Perform a query with Chronicle

Overview

Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyze, and search the massive amounts of security and network telemetry they generate.

Scenario

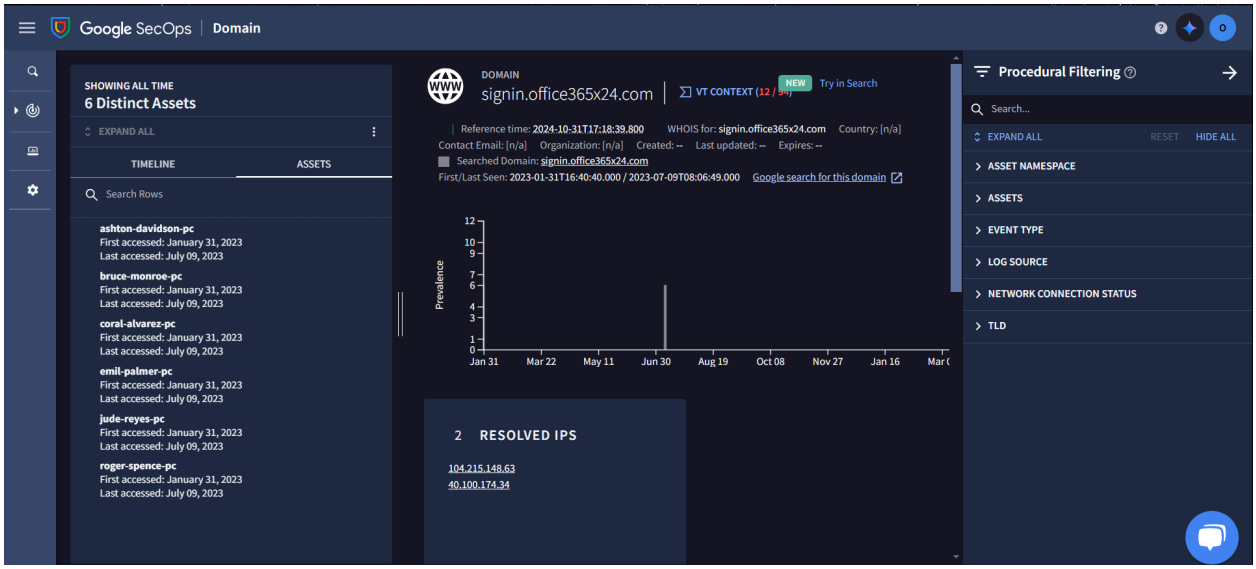
I was working as a security analyst at a financial services company when an alert popped up. An employee had received a suspicious email in their inbox. Reviewing the alert, I spotted a red flag: a strange domain name embedded in the email body: `signin.office365x24.com`. This didn't look right. To see if this was a wider phishing attempt, I decided to use Chronicle to investigate how many other employees might have been targeted and if anyone had actually visited this suspicious domain.

First Steps

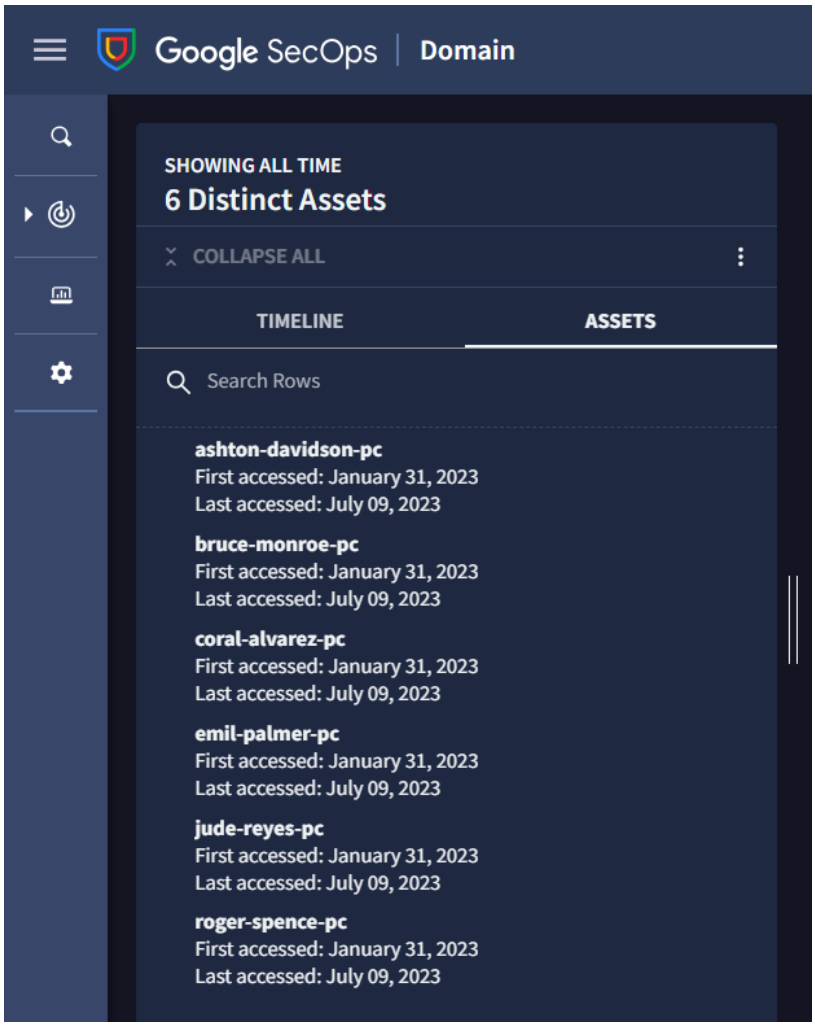
1. Launch Chronicle.
2. In the search bar, type `signin.office365x24.com` and click *Search*. Under ***DOMAINS***, `signin.office365x24.com` will be listed. This tells you that the domain exists in the ingested data.
3. Click `signin.office365x24.com` to complete the search.

Task 1. Evaluate the search results.

1. Below are the screenshots of the legacy view, VT(`VirusTotal`), and resolved IP addresses `104.215.148.63` and `40.100.174.34`.

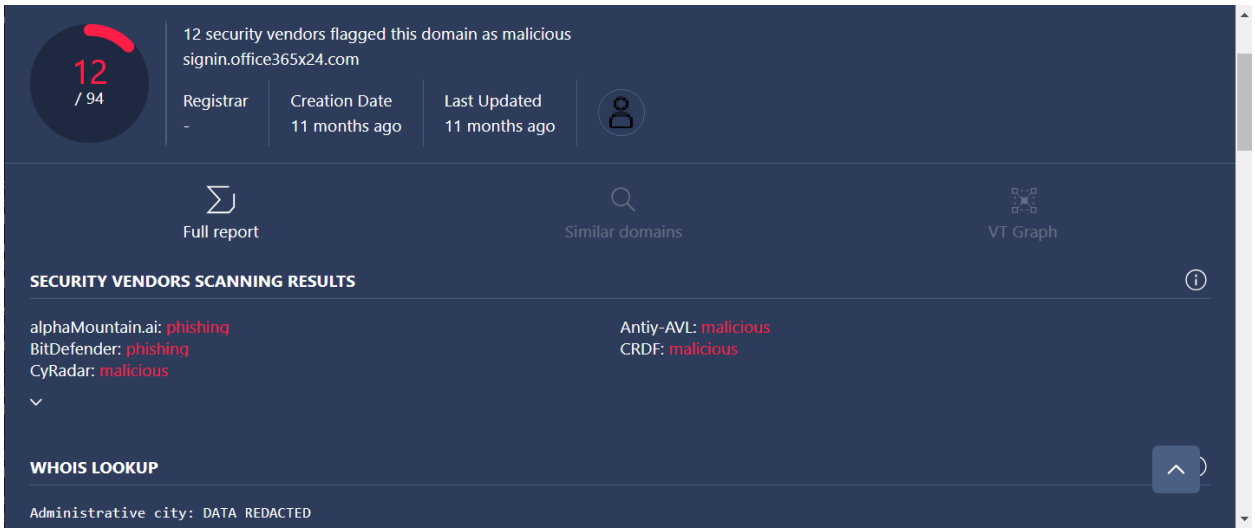


2. Next I click the ***ASSETS*** tab. This tab provides a list of the assets that have accessed the domains.



Task 2. Analyze the threat intelligence data.

1. I clicked ***VT CONTEXT*** to assess the VirusTotal information about this domain. In the pop-up, I observed that twelve vendors had flagged this domain as malicious.



Task 3. Investigate the affected assets and events

1. According to ET Intelligence Rep List, `signin.office365x24.com` is categorized as *"Drop site for logs or stolen credentials"*.
2. The following assets are those who accessed the domain:
    a. `ashton-davidson-pc`
    b. `bruce-monroe-pc`
    c. `coral-alvarez-pc`
    d. `emil-palmer-pc`
    e. `jude-reyes-pc`
    f. `roger-spence-pc`
3. I found 2 IP addresses that map to `signin.office365x24.com: 104.215.148.63 & 40.100.174.34.`
4. The IP address `40.100.174.34` resolves to `signin.office365x24.com` and `signin.accounts-google.com`.
5. As we can see from the image below, there are several POST requests made to `40.100.174.34`.


Google SecOps | Domain
SHOWING ALL TIME
24 Events
EXPAND ALL
WRAP TEXT
TIMELINE
ASSETS
POST
1/6
2023-01-31 ASSET IDENTIFIER FQDN
14:40:45 ashton-davidson-pc signin.office365x24.com
POST /login.php
Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes)
14:41:10 jude-reyes-pc signin.office365x24.com
14:41:15 coral-alvarez-pc signin.office365x24.com
14:42:14 emil-palmer-pc signin.office365x24.com
14:42:45 emil-palmer-pc signin.office365x24.com
POST /login.php
Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes)
14:43:49 bruce-monroe-pc signin.office365x24.com
14:44:50 roger-spence-pc signin.office365x24.com
2023-07-08
05:02:42 ashton-davidson-pc signin.office365x24.com
05:02:47 ashton-davidson-pc signin.office365x24.com
POST /login.php
Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes)
05:03:12 jude-reyes-pc signin.office365x24.com
05:03:17 coral-alvarez-pc signin.office365x24.com
05:04:16 emil-palmer-pc signin.office365x24.com
05:04:47 emil-palmer-pc signin.office365x24.com
POST /login.php
Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes)
05:05:51 bruce-monroe-pc signin.office365x24.com
05:06:52 roger-spence-pc signin.office365x24.com
2023-07-09
05:02:39 ashton-davidson-pc signin.office365x24.com
05:02:44 ashton-davidson-pc signin.office365x24.com
POST /login.php
Port: [Unknown] Resp. Code: 200 Resp. Size: 19,181 (bytes)
05:03:09 jude-reyes-pc signin.office365x24.com
05:03:14 coral-alvarez-pc signin.office365x24.com
05:04:13 emil-palmer-pc signin.office365x24.com
05:04:44 emil-palmer-pc signin.office365x24.com
POST /login.php
Port:

6. These POST requests were made to `signin.office365x24.com`. Their target URL of the web page was sent to `http://signin.office365x24.com/login.php`.

Recommended Actions:

1. **Isolate Affected Assets:**
    - Temporarily disconnect compromised devices from the network to prevent further data breaches.
    - Implement strict access controls to limit unauthorized access.
2. **Password Reset:**
    - Force password resets for all affected user accounts, especially those that submitted login credentials to the suspicious domain.
    - Encourage strong, unique passwords and enable multi-factor authentication (MFA) for enhanced security.
3. **Threat Hunting:**
    - Conduct a thorough threat hunt to identify any additional indicators of compromise (IOCs) or ongoing malicious activity.
    - Use advanced security tools and techniques to detect and remove any hidden threats.
4. **Incident Response Plan Activation:**
    - Follow the organization's incident response plan to coordinate efforts, contain the breach, and restore normal operations.

Summary

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