

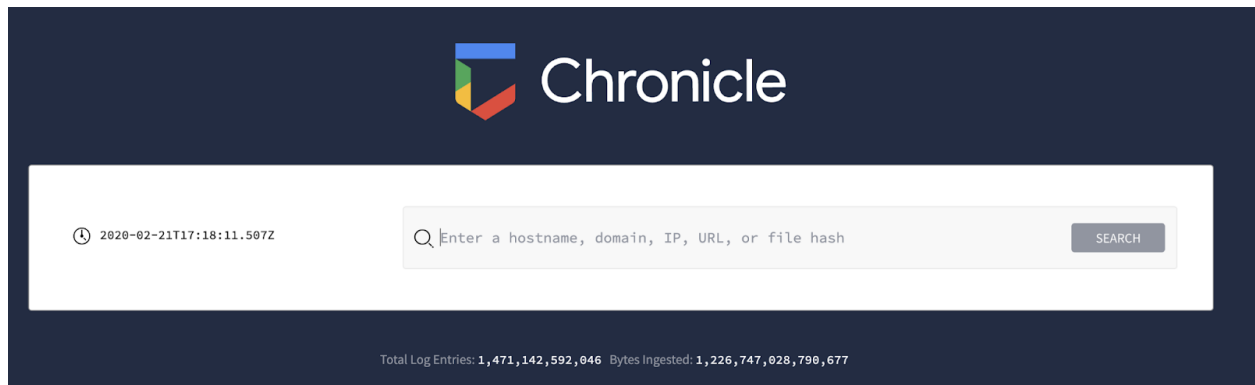
# Step-By-Step Instructions

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.

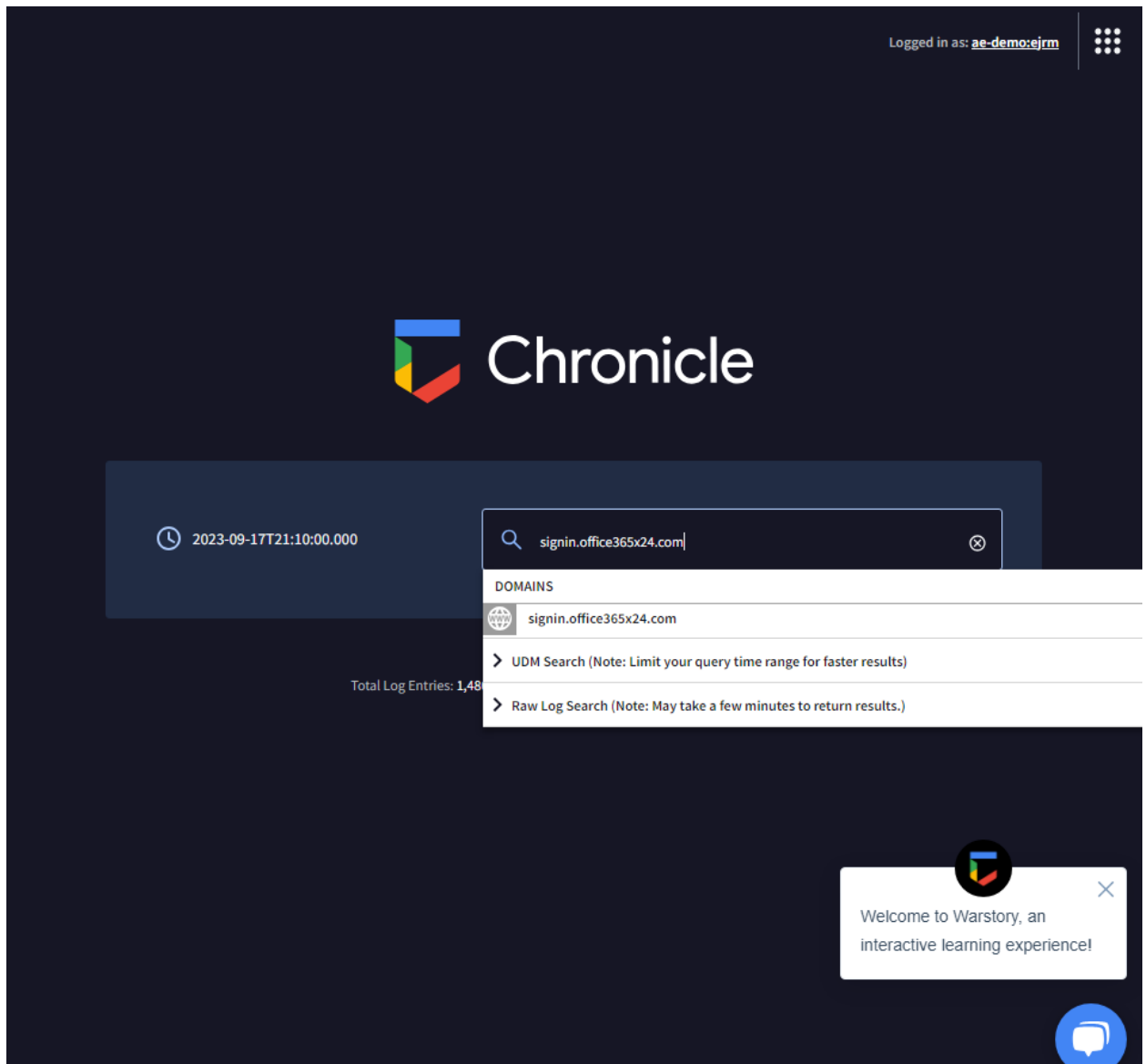


*Note: Chronicle supports Google Chrome. You may experience limited functionality if you use browsers like Firefox, Edge, or Safari. For the best experience using Chronicle, [install the latest version of Chrome](#).*

## Step 2: Perform a domain search

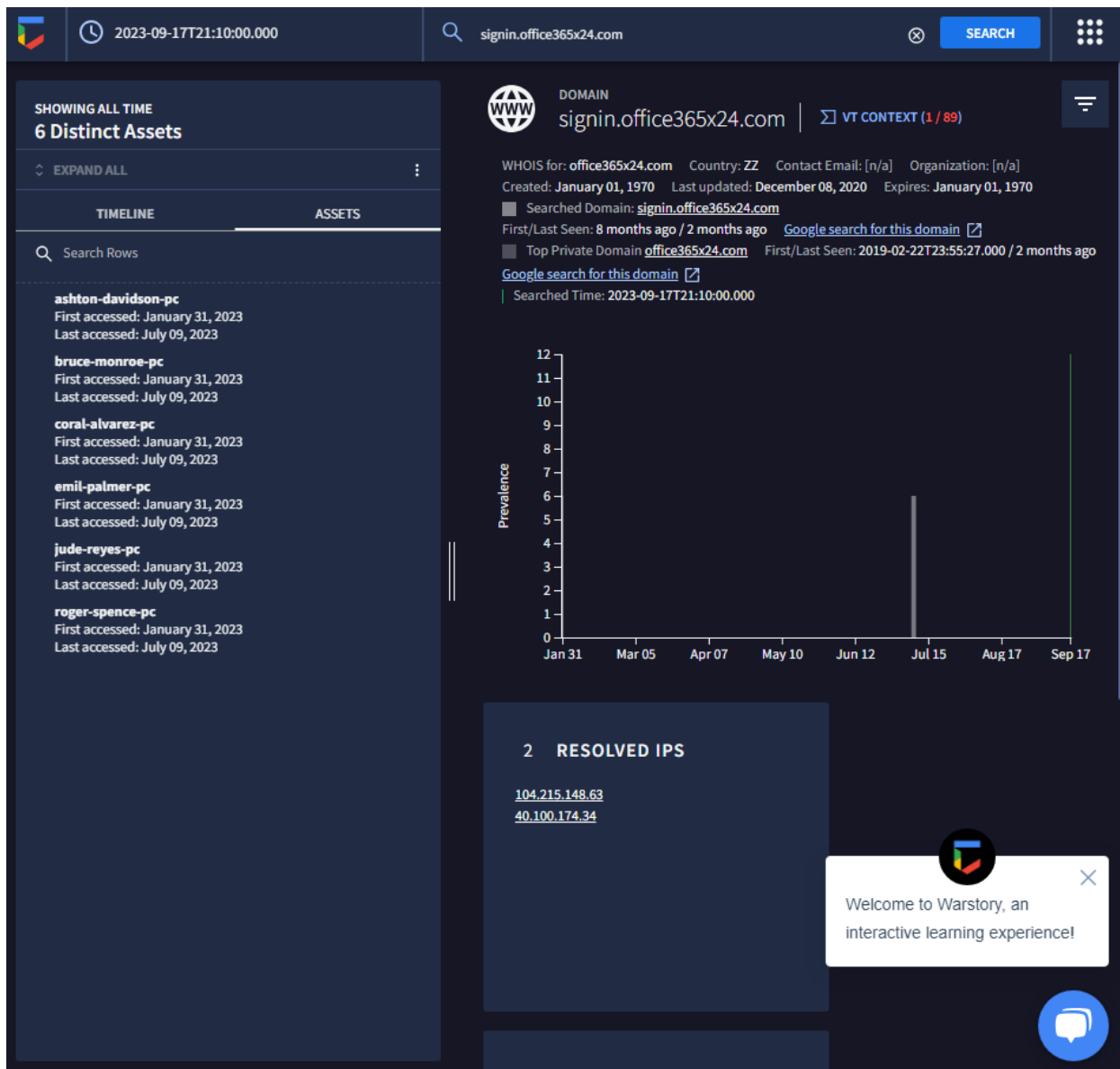
To begin, complete these steps to perform a domain search for the domain contained in the phishing email. Then, search for events using information like hostnames, domains, IP addresses, URLs, email addresses, usernames, and file hashes.

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:

The screenshot shows a web application interface for domain analysis. At the top, a search bar contains the domain 'signin.office365x24.com'. Below the search bar, a 'VT CONTEXT (1 / 89)' window is open, displaying various details about the domain. The window has tabs for 'Detections', 'IoCs', 'Graph', and 'Attribution'. The 'Detections' tab is active, showing a summary of security vendor flags and a detailed 'SECURITY VENDORS SCANNING RESULTS' section. Below this, a 'WHOIS LOOKUP' section provides registration information for the domain.

**VT CONTEXT (1 / 89)**

1 security vendors flagged this domain as malicious  
signin.office365x24.com

Registrar	Creation Date	Last Updated
PDR Ltd. d/b/a PublicDomainRegistry.com	8 years ago	3 years ago

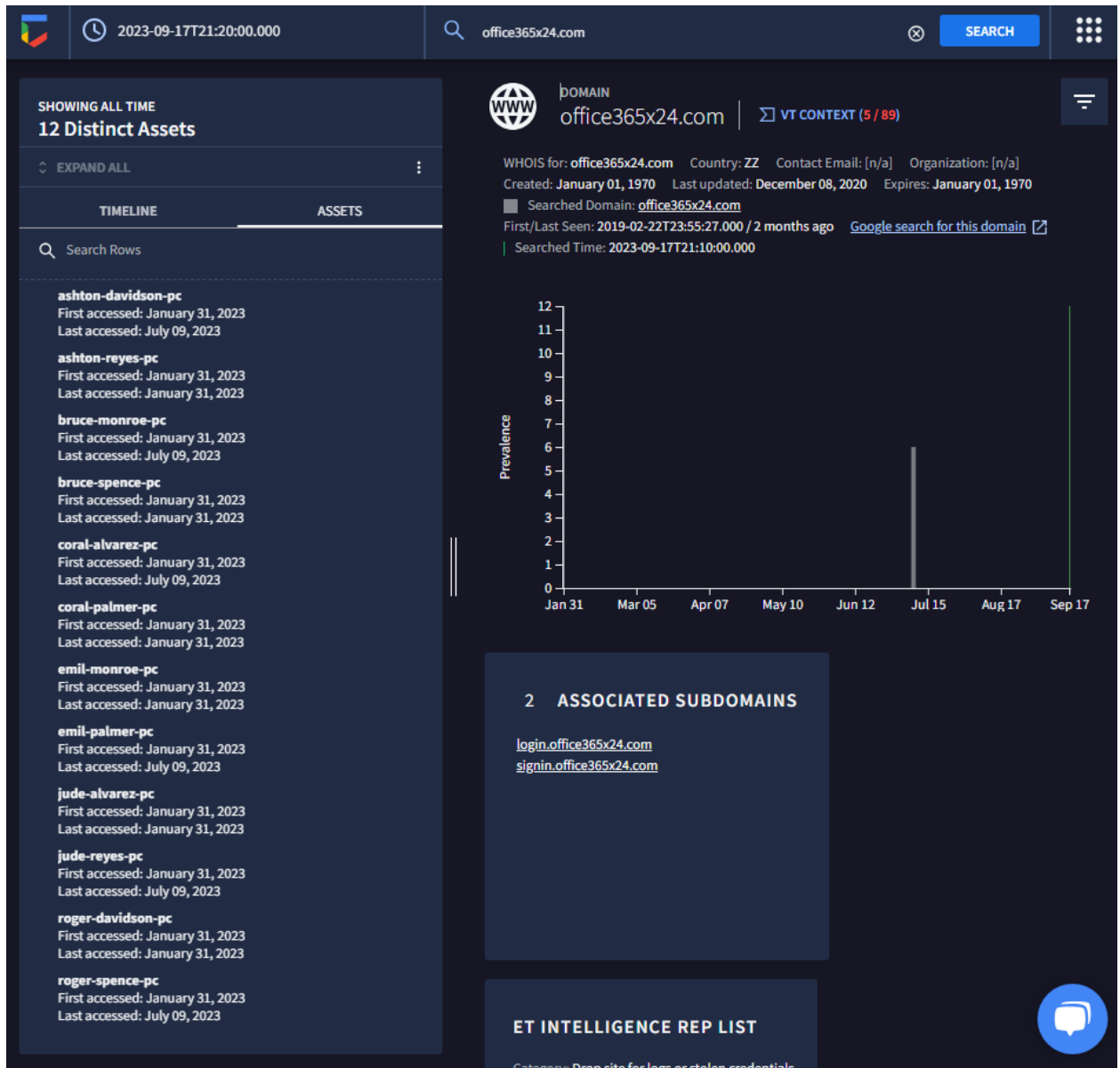
**SECURITY VENDORS SCANNING RESULTS**

Seclookup: <b>malicious</b>	CMC Threat Intelligence: <b>Undetected</b>
Snort IP sample list: <b>Undetected</b>	ViriBack: <b>Undetected</b>
K7AntiVirus: <b>Undetected</b>	

**WHOIS LOOKUP**

Admin City: New Delhi  
 Admin Country: IN  
 Admin Email: 9a6229aeb54b0cc2s@kamtrononline.com  
 Admin Organization: Kamtron Systems Pvt. Ltd.  
 Admin Postal Code: 110019  
 Admin State/Province: Delhi  
 Creation Date: 2015-04-05T08:47:39Z  
 DNSSEC: Unsigned  
 DNSSEC: unsigned  
 Domain Name: OFFICE365X24.COM  
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
 Name Server: DNS10.PARKPAGE.FOUNDATIONAPI.COM  
 Name Server: DNS11.PARKPAGE.FOUNDATIONAPI.COM

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.

2023-09-17T21:20:00.000 office365x24.com SEARCH

SHOWING ALL TIME 12 Distinct / 89

EXPAND ALL

ashton-david First accessed: Last accessed:

ashton-reyes First accessed: Last accessed:

bruce-monro First accessed: Last accessed:

bruce-spence First accessed: Last accessed:

coral-alvarez First accessed: Last accessed:

coral-palmer First accessed: Last accessed:

emil-monroe First accessed: Last accessed:

emil-palmer First accessed: Last accessed:

jude-alvarez First accessed: Last accessed:

jude-reyes-pc First accessed: Last accessed:

roger-david First accessed: Last accessed:

roger-spence-pc First accessed: January 31, 2023 Last accessed: July 09, 2023

DOMAIN office365x24.com VT CONTEXT (5 / 89)

Detections IoCs Graph Attribution VT Augment by VIRUSTOTAL

5 / 89

5 security vendors flagged this domain as malicious office365x24.com

Registrar PDR Ltd. d/b/a PublicDomainRegistry.com

Creation Date 8 years ago

Last Updated 3 years ago

Full report VT Graph

SECURITY VENDORS SCANNING RESULTS

Sophos: **malware** Seclookup: **malicious**

Xcitium Verdict Cloud: **malicious** CyRadar: **malicious**

Forcepoint ThreatSeeker: **malicious**

WHOIS LOOKUP

Admin City: New Delhi

Admin Country: IN

Admin Email: 9a6229aeb54b0cc2s@kamtrononline.com

Admin Organization: Kamtron Systems Pvt. Ltd.

Admin Postal Code: 110019

Admin State/Province: Delhi

Creation Date: 2015-04-05T08:47:39Z

DNSSEC: Unsigned

DNSSEC: unsigned

Domain Name: OFFICE365X24.COM

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Name Server: DNS10.PARKPAGE.FOUNDATIONAPI.COM

Name Server: DNS11.PARKPAGE.FOUNDATIONAPI.COM

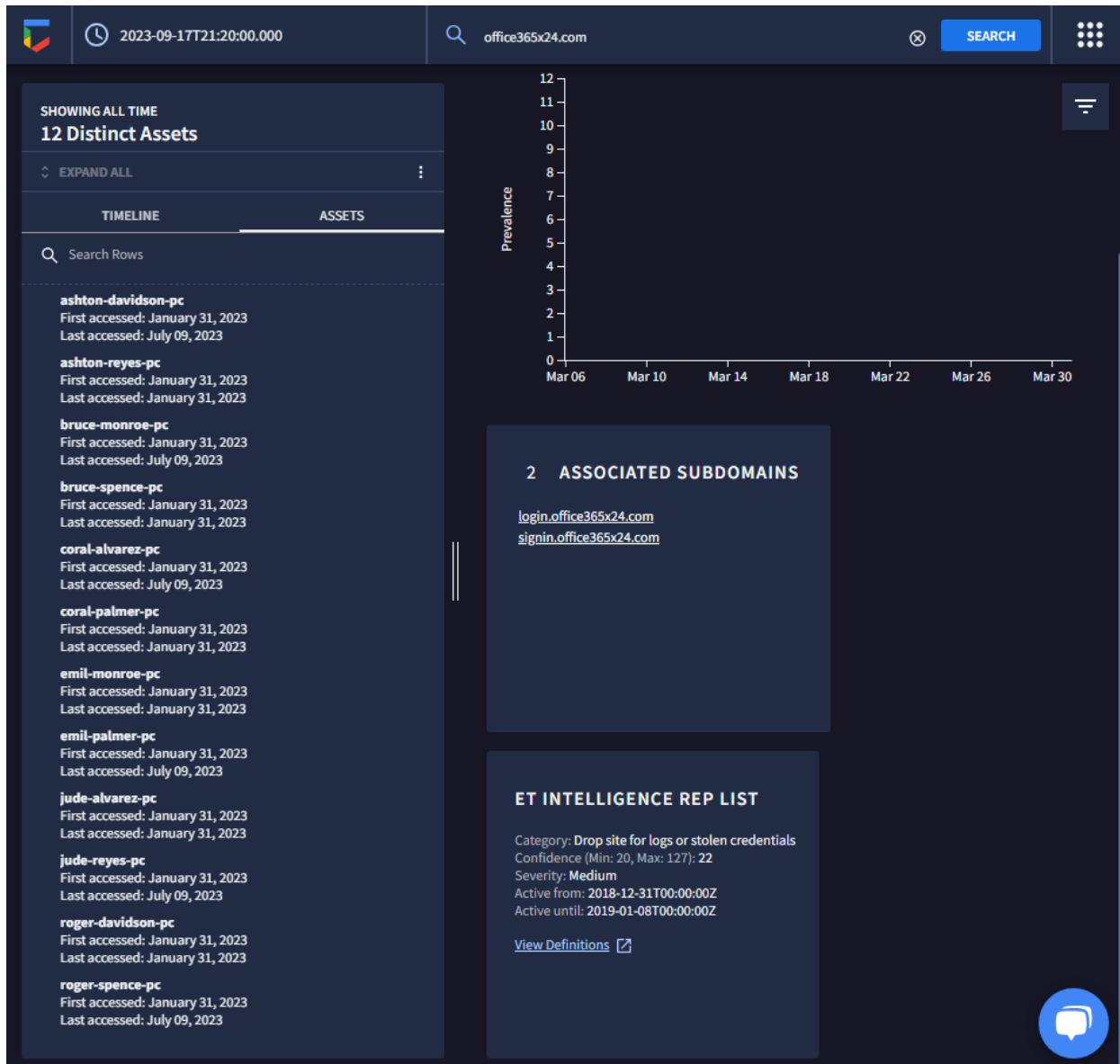
ET INTELLIGENCE REP LIST

Category: Drop site for logs or stolen credentials

https://www.virustotal.com

- 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.

The screenshot displays a network log viewer interface. On the left, a sidebar shows a list of events with columns for 'TIME', 'ASSET', and 'ACTION'. The main panel is titled 'NETWORK\_HTTP' and shows a detailed view of a specific event. The event is a POST request to the /login.php endpoint. The raw log data is displayed in a table format, showing the request details, including the client IP, user agent, and response status. The event is identified as a successful login attempt for the user 'ashton-davidson'.

TIME	ASSET	ACTION
14:40:40	ashton-davidson-pc	signin.office365x24.com
14:40:43	ashton-davidson-pc	signin.office365x24.com
14:41:10	jude-ryes-pc	signin.office365x24.com
14:41:15	coral-silvares-pc	signin.office365x24.com
14:42:14	emil-palmer-pc	signin.office365x24.com
14:42:45	emil-palmer-pc	signin.office365x24.com
14:43:49	bruce-monroe-pc	signin.office365x24.com
14:44:56	ragner-spence-pc	signin.office365x24.com

**Raw Log**

Time	Source	Destination	Protocol	Action	Request	Response
2023-01-31 14:40:45	ashton-davidson-pc	signin.office365x24.com	HTTP	Allowed	POST /login.php	200

**Event Details**

- event\_id: 223093606883153942
- protocol: HTTP
- action: Allowed
- transaction\_id: 75290
- response\_size: 19181
- request\_size: 983
- url\_category: Internet Services
- server\_ip: 48.100.174.34
- client\_transaction\_id: 4657
- request\_method: POST
- referrer: None
- user\_agent: Google Chrome (76.x)
- product: MS5
- location: Corp
- status: 200
- url: http://signin.office365x24.com/login.php
- vendor: Zscaler
- hostname: signin.office365x24.com
- client\_ip: 10.100.174.34
- threat\_category: None
- threat\_name: None
- file\_type: None
- application: General Browsing
- page\_id: 1380
- department: Default
- department\_urlsupercategory: Internet
- appliance: Business
- dlpengine: None
- urlclass: Business Use
- threatclass: None
- dictionary: None
- fileclass: None
- batchsize: NO
- server\_transaction\_id: 9001
- event\_timestamp: 2023-01-31 14:40:44
- client\_ip: 10.100.174.34
- user: ashton-davidson

**Metadata**

- metadata.product\_log\_id: "223093606883153942"
- metadata.event\_timestamp: "2023-01-31T14:40:45Z"
- metadata.event\_type: "NETWORK\_HTTP"
- metadata.vendor\_name: "Zscaler"
- metadata.product\_name: "MS5"
- metadata.requested\_timestamp: "2023-01-31T15:58:14.673865Z"
- metadata.id: "AAAAABGd+zEY+49MfGASDw2RgAAAAAQAAAAEAAA"
- additional\_fields["urlclass"]: "Business Use"
- additional\_fields["appliance"]: "Business"
- principal.hostname: "ashton-davidson-pc"
- principal.user.userid: "ashton-davidson"
- principal.user.department[0]: "Default Department"
- principal.ip[0]: "10.100.174.34"
- principal.mac[0]: "5a:8d:f9:89:31:a1"
- principal.application: "General Browsing"
- principal.location.name: "Corp"
- principal.asset.hostname: "ashton-davidson-pc"
- principal.asset.ip[0]: "10.100.174.34"
- principal.asset.mac[0]: "5a:8d:f9:89:31:a1"
- target.hostname: "signin.office365x24.com"
- target.ip[0]: "48.100.174.34"
- target.url: "https://signin.office365x24.com/login.php"
- target.asset.hostname: "signin.office365x24.com"
- target.asset.ip[0]: "48.100.174.34"
- security\_result[0].category\_details[0]: "Internet Services"
- security\_result[0].category\_details[1]: "Internet"
- security\_result[0].action[0]: "ALLOW"
- security\_result[0].action\_details: "Allowed"
- network.sent\_bytes: 983
- network.received\_bytes: 19181
- network.application\_protocol: "HTTP"
- network.http.method: "POST"
- network.http.user\_agent: "Google Chrome (76.x)"
- network.http.response\_code: 200

2023-01-31 09:40:00

SEARCH

SHOWING ALL TIME PERIOD

### 37 Events

COLLAPSE ALL WRAP TEXT

TIMELINE ASSETS

Q Search Rows

2019-02-22	ASSET IDENTIFIER	FQDN
23:55:27	10.0.29.22	office365x24.com
GET /	Port: (Unknown)	Resp. Code: 200 Resp. Size: 15...
23:55:42	10.0.29.22	office365x24.com
POST /login.php	Port: (Unknown)	Resp. Code: 200 Resp. Size: 15...
23:56:19	10.0.31.46	office365x24.com
GET /	Port: (Unknown)	Resp. Code: 200 Resp. Size: 15...
23:58:25	10.0.28.232	office365x24.com
GET /	Port: (Unknown)	Resp. Code: 200 Resp. Size: 15...
23:59:02	10.0.30.34	office365x24.com
GET /	Port: (Unknown)	Resp. Code: 200 Resp. Size: 15...
2023-01-31		
09:40:40	roger-davidson...	office365x24.com
GET /	Port: (Unknown)	Resp. Code: 200 Resp. Size: 15...

2023-01-31 09:40:40

### NETWORK\_HTTP

Raw Log Event/Entity

2023-01-31 09:40:40

Log Source: Zscaler

View as: Raw

Wrap Text

COPY RAW LOG

09:40:40.000

2023-01-31 09:40:48

reason=Allowed event\_id=2230936060803153941 protocol=HTTP action=Allow

d transactionSize=65298 responseSize=15188 requestSize=683 urlcategory=Internet Services

d serverip=199.59.243.222 clienttransitTime=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=1.2.180.101 threatCategory=None threatName=None appname=General Browsing pagerisk=100 department=De

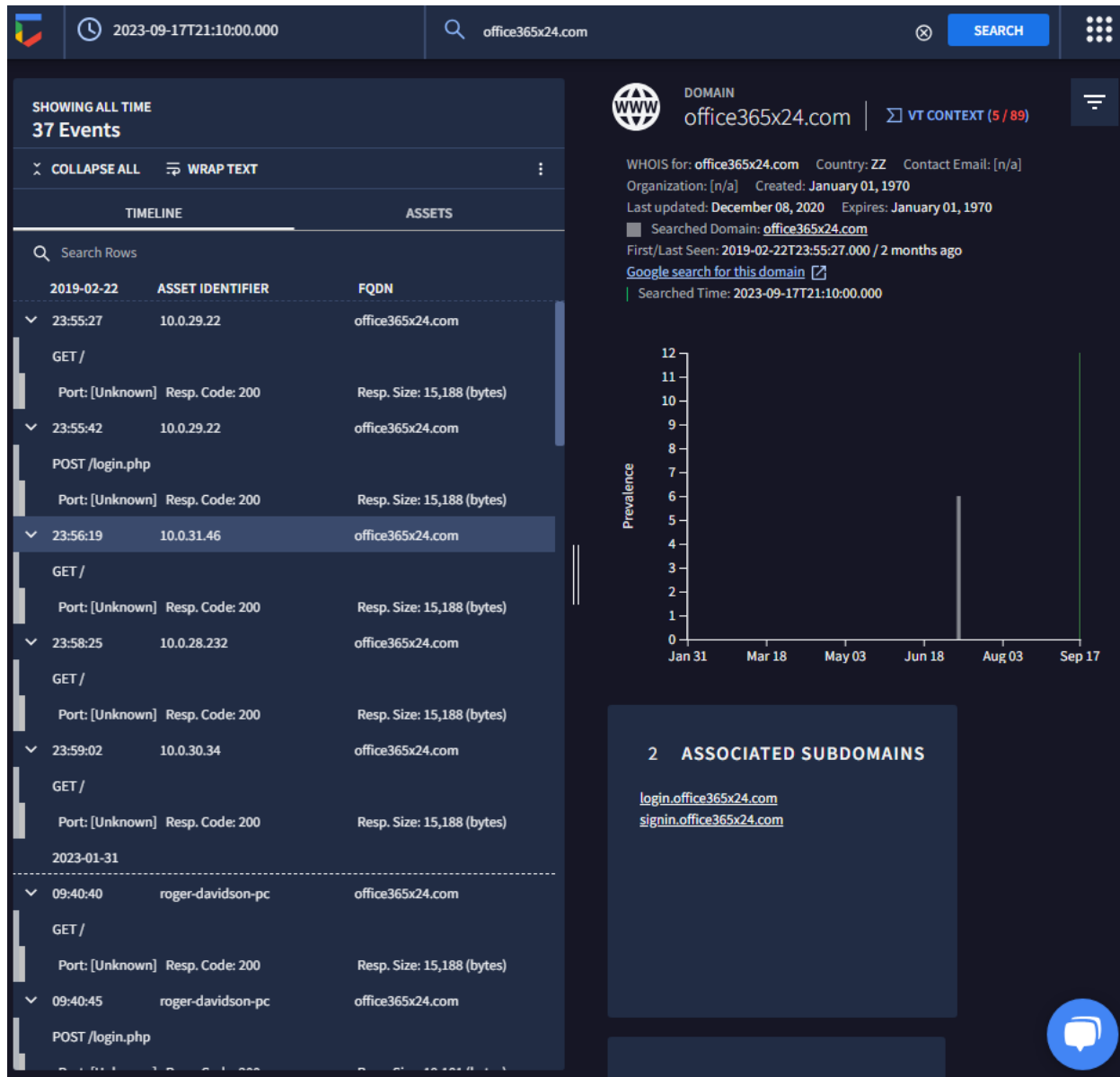
fault Department urlcategory=Internet appClass=Business durlName=None url=assBusiness Use threatClass=None dlpdictictionaries=None fileClass=None bwhrottle=NO

servertransitTime=7501 event\_timestamp=2023-01-31 09:40:48 clientIP=10.100.1.11 user=roger-da

vidson

0 selected COPY UDM

- Intermediate[id].ip[0]: "199.59.243.222"
- metadata.event\_timestamp: "2023-01-31T09:40:40Z"
- metadata.event\_type: "NETWORK\_HTTP"
- metadata.id: b"AAAAAGGVFA90/jbP17G2B4YMAAAABQAAAAAA"
- metadata.ingested\_timestamp: "2023-01-31T14:36:54.018049Z"
- metadata.product\_log\_id: "2230936060803153941"
- metadata.product\_name: "Zscaler NSS"
- 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]: "10.180.1.11"
- principal.user\_id: "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

**lamir-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

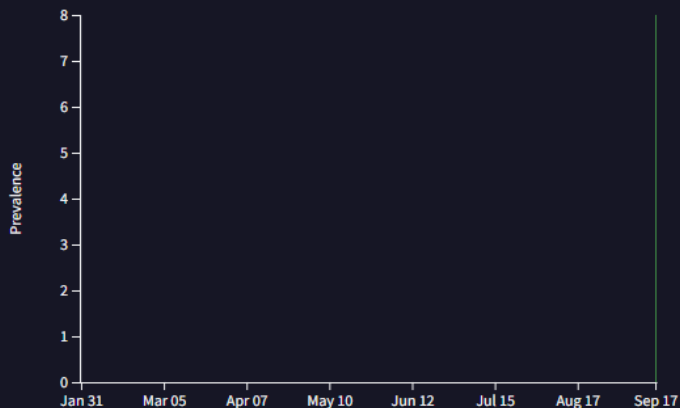
Reverse DNS: [n/a]

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



#### ESET THREAT INTELLIGENCE

Category: Blocked

Confidence: High

Severity: High

Active until: 2023-02-23T21:50:16Z

The screenshot shows the Chronicle interface with the IP address 40.100.174.34 selected. A 'Detections' overlay is displayed, showing that no security vendors flagged this IP address as malicious. The overlay also shows the location as GB - United Kingdom and provides links to the full report, similar IPs, and VT Graph. Below this, the 'SECURITY VENDORS SCANNING RESULTS' section lists several vendors (CMC Threat Intelligence, ViriBack, CINS Army, Snort IP sample list, K7AntiVirus) all marked as 'Undetected'. A 'WHOIS LOOKUP' section is also visible, showing details for the IP address block 38.0.0.0 - 40.168.255.255, including the netname 'NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK' and various remarks.

## 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. `signin.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.