AXIAL

A SURVEY ON APT39: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT39 a.k.a. Remix Kitten, Chafer, ITG07, TA454 is a threat group originating from Iran that had been active from 2014 to 2018 with the prime-motivation of Information theft and Cyber Espionage. APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. While APT39's targeting scope is global, its activities are concentrated in the Middle East.

II. TARGET SECTORS

Targeted Sectors are Aviation, Engineering, Government, High-Tech, IT, Shipping and Logistics, Telecommunications, Transportation.

III. METHODS USED

According to FireEye, for initial compromise, APT39 leverage spear-phishing with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection. In some cases previously compromised email accounts have also been leveraged, likely to abuse inherent trusts and increase the chances of a successful attack. APT39 frequently registers and leverages domains that masquerade as legitimate web services and organizations that are relevant to the intended target. Furthermore, this group has routinely identified and exploited vulnerable web servers of targeted organizations to install web shells, such as ANTAK and ASPXSPY, and used stolen legitimate credentials to compromise externally facing Outlook Web Access (OWA) resources.

AX1AL

IV. IOC

MD5

- f01a9a2d1e31332ed36c1a4d2839f412
- 7fac7a0843f65135832ac5685750cc6c
- cec4bb3b2f4d2ca2f3468103efb5967d
- 01e4391421d56698bcaa1f3c05bd9818 (TREKX RAT)
- cf7d3e9ca78ab23929e94215d871bd51 (TREKX RAT)
- ede89b446d8703dd13d26168e8d58865 (TREKX Config File)
- 7c08601341888b413779a3b33d8bf6dc (TREKX Config File)
- d0e74da12c5e8d35f6db1ae0c60748b7 (Custom Mimikatz)
- 405506980d6057a0b1c756e3c67641a0 (Data exfiltration tool)
- ade5518c61a620c5e3b226ce3c84e7af (JSPSpy)

DOMAINS

1. dropboxengine[.]com
2. redjewelry[.]biz
3. apigoogle-accounts[.]biz
4. update-microsoft[.]space
5. nvidia-services[.]com
6. sabre-css[.]com
7. sabre-airlinesolutions[.]com
8. turkiyeburslari[.]tk
9. xn--mgbfv9eh74d[.]com (تلگرام[.]com)
10. ytb[.]services
11. eseses[.]tk
12. s224.win7-update[.]com
13. s5060.win7-update[.]com
14. s21.win7-update[.]com

V. OPERATIONS

- **2017**
  - From 2015 to 2017, it was reported that APT39 inducted 7 new tools and rolled out new infrastructure targeting nine new organizations. Targeted countries were Israel, Jordan, the UAE, Saudi Arabia and Turkey. Outside of the Middle East
- **2018**
  - In November 2018 the Chafer threat group targeted a Turkish government entity reusing infrastructure that they used in campaigns reported earlier in 2018. This new secondary payload is Python-based and compiled into executable form using the PyInstaller utility.
  - In Fall of 2018, Securelist analyzed a cyber-espionage campaign that was targeting foreign diplomatic entities based in Iran. The attackers were using an improved version of Remexi in what the victimology suggests might be a domestic cyber-espionage operation.
  - Bitdefender researchers have found attacks conducted by this actor in the Middle East region, dating back to 2018. The campaigns were based on several tools, including “living off the land” tools, which makes attribution difficult, as well as different hacking tools and a custom built backdoor.

VI. REFERENCES

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
- https://securelist.com/chafer-used-remexi-malware/89538/
- https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/
- https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf
- https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html