentinel vaak voorkomt is hiervoor een voorbeeld query beschikbaar:

```
DeviceNetworkEvents
| where RemoteUrl contains "example.com" or RemoteIP == "203.0.113.5"
| project TimeGenerated, DeviceName, InitiatingProcessFileName,
RemoteUrl, RemoteIP, ActionType, ReportId, InitiatingProcessAccountName
```

## 2.5 Hostname of IP

Wanneer bij de analyse van de Firewall, netwerksensor of DNS server geen hostname maar een IP-adres wordt weergegeven als de bron van een systeem is het (zeker in een omgeving met veel vluchtige systemen) belangrijk om te controleren welke host hoorde bij dat IP op het moment van de infectie.

**DHCP**
DHCP (Dynamic Host Configuration Protocol) wijst dynamisch IP-adressen toe aan apparaten in een netwerk. Als je een geïnfecteerd systeem hebt ontdekt die afkomstig is van een specifiek IP-adres, kun je via de DHCP-logs achterhalen welk apparaat dat IP-adres op dat moment had. Kijk hierbij goed naar het timeframe waarin je zoekt om te zorgen dat je niet het verkeerde systeem associeert met het IP. Hieronder staat een voorbeeld van DHCP-logs in Splunk. Mocht er geen centraal systeem beschikbaar zijn om te doorzoeken, dan zijn de DHCP-logs meestal terug te vinden in het daarvoor aangewezen systeem. In veel gevallen is dit een Microsoft Server. DHCP logging hierbij is niet makkelijk doorzoekbaar en staat vaak niet aan en/of is snel overschreven door de grote hoeveelheid gegevens en de beperkte beschikbare opslagruimte.

SPL:
```
index=dhcp_logs sourcetype=dhcp
| search (assigned_ip="192.168.1.50")
| stats earliest(_time) as assignment_time, latest(_time) as
release_time, values(hostname) as device_hostname, values(mac_address)
as mac_address by assigned_ip
| eval duration=tostring(release_time - assignment_time, "duration")
| table assignment_time, release_time, duration, assigned_ip,
device_hostname, mac_address
| sort -assignment_time
```

**Alternatief**
Wanneer DHCP logging niet beschikbaar is, is het mogelijk om te kijken of er binnen een organisatie een bron aanwezig is die zowel het interne IP-adres van een host als de bijbehorende hostname vastlegt. Op deze manier kan de host vaak alsnog worden geïdentificeerd, of in elk geval kan het zoekgebied worden beperkt tot een aantal hosts.

## 2.6 Vinden van de user

Alle eerdergenoemde analysemogelijkheden zouden op dit moment, indien goed uitgevoerd, ten minste de volgende informatie moeten hebben opgeleverd.

- Bron IP;
- Hostname.

Hiermee is de vraag over de locatie van de infectie beantwoord. Vaak staat bij de firewall- of DNS-logging ook de gebruiker vermeld die wordt geassocieerd met het geïnfecteerde systeem, maar dit is niet altijd het geval. Vooral bij BYOD is het mogelijk dat een gebruiker nog niet geassocieerd wordt met het systeem dat is gevonden. In dergelijke gevallen is het gebruikelijk om authenticatielogging te doorzoeken. Dit kan betrekking hebben op authenticatie van veelgebruikte applicaties of (bij voorkeur) authenticaties via SSO (Single Sign-On).

Deze logging bevat naast het bron IP of de hostname ook de gebruikersnaam, en de gebruikersnaam kan, aan de hand van naamgevingsconventies, weer leiden naar de daadwerkelijke gebruiker en/of beheerder die aan een systeem is toegewezen.

Met de verkregen informatie (meestal met minstens twee van de drie onderstaande elementen) is het mogelijk om vervolgstappen te ondernemen:

- Bron IP;
- Hostname;
- Gebruiker.

Bij een geïnfecteerde host is het belangrijk om de juiste vervolgstappen te nemen. Deze stappen worden meestal beschreven in een Incident Response Plan. Het is aan te raden om specifiek voor (relatief) vaak voorkomende beveiligingsincidenten, zoals een virusinfectie, een standaard werkinstructie of playbook op te stellen, waarin de te nemen stappen worden beschreven. CERT Societe Generele heeft een aantal incident response plannen gepubliceerd voor verschillende soorten incidenten.[1]

**eduroam**

Het SSID eduroam wordt vaak gebruikt om smartphones/laptops en andere apparatuur via wifi te verbinden met het netwerk. Indien wordt vastgesteld dat het geïnfecteerde systeem via eduroam toegang kreeg tot het netwerk dan zal eerst moeten worden achterhaald of de gebruiker zich authenticeerde bij de eigen onderwijsinstelling of dat het gaat om een gastbezoeker. Hiervoor biedt de eduroam gebruikersnaam uitkomst. Die gebruikersnaam lijkt op een email adres (bijvoorbeeld naam@onderwijsinstelling.nl). De naam in dit voorbeeld hoeft niet te corresponderen met de naam van een persoon; het zou ook een studentnummer kunnen zijn (en ‘anoniem’ is vanuit privacy overwegingen ook toegestaan). De wifi beheeromgeving kan worden gebruikt om de eduroam gebruikersnaam te achterhalen. Indien de wifi beheeromgeving die mogelijkheid niet biedt dan is de RADIUS-server (op basis van het IP-adres of het MAC-adres en de DHCP-server in combinatie met het tijdstip waarop de infectie is gedetecteerd) een geschikte bron om de eduroam gebruikersnaam te achterhalen. Het identity en access management systeem (bijvoorbeeld LDAP, Azure AD/Entra) geeft vervolgens inzicht aan welke persoon de gebruikersnaam is toegekend.
Indien de realm in de eduroam gebruikersnaam (in het voorbeeld ‘onderwijsintelling.nl’) aangeeft dat het om een gastgebruiker gaat, zal die instelling moeten worden benaderd om de persoon te achterhalen. Hiervoor kan SURF of Kennisnet worden benaderd.

[1] https://github.com/certsocietegenerale/IRM/tree/main/EN

# 3 Verwijzingen

## 3.1 Relatie met SURF Security Baseline

Deze handreiking heeft raakvlak met de volgende elementen van de SURF Security Baseline:

SB.01.004 Asset inventory
SB.01.005 Asset registration
SB.01.006 Detection of assets
SB.04.001 Incident response procedure
SB.04.004 CSIRT
SB.07.002 Anti-Malware protection
SB.09.001 Authentication through organizational identity
SB.09.013 Digital identities
SB.10.001 Privilege account monitoring
SB.10.002 Account monitoring
SB.10.003 Session and Identity monitoring
SB.10.004 Logging events
SB.10.006 Mutation and Data access logs
SB.10.007 Access and authentication attempts
SB.10.008 Risk Monitoring
SB.10.009 Password Monitoring
SB.10.011 Network Intrusion Detection and Prevention Systems
SB.11.006 Firewall Rule Management

## 3.2 Relatie met SURFaudit toetsingskader

Deze handreiking heeft raakvlak met de volgende elementen van de SURFaudit toetsingskader:

Incident/probleembeheer
IM.01 Incidentmanagement
IM.02 Incident escalatie
IM.03 Incident response op (cyber) beveiligingsincidenten

Beveiligingsbeheer
SM.02 Authenticatiemechanismes
SM.03 Mobiele apparaten en telewerken
SM.04 Logging
SM.12 Beheersing van malware-aanvallen

## 3.3 SURF dienstverlening

Een aantal diensten van SURF kunnen bijdragen aan het detecteren en identificeren van infecties.

| Dienst | Relevantie | Contactpersoon |
|---|---|---|
| SURFsoc | Het monitoren op malafide gedrag in netwerken en systemen en het genereren van meldingen daarover. | SURFsoc@surf.nl |
| SURFcert | Het ontvangen van infectiemeldingen en ondersteuning bij het afhandelen daarvan. | cert@surfcert.nl |