用于威胁分析的基本轨道搜索查询

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

接入

自定义查询

- 1.启动项目
- 2.Sha256正在运行的进程的散列
- 3.网络连接过程
- 4.非本地主机网络连接的特权进程
- 5.备份/恢复注册表监控
- 6.文件搜索
- 7.Powershell历史记录监控
- 8.预取查询
- 9.地址解析协议(ARP)缓存检测

简介

本文档介绍用于威胁分析的基本轨道搜索查询。

先决条件

要求

思科建议您了解对威胁和恶意软件的了解以及结构化查询语言(SQL)表的基本了解。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 用于Windows的安全终端连接器7.1.5版或更高版本
- 适用于Mac的安全终端连接器1.16版或更高版本
- Secure Endpoint Connector 1.17或更高版本，适用于Linux
- 安全终端用户必须分配管理员角色才能部署Orbital

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

利用自定义查询，必须帮助您快速了解轨道和蠕虫在威胁搜索方面的强大功能。

Orbital除了使用Orbital特定表外，还使用osquerys库存表。通过Orbital返回的结果可以发送到其他应用，如安全终端、安全恶意软件分析和SecureX威胁响应，并且可以存储在远程数据存储(RDS)中，如Amazon S3、Microsofts Azure和Splunk。

使用Orbital Investigate页可以在终端上构建和执行实时查询，以便从终端收集更多信息。Orbital使用osquery，它允许使用基本的SQL命令像数据库一样查询设备。

下面是一个简单的示例：SELECT column1, column2 FROM table1, table2 WHERE column2='value'。

在本示例中，column1和column2是要从中选择数据的表的字段名称。要选择表中的所有可用字段，请使用以下语法：从TABLE1中选择*。

接入

Open Orbital直接位于以下站点：

北美 — https://orbital.amp.cisco.com

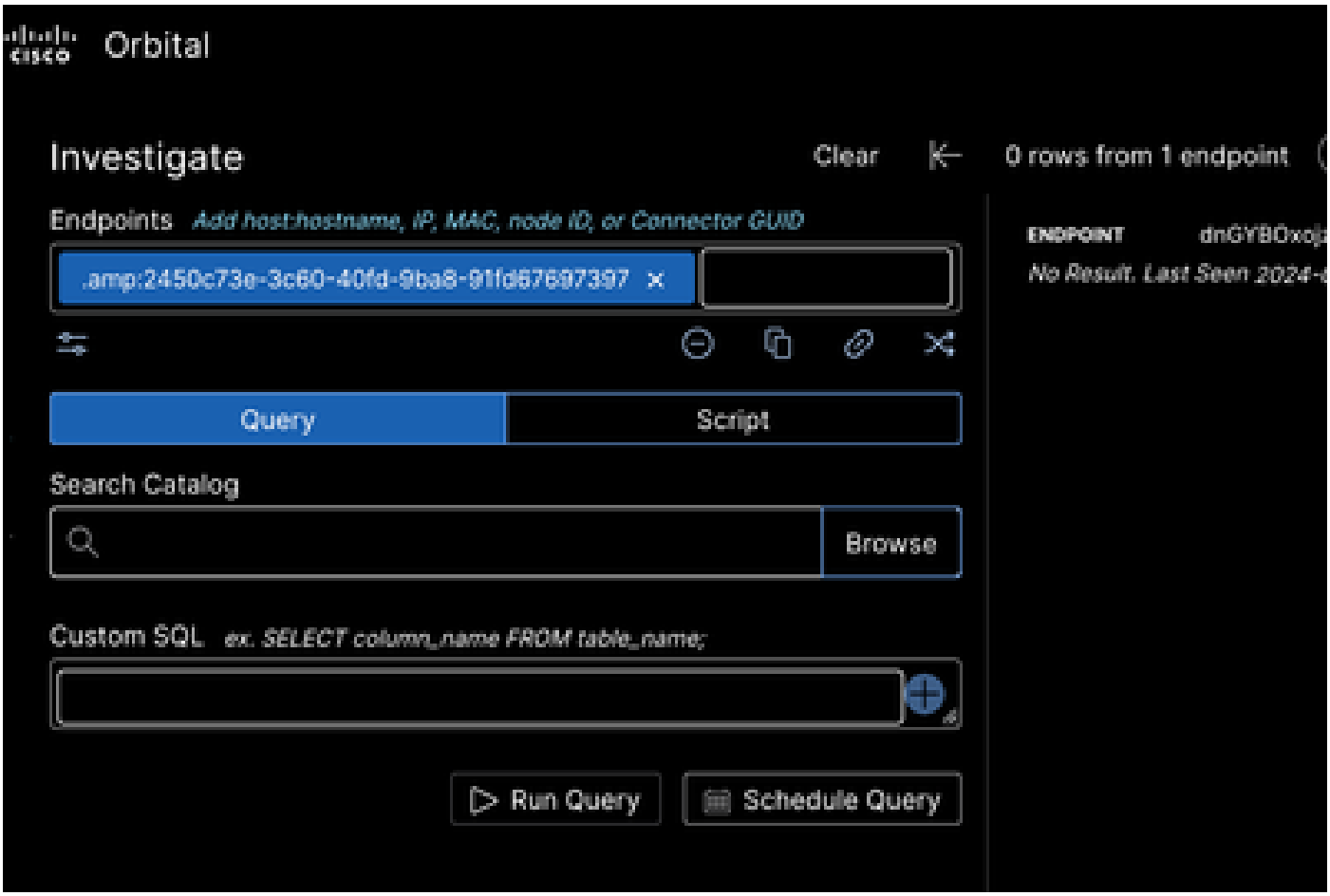
欧洲 — https://orbital.eu.amp.cisco.com

亚太地区 — https://orbital.apjc.amp.cisco.com

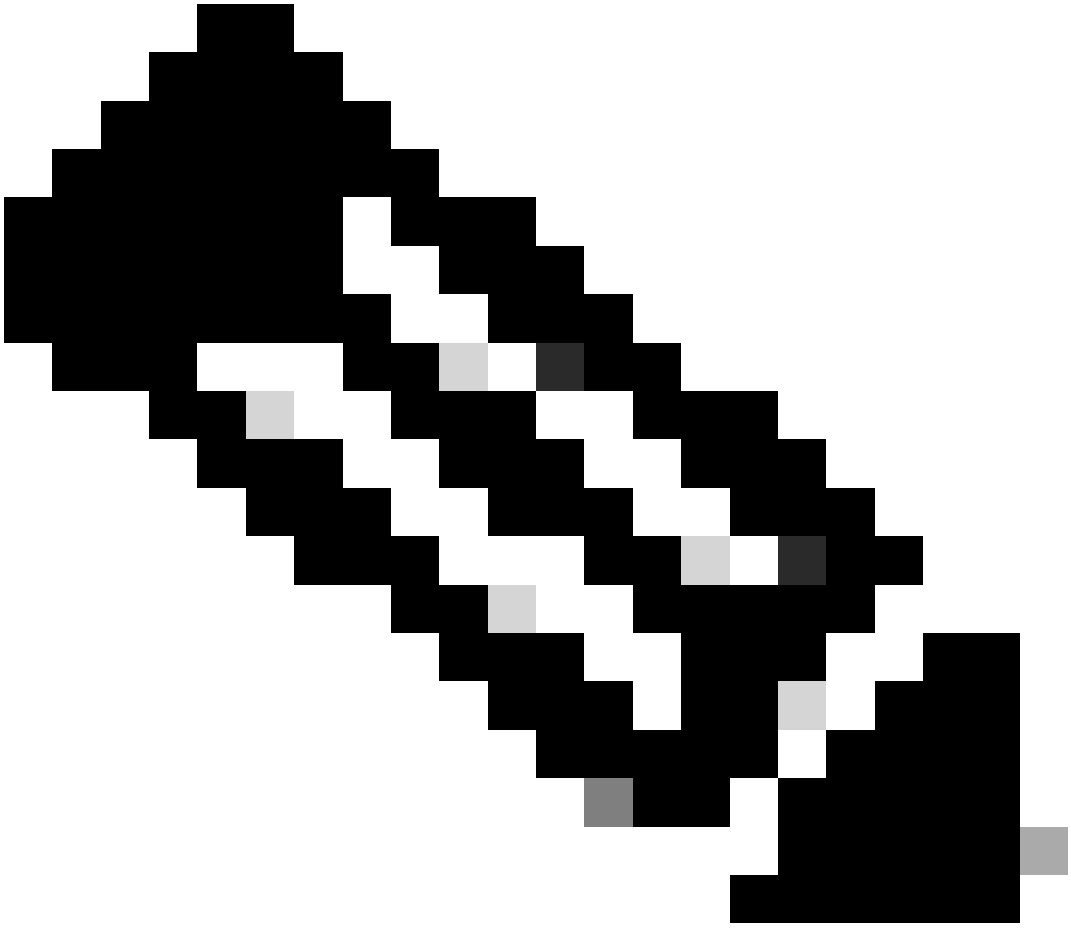
或者

在Secure Endpoint Console上，选择受影响的主机系统，然后点击Investigate in Orbital。

可以使用轨道目录(点击浏览)或Custom SQL部分下的Enter the Custom Queries，如前所述：


Orbital
Investigate
Clear
0 rows from 1 endpoint
Endpoints
Add host:hostname, IP, MAC, node ID, or Connector GUID
.amp:2450c73e-3c60-40fd-9ba8-911d67697397
ENDPOINT
No Result. Last Seen 2024-
Query
Script
Search Catalog
Browse
Custom SQL
ex. SELECT column_name FROM table_name;
Run Query
Schedule Query

自定义查询

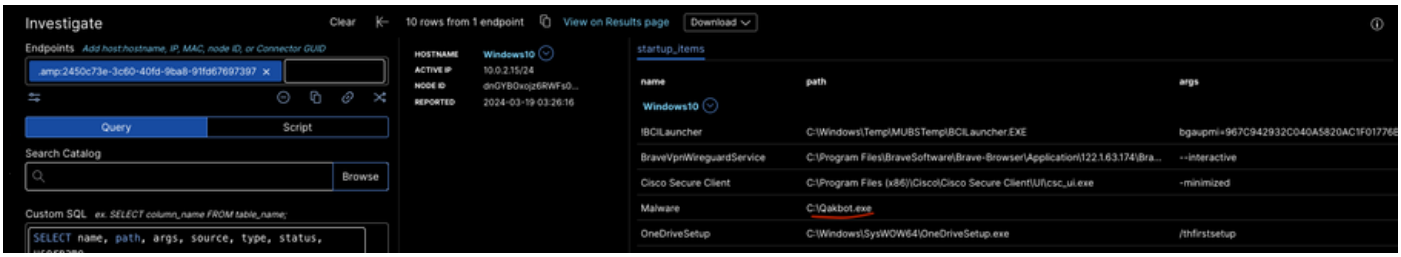


注意：主机系统位于实验网络中，它尝试保持系统/网络不受损害。

1.启动项目

攻击者可以利用启动项目在受感染的系统上保持持久性，这意味着恶意软件将继续运行，或者在每次系统重新启动后自动重新启动。在下一个示例中，Qakbot.exe正在主机系统中运行。

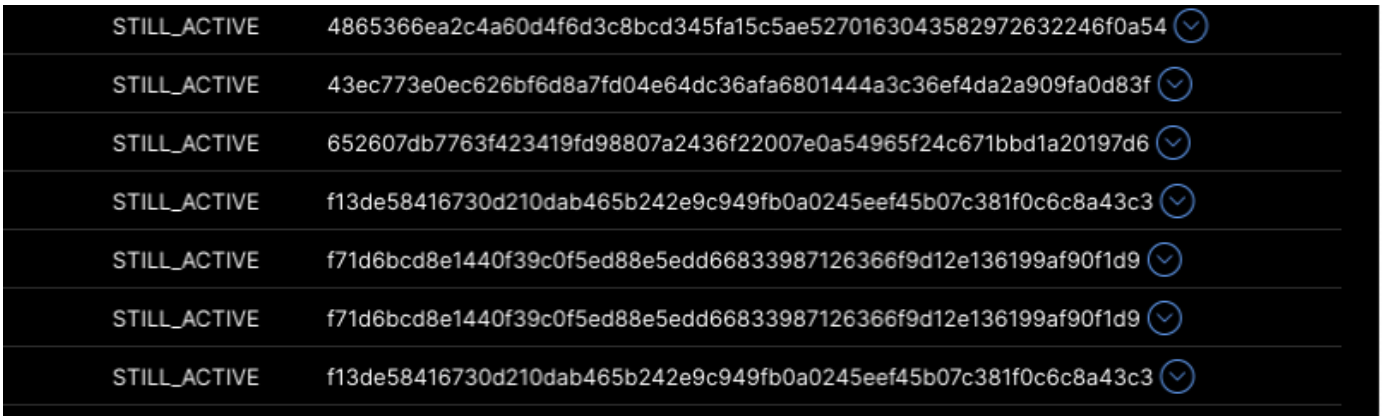
```
SELECT name, path, args, source, type, status, username
FROM startup_items;
```



2. Sha256正在运行的进程的散列

SHA256散列不会与其自然状态下运行的进程内在关联。但是，安全软件和系统监控工具可以计算可执行文件的运行进程的SHA256哈希值，以帮助验证其完整性和真实性。

```
 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;
```



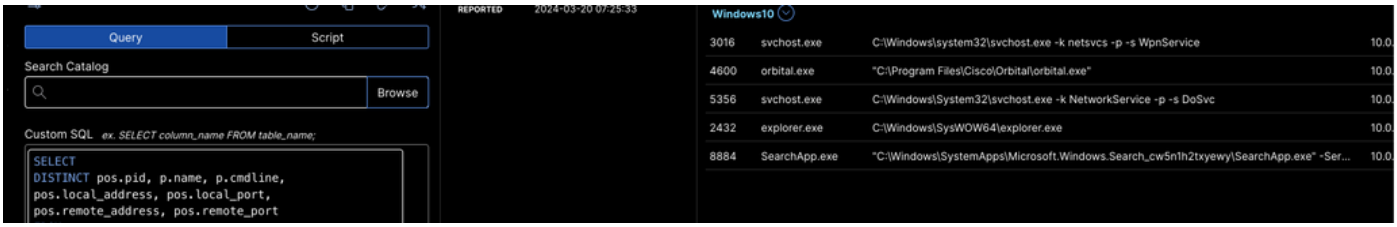
如果文件的关联散列值是恶意的，您将能够使用此查询进行识别。

3.网络连接过程

带有网络连接的进程是主动使用网络接口以便与网络上的其他设备通信或通过Internet通信的程序或系统服务。

```
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.非本地主机网络连接的特权过程

运行具有提升权限（如管理员或系统帐户的权限）的程序或服务，并通过网络与外部设备或服务进行通信，这意味着除127.0.0.1(localhost)或：:1(IPv6 localhost)以外的任何IP地址。

```
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")
```

一旦您拥有数据包标识符(PID)列表，您就可以相应地将其添加到自定义查询中。

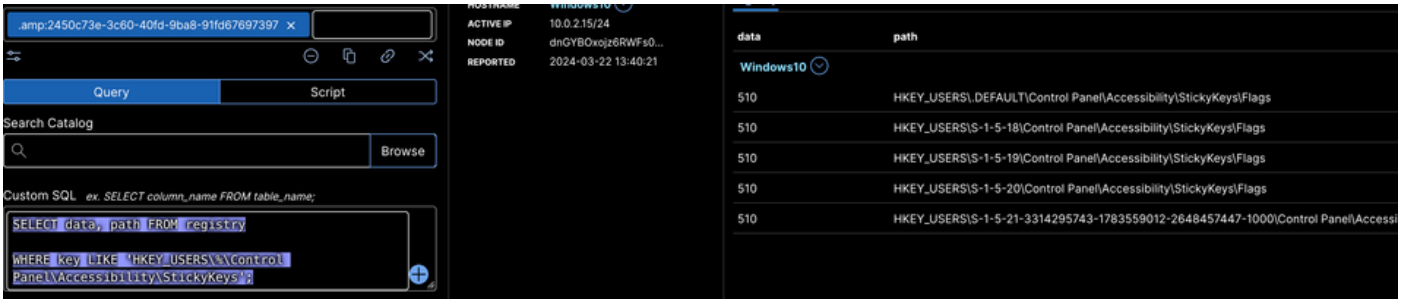
```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1") and p.uid=1436
```

5.备份/恢复注册表监控

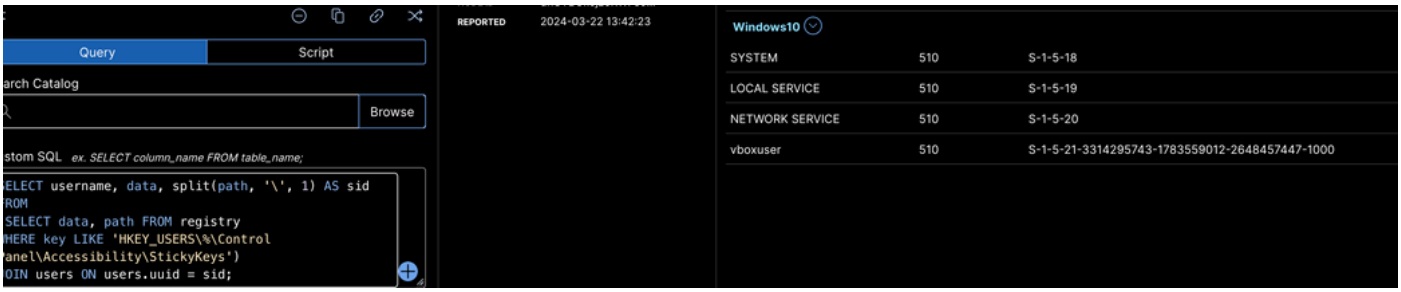
跟踪通过备份或还原操作对Windows注册表进行更改的事件。Windows注册表是在Microsoft Windows操作系统上存储配置设置和选项的分层数据库。

```
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.文件搜索

允许用户使用各种条件（如文件名、内容、属性或元数据）在其计算机上查找文件和文件夹。

```
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");
```

导航到PARAMETERS > File Path，然后单击%。dll、%。exe或%。png。

7. Powershell历史监控

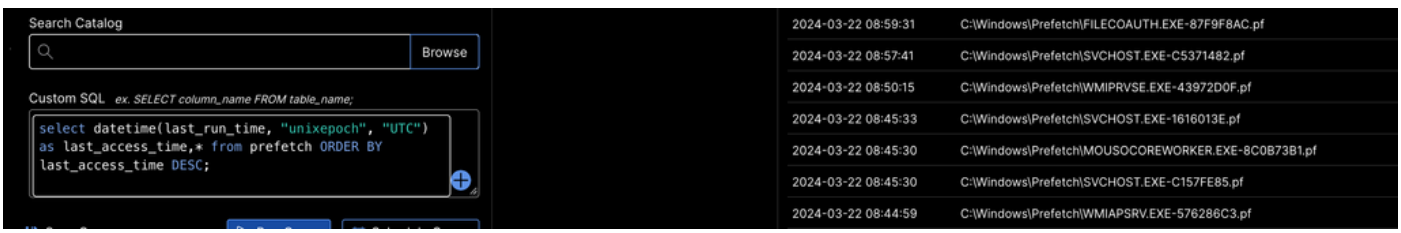
跟踪已在PowerShell会话中执行的命令的做法。出于安全和合规性的原因，监视PowerShell历史记录可能尤为重要。

```
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.预取查询

一种性能功能，可加速应用程序的加载。预取包括分析软件在系统上加载和运行的方式，然后将相关信息存储在特定文件中。

```
select datetime(last_run_time, "unixepoch", "UTC") as last_access_time,*
from prefetch
ORDER BY last_access_time DESC;
```

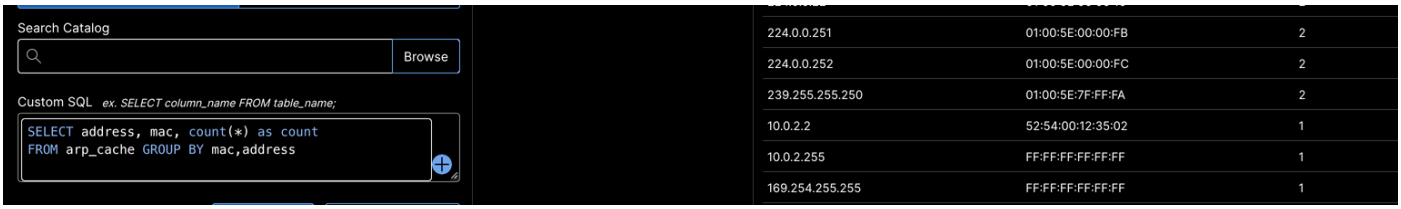


预取是一种机制，SQL Server可通过该机制为嵌套循环连接并行启动多个I/O请求。

9.地址解析协议(ARP)缓存检测

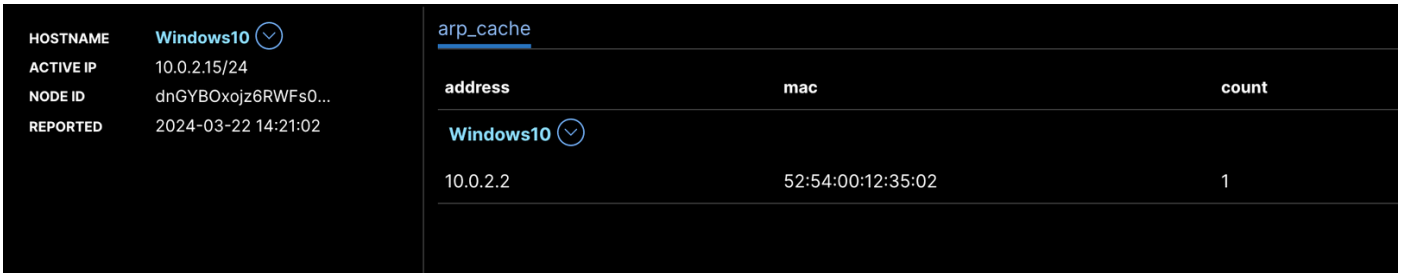
涉及检查计算机或网络设备上的ARP缓存的内容。ARP缓存是一个表，用于存储IP地址与其相应MAC地址之间的映射。

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



下一个示例从ARP缓存中找出可疑MAC地址及其计数。

```
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");
```



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。