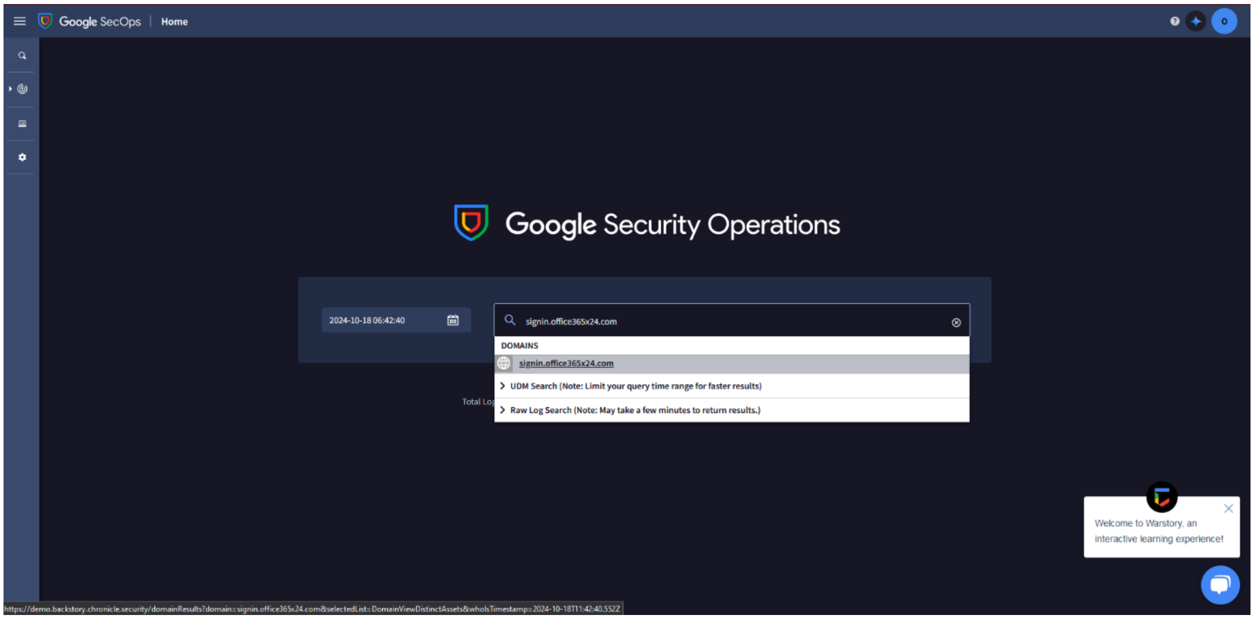
Performing Queries with Google Chronicle

In this project I am responding alert regarding a potential phishing email received by an employee. I investigate the suspicious domain, *signin.office365x24.com*, using Google Chronicle and also check whether other employees have received emails from it and whether they have visited it.

Performing a domain search

First, the domain is looked up using the main search bar of the Chronicle instance. A result pops-up under "DOMAINS" which shows that this domain exists within the data ingested by the SIEM.


Google SecOps
Home
Google Security Operations
Total Lo
DOMAINS
signin.office365x24.com
UDM Search (Note: Limit your query time range for faster results)
Raw Log Search (Note: May take a few minutes to return results.)

2024-10-18 06:42:40

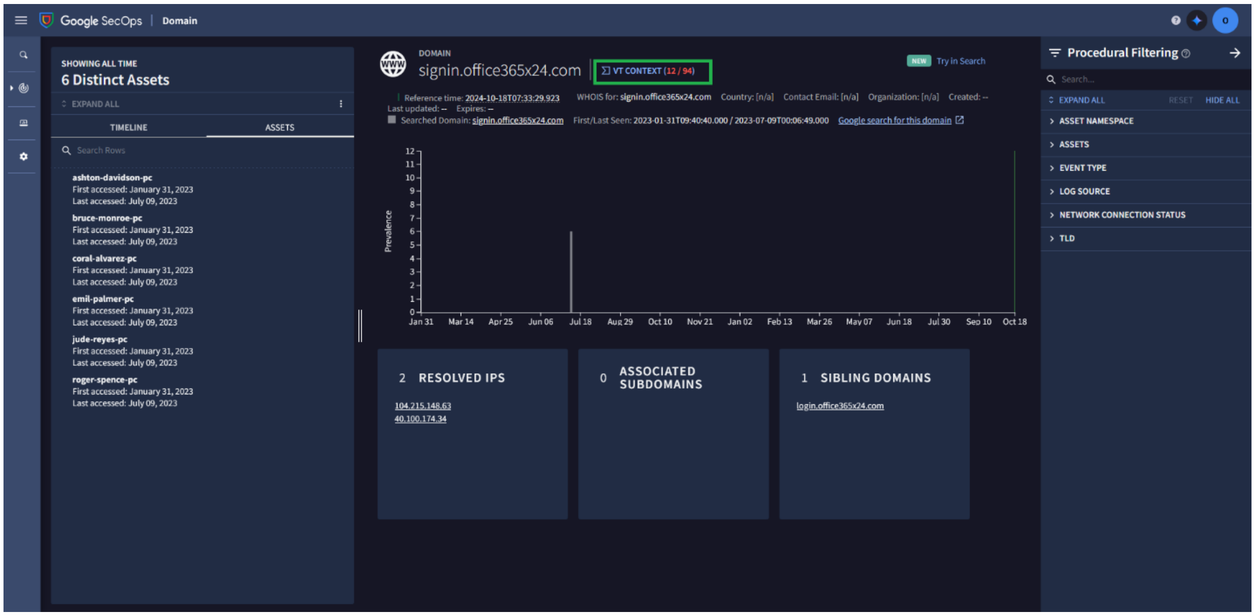
signin.office365x24.com

Welcome to Warstory, an interactive learning experience!

https://demo.backstory.chronicle.security/domainResults?domain=signin.office365x24.com&selectedList=DomainViewDistinctAssets&whoIsTimestamp=2024-10-18T11:42:40.552Z

Investigate threat intelligence data

Now that there is access to the search results, we need to identify whether the domain is malicious. In Google Chonicle, threat intelligence data can be viewed by clicking on the **VT CONTEXT** to analyse VirusTotal information about the domain.



SHOWING ALL TIME
6 Distinct Assets

ashton-davidson-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

bruce-monroe-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

coral-alvarez-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

emil-palmer-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

jude-reyes-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

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

DOMAIN
signin.office365x24.com | VT CONTEXT (12 / 94)

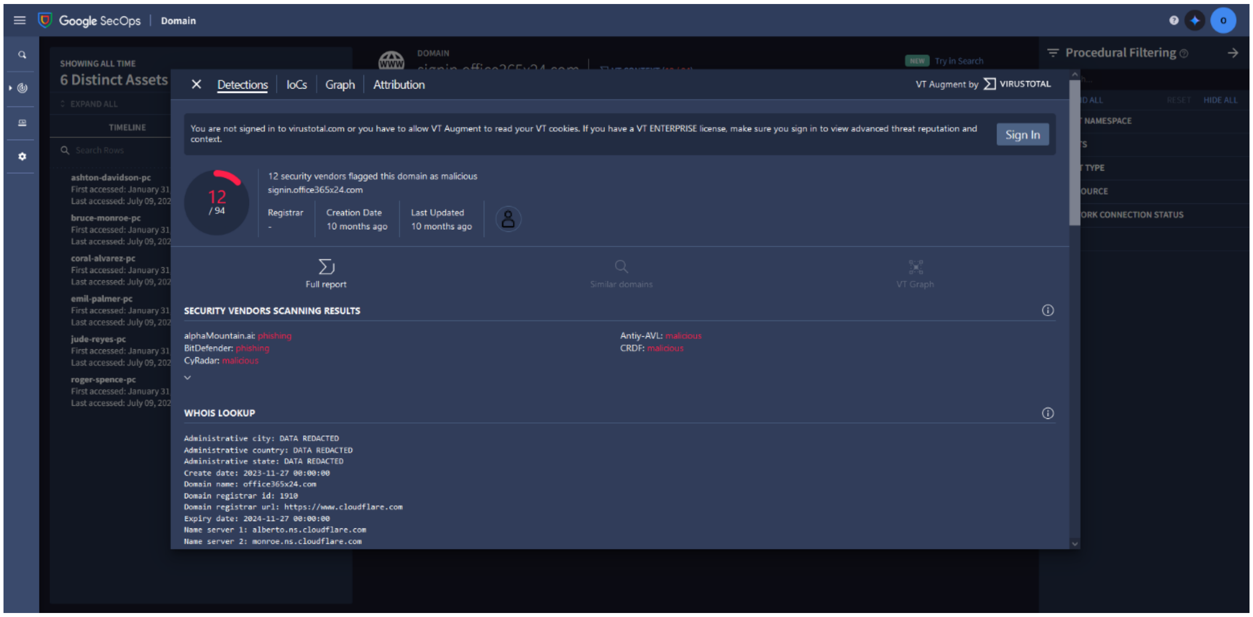
Reference time: 2024-10-18T07:33:29.923 WHOIS for: signin.office365x24.com Country: [n/a] Contact Email: [n/a] Organization: [n/a] Created: --
Last updated: -- Expires: --
Searched Domain: signin.office365x24.com First/Last Seen: 2023-01-31T09:40:40.000 / 2023-07-09T00:06:49.000 Google search for this domain

2 RESOLVED IPS
104.215.148.63
40.100.174.34

0 ASSOCIATED SUBDOMAINS

1 SIBLING DOMAINS
login.office365x24.com

Doing so shows us that 12 vendors have flagged this particular domain as malicious.



You are not signed in to virustotal.com or you have to allow VT Augment to read your VT cookies. If you have a VT ENTERPRISE license, make sure you sign in to view advanced threat reputation and context.

12 / 94

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

Registrar: -
Creation Date: 10 months ago
Last Updated: 10 months ago

SECURITY VENDORS SCANNING RESULTS

alphaMountain.ai: phishing
BitDefender: phishing
CyRadar: malicious
Antiy-AVL: malicious
CRDF: malicious

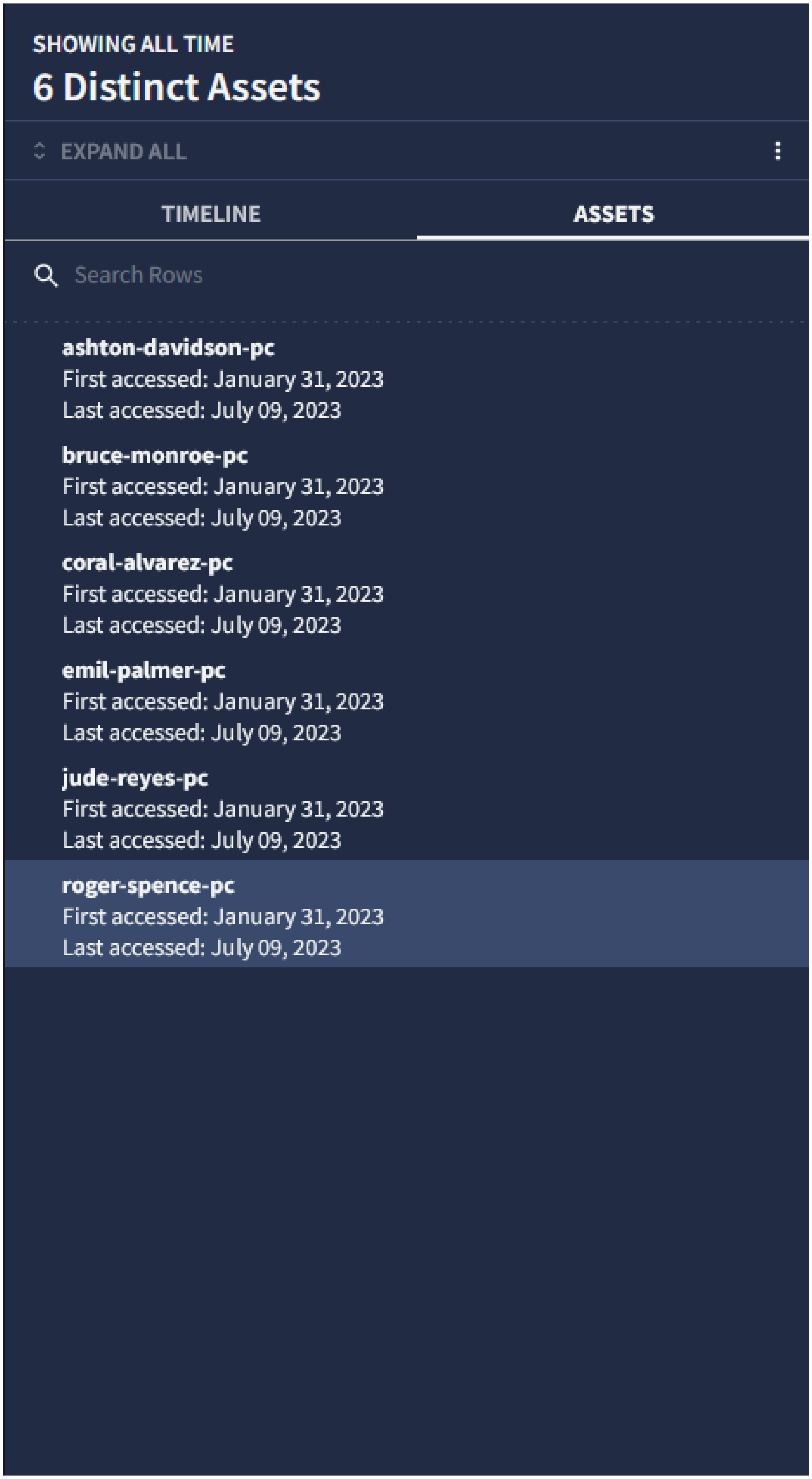
WHOIS LOOKUP

```
Administrative city: DATA REDACTED
Administrative country: DATA REDACTED
Administrative state: DATA REDACTED
Create date: 2023-11-27 00:00:00
Domain name: office365x24.com
Domain registrar id: 1910
Domain registrar url: https://www.cloudflare.com
Expiry date: 2024-11-27 00:00:00
Name server 1: alberto.ns.cloudflare.com
Name server 2: monroe.ns.cloudflare.com
```

Investigating affected assets and events

On the left side of the domain view page, we can see events and assets related to this domain on the **TIMELINE** and **ASSETS** tabs. **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.

On the **ASSETS** tab we can see that 5 assets have have accessed this domain on the same day: **ashton-davidson-pc**, **bruce-monroe-pc**, **coral-alvarez-pc**, **emil-palmer-pc**, **jude-reyes-pc, and roger-spence-pc**.



ashton-davidson-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

bruce-monroe-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

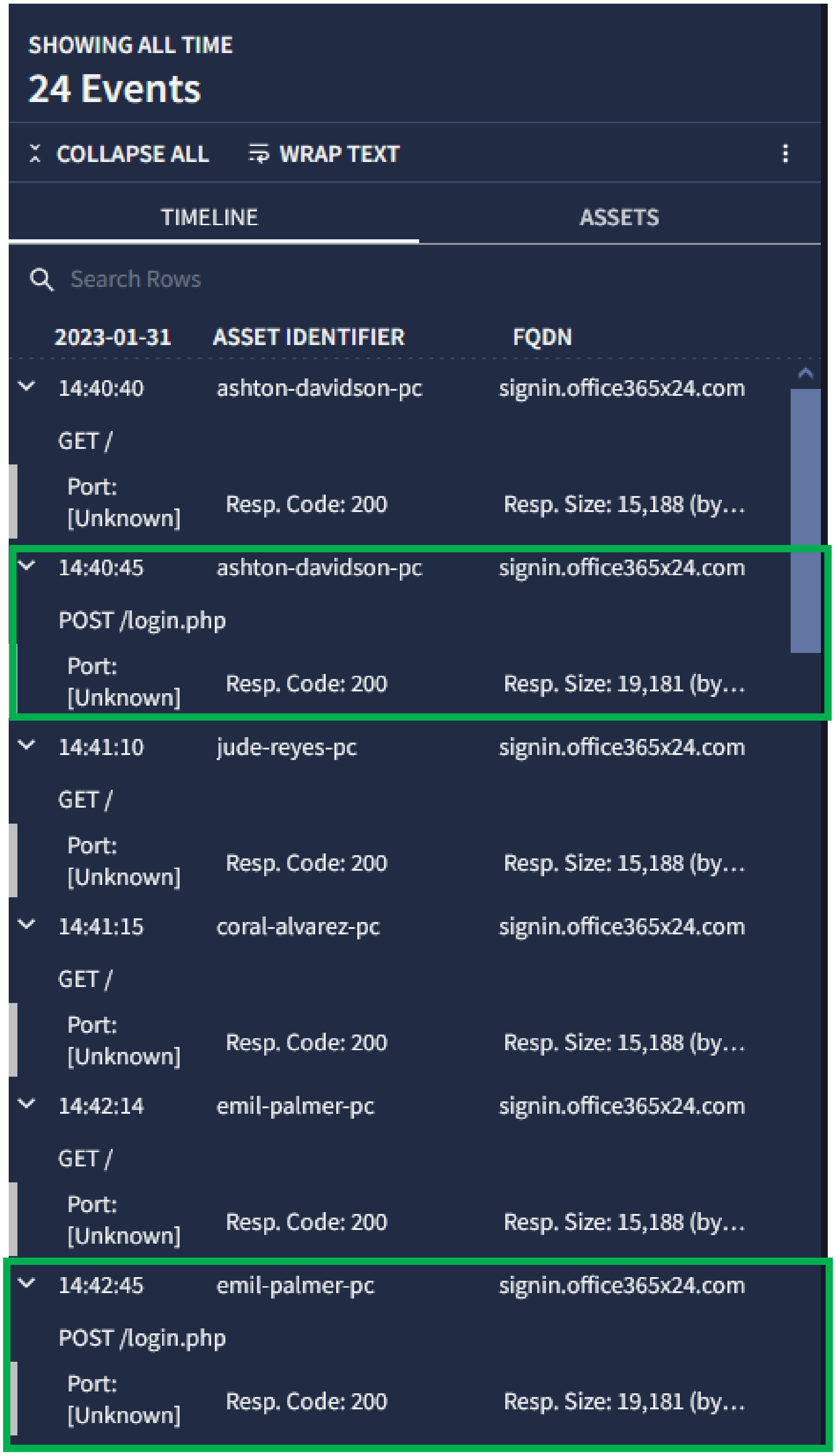
coral-alvarez-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

emil-palmer-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

jude-reyes-pc
First accessed: January 31, 2023
Last accessed: July 09, 2023

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

On the **TIMELINE** tab, clicking on **EXPAND ALL** reveals details about the HTTP requests made, including *GET* and *POST* requests. The more critical infromation here are the *POST* requests to the */login.php* page, because these may indicate a successful phishing attempt.

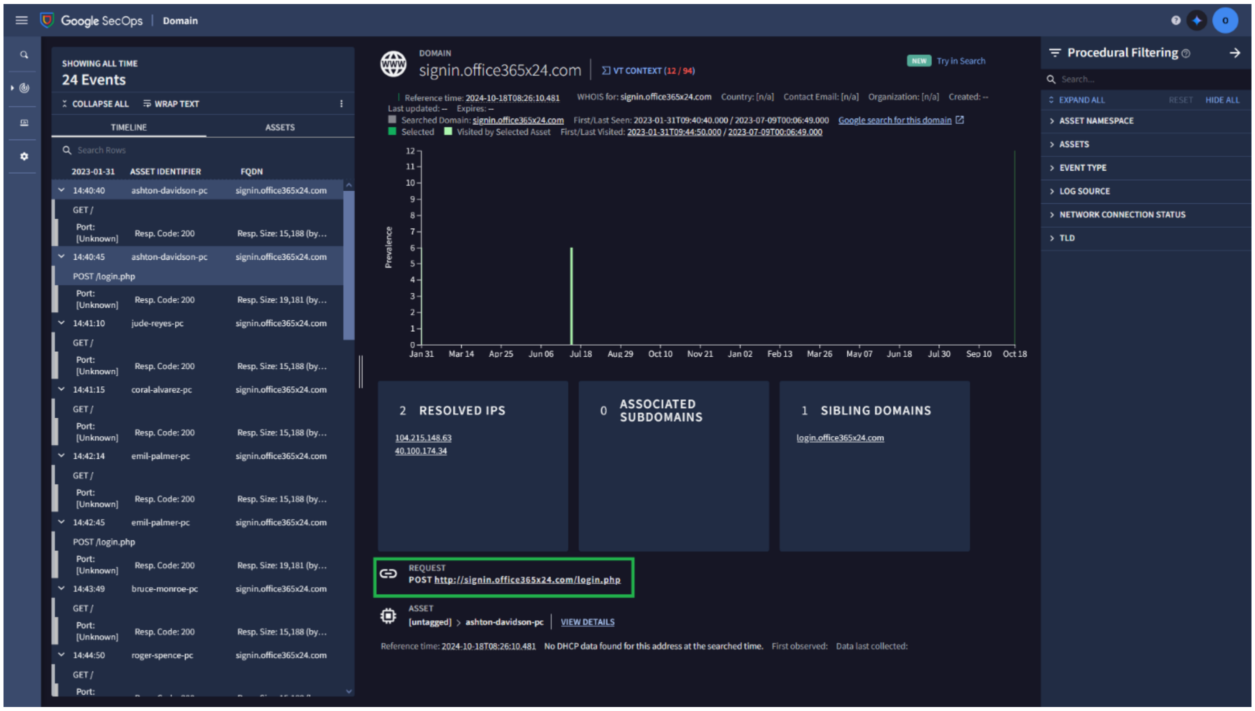


SHOWING ALL TIME

24 Events

2023-01-31	ASSET IDENTIFIER	FQDN
14:40:40	ashton-davidson-pc	signin.office365x24.com
GET /		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 15,188 (by…
14:40:45	ashton-davidson-pc	signin.office365x24.com
POST /login.php		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 19,181 (by…
14:41:10	jude-reyes-pc	signin.office365x24.com
GET /		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 15,188 (by…
14:41:15	coral-alvarez-pc	signin.office365x24.com
GET /		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 15,188 (by…
14:42:14	emil-palmer-pc	signin.office365x24.com
GET /		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 15,188 (by…
14:42:45	emil-palmer-pc	signin.office365x24.com
POST /login.php		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 19,181 (by…

We identify 2 *POST* requests, one from **ashton-davidson-pc**, and one from **emil-palmer-pc** meaning that these two users' credentails may have been compromized. Clicking on any of these post requests shows that the target URL of the web page that the *POST* requests were made to is http://signin.office365x24.com/login.php.



SHOWING ALL TIME
24 Events

```
2023-01-31  ASSET IDENTIFIER     FQDN
14:40:40    ashton-davidson-pc   signin.office365x24.com
  GET /
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 15,188 (by…
14:40:45    ashton-davidson-pc   signin.office365x24.com
  POST /login.php
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 19,181 (by…
14:41:10    jude-reyes-pc        signin.office365x24.com
  GET /
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 15,188 (by…
14:41:15    coral-alvarez-pc     signin.office365x24.com
  GET /
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 15,188 (by…
14:42:14    emil-palmer-pc       signin.office365x24.com
  GET /
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 15,188 (by…
14:42:45    emil-palmer-pc       signin.office365x24.com
  POST /login.php
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 19,181 (by…
14:43:49    bruce-monroe-pc      signin.office365x24.com
  GET /
  Port: [Unknown]   Resp. Code: 200   Resp. Size: 15,188 (by…
14:44:50    roger-spence-pc      signin.office365x24.com
  GET /
  Port:
```

DOMAIN
signin.office365x24.com | VT CONTEXT (12 / 94)

Reference time: 2024-10-18T08:26:10.481 WHOIS for: signin.office365x24.com Country: [n/a] Contact Email: [n/a] Organization: [n/a] Created: --
Last updated: -- Expires: --
▨ Searched Domain: signin.office365x24.com First/Last Seen: 2023-01-31T09:40:40.000 / 2023-07-09T00:06:49.000 Google search for this domain
🟩 Selected 🟩 Visited by Selected Asset First/Last Visited: 2023-01-31T09:44:50.000 / 2023-07-09T00:06:49.000

2 RESOLVED IPS
104.215.148.63
40.100.174.34

0 ASSOCIATED SUBDOMAINS

1 SIBLING DOMAINS
login.office365x24.com

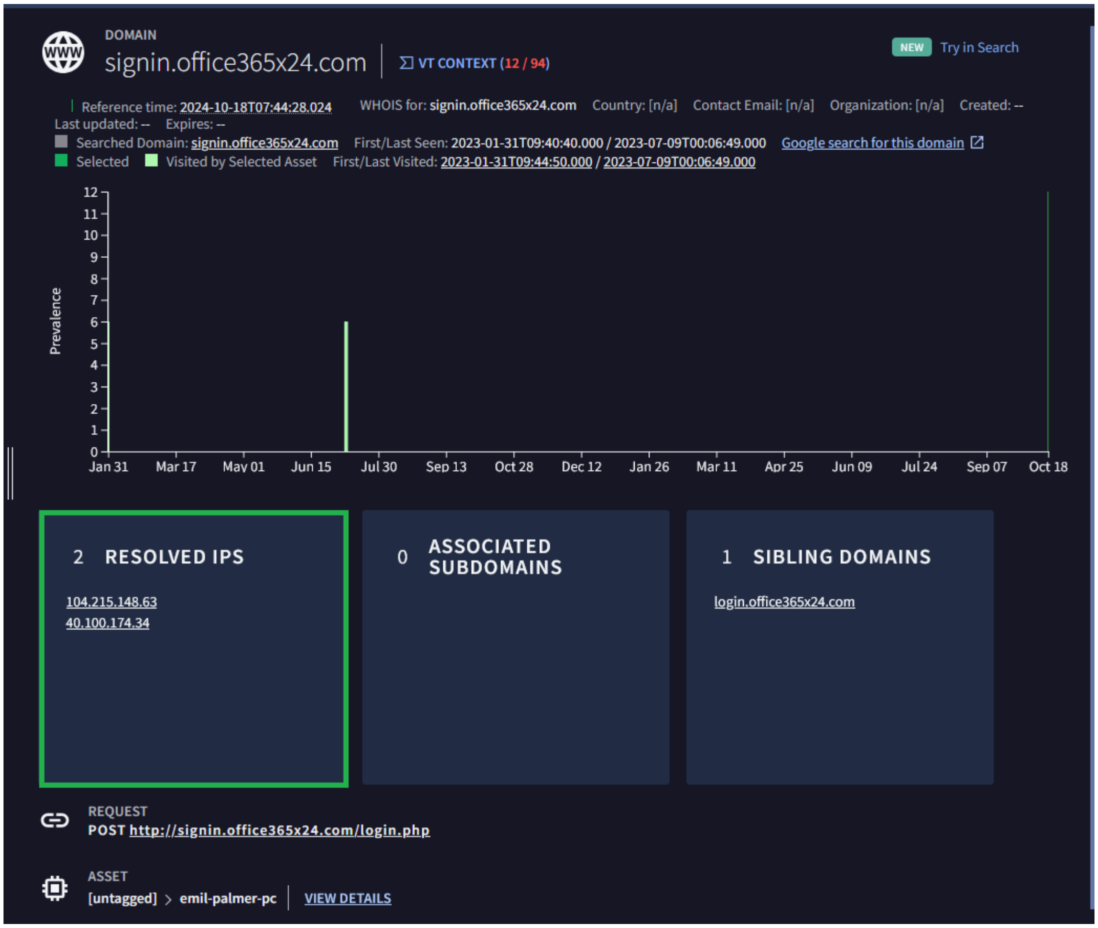
REQUEST
POST http://signin.office365x24.com/login.php

ASSET
[untagged] > ashton-davidson-pc

Reference time: 2024-10-18T08:26:10.481 No DHCP data found for this address at the searched time. First observed: Data last collected:

Investigating the resolved IP address

There is one more thing to do before concluding the investigation. Since attackers usually reuse the same infrastructure for multiple attacks, it is possible that multiple domain names resolve to the same IP address. We can go under the **RESOLVED IPS** insight card to identify if the *signin.office365x24.com* domain uses another domain.



DOMAIN

signin.office365x24.com

Reference time: 2024-10-18T07:44:28.024 WHOIS for: signin.office365x24.com Country: [n/a] Contact Email: [n/a] Organization: [n/a] Created: --
Last updated: -- Expires: --

Searched Domain: signin.office365x24.com First/Last Seen: 2023-01-31T09:40:40.000 / 2023-07-09T00:06:49.000

Selected Visited by Selected Asset First/Last Visited: 2023-01-31T09:44:50.000 / 2023-07-09T00:06:49.000

2 RESOLVED IPS

104.215.148.63
40.100.174.34

0 ASSOCIATED SUBDOMAINS

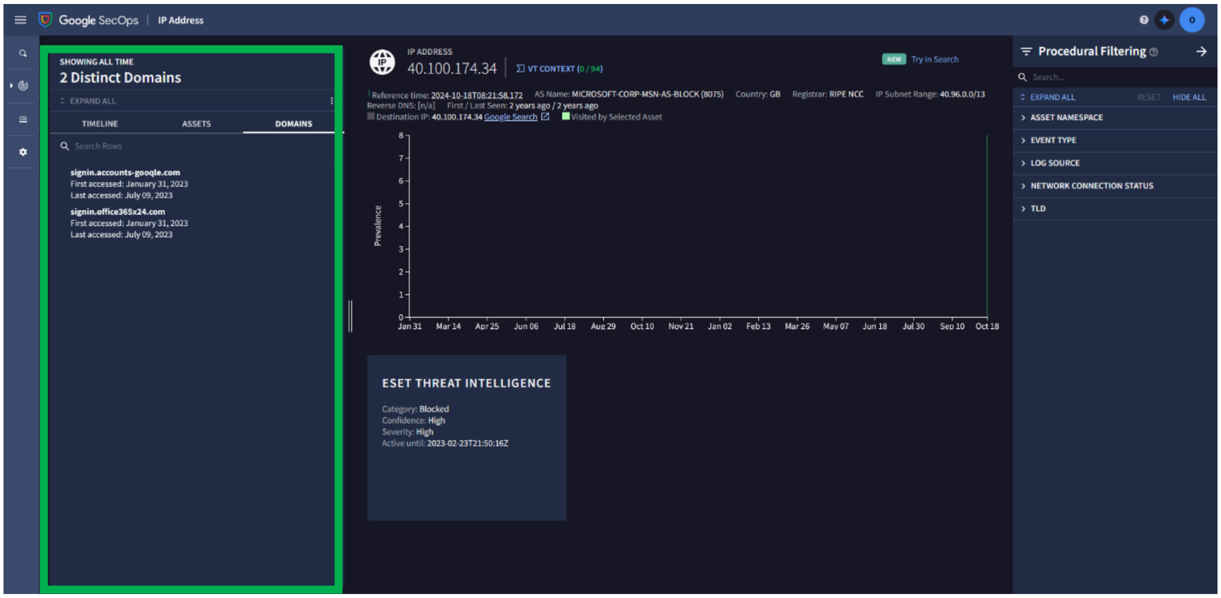
1 SIBLING DOMAINS

login.office365x24.com

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

ASSET
[untagged] > emil-palmer-pc

In this lab, querying for both *104.215.148.63* and *40.100.174.34* gives almost identical results, so in this case, let's take a look at *40.100.174.34* and select the **DOMAINS** tab. We can see that *40.100.174.34* resolves to both *signin.accounts-googqle.com* and *signin.office365x24.com*.



SHOWING ALL TIME
2 Distinct Domains

signin.accounts-googqle.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

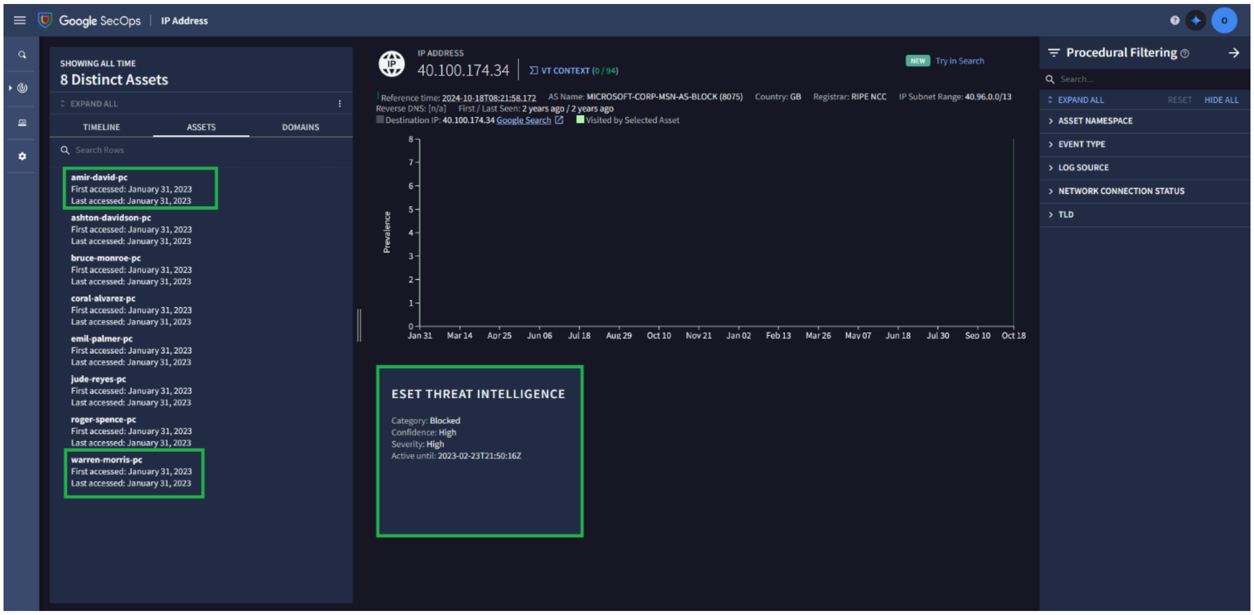
Reference time: 2024-10-18T08:21:58.172 AS Name: MICROSOFT-CORP-MSN-AS-BLOCK (8075) Country: GB Registrar: RIPE NCC IP Subnet Range: 40.96.0.0/13
Reverse DNS: [n/a] First / Last Seen: 2 years ago / 2 years ago
Destination IP: 40.100.174.34 Google Search Visited by Selected Asset

ESET THREAT INTELLIGENCE

Category: Blocked
Confidence: High
Severity: High
Active until: 2023-02-23T21:50:16Z

Let’s see if we can find any additonal infromation on the results page for this IP address that could help us with our investigation:

In the **ASSETS** tab we find that 2 additional assets have interacted with this malicious IP – **amir-david.pc** and **warren-morris-pc**. The **ESET THREAT INTELLIGENCE** insight card further confirms with high confidence that this IP address is indeed malicious and should be blocked.



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

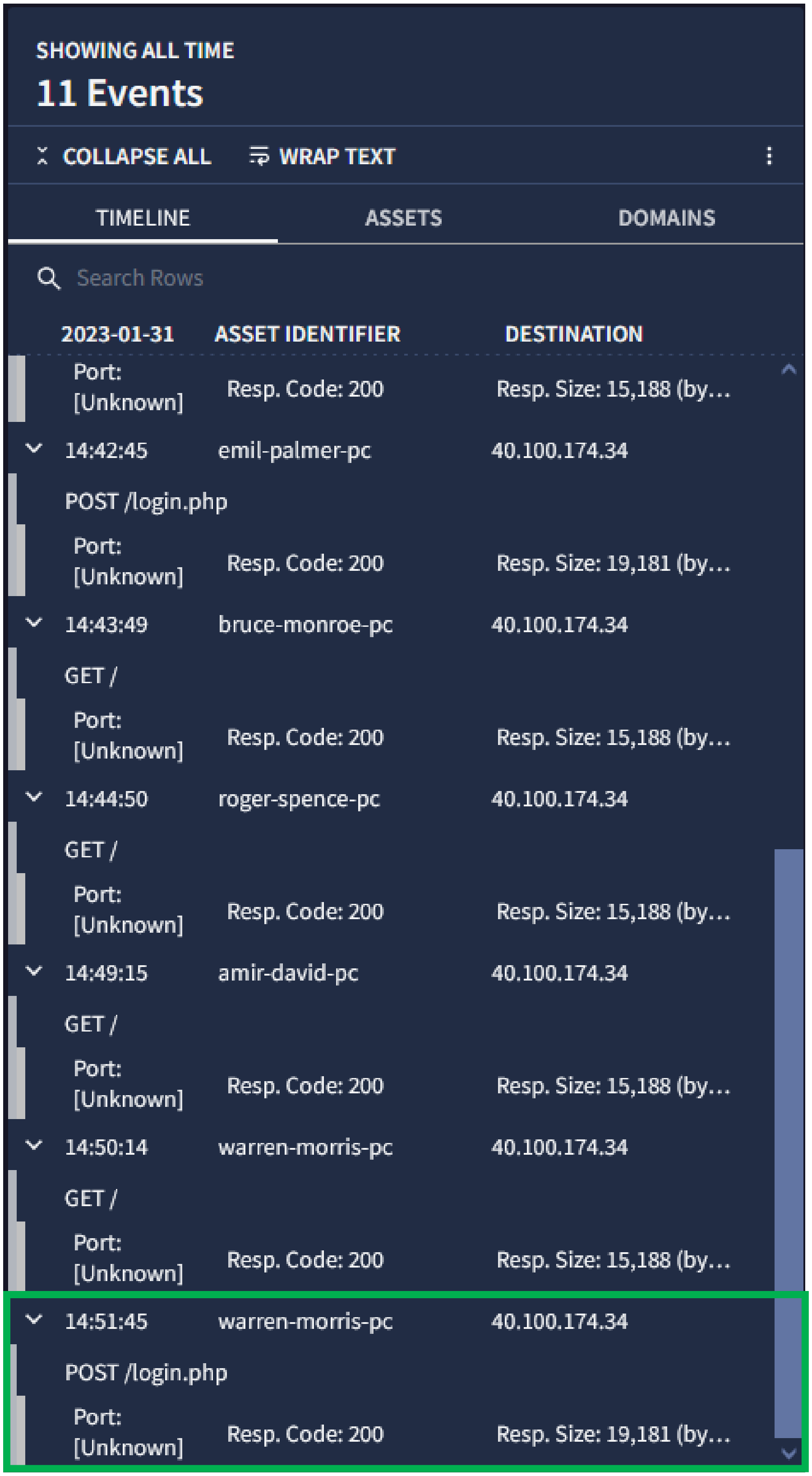
warren-morris-pc
First accessed: January 31, 2023
Last accessed: January 31, 2023

Reference time: 2024-10-18T08:21:58.172 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: 2 years ago / 2 years ago
Destination IP: 40.100.174.34 Google Search 🟩 Visited by Selected Asset

ESET THREAT INTELLIGENCE

Category: Blocked
Confidence: High
Severity: High
Active until: 2023-02-23T21:50:16Z

Clicking on **EXPAND ALL** on the **TIMELINE** tab reveals that an additioanal user’s credentials may have been compromised – **warren-morris-pc** has also made a *POST* request to this IP address.



```
   2023-01-31   ASSET IDENTIFIER   DESTINATION
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 15,188 (by...
   14:42:45     emil-palmer-pc     40.100.174.34
   POST /login.php
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 19,181 (by...
   14:43:49     bruce-monroe-pc    40.100.174.34
   GET /
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 15,188 (by...
   14:44:50     roger-spence-pc    40.100.174.34
   GET /
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 15,188 (by...
   14:49:15     amir-david-pc      40.100.174.34
   GET /
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 15,188 (by...
   14:50:14     warren-morris-pc   40.100.174.34
   GET /
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 15,188 (by...
   14:51:45     warren-morris-pc   40.100.174.34
   POST /login.php
   Port:
   [Unknown]    Resp. Code: 200    Resp. Size: 19,181 (by...
```

A more thorough investigation has thus allowed for a more accurate estimation of the scope of the phishing attack and its potential consequences.