apl33

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

APT33 also known as Refined Kitten, Magnallium, Holmium, or Elfin, is a threat group from Iran with destructive capabilities. APT33 is a capable group that has carried out cyber-espionage operations since at least 2013. APT33 has targeted organizations – spanning multiple industries – headquartered in the United States, Saudi Arabia, and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.

II. TARGET SECTORS

The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.

III. METHODS USED

APT33 sent spear-phishing emails to employees whose jobs were related to the aviation industry. These emails included recruitment themed lures and contained links to malicious HTML application (.hta) files. The .hta files contained job descriptions and links to legitimate job postings on popular employment websites that would be relevant to the targeted individuals.

IV. IOC

C2

1. n3tc4t.hopto[.]com
2. newhost.hopto[.]org
3. njrat12.ddns[.]net
4. remote-server.ddns[.]net
5. remserver.ddns[.]net
6. securityupdated[.]com
7. servhost.hopto[.]org
8. service-avant[.]com
9. srvhost.servehttp[.]com
10. svcexplores[.]com
11. trojan1117.hopto[.]org
12. update-sec[.]com
13. windowsx.sytes[.]net

SHA256

- 394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b
- 61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842
- 128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd
- 4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6
- 448ad1bc06ea26f4709159f72ed70ca199ff2176182619afa03435d38cd53237
- 47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34
- c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a
- 5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a
- e4b2d326f9c47eb1d79aa59381f8c93b50dc6c0c427eff8a330c49d2beed6d3a

V. ENGAGEMENTS

- In March 2019, a report released by Symantec stated that APT33 had been active for the past 3 years targeting at least 50 organizations in Saudi Arabia, the United States, and other countries.
- In July 2019, US Cyber Command released a statement that threat actors are abusing an Outlook vulnerability CVE-2017-11774.
- In November 2019, More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting.

VI. ATTRIBUTIONS

FireEye and Kaspersky Lab noted similarities between the ShapeShift and Shamoon, another virus linked to Iran. APT33 also used Farsi in ShapeShift and DropShot, and was most active during Iran Standard Time business hours, remaining inactive on the Iranian weekend. One hacker known by the pseudonym of xman_1365_x was linked to both the TurnedUp tool code and the Iranian Nasr Institute, which has been connected to the Iranian Cyber Army. xman_1365_x has accounts on Iranian hacker forums, including Shabgard and Ashiyane.

VII. REFERENCES

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/elfin-apt33-espionage
- https://www.trendmicro.com/en_us/research/19/l/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting.html
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT 33%2C Elfin%2C Magnallium