Case Study:

Perform a Query with Chronicle

Skills Acquired:

By using Chronicle's domain search to investigate a suspicious domain, I was able to:

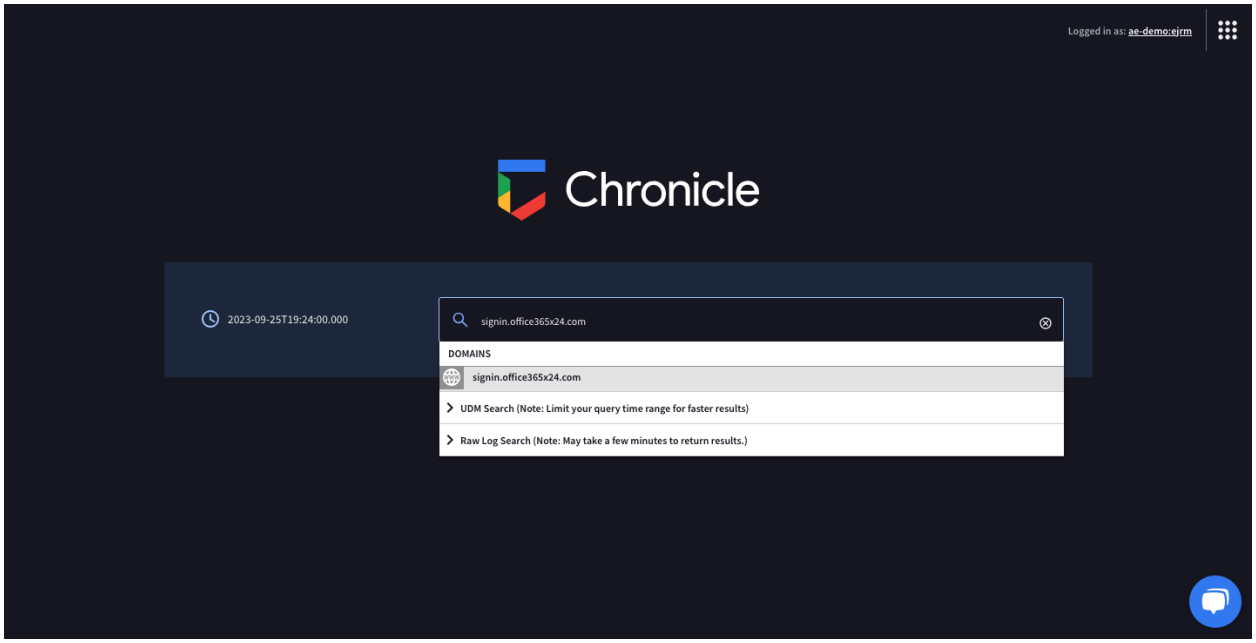
- Access threat intelligence reports on the domain
- Identify the assets that accessed the domain
- Evaluate the HTTP events associated with the domain
- Identify which assets submitted login information to the domain
- Identify additional domains

Scenario:

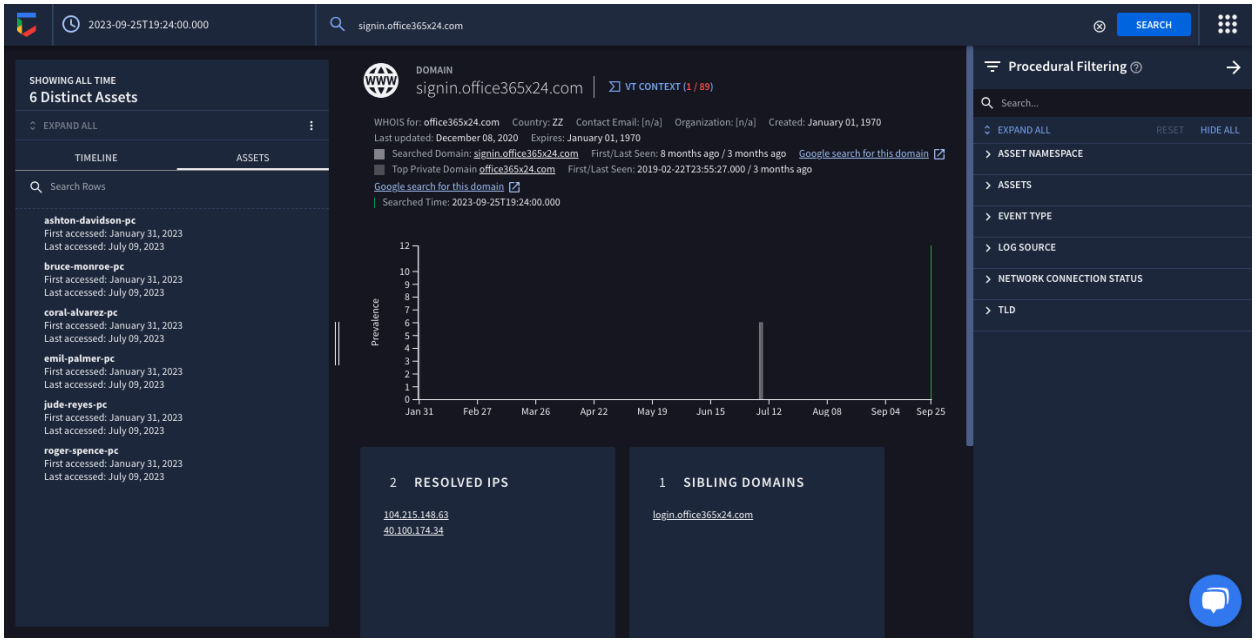
You are a security analyst at a financial services company. You receive an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: **signin.office365x24.com**. You need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. You will use Chronicle to investigate this domain.

Task 1 Perform a Domain Search

1. In the search bar, type **signin.office365x24.com** and click Search. Under DOMAINS, **signin.office365x24.com** will be listed. This tells you that the domain exists in the ingested data.



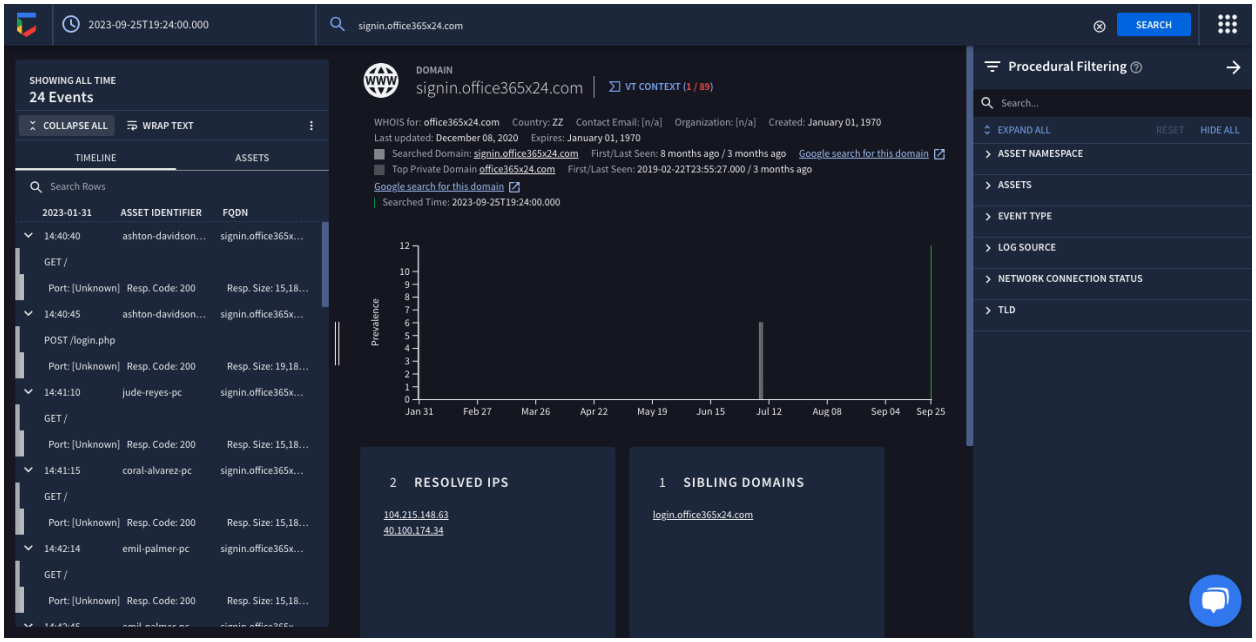
2. Click **signin.office365x24.com** to complete the search.



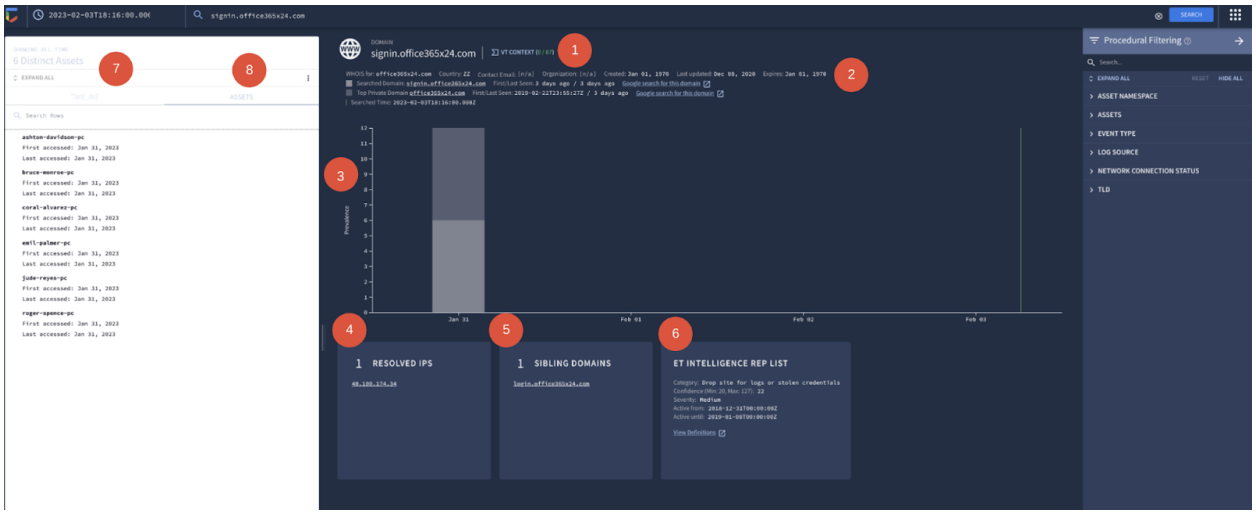
Task 2 Evaluate the Search Results

1. VT CONTEXT: This section provides the VirusTotal information available for the domain.
2. WHOIS: This section provides a summary of information about the domain using WHOIS, a free and publicly available directory that includes information about registered domain names, such as the name and contact information of the domain owner. In cybersecurity, this information is helpful in assessing a domain's reputation and determining the origin of malicious websites.
3. Prevalence: This section provides a graph which outlines the historical prevalence of the domain. This can be helpful when you need to determine whether the domain has been accessed previously. Usually, less prevalent domains may indicate a greater threat.

4. RESOLVED IPS: This insight card provides additional context about the domain, such as the IP address that maps to **signin.office365x24.com**, which is **40.100.174.34**. Clicking on this IP will run a new search for the IP address in Chronicle. Insight cards can be helpful in expanding the domain investigation and further investigating an indicator to determine whether there is a broader compromise.
5. SIBLING DOMAINS: This insight card provides additional context about the domain. Sibling domains share a common top or parent domain. For example, here the sibling domain is listed as **login.office365x24.com**, which shares the same top domain **office365x24.com** with the domain you're investigating: **signin.office365x24.com**.
6. ET INTELLIGENCE REP LIST: This insight card includes additional context on the domain. It provides threat intelligence information, such as other known threats related to the domains using ProofPoint's Emerging Threats (ET) Intelligence Rep List.
7. Click TIMELINE. This tab provides information about the events and interactions made with this domain. Click EXPAND ALL to reveal the details about the HTTP requests made including **GET** and **POST** requests. A GET request retrieves data from a server while a POST request submits data to a server.



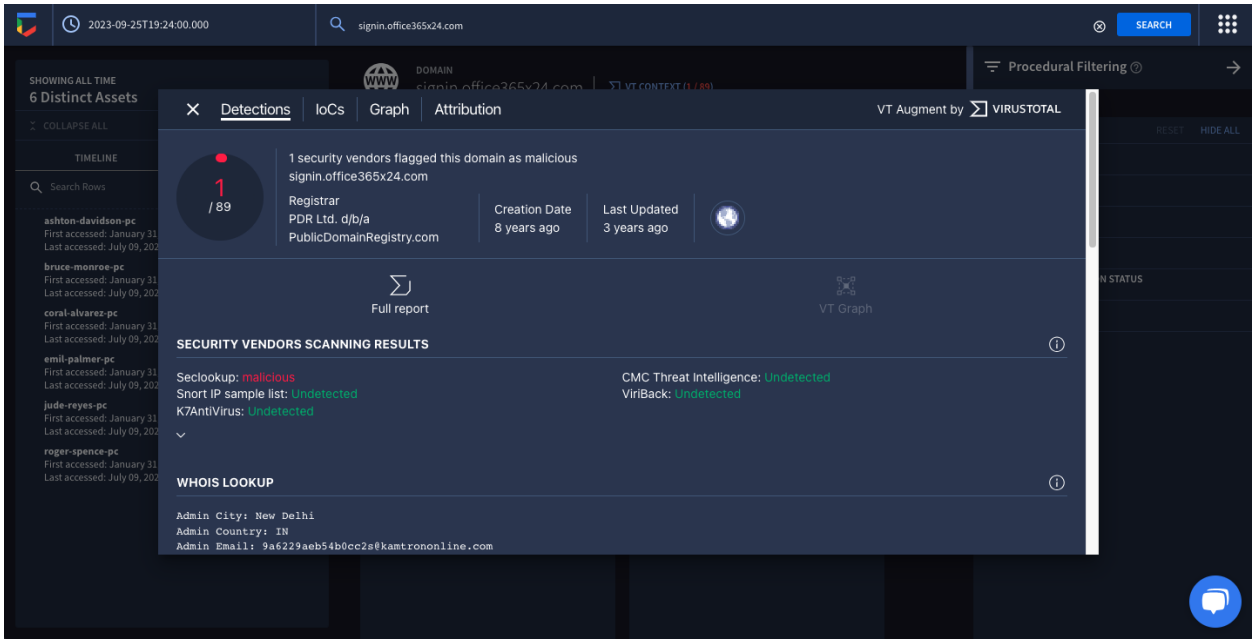
8. Click ASSETS. This tab provides a list of the assets that have accessed the domain.



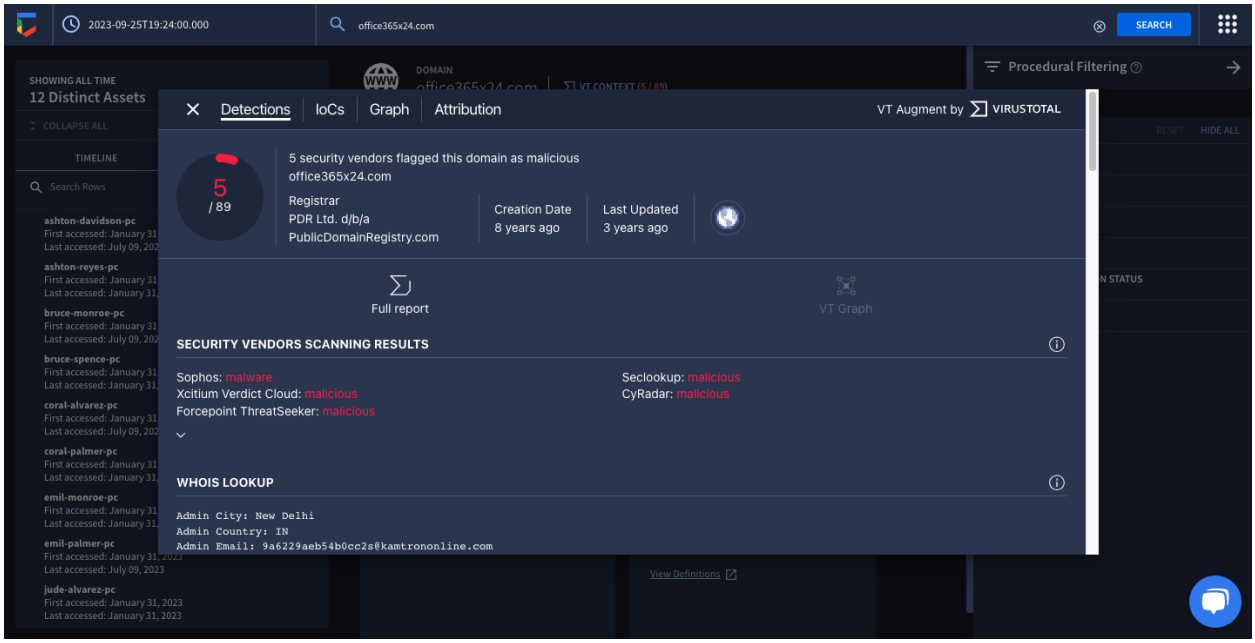
Task 3 Investigate the Threat Intelligence data

Determine whether the domain is malicious. Chronicle provides quick access to threat intelligence data from the search results that you can use to help your investigation.

1. Click on VT CONTEXT to analyze the available VirusTotal information about this domain. There is no VirusTotal information about this domain. To exit the VT CONTEXT window, click the X.



2. By Top Private Domain, click **office365x24.com** to access the domain view for **office365x24.com**. Click VT CONTEXT to assess the VirusTotal information about this domain. In the pop up, you can observe that one vendor has flagged this domain as malicious. Exit the VT CONTEXT window. Click the back button in your browser to go back to the domain view for the **signin.office365x24.com** search.



3. Click on the ET INTELLIGENCE REP LIST insight card to expand it, if needed.

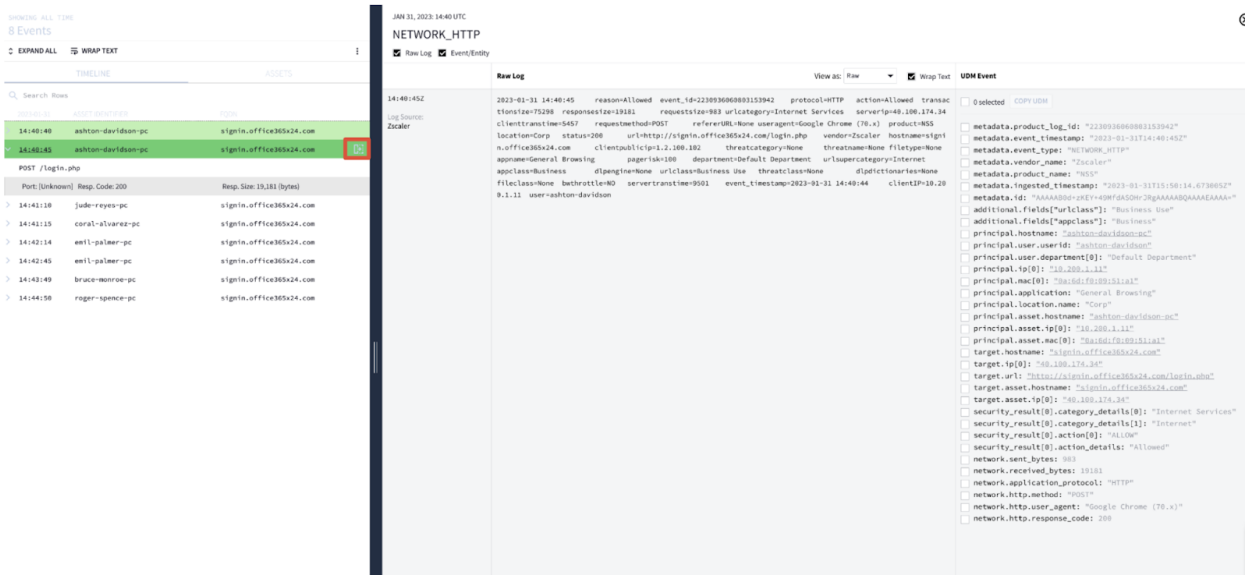
   Take note of the category.

Task 4 Investigate the Affected Assets and events

Information about the events and assets relating to the domain are separated into the two tabs: TIMELINE and ASSETS. TIMELINE shows the timeline of events that includes when each asset accessed the domain. ASSETS list hostnames, IP addresses, MAC addresses, or devices that have accessed the domain.

Investigate the affected assets and events by exploring the tabs:

1. ASSETS: There are several different assets that have accessed the domain, along with the date and time of access. Using your incident handler's journal, record the name and number of assets that have accessed the domain.
2. TIMELINE: Click EXPAND ALL to reveal the details about the HTTP requests made, including **GET** and **POST** requests. The **POST** information is especially useful because it means that data was sent to the domain. It also suggests a possible successful phish. For more details about the connections, open the raw log viewer by clicking the open icon.



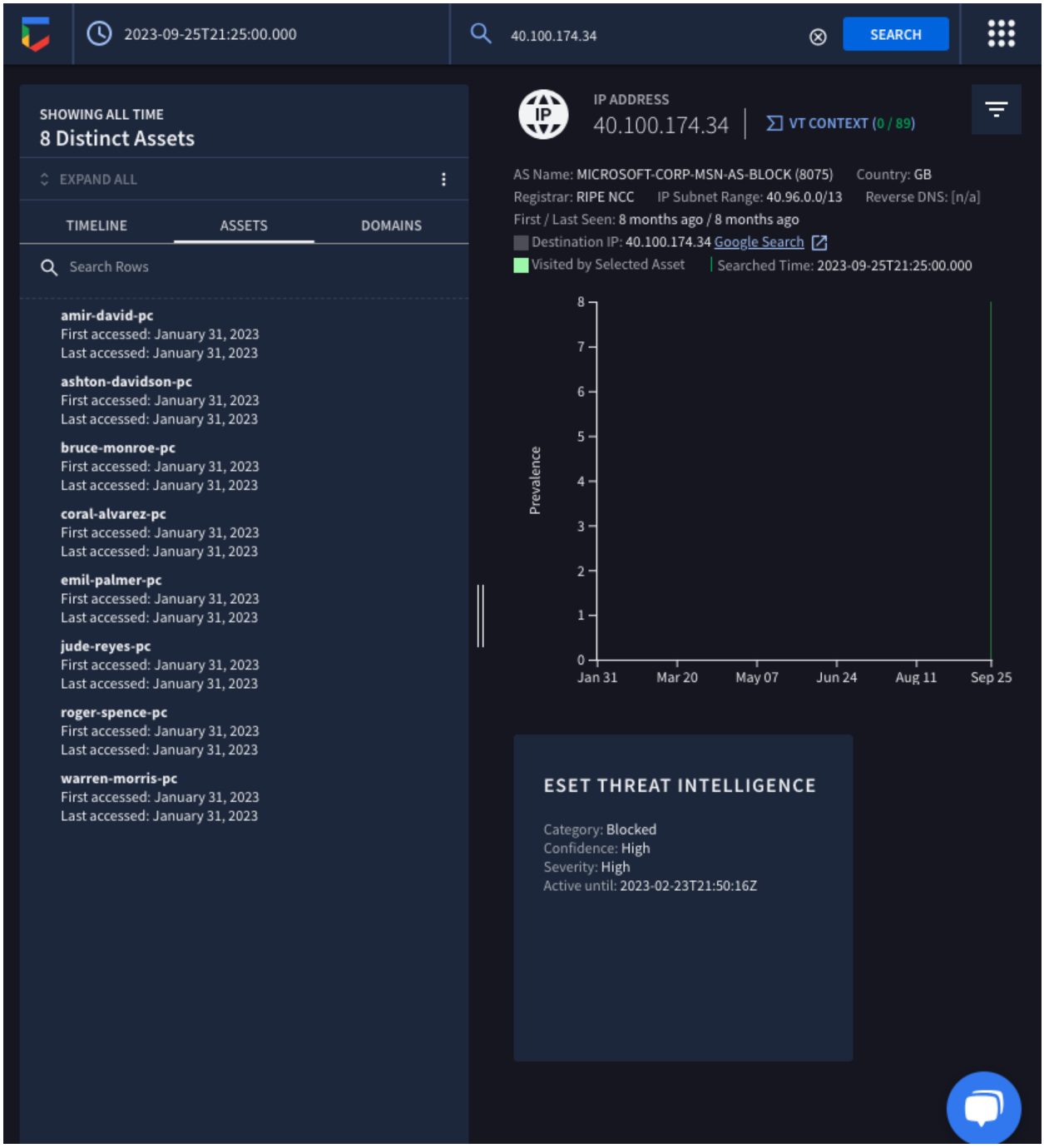
Task 5 Investigate the Resolved IP Address

So far, you have collected information about the domain's reputation using threat intelligence, and you've identified the assets and events associated with the domain. Based on this information, it's clear that this domain is suspicious and most likely malicious. But before you can confirm that it is malicious, there's one last thing to investigate.

Attackers sometimes reuse infrastructure for multiple attacks. In these cases, multiple domain names resolve to the same IP address.

Investigate the IP address found under the RESOLVED IPS insight card to identify if the **signin.office365x24.com** domain uses another domain. Follow these steps:

1. Under RESOLVED IPS, click the IP address **40.100.174.34**.

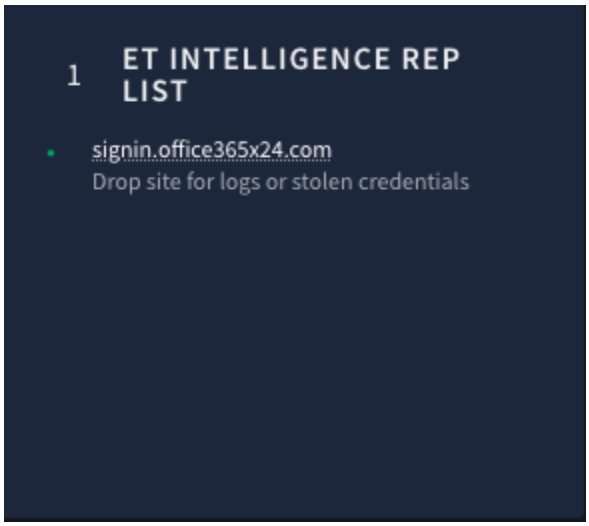


2. Evaluate the search results for this IP address and use your incident handler's journal to take note of the following:
    a. TIMELINE: Take note of the additional **POST** request. A new **POST** suggests that an asset may have been phished.
    b. ASSETS: Take note of the additional affected assets.
    c. DOMAINS: Take note of the additional domains associated with this IP address.

Questions

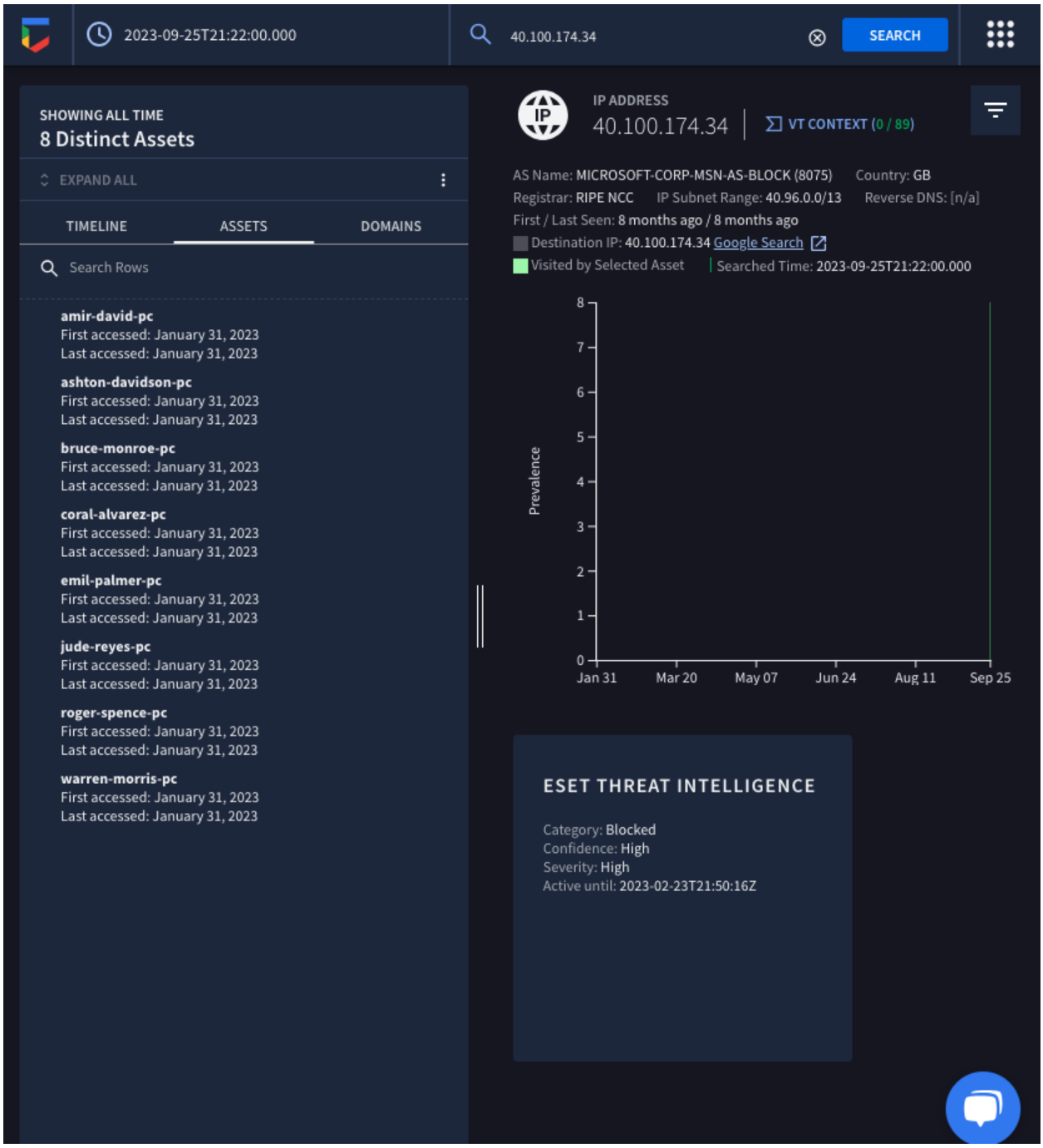
1. According to the available ET Intelligence Rep List, how is signin.office365x24.com categorized?

   Drop site for logs or stolen credentials



2. Which assets accessed the signin.office365x24.com domain?

   Coral-alvarez-pc, emil-palmer-pc and roger-spence-pc



3. What IP address does the signin.office365x24.com domain resolve to ?

   40.100.174.34

4. How many POST requests were made to the signin.office365x24.com domain?

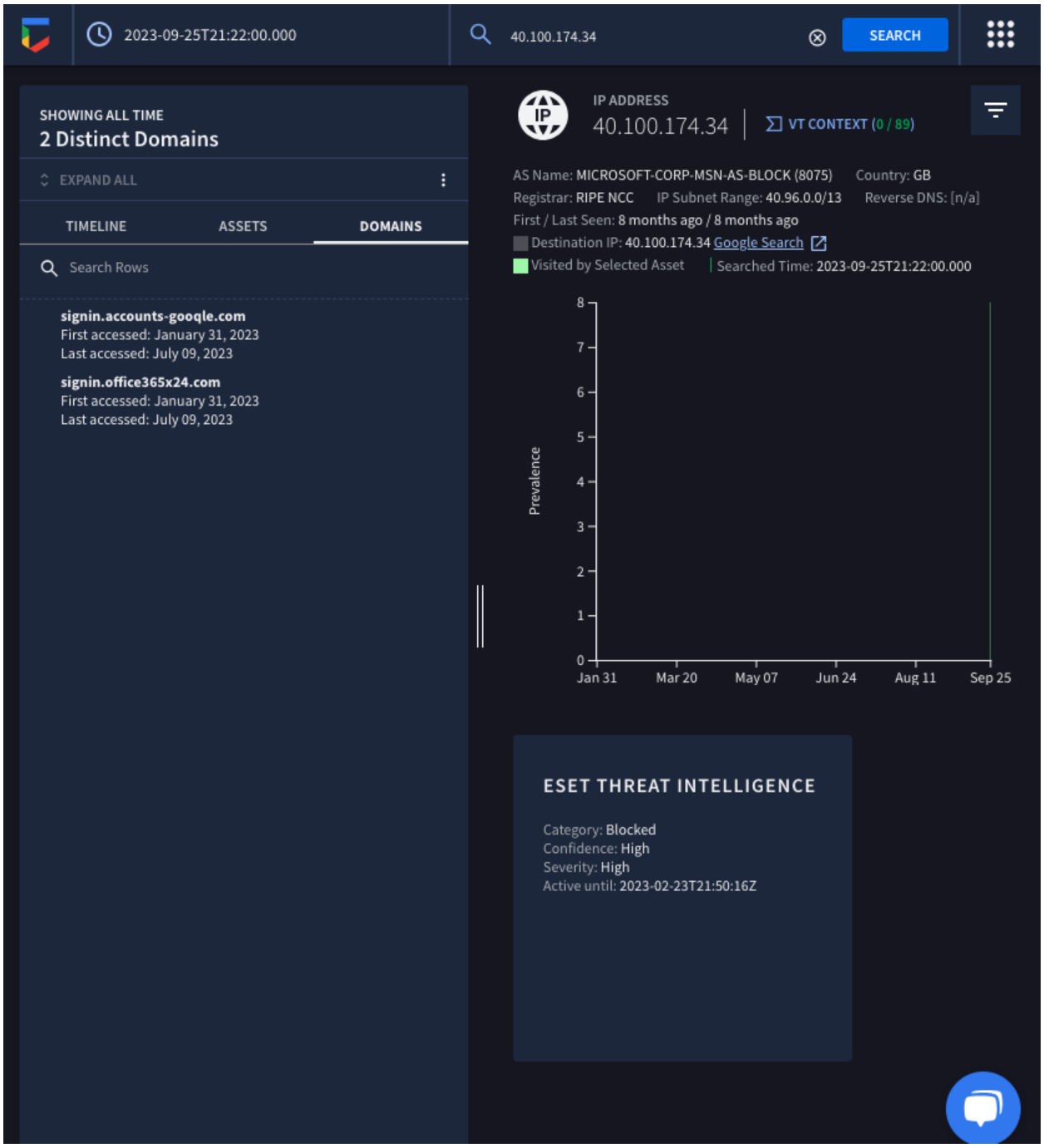
   2

5. Some POST requests were made to signin.office365x24.com. What is the target URL of the web page that the POST requests were made to?

   http://signin.office365x24.com/login.php

6. Which domains does the IP address 40.100.174.34 resolve to?

   Signin.office365x24.com and signin.accounts-google.com


2023-09-25T21:22:00.000
40.100.174.34
SEARCH
SHOWING ALL TIME
2 Distinct Domains
EXPAND ALL
TIMELINE
ASSETS
DOMAINS
Search Rows
signin.accounts-google.com
First accessed: January 31, 2023
Last accessed: July 09, 2023
signin.office365x24.com
First accessed: January 31, 2023
Last accessed: July 09, 2023
IP ADDRESS
40.100.174.34
VT CONTEXT (0 / 89)
AS Name: MICROSOFT-CORP-MSN-AS-BLOCK (8075)
Country: GB
Registrar: RIPE NCC
IP Subnet Range: 40.96.0.0/13
Reverse DNS: [n/a]
First / Last Seen: 8 months ago / 8 months ago
Destination IP: 40.100.174.34 Google Search
Visited by Selected Asset
Searched Time: 2023-09-25T21:22:00.000
Prevalence
0
1
2
3
4
5
6
7
8
Jan 31
Mar 20
May 07
Jun 24
Aug 11
Sep 25
ESET THREAT INTELLIGENCE
Category: Blocked
Confidence: High
Severity: High
Active until: 2023-02-23T21:50:16Z