**Chronicle (Google SecOps)**

Scenario

You are a security analyst at a financial services company. You receive an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: **signin.office365x24.com**. You need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. You will use Chronicle to investigate this domain.

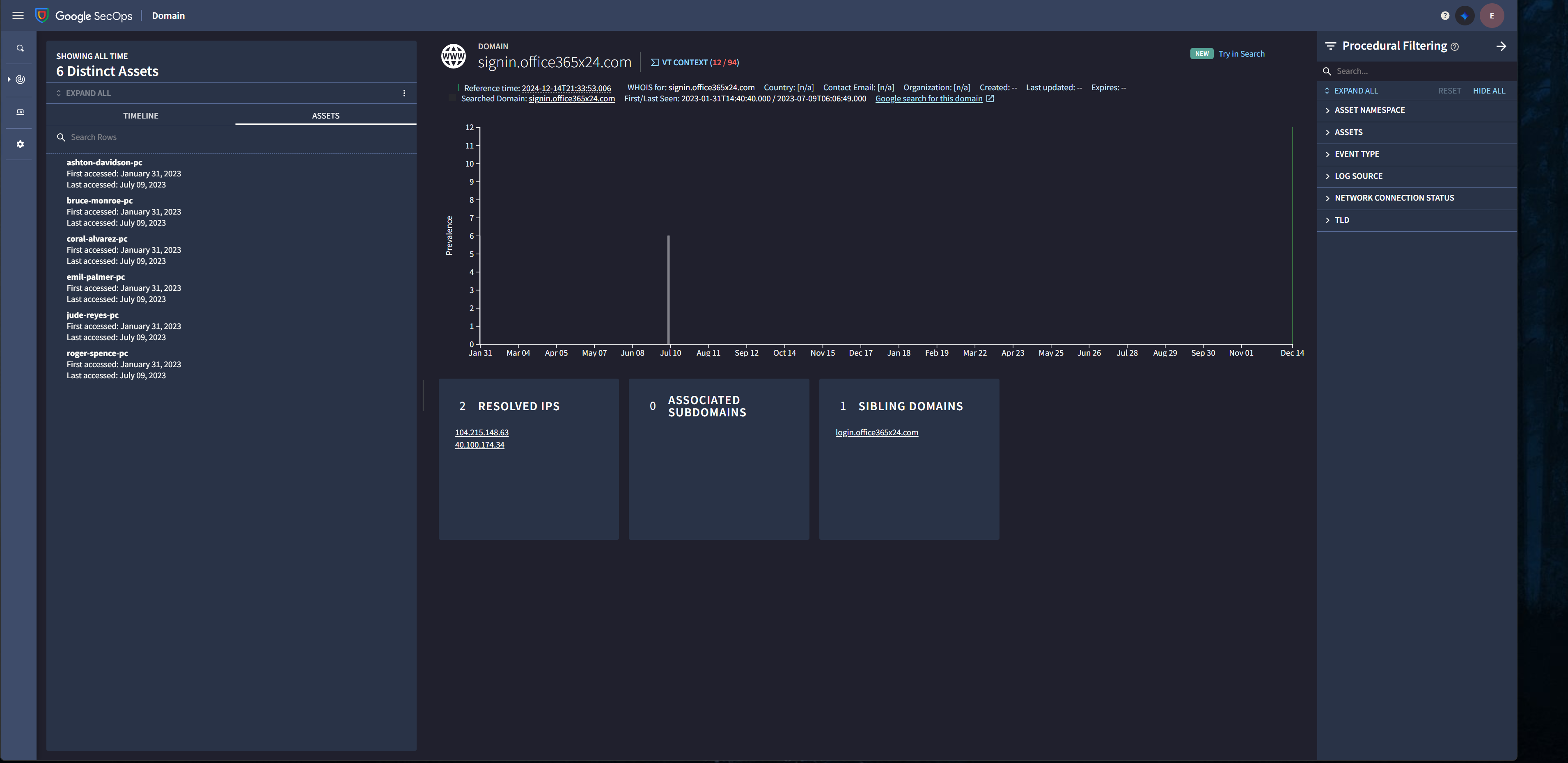
Overview

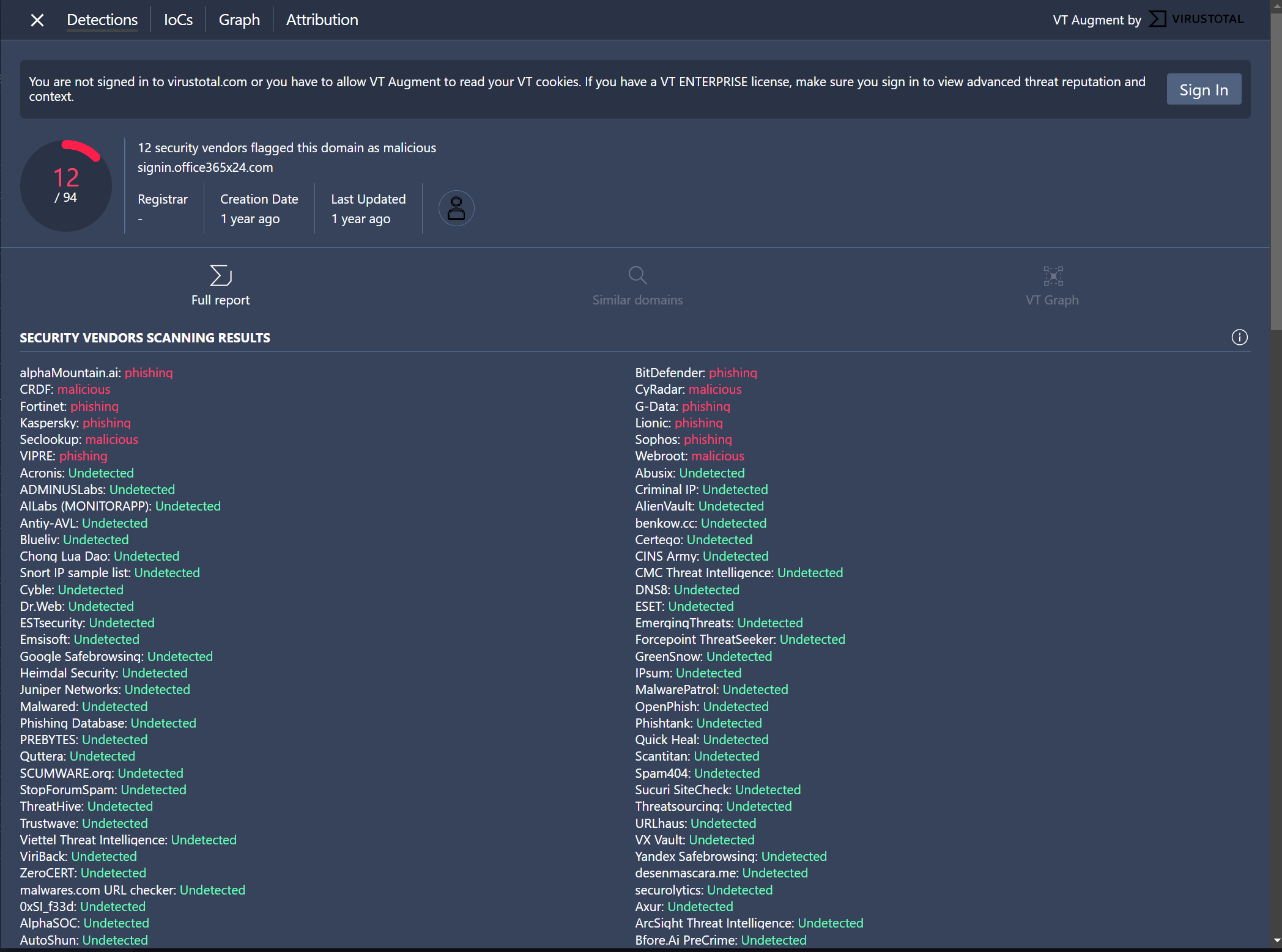
* Access threat intelligence reports on the domain
* Identify the assets that accessed the domain
* Evaluate the HTTP events associated with the domain
* Identify which assets submitted login information to the domain
* Identify additional domains

Solutions

1. Launch Chronicled
2. Perform a Domain Search

* In the search bar, type signin.office365x24.com and click Search. Under DOMAINS, signin.office365x24.com will be listed.
* Click signin.office365x24.com to complete the search.





Evaluate the search results

|  |  |  |
| --- | --- | --- |
| **Observe** | **Description** | **Note** |
| VT context | Provides VirusTotal information available for the domain. | Chronicle found 7 security vendors flagged this domain as malicious. |
| WHOIS | Summary of information about the domain using WHOIS which includes domain names, contact information of the domain owner. This may help determining the origin of malicious websites. | First Last Seen shows as 2023-01-31/ 2023-07-09 |
| Prevalence | A graph which outlines historical prevalence of the domain. | The domain has been accessed on July 9th, 2023 and February 10th, 2024. |
| Resolve IP | This provides additional context about the domain such as the IP address to signin.office365x24.com. This can be helpful for further investigation to determine whether there is a broader compromise. | We found 2 IP addresses that map to signin.office365x24.com: 104.215.148.63 & 40.100.174.34. |
| Sibling Domains | This provides additional context about the domain, such as the top or parent domain. | We found one sibling domain: login.office365x24.com |
| ET Intelligence Rep List | This includes additional context on the domain, such as known threats using ProofPoint's Emerging Threats (ET) Intelligence Rep List | Category: Drop site for logs or stolen credentials. Confidence (Min: 20, Max 127): 22, Severity: Medium, Active from: 2018-12-31 T00:00:00Z, Active until: 2019-0-8T00:00:00Z. |
| Timeline | his provides information about the events and interactions made with the domain. | It reveals the details about the HTTP requests made including GET and POST. GET retrieves the data from a server while a POST request submits data to a server`. |
| ASSETS | This provides a list of the assets that have been assessed the domain. | There are 6 assets that have accessed the domain. |

**Investigate**

Launch an Investigation.

According to ET Intelligence Rep List, signin.office365x24.com is categorized as "Drop site for logs or stolen credentials".

* The following assets are those who accessed the domain:
  1. ashton-davidson-pc
  2. bruce-monroe-pc
  3. coral-alvarez-pc
  4. emil-palmer-pc
  5. jude-reyes-pc
  6. roger-spence-pc
* The are 2 IP addresses that map to signin.office365x24.com: 104.215.148.63 & 40.100.174.34.
* The IP address 40.100.174.34 resolves to signin.office365x24.com and signin.accounts-google.com.
* There are three POST requets made to 40.100.174.34.
* Some POST requests were made to signin.office365x24.com. Their target URL of the web page were sent to http://signin.office365x24.com/login.php.