Basis Orbital Zoekopdrachten voor Threat Analysis

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

toegang

Aangepaste zoekopdrachten

- 1. Opstartitems
- 2.SHA256 Hashes van lopende processen
- 3.Process met Netwerkverbindingen
- 4.Privileged proces met niet-localhost netwerkverbinding
- 5.Back-up/herstel registerbewaking
- 6. Bestand zoeken
- 7.Powershell geschiedenisbewaking
- 8.Prefetch-zoekopdracht
- 9.Address Resolution Protocol (ARP)-cachecontrole

Inleiding

Dit document beschrijft de basis orbitale zoekopdrachten voor dreigingsanalyse.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de interesse in het begrijpen van bedreigingen en malware en een basiskennis van Structured Query Language (SQL) -tabellen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Endpoint Connector versie 7.1.5 of hoger voor Windows
- Secure Endpoint Connector versie 1.16 of hoger voor Mac
- Secure Endpoint Connector versie 1.17 of hoger voor Linux
- Secure Endpoint-gebruiker moet de rol van beheerder toegewezen krijgen om Orbital te implementeren

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Custom Query's worden gebruikt om u te helpen snel de kracht van Orbital en osquery voor dreigingsjacht te leren.

Orbital maakt gebruik van osquerys stock tables naast Orbital-specifieke tabellen. De resultaten die via Orbital worden geretourneerd, kunnen naar andere toepassingen worden verzonden, zoals Secure Endpoint, Secure Malware Analytics en SecureX Threat Response, en kunnen worden opgeslagen in externe gegevensopslag (RDS), zoals Amazon S3, Microsoft Azure en Splunk.

Gebruik de Orbital Investigate-pagina om live, live query's op eindpunten te construeren en uit te voeren om meer informatie van hen te verzamelen. Orbital maakt gebruik van osquery, waarmee u uw apparaten kunt bevragen als een database met eenvoudige SQL-opdrachten.

Hier is een eenvoudig voorbeeld: SELECTEER kolom 1, kolom 2 UIT tabel 1, tabel 2 WAAR kolom 2='waarde'.

In dit voorbeeld zijn kolom 1 en kolom 2 de veldnamen van de tabel waaruit u gegevens wilt kiezen. Als u alle beschikbare velden in de tabel wilt kiezen, gebruikt u deze syntaxis: SELECTEREN * UIT tabel 1.

toegang

Open Orbital rechtstreeks op deze sites:

Noord-Amerika - https://orbital.amp.cisco.com

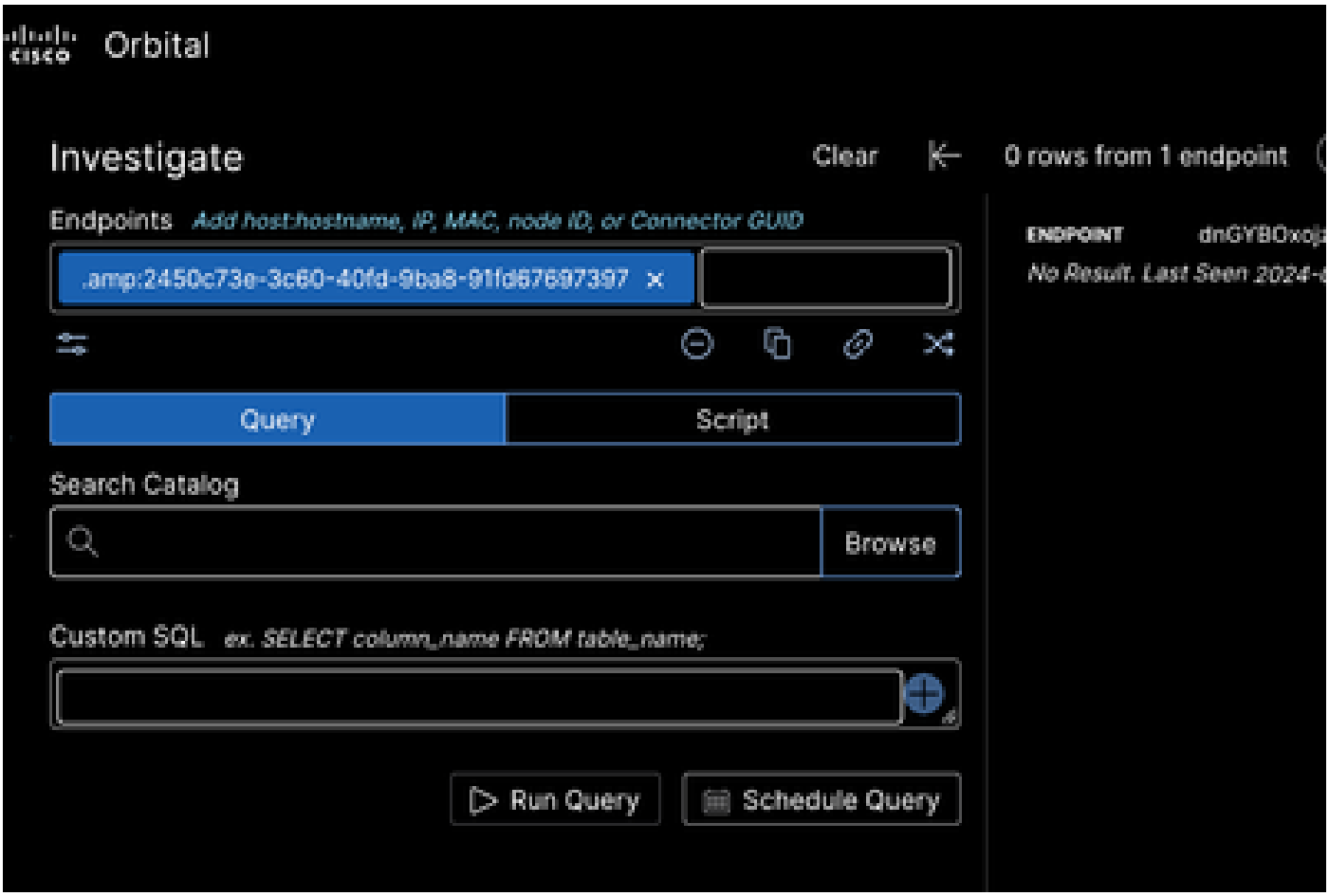
Europa - https://orbital.eu.amp.cisco.com

Azië en Stille Oceaan - https://orbital.apjc.amp.cisco.com

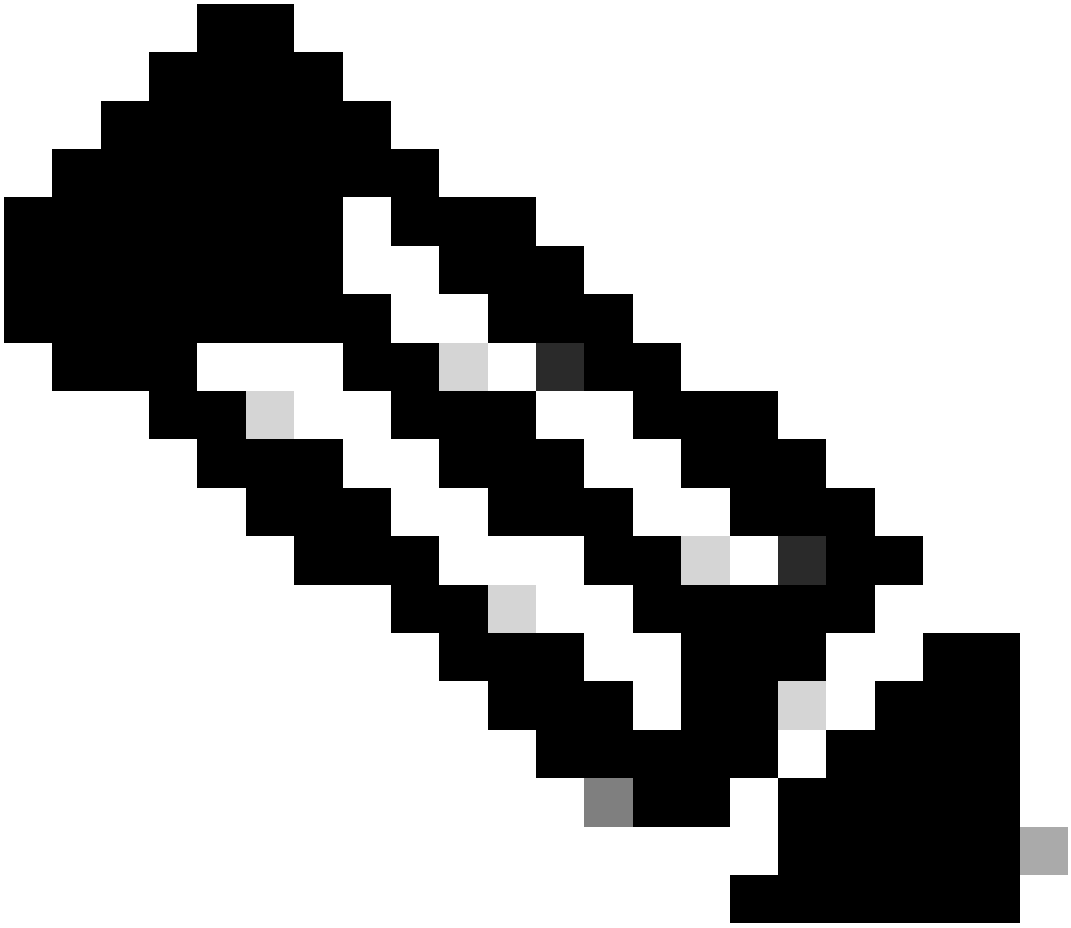
OF

Kies op de Secure Endpoint Console het getroffen hostsysteem en klik op Onderzoeken in Orbital.

Er zijn opties voor het gebruik van de Orbital Catalog (Klik op Bladeren) of Voer de Aangepaste query's in onder Aangepaste SQL-sectie zoals vermeld:



Aangepaste zoekopdrachten

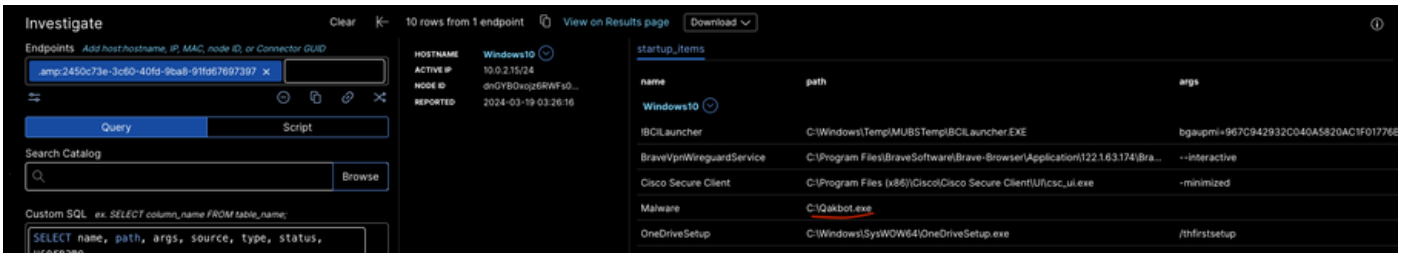


Opmerking: het hostsysteem bevindt zich in het labnetwerk en er wordt geprobeerd het systeem/netwerk ongedeerd te houden.

1. Opstartitems

Startup items kunnen worden uitgebuit door aanvallers om de persistentie op een gecompromitteerd systeem te behouden, wat betekent dat de schadelijke software zal blijven draaien of automatisch opnieuw worden gestart bij elke systeemherstart. In het volgende voorbeeld wordt Qakbot.exe uitgevoerd in het hostsysteem.

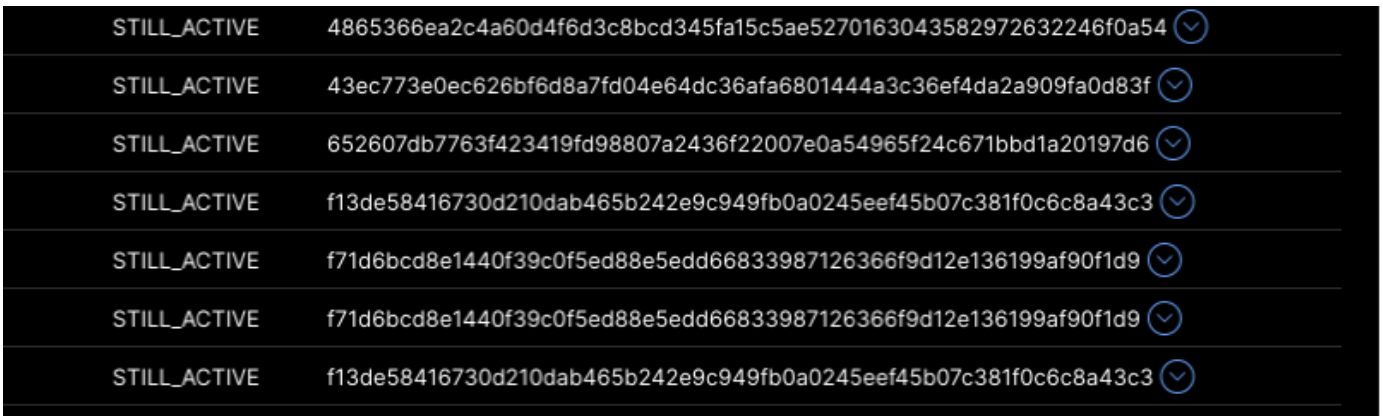
```
SELECT name, path, args, source, type, status, username
FROM startup_items;
```



2. SHA256 Hashes van lopende processen

SHA256-hashes zijn niet inherent geassocieerd met het uitvoeren van processen in hun natuurlijke staat. Beveiligingssoftware en systeembewakingstools kunnen echter de SHA256-hash van een lopend proces van het uitvoerbare bestand berekenen om de integriteit en authenticiteit ervan te helpen verifiëren.

```
 SELECT
p.pid, p.name, p.path, p.cmdline, p.state, h.sha256
FROM processes p
INNER JOIN hash h
ON p.path=h.path;
```

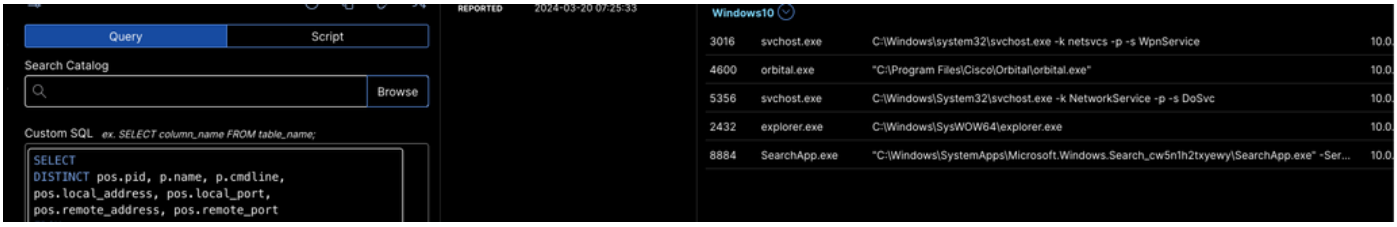


als de bijbehorende hash van een bestand kwaadaardig is, kunt u zich identificeren met deze zoekopdracht.

3. Proces met netwerkverbindingen

Processen met netwerkverbindingen zijn programma's of systeemdiensten die actief gebruik maken van de netwerkinterface om te communiceren met andere apparaten op een netwerk of via internet.

```
SELECT
DISTINCT pos.pid, p.name, p.cmdline, pos.local_address, pos.local_port, pos.remote_address, pos.remote_
FROM processes p
JOIN process_open_sockets pos USING (pid)
WHERE
pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1", “0");
```



4. Bevoorrecht proces met netwerkverbinding van een niet-localhost

Een programma of service uitvoeren met verhoogde machtigingen (zoals die van een beheerder of systeemaccount) en via het netwerk communiceren met een extern apparaat of service, wat betekent dat een ander IP-adres dan 127.0.0.1 (localhost) of::1 (IPv6 localhost).

```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1")
```

Zodra u de Packet Identifier (PID) lijst hebt, kunt u deze dienovereenkomstig toevoegen in de Aangepaste query's.

```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1") and p.uid=1436
```

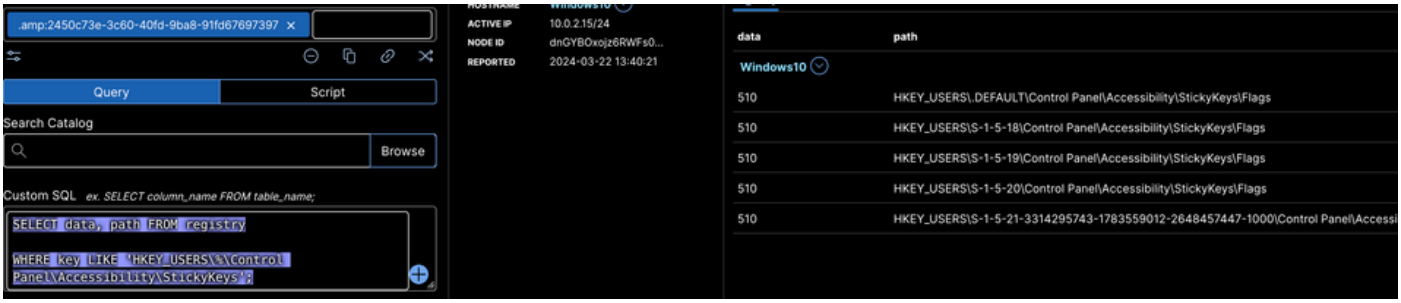
5. Controle van back-up-/herstelregister

Volgen van gebeurtenissen waarbij wijzigingen in het Windows-register worden aangebracht door middel van back-up- of terugzetbewerkingen. Het Windows-register is een hiërarchische database waarin configuratie-instellingen en opties voor Microsoft Windows-besturingssystemen worden

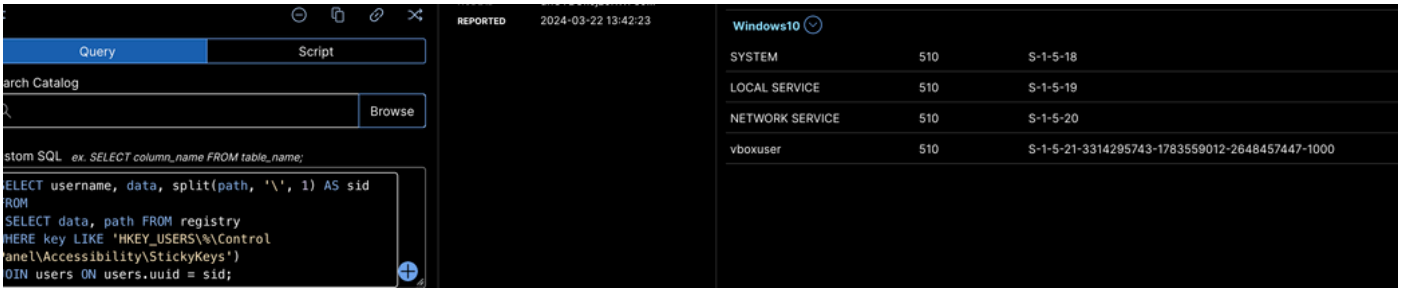
opgeslagen.

```
SELECT key AS reg_key, path, name, data, DATETIME(mtime, "unixepoch") as last_modified
FROM registry
WHERE key LIKE "HKEY_LOCAL_MACHINE\system\currentcontrolset\control\backuprestore\filesnottosnapshot";
```

```
SELECT data, path FROM registry
WHERE key LIKE 'HKEY_USERS\%\Control Panel\Accessibility\StickyKeys';
```




```
SELECT username, data, split(path, '\', 1) AS sid
FROM
(SELECT data, path FROM registry
WHERE key LIKE 'HKEY_USERS\%\Control Panel\Accessibility\StickyKeys')
JOIN users ON users.uuid = sid;
```



6. Bestand zoeken

Hiermee kunnen gebruikers bestanden en mappen op hun computer vinden met behulp van verschillende criteria, zoals bestandsnaam, inhoud, eigenschappen of metagegevens.

```
SELECT
f.directory, f.filename, f.uid, f.gid,
f.mode, f.device, f.size,
f.atime,
f.mtime,
```

```
f.ctime,
f.btime,
f.hard_links, f.symlink, f.file_id, h.sha256
FROM file f
LEFT JOIN hash h on f.path=h.path
WHERE
f.path LIKE (SELECT v from __vars WHERE n="file_path") AND
f.path NOT LIKE (SELECT v from __vars WHERE n="not_file_path");
```

Navigeer naar PARAMETERS > Bestandspad en klik op %.dll of %.exe of %.png.

7. Monitoring van de PowerShell-geschiedenis

Praktijk van het bijhouden van de opdrachten die zijn uitgevoerd in PowerShell-sessies. Het bewaken van de geschiedenis van PowerShell kan bijzonder belangrijk zijn om veiligheids- en nalevingsredenen.

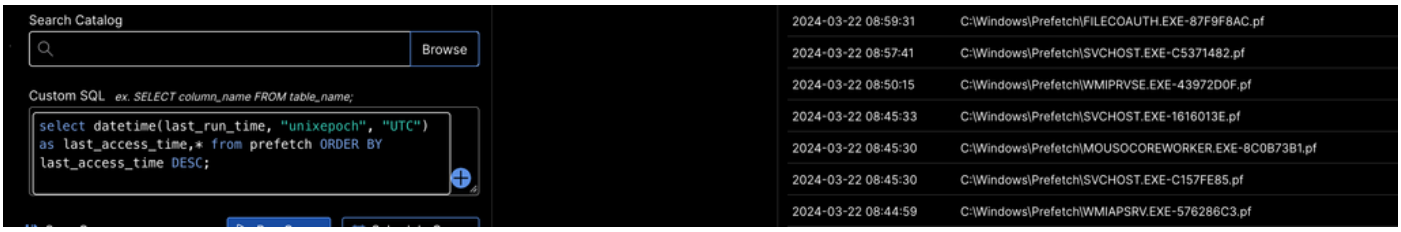
```
SELECT time, datetime, script_block_id, script_block_count, script_text, script_name, script_path
FROM orbital_powershell_events
ORDER BY datetime DESC
LIMIT 500;
```

8. Prefetch-zoekopdracht

Prestatiefunctie die het laden van toepassingen versnelt. Prefetching omvat het analyseren van de manier waarop software wordt geladen en uitgevoerd op een systeem en het opslaan van informatie hierover in specifieke bestanden.

```
select datetime(last_run_time, "unixepoch", "UTC") as last_access_time,*
from prefetch
```

```
ORDER BY last_access_time DESC;
```

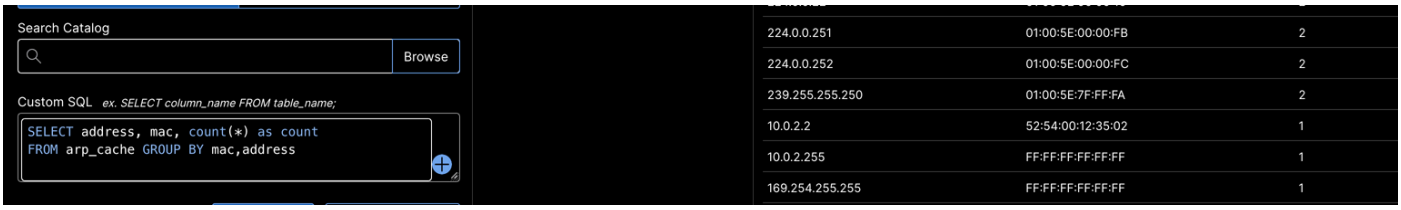


Prefetch is een mechanisme waarmee SQL Server veel I/O-verzoeken parallel kan starten voor een Nested Loop-join.

9. Inspectie van de cache van het Address Resolution Protocol (ARP)

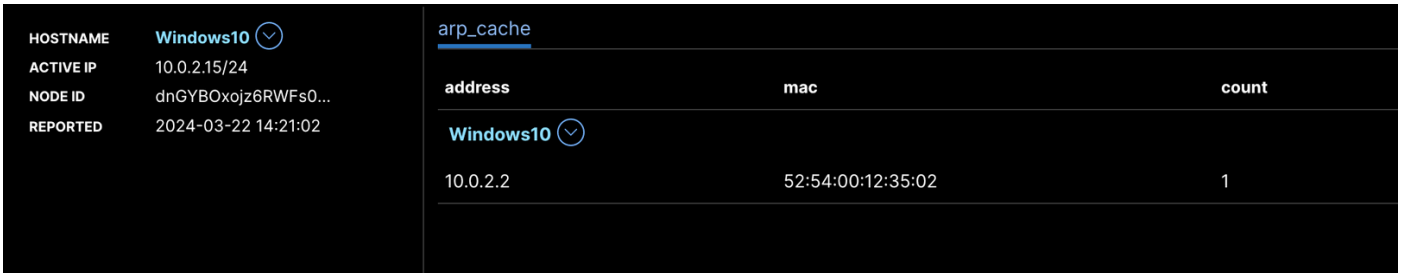
Hierbij wordt de inhoud van de ARP-cache op een computer of netwerkapparaat onderzocht. De ARP-cache is een tabel waarin toewijzingen tussen IP-adressen en de bijbehorende MAC-adressen worden opgeslagen.

```
SELECT address, mac, count(*) as count
FROM arp_cache GROUP BY mac,address;
```



In het volgende voorbeeld wordt het verdachte MAC-adres en het aantal ervan berekend vanuit de ARP-cache.

```
SELECT address, mac, count(*) as count
FROM arp_cache GROUP BY mac,address
HAVING COUNT(mac) >= (SELECT count FROM arp_cache WHERE count>=1)
AND mac LIKE (SELECT mac FROM arp_cache WHERE mac="52:54:00:12:35:02");
```



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.