APT39 CONDUCTS CYBERESPIONAG OPERATIONS TARGETED AT THE MIDDLE EAST

Delaware, USA – January 31, 2019 – The newly discovered Iranian APT group collects personal information about its victims attacking telecommunications and traveling companies. The primary targets of APT39 attacks are located in the Middle East and the United States. FireEye researchers discovered the group's operations at the end of 2018 and tracked its activities to 2014. APT39 is linked with other well-known Threat Actor, APT34 (in addition to using similar malware, the groups' targets and infrastructure are partially matched). The researchers think that attackers can collect data and prepare a foothold for the further operations of other Iranian groups. The main tools of APT39 are SEAWEED and CACHEMONEY backdoors, in addition, the attackers modified the POWBAT backdoor for their purposes. After the initial compromise, members of the group also use both legitimate Windows programs and publicly available tools like Mimikatz. Stolen data before exfiltration is usually archived using WinRAR or 7-ZIP.

Recently, Iran has been actively conducting operations in the Middle East, including devastating attacks of APT33 using Shamoon malware and less sophisticated cyber espionage campaigns of Leafminer group. To detect the actions of skilled attackers in a timely manner, you can use the APT Framework rule pack, which adds sophistication to your existing security solutions connecting the dots between low-level SIEM incidents and linking them to high-confidence compromises:
https://my.socprime.com/en/integrations/apt-framework-arcsight

RELATED POSTS

BlackWater Backdoor Finds New Way to Misuse Cloudflare Workers


Turla APT Uses NetFlash Dropper and PyFlash Backdoor in Watering Hole Attacks


Hacker Wars: njRat Hides in "Free" Hacking Tools Published on Underground Forums