STOLEN PENCIL

AXIAL

A SURVEY ON STOLEN PENCIL: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Operation Stolen Pencil was discovered by ASERT Team and had been going on since May 2018, targeting academic institutions that had expertise in Biomedical Engineering. The threat actors behind the attacks use a malicious Google Chrome extension to gain access to the victim’s network. Once inside the attacker uses Microsoft Windows administration tools including Remote Desktop Protocol (RDP) to maintain persistence. The malware used in the attacks is also able to log keystrokes and change Ethereum wallet addresses to addresses under the threat actors' control.

II. TARGET SECTORS

Targets were a large number of the victims, across multiple universities, having expertise in biomedical engineering.

III. METHODS USED

Targets are sent spear-phishing e-mails that lead them to a web site displaying a lure document and are immediately prompted to install a malicious Google Chrome extension.

IV. ATTRIBUTION

Operation Stolen Pencil most likely represents only a small set of the threat actor’s activity. The use of basic techniques, off-the-shelf programs, a cryptojacker, and the use of Korean language suggests the actor is of North Korean origin.

V. LINKS TO THREAT ACTORS

Some researchers state that this Operation ties in with Kimsuky APT's campaign, but this remains inconclusive.

V. OPERATIONS

- According to ASERT Team, many of the subdomains contain basic phishing pages, consisting of saved HTML of common web login properties. Some of the pages contain the “MarkOfTheWeb” artifact inserted by the web browser. The more sophisticated phishing pages targeting academic institutions display a benign PDF in an IFRAME. It then redirects the user to install a “Font Manager” extension from the Chrome Web Store. The malicious Chrome extensions declare permissions to run on every URL in the browser then extensions would have loaded JavaScript from a separate site.
- The malicious extension allows the attacker to read data from all the websites accessed by the victim, a circumstance that suggests attackers were looking to steal browser cookies and passwords.
- Once gaining a foothold on a target system, the actors Remote Desktop Protocol (RDP) for remote access. RDP access occurred daily from 06:00-09:00 UTC (01:00-04:00 EST). In one case, it was seen that the threat actor changed the victim’s keyboard layout to Korean. A compromised or stolen certificate was used to sign several PE files.

IV. IOC

MD5

- 9d1e11bb4ec34e82e09b4401cd37cf71
- 8b8a2b271ded23c40918f0a2c410571d
- 2ec54216e79120ba9d6ed2640948ce43
- 6a127b94417e224a237c25d0155e95d6
- fd14c377bf19ed5603b761754c388d72
- 1d6ce0778cabecea9ac6b985435b268b
- ab4a0b24f706e736af6052da540351d8
- f082f689394ac71764bca90558b52c4e
- ecda8838823680a0dfc9295bdc2e31fa
- 1cdb3f1da5c45ac94257dbf306b53157
- 2d8c16c1b00e565f3b99ff808287983e
- 5b32288e93c344ad5509e76967ce2b18
- 4e0696d83fa1b0804f95b94fc7c5ec0b
- af84eb2462e0b47d9595c21cf0e623a5
- 75dd30fd0c5cf23d4275576b43bbab2c
- 98de4176903c07b13dfa4849ec88686a

IPs

- 104.148.109[.]48
- 107.175.130[.]191
- 132.148.240[.]198
- 134.73.90[.]114
- 172.81.132[.]211
- 173.248.170[.]149
- 5.196.169[.]223
- 74.208.247[.]127
- 92.222.212[.]0

PHISHING SITES

1. world-paper[.]net
2. docsdriver[.]com
3. grsvps[.]com
4. coreytrevathan[.]com
5. gworldtech[.]com

DOMAINS

1. bizsonet.ayar[.]biz
2. bizsonet[.]com
3. client-message[.]com
4. client-screenfonts[.]com
5. *.coreytrevathan[.]com (possibly compromised legitimate site)
6. docsdriver[.]com grsvps[.]com
7. *.gworldtech[.]com (possibly compromised legitimate site)
8. itservicedesk[.]org
9. pqexport[.]com
10. scaurri[.]com
11. secozco[.]com
12. sharedriver[.]pw
13. sharedriver[.]us
14. tempdomain8899[.]com
15. world-paper[.]net
16. zwfaxi[.]com

VIII. REFERENCES

- https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia