Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

Step 1: Launch Chronicle

Click the link to launch Chronicle.

On the Chronicle home page, you'll find the current date and time, a search bar, and details about the total number of log entries. There are already a significant number of log events ingested into the Chronicle instance.

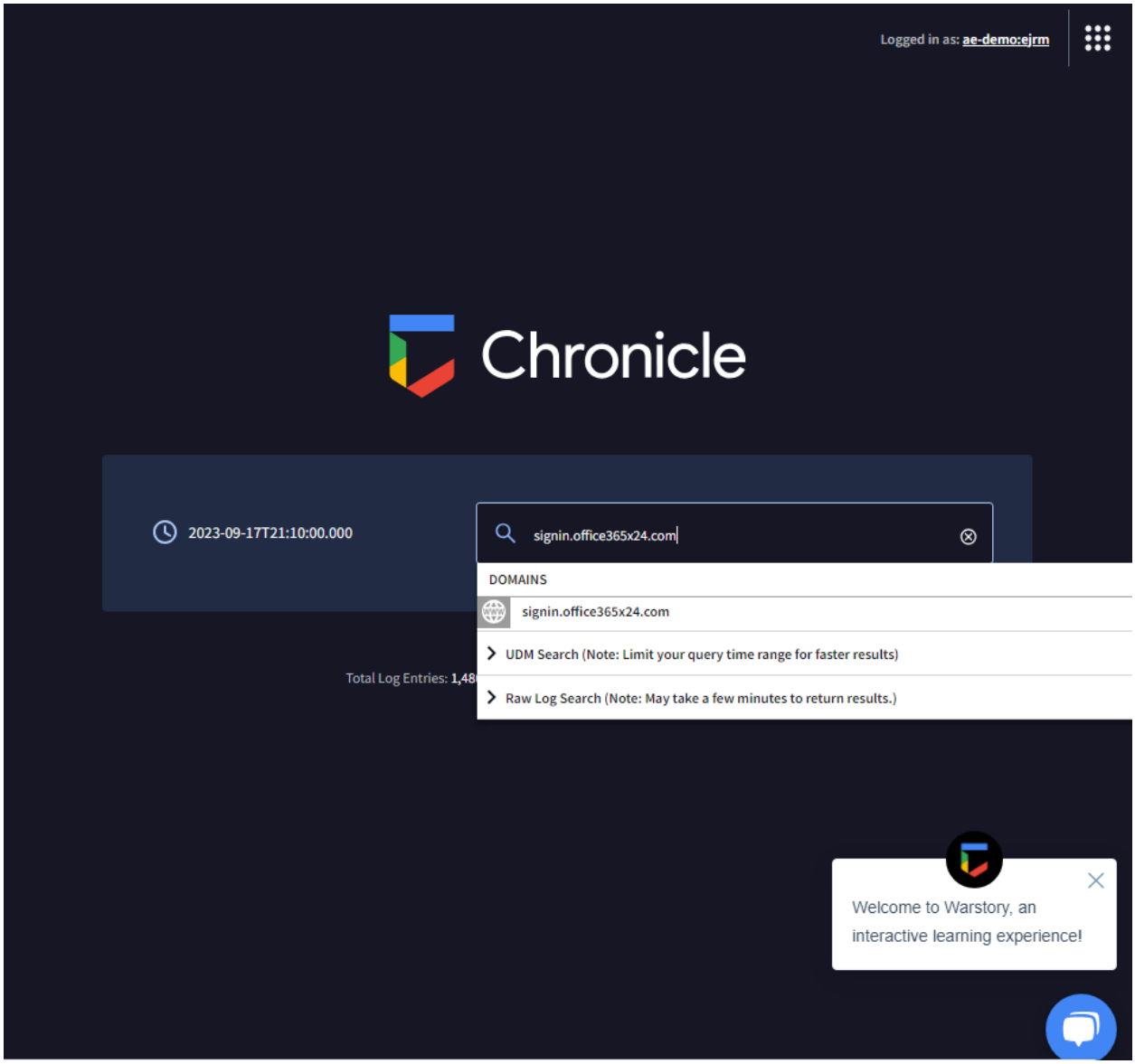
Note: Chronicle supports Google Chrome. You may experience limited functionality if you use browsers like Firefox, Edge, or Safari. For the best experience using Chronicle, install the latest version of Chrome.

Step 2: Perform a domain search

To begin, complete these steps to perform a domain search for the domain contained in the phishing email. Then, search for events using information like hostnames, domains, IP addresses, URLs, email addresses, usernames, and file hashes.

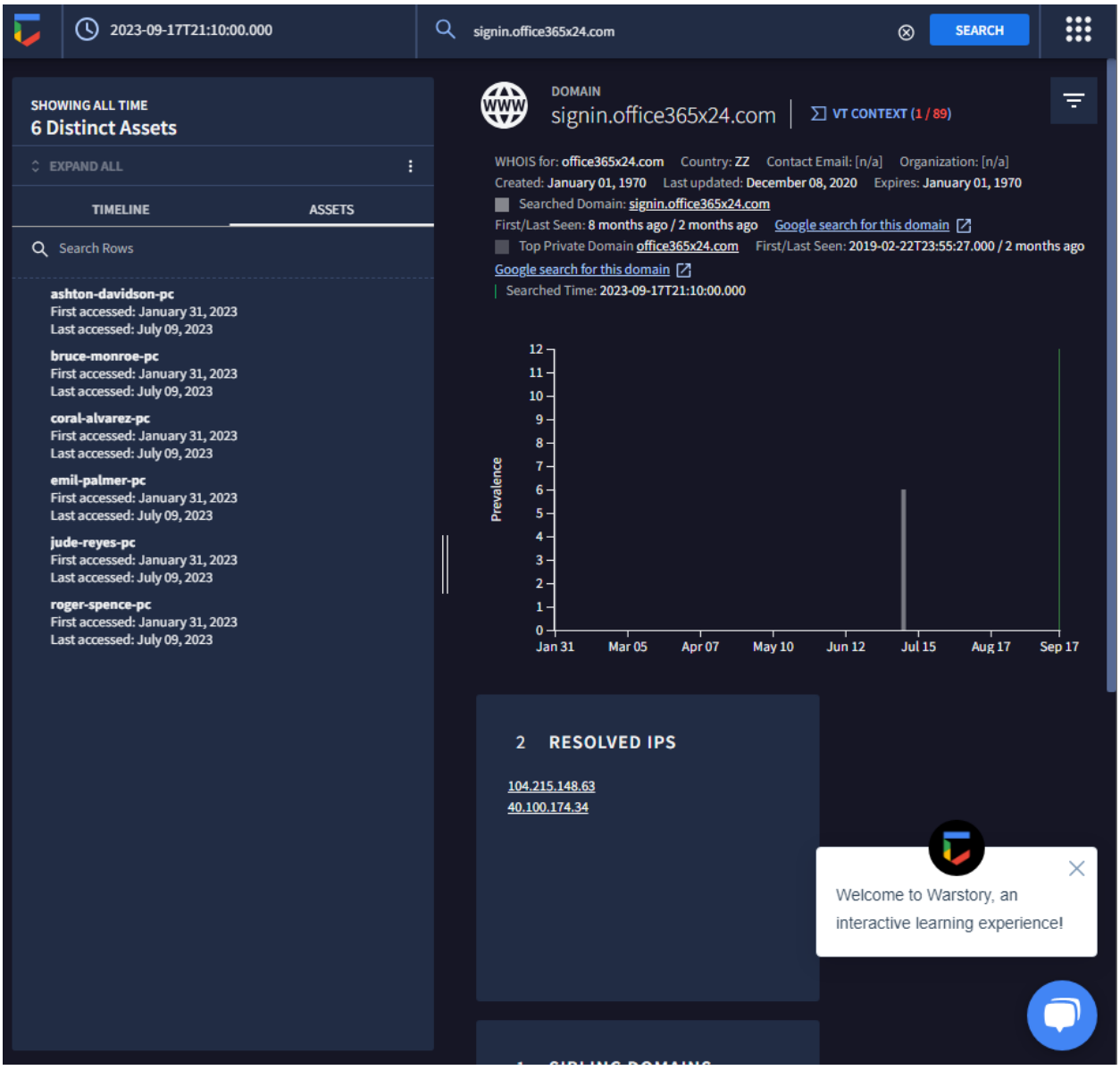
1. In the search bar, type `signin.office365x24.com` and click **Search**. Under **DOMAINS**, `signin.office365x24.com` will be listed. This tells you that the domain exists in the ingested data.

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



Step 3: Evaluate the search results

After performing a domain search, you'll be in the domain view. Evaluate the search results and observe the following:



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`.

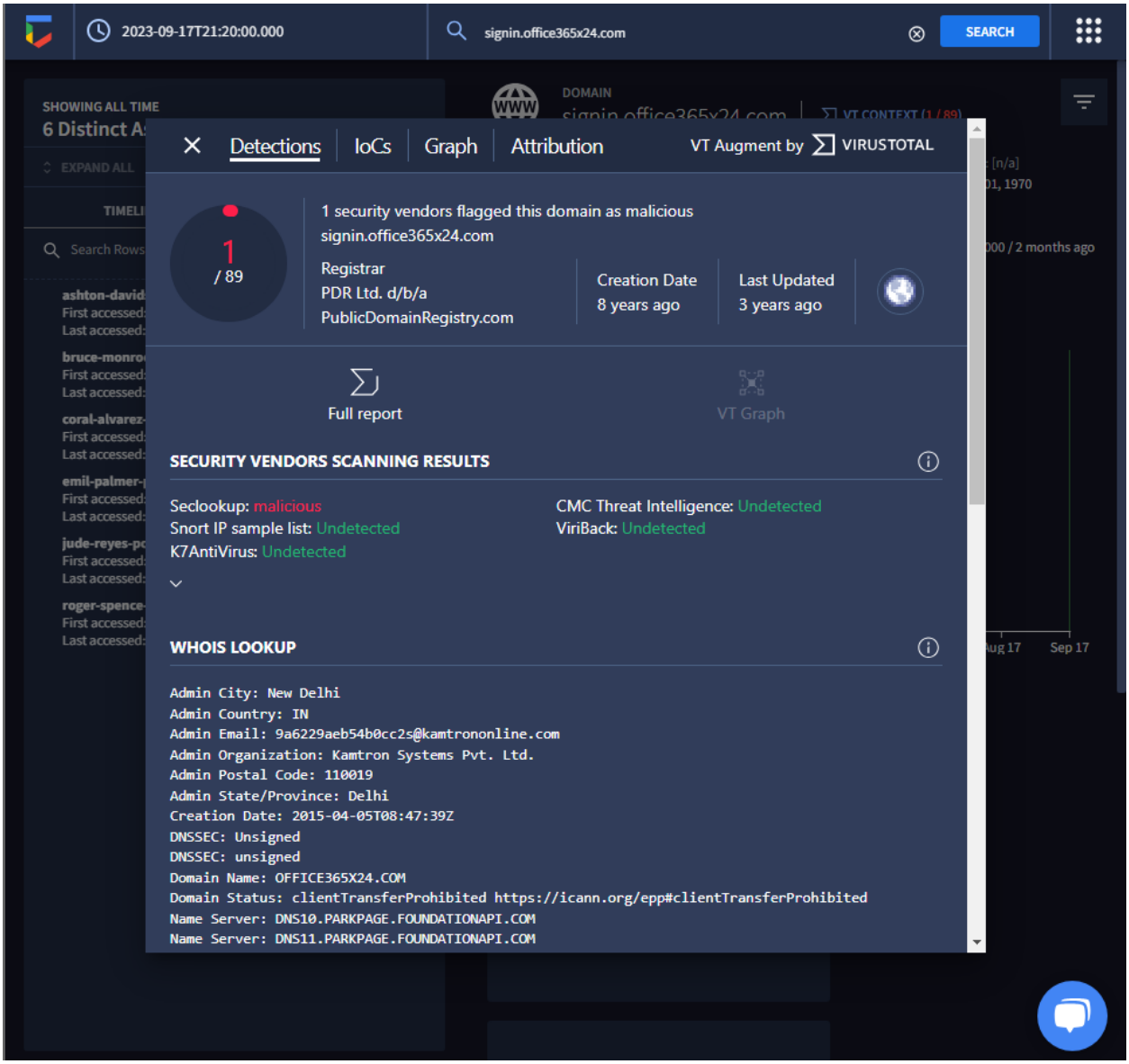
6. **ET INTELLIGENCE REP LIST:** This insight card includes additional context on the domain. It provides threat intelligence information, such as other known threats related to the domains using ProofPoint's Emerging Threats (ET) Intelligence Rep List.

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.

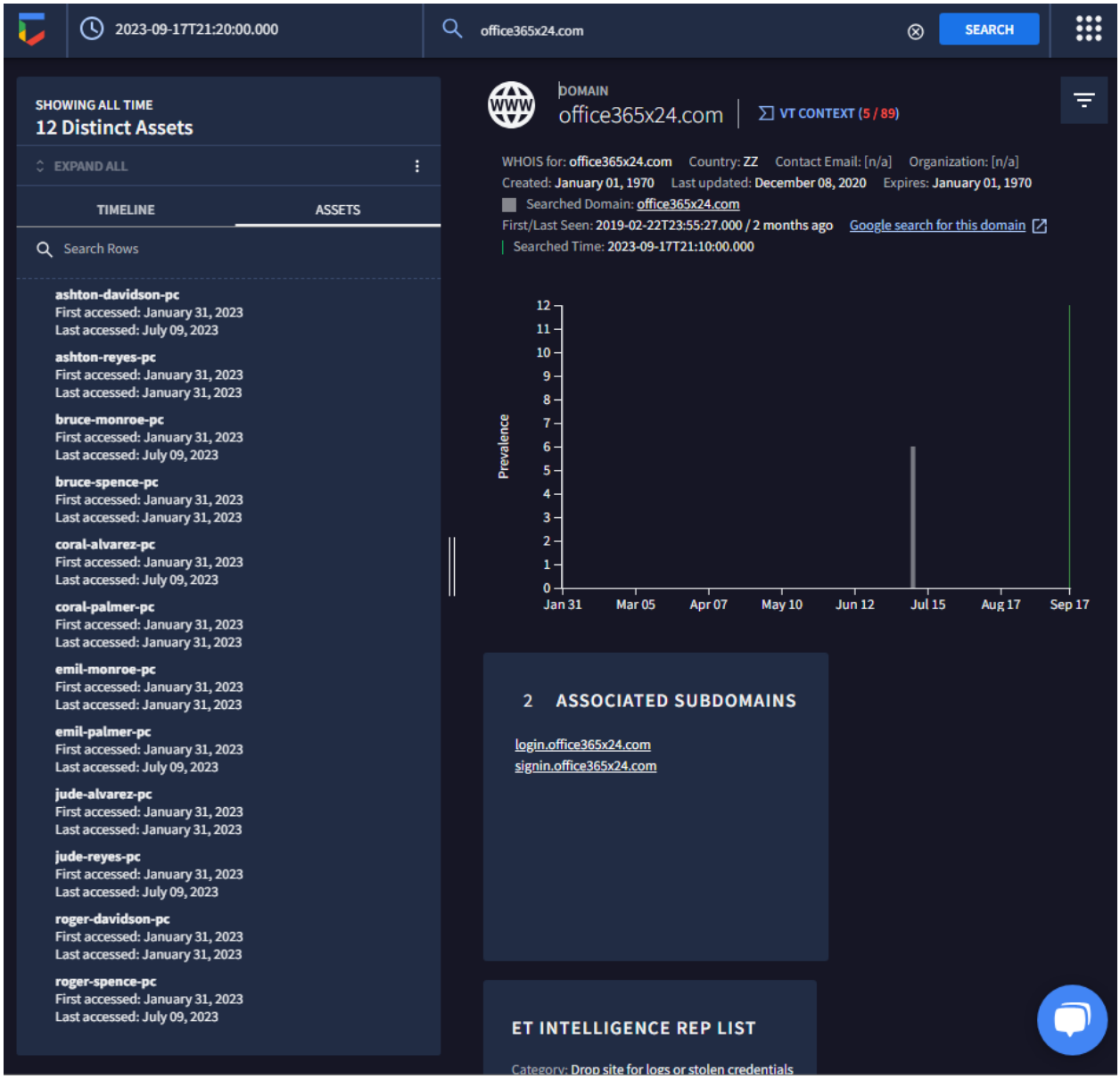
8. Click **ASSETS.** This tab provides a list of the assets that have accessed the domain.

Step 4: Investigate the threat intelligence data

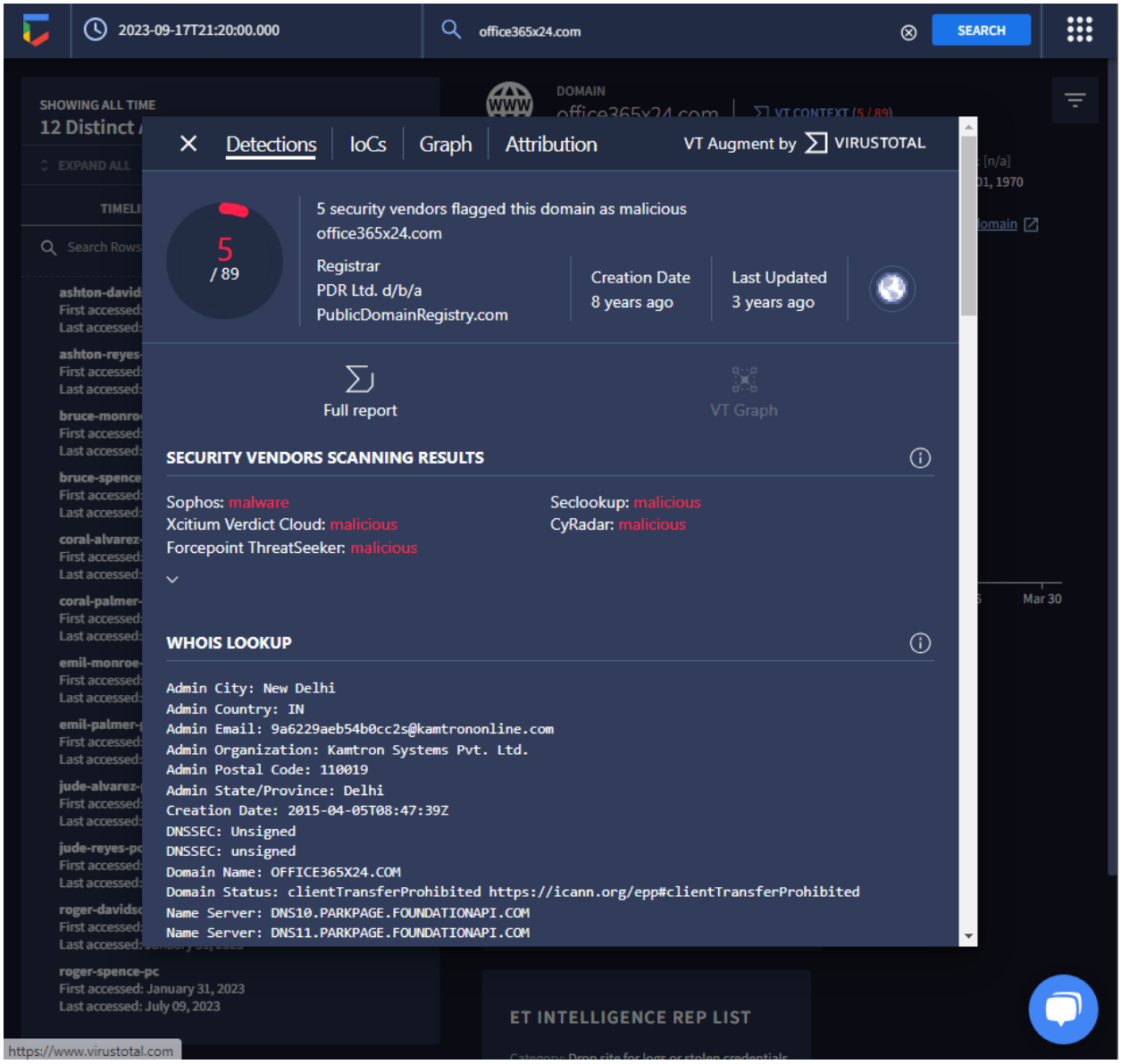
Now that you've retrieved results for the domain name, the next step is to determine whether the domain is malicious. Chronicle provides quick access to threat intelligence data from the search results that you can use to help your investigation. Follow these steps to analyze the threat intelligence data and use your incident handler's journal to record interesting data:



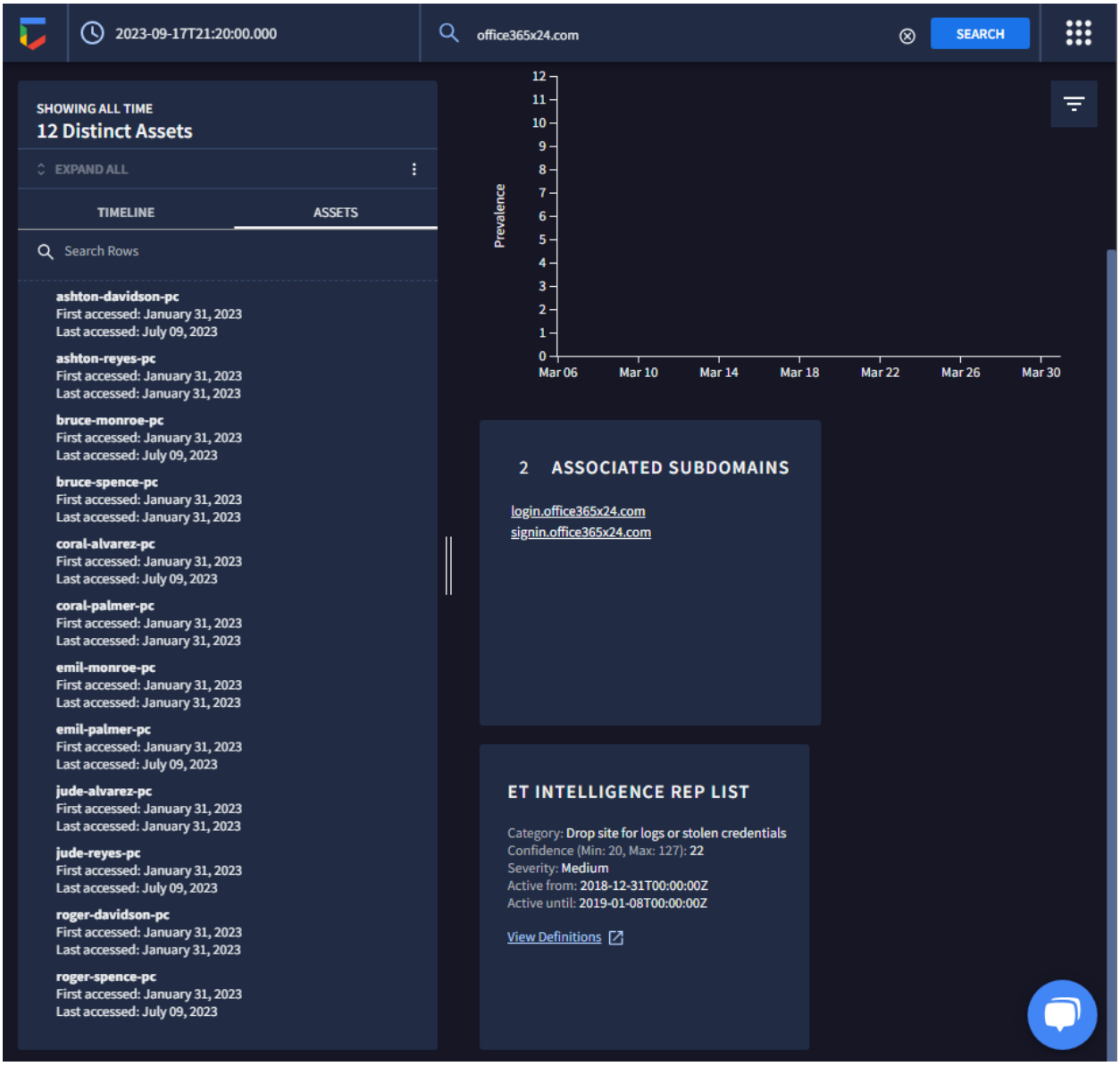
1. Click on **VT CONTEXT** to analyze the available VirusTotal information about this domain. There is no VirusTotal information about this domain. To exit the VT CONTEXT window, click the **X**.



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.



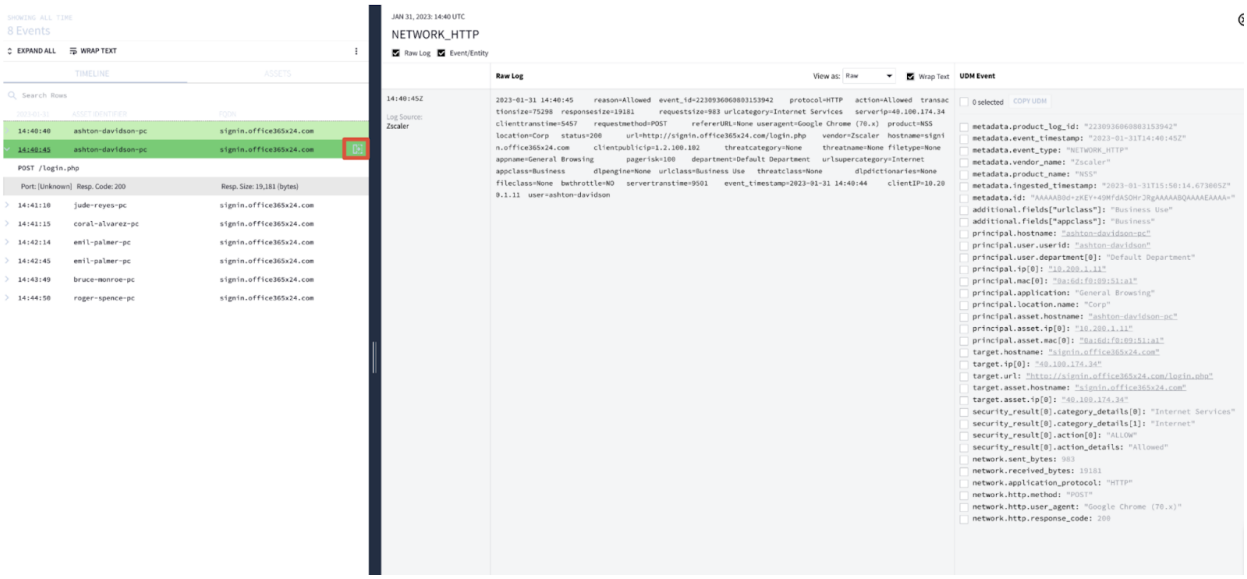
Step 5: Investigate the affected assets and events

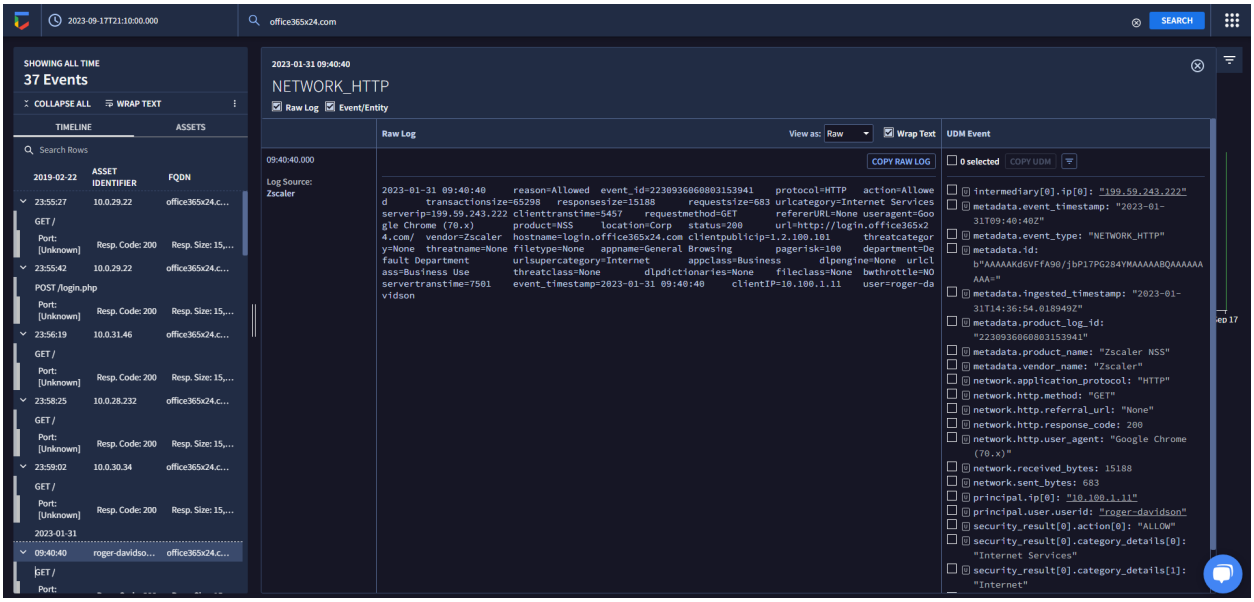
Information about the events and assets relating to the domain are separated into the two tabs: **TIMELINE** and **ASSETS**. **TIMELINE** shows the timeline of events that includes when each asset accessed the domain. **ASSETS** list hostnames, IP addresses, MAC addresses, or devices that have accessed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

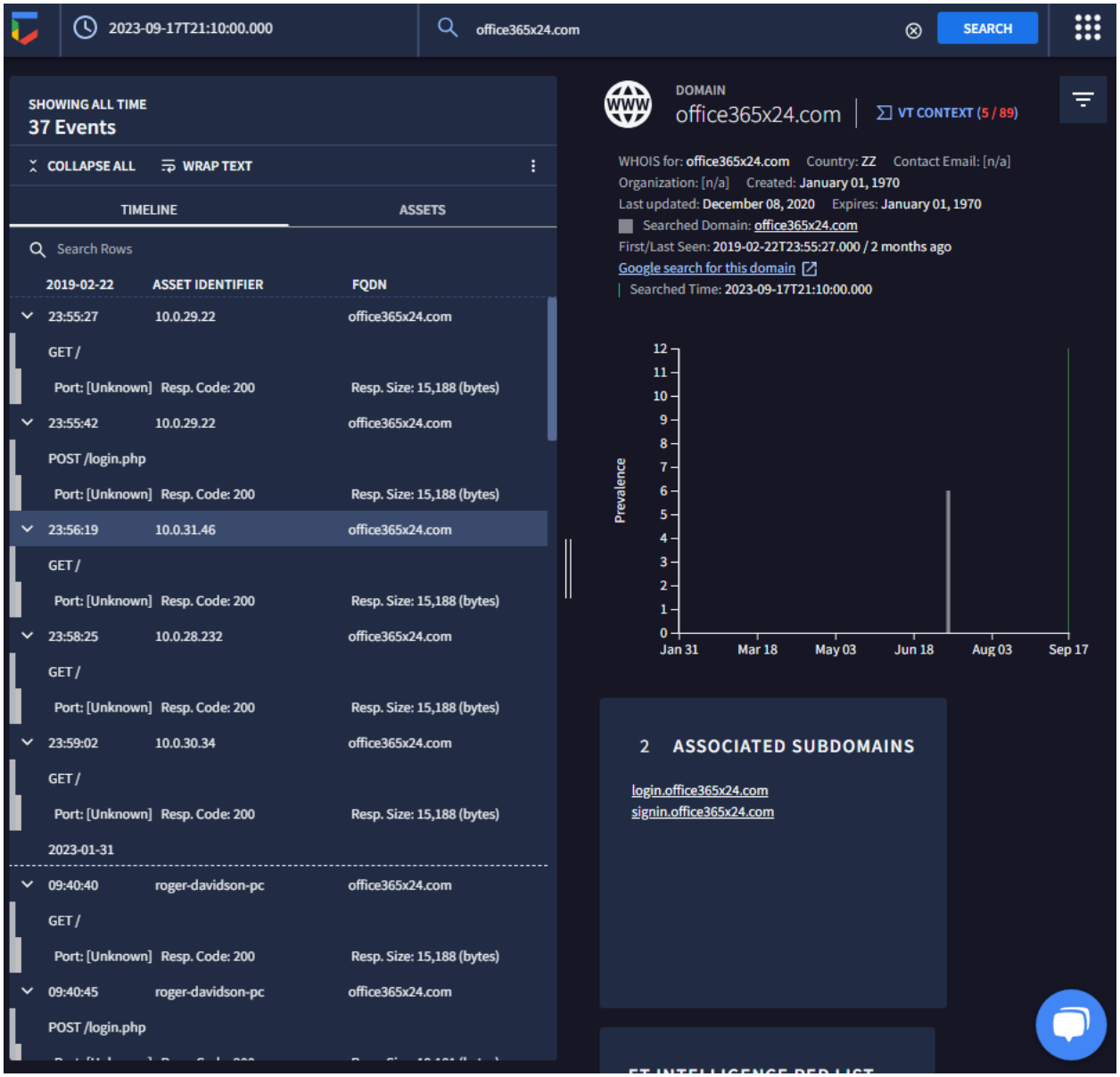
Investigate the affected assets and events by exploring the tabs:

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. Using your incident handler's journal, take note of the `POST` requests to the `/login.php` page. For more details about the connections, open the raw log viewer by clicking the open icon.




2023-09-17T21:10:00.000
office365x24.com
SEARCH
SHOWING ALL TIME
37 Events
COLLAPSE ALL
WRAP TEXT
TIMELINE
ASSETS
Search Rows
2019-02-22
ASSET IDENTIFIER
FQDN
23:55:27 10.0.29.22 office365x24.c...
GET /
Port: [Unknown] Resp. Code: 200 Resp. Size: 15,...
23:55:42 10.0.29.22 office365x24.c...
POST /login.php
Port: [Unknown] Resp. Code: 200 Resp. Size: 15,...
23:56:19 10.0.31.46 office365x24.c...
GET /
Port: [Unknown] Resp. Code: 200 Resp. Size: 15,...
23:58:25 10.0.28.232 office365x24.c...
GET /
Port: [Unknown] Resp. Code: 200 Resp. Size: 15,...
23:59:02 10.0.30.34 office365x24.c...
GET /
Port: [Unknown] Resp. Code: 200 Resp. Size: 15,...
2023-01-31
09:40:40 roger-davidso... office365x24.c...
GET /
Port:
2023-01-31 09:40:40
NETWORK_HTTP
Raw Log
Event/Entity
Raw Log
View as: Raw
Wrap Text
UDM Event
09:40:40.000
Log Source: Zscaler
COPY RAW LOG
2023-01-31 09:40:40 reason=Allowed event_id=2230936060803153941 protocol=HTTP action=Allowed transactionsize=65298 responsesize=15188 requestsize=683 urlcategory=Internet Services serverip=199.59.243.222 clienttranstime=5457 requestmethod=GET refererURL=None useragent=Google Chrome (70.x) product=NSS location=Corp status=200 url=http://login.office365x24.com/ vendor=Zscaler hostname=login.office365x24.com clientpublicip=1.2.100.101 threatcategory=None threatname=None filetype=None appname=General Browsing pagerisk=100 department=Default Department urlsupercategory=Internet appclass=Business dlpengine=None urlclass=Business Use threatclass=None dlpdictionaries=None fileclass=None bwthrottle=NO servertranstime=7501 event_timestamp=2023-01-31 09:40:40 clientIP=10.100.1.11 user=roger-davidson
0 selected
COPY UDM
intermediary[0].ip[0]: "199.59.243.222"
metadata.event_timestamp: "2023-01-31T09:40:40Z"
metadata.event_type: "NETWORK_HTTP"
metadata.id: b"AAAAAKd6VFfA90/jbP17PG284YMAAAAABQAAAAAAAAA="
metadata.ingested_timestamp: "2023-01-31T14:36:54.018949Z"
metadata.product_log_id: "2230936060803153941"
metadata.product_name: "Zscaler NSS"
metadata.vendor_name: "Zscaler"
network.application_protocol: "HTTP"
network.http.method: "GET"
network.http.referral_url: "None"
network.http.response_code: 200
network.http.user_agent: "Google Chrome (70.x)"
network.received_bytes: 15188
network.sent_bytes: 683
principal.ip[0]: "10.100.1.11"
principal.user.userid: "roger-davidson"
security_result[0].action[0]: "ALLOW"
security_result[0].category_details[0]: "Internet Services"
security_result[0].category_details[1]: "Internet"



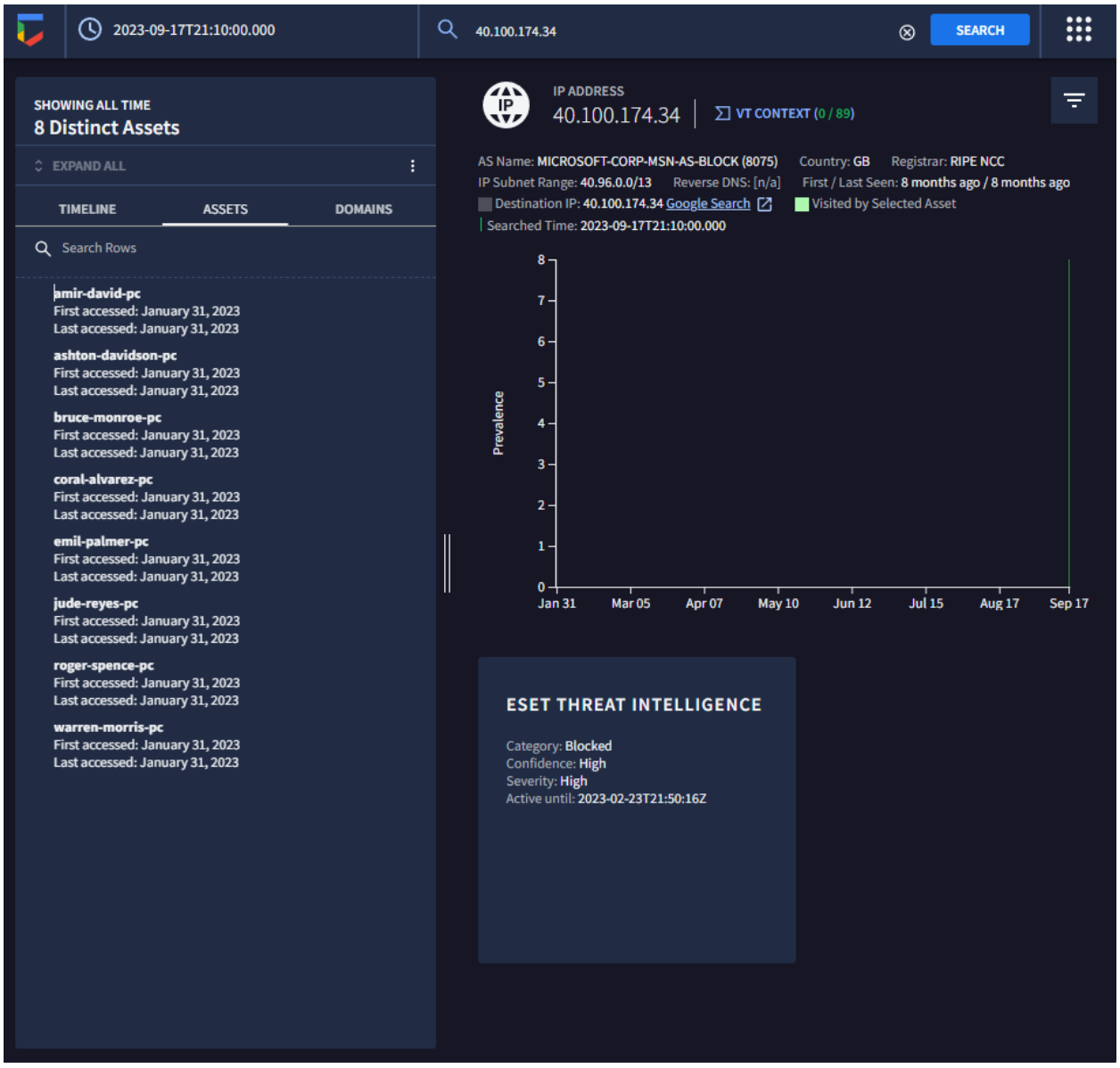
Step 6: Investigate the resolved IP address

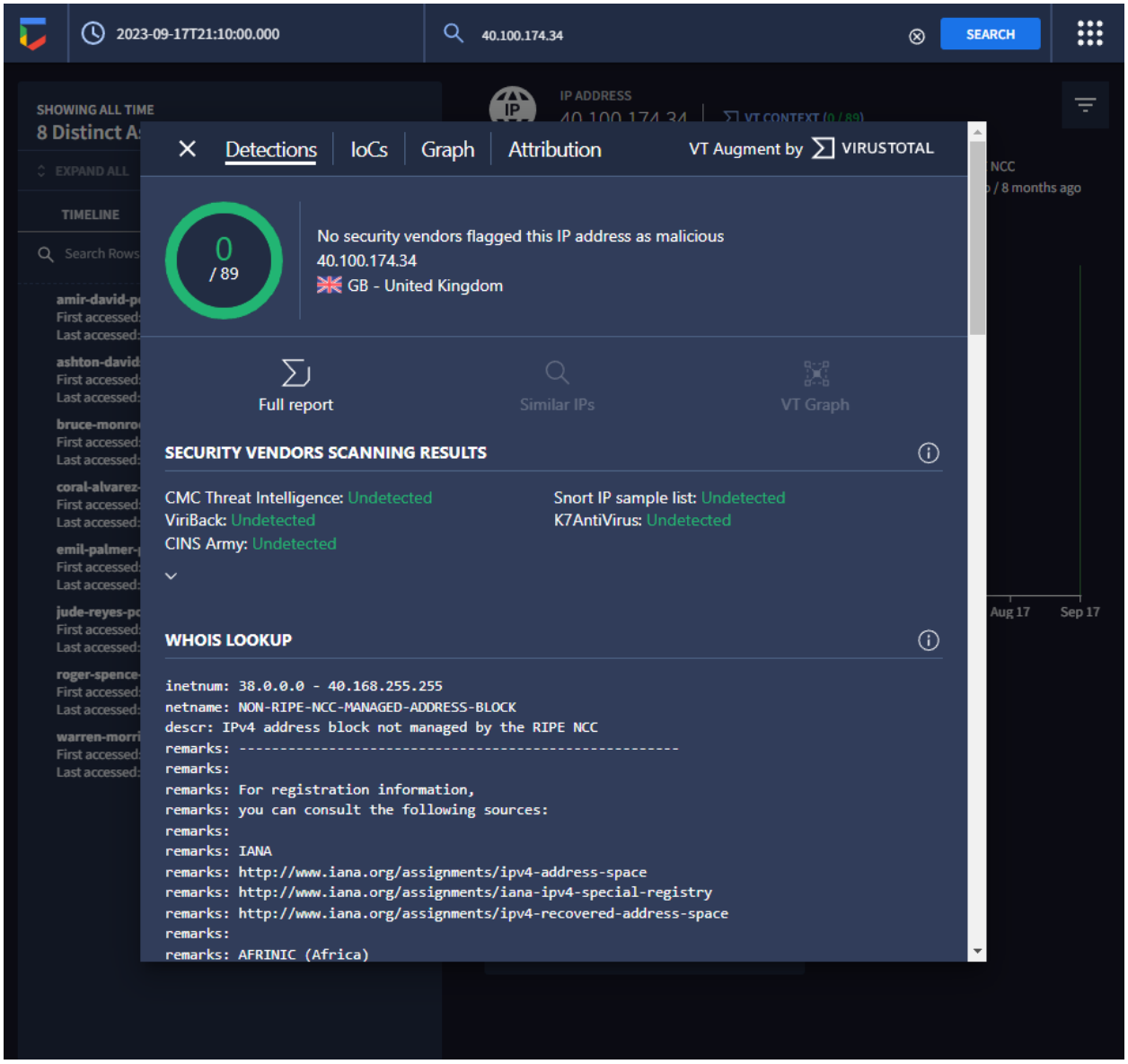
So far, you have collected information about the domain's reputation using threat intelligence, and you've identified the assets and events associated with the domain. Based on this information, it's clear that this domain is suspicious and most likely malicious. But before you can confirm that it is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


2023-09-17T21:10:00.000
40.100.174.34
SEARCH
SHOWING ALL TIME
8 Distinct Assets
EXPAND ALL
TIMELINE
ASSETS
DOMAINS
Search Rows
amir-david-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
ashton-davidson-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
bruce-monroe-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
coral-alvarez-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
emil-palmer-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
jude-reyes-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
roger-spence-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023
warren-morris-pc
First accessed: January 31, 2023
Last accessed: January 31, 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: 2023-09-17T21:10:00.000
Prevalence
0
1
2
3
4
5
6
7
8
Jan 31
Mar 05
Apr 07
May 10
Jun 12
Jul 15
Aug 17
Sep 17
ESET THREAT INTELLIGENCE
Category: Blocked
Confidence: High
Severity: High
Active until: 2023-02-23T21:50:16Z



Step 7: Answer questions about domain investigation

Use the notes you've taken in your incident handler's journal and the Chronicle search results to answer the following questions about the investigation. Be sure to query the correct domain listed in each question.

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

a. Drop site for logs or stolen credentials
b. Spam site
c. Phishing site
d. Command and control server

2. Which assets accessed the `signin.office365x24.com` domain? Select three answers.

    a. `coral-alvarez-pc`
    b. `roger-spence-pc`
    c. `thomas-garcia-pc`
    d. `emil-palmer-pc`

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

    a. `10.0.29.22`
    b. `45.32.8.8`
    c. `40.100.174.34`
    d. `10.0.0.222`

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

    a. 2
    b. 8
    c. 1
    d. 6

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?

    a. `http://accounts-google.com/login.txt`
    b. `http://office365x24.com/login.exe`
    c. `http://accounts-google.com/login.php`
    d. `http://signin.office365x24.com/login.php`

6. Which domains does the IP address `40.100.174.34` resolve to? Select two answers.

    a. `euw.adserver.snapads.com`

b. `signin.accounts-google.com`
c. `cloud2.xdncloud.com`
d. `sigin.office365x24.com`

Key takeaways

In this activity, you used Chronicle to investigate a suspicious domain used in a phishing email. Using Chronicle's domain search, you were 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

After investigation, you determined that the suspicious domain has been involved in phishing campaigns. You also determined that multiple assets might have been impacted by the phishing campaign as logs showed that login information was submitted to the suspicious domain via `POST` requests. Finally, you identified two additional domains related to the suspicious domain by examining the resolved IP address.

If you would like to explore more investigations, check out the chat bot feature on Chronicle's home page.