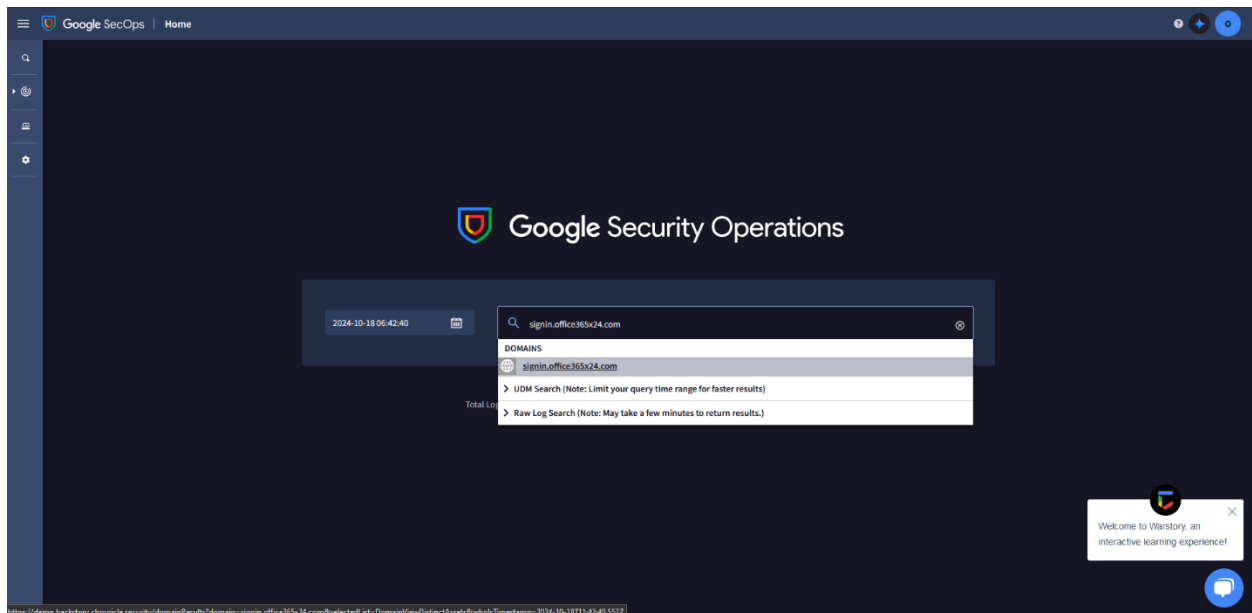


Performing Queries with Google Chronicle

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.

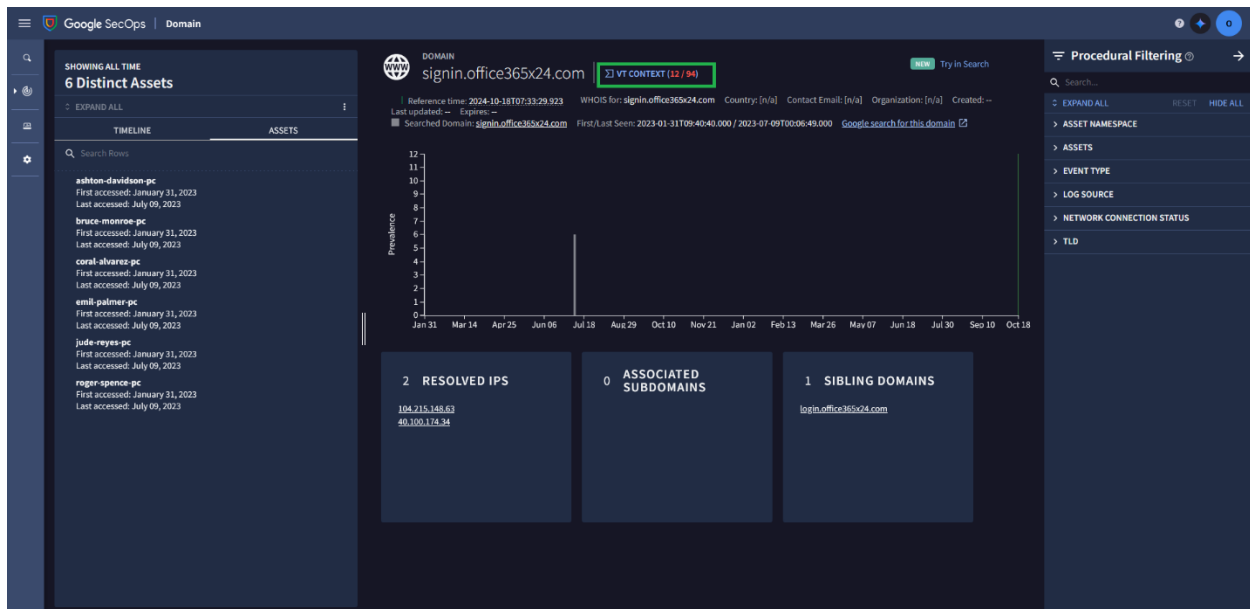
Performing a domain search

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.

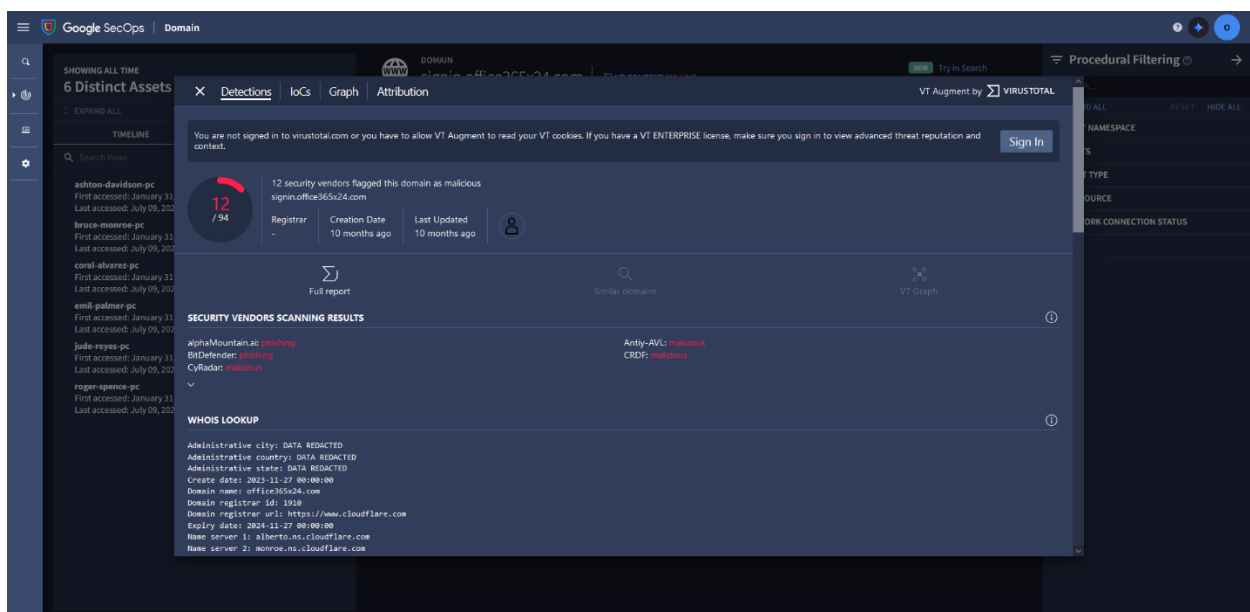


Investigate Threat Intelligence Data

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



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



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 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**.

SHOWING ALL TIME

6 Distinct Assets

EXPAND ALL



TIMELINE

ASSETS

Search Rows

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 information here are the *POST* requests to the */login.php* page, because these may indicate a successful phishing attempt.

SHOWING ALL TIME

24 Events

✕ COLLAPSE ALL

⇌ WRAP TEXT

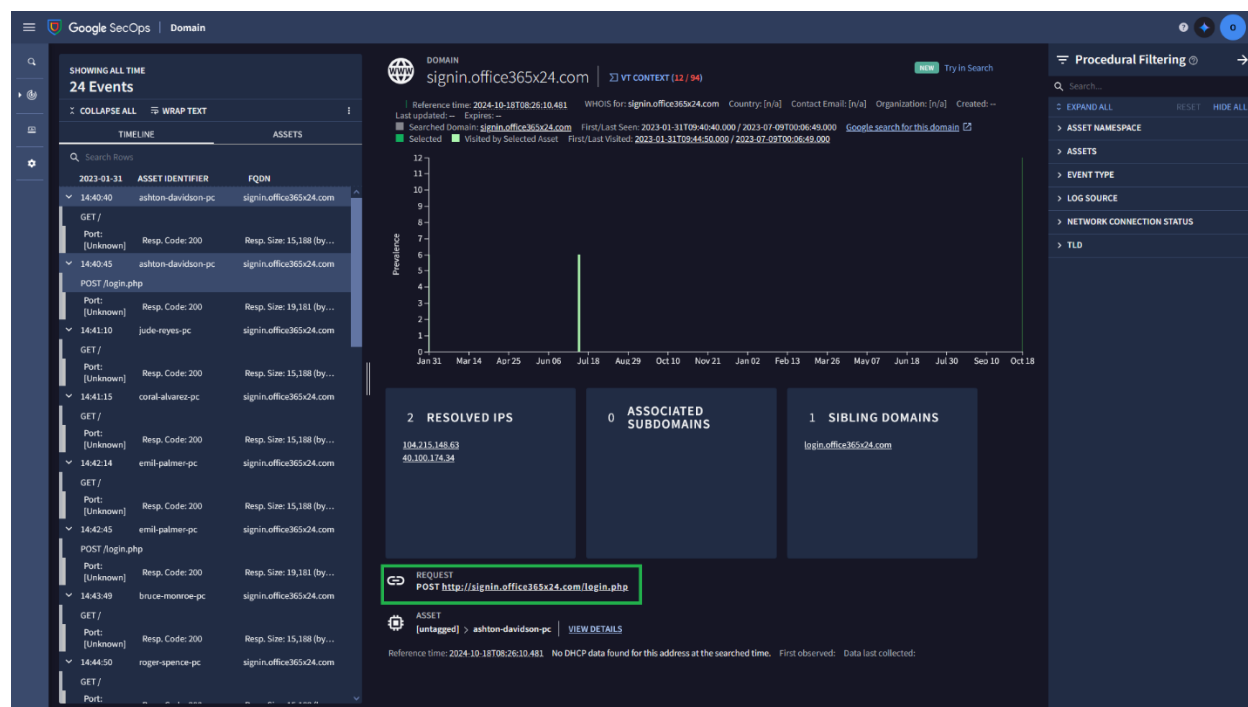
TIMELINE

ASSETS

🔍 Search Rows

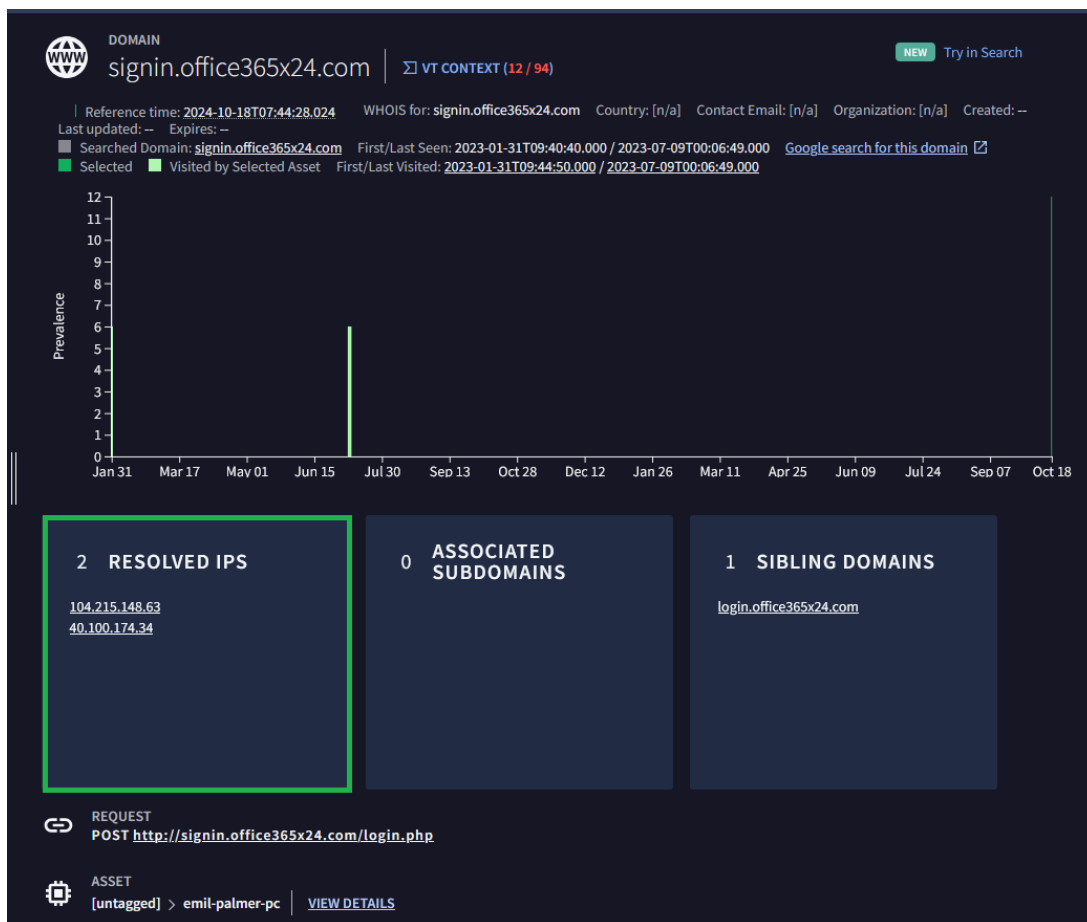
2023-01-31	ASSET IDENTIFIER	FQDN
▼ 14:40:40	ashton-davidson-pc	signin.office365x24.com
GET /		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 15,188 (by...
▼ 14:40:45	ashton-davidson-pc	signin.office365x24.com
POST /login.php		
Port: [Unknown]	Resp. Code: 200	Resp. Size: 19,181 (by...
▼ 14:41:10	jude-reyes-pc	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' credentials may have been compromised. 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>.

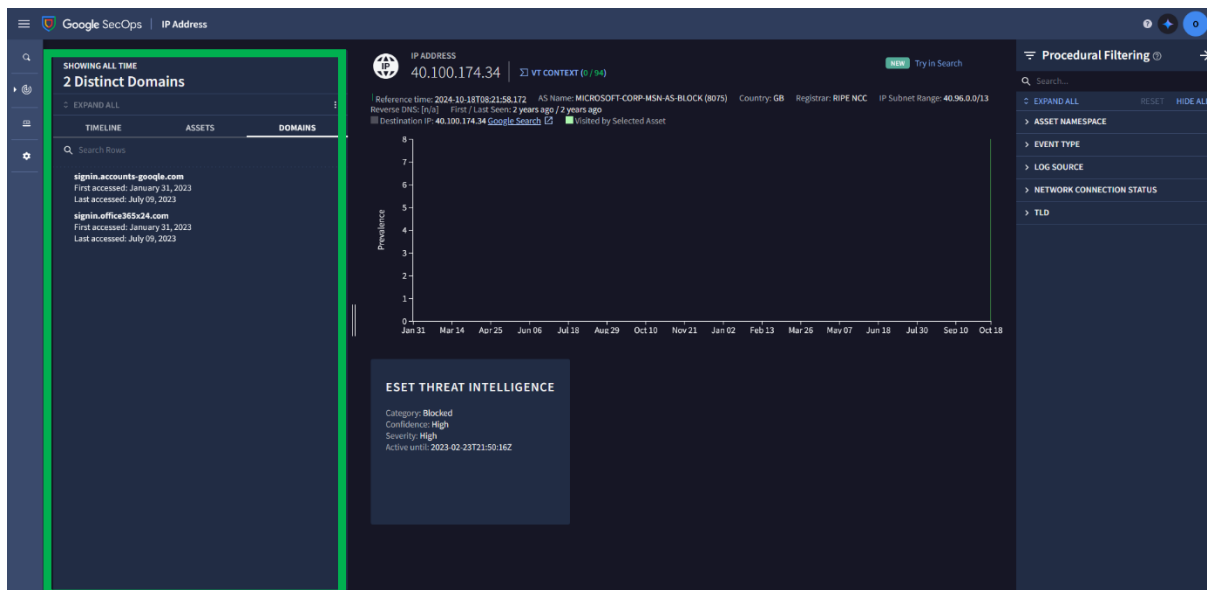


Investigating the Resolved IP Address

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.

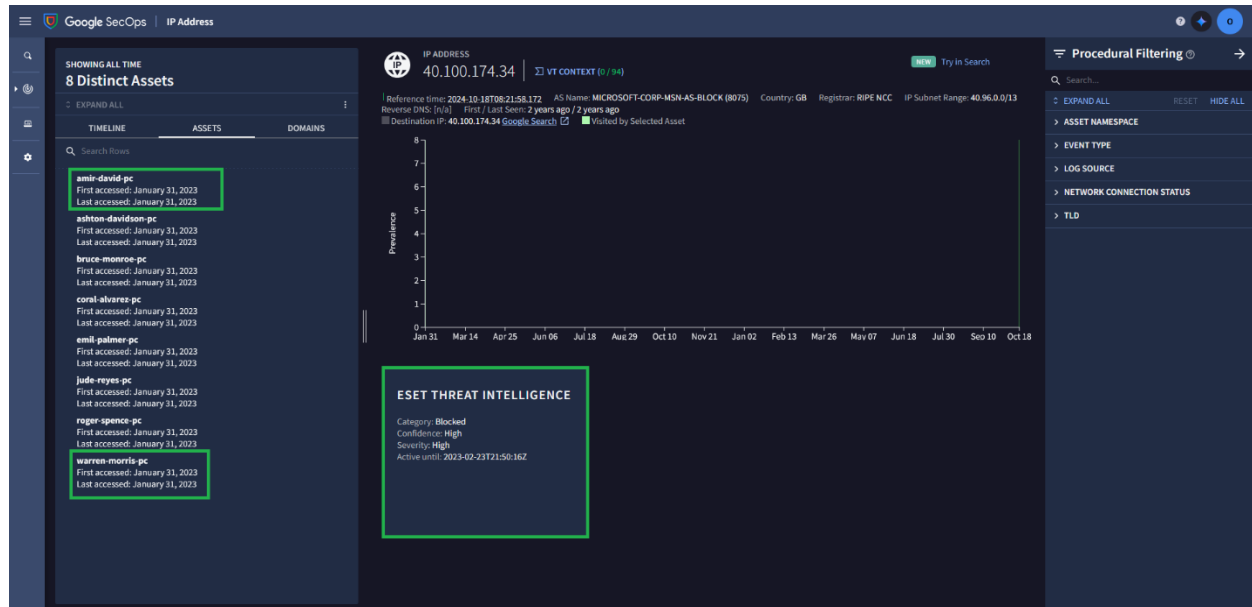


In this lab, querying for both *104.215.148.63* and *40.100.174.34* gives almost identical results, so in this case, let's take a look at *40.100.174.34* and select the **DOMAINS** tab. We can see that *40.100.174.34* resolves to both *signin.accounts-google.com* and *signin.office365x24.com*.



Let's see if we can find any additional information 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.



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

SHOWING ALL TIME

11 Events

✕ COLLAPSE ALL

⇌ WRAP TEXT

TIMELINE

ASSETS

DOMAINS

🔍 Search Rows

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.