USE CHRONICLE TO INVESTIGATE A SUSPICIOUS DOMAIN USED IN A PHISHING EMAIL

Pedro Osorio Lopez.

1. High-Level Project Description:

*In this activity, we'll explore the several capabilities of the Google's native Chronicle SIEM tool to investigate a suspicious domain used in a phishing email.

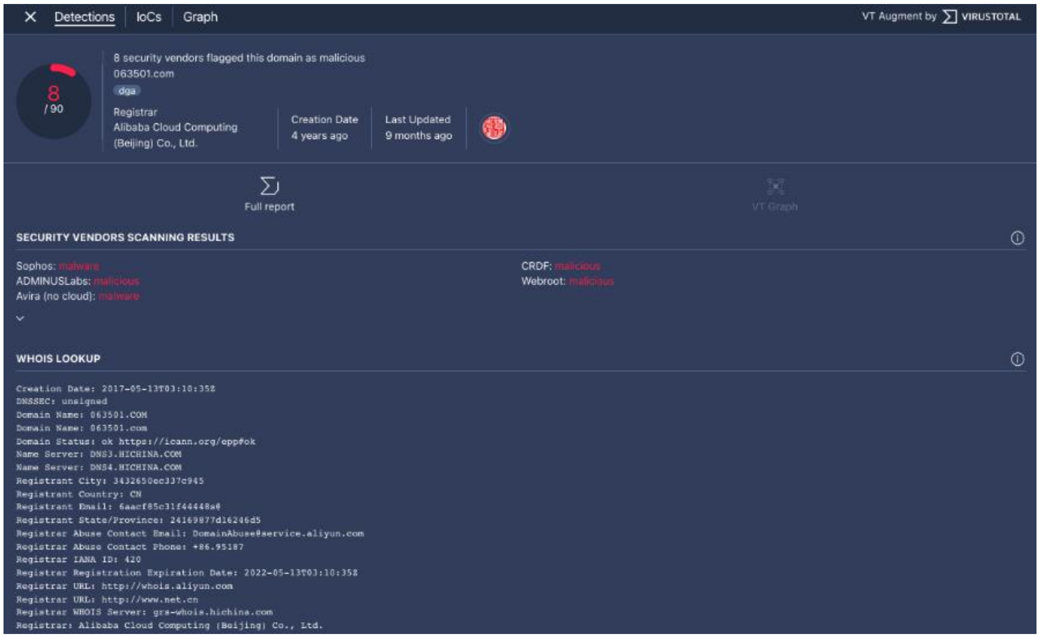
2. Project Setup and Required Tools:

*For this assignment, Google provided us a VM in which we had access to the tool. If doing this assignment in our own account, we would need to set up a Google Cloud Account first..

3. Step by Step Project Walkthrough

*In this lab, we will: 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, and identify additional domains.

*We will start by confirming whether the suspicious domain has been determined dangerous. For this purpose, Chronicle includes the information from VirusTotal so we can easily check this in the same interface. For instance:



8 security vendors flagged this domain as malicious
063501.com
dga

Registrar
Alibaba Cloud Computing (Beijing) Co., Ltd.

Creation Date
4 years ago

Last Updated
9 months ago

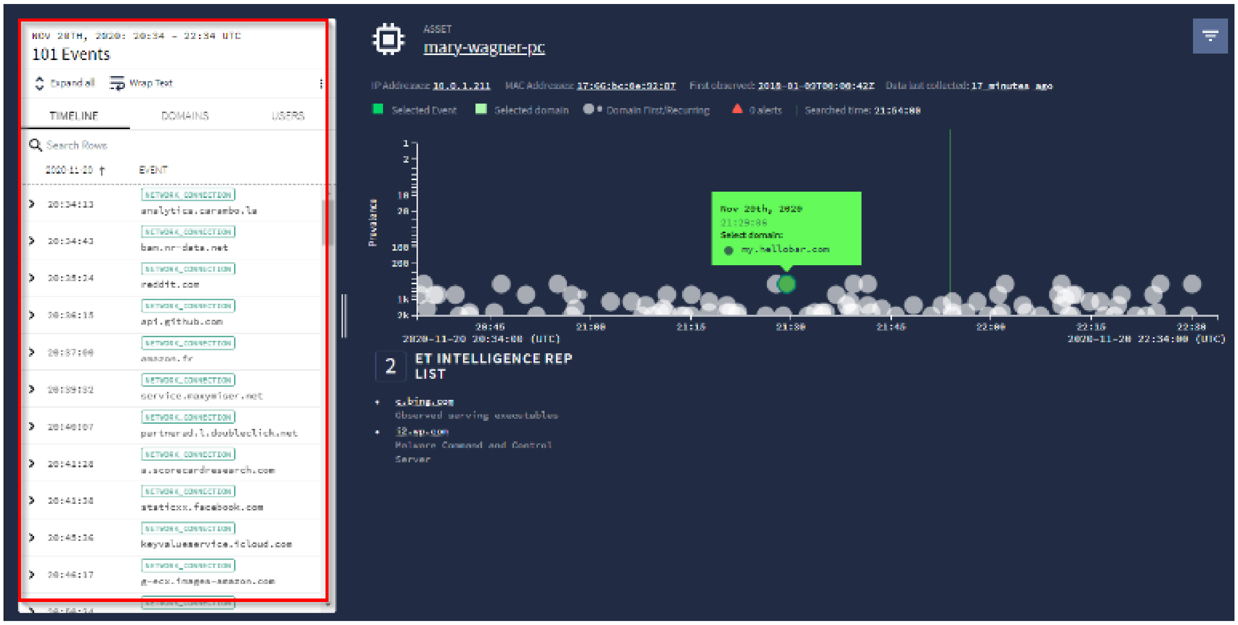
SECURITY VENDORS SCANNING RESULTS

Sophos: malware
ADMINUSLabs: malicious
Avira (no cloud): malware
CRDF: malicious
Webroot: malicious

WHOIS LOOKUP

```
Creation Date: 2017-05-13T03:10:35Z
DNSSEC: unsigned
Domain Name: 063501.COM
Domain Name: 063501.com
Domain Status: ok https://icann.org/epp#ok
Name Server: DNS3.HICHINA.COM
Name Server: DNS4.HICHINA.COM
Registrant City: 3432650ec337c945
Registrant Country: CN
Registrant Email: 6aacf85c31f44448a@
Registrant State/Province: 24169877d16246d5
Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
Registrar IANA ID: 420
Registrar Registration Expiration Date: 2022-05-13T03:10:35Z
Registrar URL: http://whois.aliyun.com
Registrar URL: http://www.net.cn
Registrar WHOIS Server: grs-whois.hichina.com
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
```

*Next, we will proceed to identify the assets that accessed the domain and evaluate the HTTP events associated with the domain. If we go to the Chronicle dashboard and look to the panel on the left, we can see several information including the asset view.



NOV 20TH, 2020: 20:34 - 22:34 UTC
101 Events

2020-11-20 ↑	EVENT
20:34:13	NETWORK_CONNECTION analytics.carambo.la
20:34:43	NETWORK_CONNECTION bam.nr-data.net
20:35:24	NETWORK_CONNECTION reddit.com
20:36:15	NETWORK_CONNECTION api.github.com
20:37:00	NETWORK_CONNECTION amazon.fr
20:39:32	NETWORK_CONNECTION service.maxymiser.net
20:40:07	NETWORK_CONNECTION partnerad.l.doubleclick.net
20:41:28	NETWORK_CONNECTION a.scorecardresearch.com
20:41:38	NETWORK_CONNECTION staticxx.facebook.com
20:45:36	NETWORK_CONNECTION keyvalueservice.icloud.com
20:46:17	NETWORK_CONNECTION g-ecx.images-amazon.com

ASSET
mary-wagner-pc

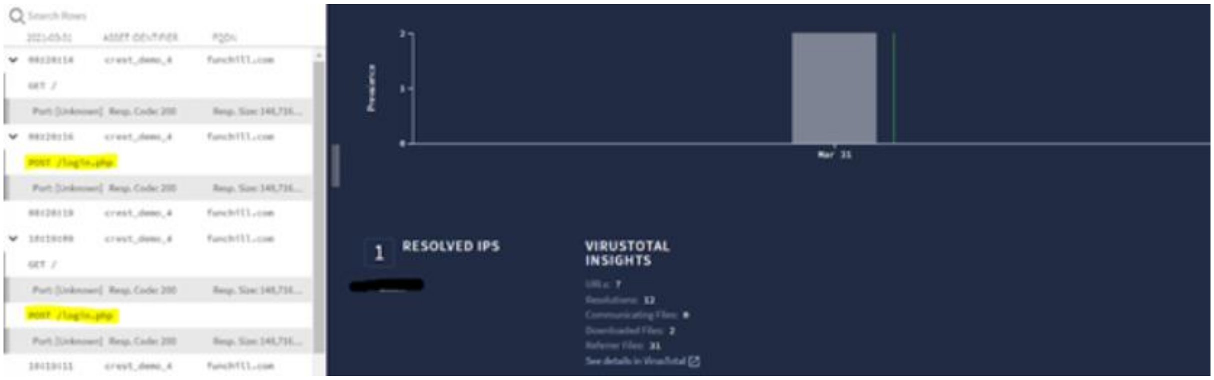
IP Address: 10.0.1.211 MAC Address: 17:66:bc:0e:02:07 First observed: 2018-01-09T00:00:42Z Data last collected: 17 minutes ago

🟩 Selected Event 🟩 Selected domain ● Domain First/Recurring ▲ 0 alerts | Searched time: 21:54:00

Nov 20th, 2020
21:29:06
Select domain:
● my.hellobar.com

2 ET INTELLIGENCE REP LIST
- s.bing.com
  Observed serving executables
- i2.ap.com
  Malware Command and Control Server

*Once there, we will search and click on the requests related to the suspicious address (the one we were exploring in the VM provided by Google was signin.office365x24.com) to evaluate HTTP events associated to this account. We will pay special attention to the POST requests, since these can help us finding out which assets submitted login information to the suspicious domain.

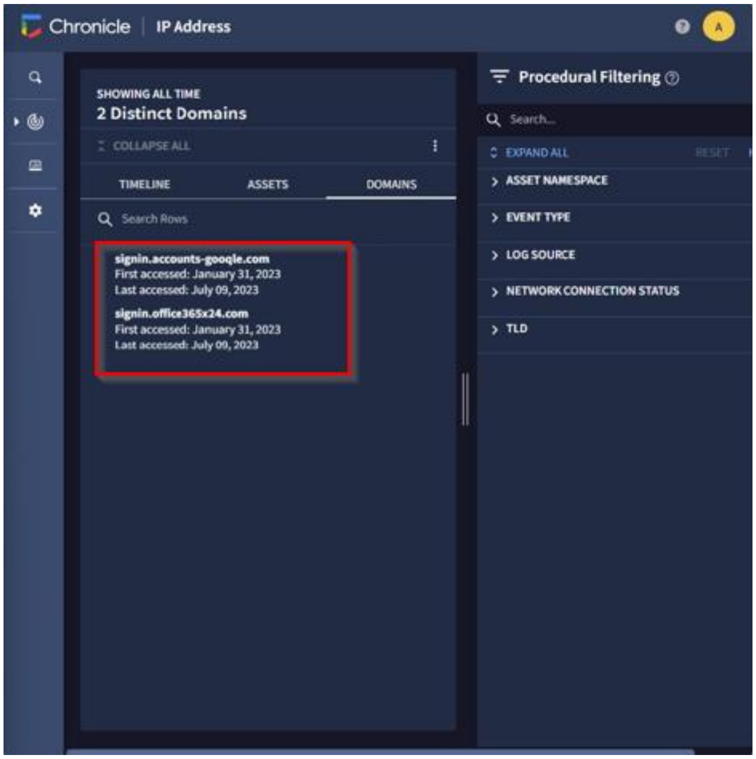


2021-03-31	ASSET IDENTIFIER	FQDN
08:28:14	crest_demo_4	funchill.com
GET /		
Port [Unknown]	Resp. Code: 200	Resp. Size: 148,716...
08:28:16	crest_demo_4	funchill.com
POST /login.php		
Port [Unknown]	Resp. Code: 200	Resp. Size: 148,716...
08:28:19	crest_demo_4	funchill.com
10:10:00	crest_demo_4	funchill.com
GET /		
Port [Unknown]	Resp. Code: 200	Resp. Size: 148,716...
POST /login.php		
Port [Unknown]	Resp. Code: 200	Resp. Size: 148,716...
10:10:11	crest_demo_4	funchill.com

1 RESOLVED IPS
[redacted]

VIRUSTOTAL INSIGHTS
URLs: 7
Resolutions: 12
Communicating Files: 0
Downloaded Files: 2
Referrer Files: 31
See details in VirusTotal

*Lastly, we will find other domains associated to this account by going to the Resolved IP address section. With that information, we were able to find that the domain signin.accounts-google.com is related to the suspicious account signin.office365x24.com, so this could be used for further investigation.



signin.accounts-gooqle.com
First accessed: January 31, 2023
Last accessed: July 09, 2023

signin.office365x24.com
First accessed: January 31, 2023
Last accessed: July 09, 2023

*Note that only the last screenshot was actually taken while doing this lab, all other images are shown for illustration purposes only.

4. Summary and/or Recommendations:

*In this activity, we determined that the suspicious domain has been involved in phishing campaigns. We 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, we identified two additional domains related to the suspicious domain by examining the resolved IP address.