用於威脅分析的基本軌道搜尋查詢

目錄

簡介

本檔案介紹用於威脅分析的基本軌道搜尋查詢。

必要條件

需求

思科建議您瞭解對威脅和惡意軟體的瞭解以及結構化查詢語言(SQL)表的基本瞭解。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於Windows的安全終端聯結器7.1.5版或更高版本
- 適用於Mac的安全終端聯結器版本1.16或更高版本
- 適用於Linux的安全終端聯結器版本1.17或更高版本
- 安全終端使用者必須分配管理員角色才能部署Orbital

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

利用自定義查詢，必須幫助您快速瞭解軌道和衛星在威脅搜尋方面的強大功能。

Orbital除了使用Orbital特定的表格外，還使用osquerys庫存表。通過Orbital返回的結果可以傳送到其他應用程式，如安全終端、安全惡意軟體分析和SecureX威脅響應，並且可以儲存在遠端資料儲存(RDS)中，如Amazon S3、Microsofts Azure和Splunk。

使用Orbital Investigate頁可以在終端上構建和執行即時查詢，以便從終端收集更多資訊。Orbital使用osquery，它允許您使用基本的SQL命令像查詢資料庫一樣查詢裝置。

以下是簡單的範例：SELECT column1, column2 FROM table1, table2 WHERE column2='value'。

在此示例中，column1和column2是要從中選擇資料的表的欄位名稱。若要選擇表中所有可用的欄位，請使用以下語法：從表1中選擇*。

存取

直接在這些地點開放軌道：

北美 — https://orbital.amp.cisco.com

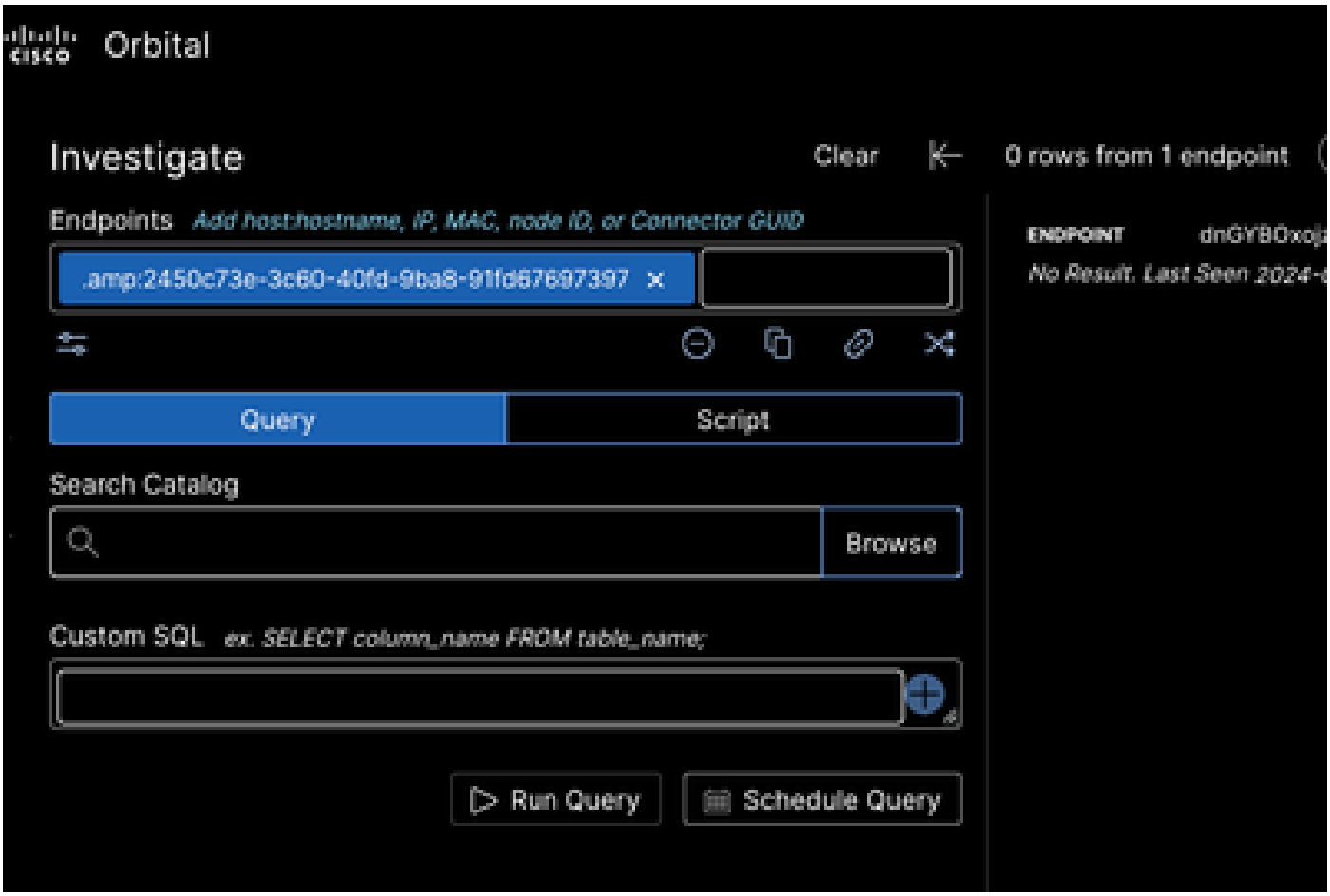
歐洲 — https://orbital.eu.amp.cisco.com

亞太地區 — https://orbital.apjc.amp.cisco.com

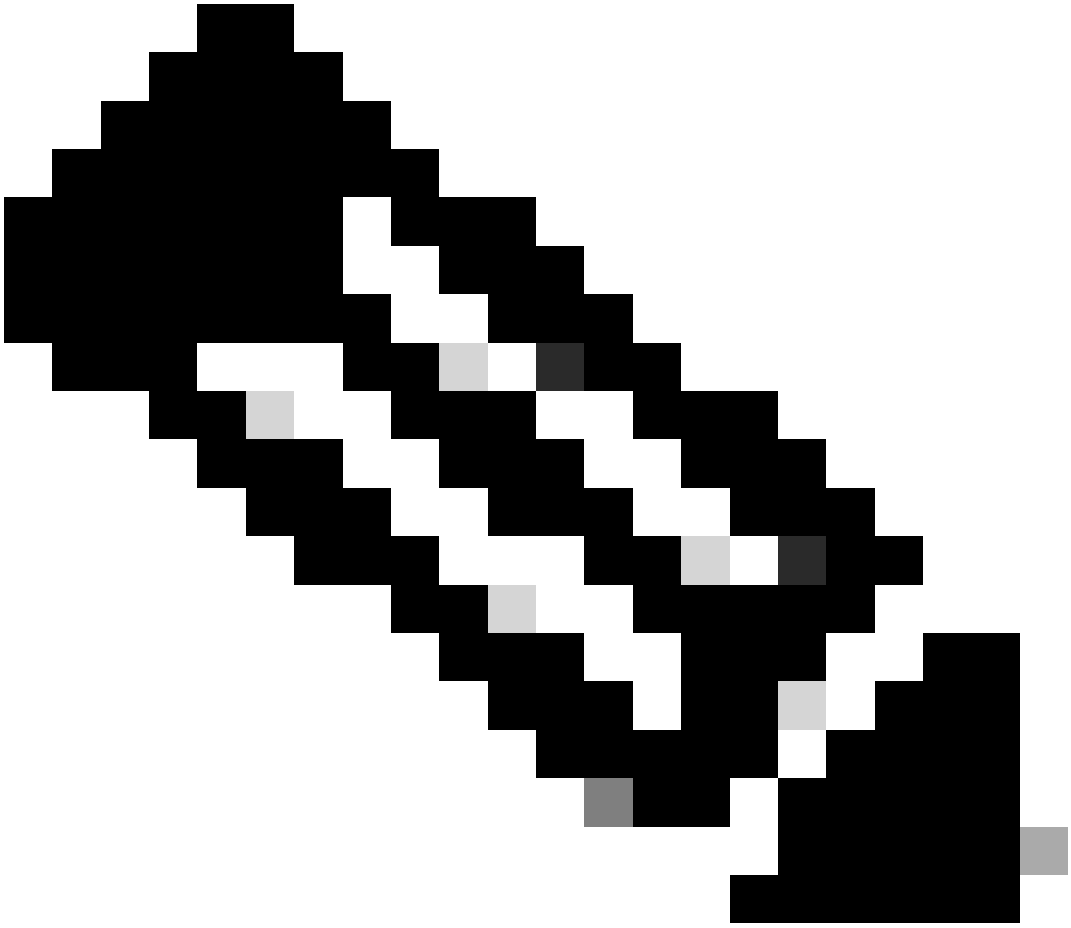
或

在安全終端控制檯上，選擇受影響的主機系統，然後點選在軌道中調查。

可以使用軌道目錄(按一下瀏覽)或Enter the Custom Queries under Custom SQL部分的選項，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

自定義查詢

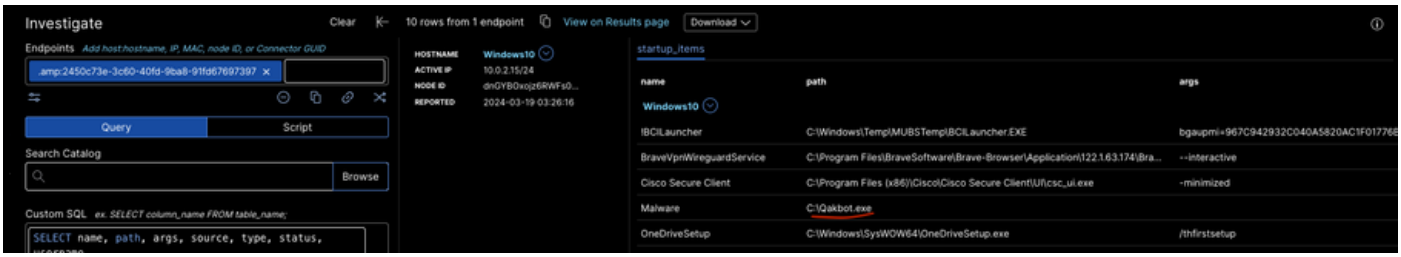


附註：主機系統位於實驗網路中，它嘗試保持系統/網路不受損害。

1.啟動專案

攻擊者可以利用啟動專案在被入侵的系統上保持永續性，這意味著惡意軟體將在每次系統重新啟動後繼續運行或重新自動啟動。在下一個示例中，Qakbot.exe正在主機系統中運行。

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



2. Sha256正在運行的進程的雜湊

SHA256雜湊不會與其自然狀態下運行的進程內在關聯。但是，安全軟體和系統監控工具可以計算執行檔的運行進程的SHA256雜湊，以幫助驗證其完整性和真實性。

```
 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;
```

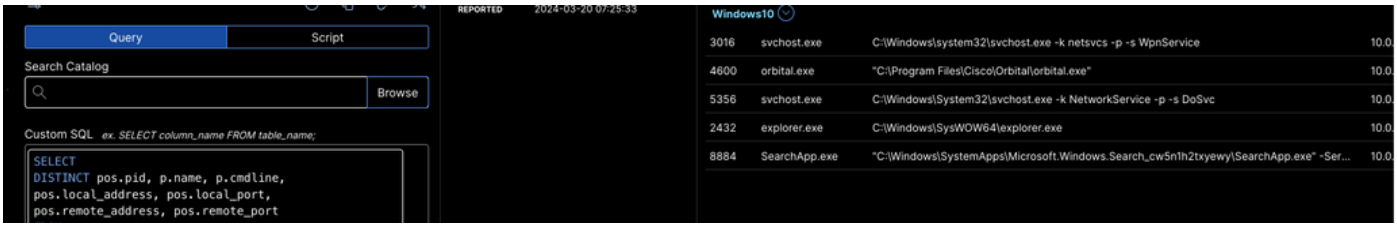
如果檔案的關聯雜湊值是惡意的，您將能夠識別此查詢。

3.使用網路連線的流程

網路連線進程是主動使用網路介面以便與網路上的其他裝置通訊或通過Internet通訊的程式或系統服務。

```
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.具有非本地主機網路連線的特權進程

正在運行具有提升許可權的程式或服務（如管理員或系統帳戶的許可權），並且正在通過網路與外部裝置或服務進行通訊，這意味著除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")
```

一旦您擁有資料包識別符號(PID)清單，您就可以相應地將其新增到自定義查詢中。

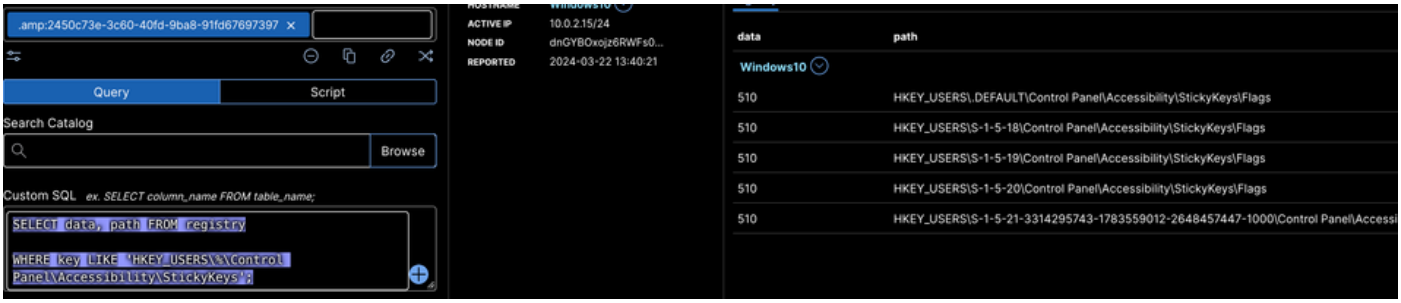
```
SELECT DISTINCT p.name, p.cmdline, pos.pid, pos.local_address, pos.local_port, pos.remote_address, pos.
FROM processes p JOIN process_open_sockets pos USING (pid)
WHERE pos.remote_address NOT IN ("", "0.0.0.0", "127.0.0.1", "::", "::1") and p.uid=1436
```

5.備份/恢復登錄檔監視

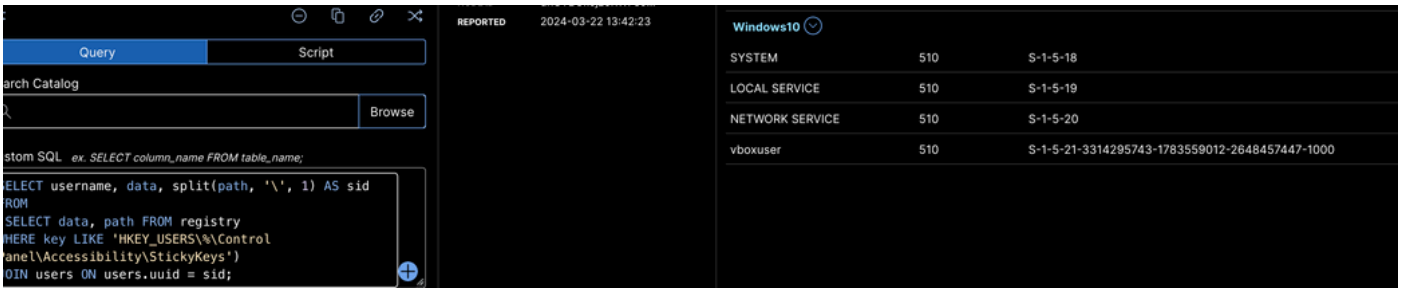
跟蹤通過備份或還原操作對Windows登錄檔進行更改的事件。Windows登錄檔是在Microsoft Windows作業系統上儲存配置設定和選項的分層資料庫。

```
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.檔案搜尋

允許使用者使用各種條件（如檔名、內容、屬性或後設資料）來查詢其電腦上的檔案和資料夾。

```
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");
```

導航到PARAMETERS > File Path，然後按一下%。dll、%。exe或%。png。

7. Powershell歷史監控

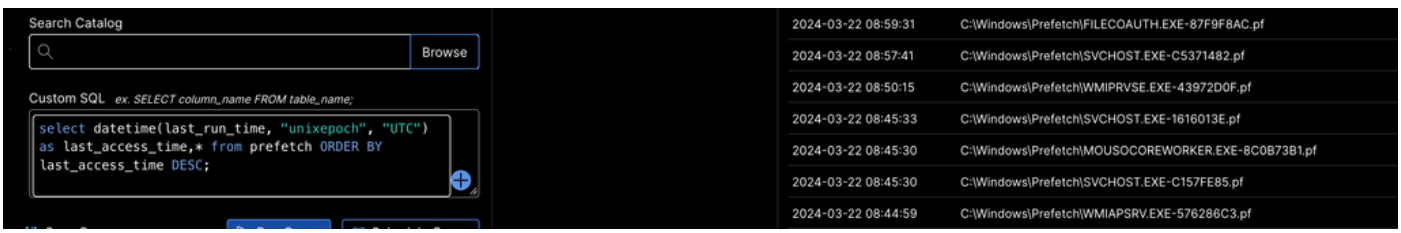
跟蹤已在PowerShell會話中執行的命令的做法。出於安全和合規性的原因，監視PowerShell歷史記錄可能特別重要。

```
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.預取查詢

加速應用程式載入的效能功能。預取過程包括分析軟體在系統上載入和運行的方式，然後將相關的資訊儲存在特定檔案中。

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

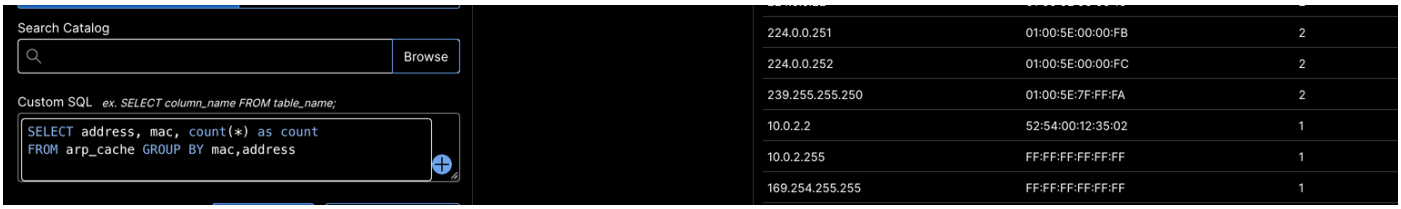


預取是一種機制，SQL Server可通過該機製為巢狀循環連線並行啟動多個I/O請求。

9.位址解析通訊協定(ARP)快取檢查

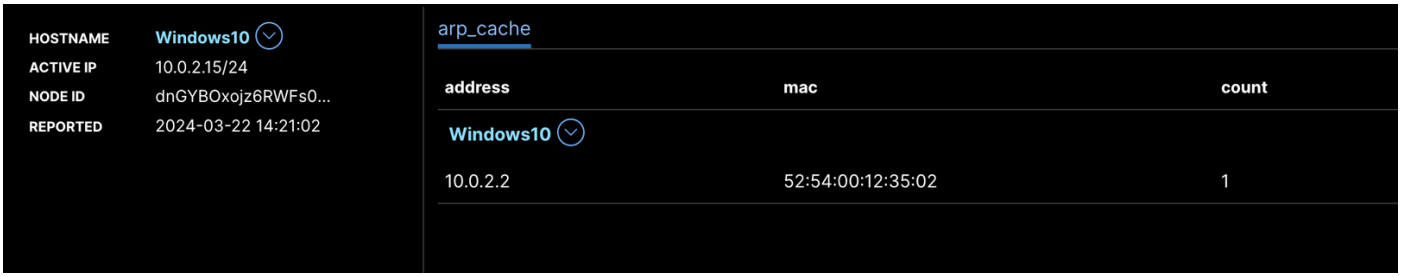
涉及檢查電腦或網路裝置上的ARP快取內容。ARP快取是一個表，用於儲存IP地址與其對應的MAC地址之間的對映。

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



下一個示例從ARP快取中找出可疑MAC地址及其計數。

```
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");
```



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。