Iranian hackers are selling access to compromised companies on an underground forum

zdnet.com/article/iranian-hackers-are-selling-access-to-compromised-companies-on-an-underground-forum

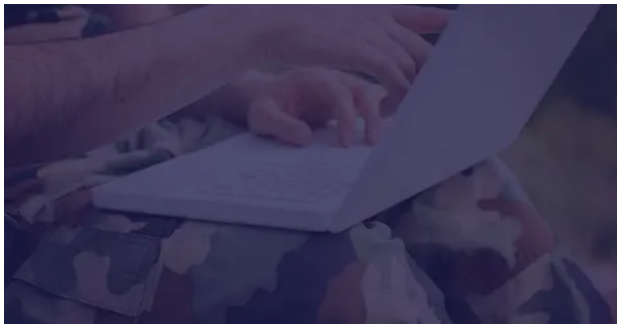
Home Innovation Security

The Iranian hacker group who's been attacking corporate VPNs for months is now trying to monetize some of the hacked systems by selling access to some networks to other hackers.

Written by Catalin Cimpanu, Contributor on Aug. 31, 2020

-
-
-
-
-

Special feature



One of Iran's state-sponsored hacking groups has been spotted selling access to compromised corporate networks on an underground hacking forum, cyber-security firm Crowdstrike said in a report today.

Also: The best VPNs in 2020

The company identified the group using the codename **Pioneer Kitten**, which is an alternative designation for the group, also known as Fox Kitten or Parisite.

The group, which Crowdstrike believes is a contractor for the Iranian regime, has spent 2019 and 2020 hacking into corporate networks via vulnerabilities in VPNs and networking equipment, such as:

- Pulse Secure "Connect" enterprise VPNs (CVE-2019-11510)
- Fortinet VPN servers running FortiOS (CVE-2018-13379)
- Palo Alto Networks "Global Protect" VPN servers (CVE-2019-1579)
- Citrix "ADC" servers and Citrix network gateways (CVE-2019-19781)
- F5 Networks BIG-IP load balancers (CVE-2020-5902)

The group has been breaching network devices using the above vulnerabilities, planting backdoors, and then providing access to other Iranian hacking groups, such as APT33 (Shamoon), Oilrig (APT34), or Chafer, according to reports from cyber-security firms ClearSky and Dragos.

These other groups would then come in, expand the "initial access" Pioneer Kitten managed to obtain by moving laterally across a network using more advanced malware and exploits, and then searching and stealing sensitive information likely of interest to the Iranian government.

However, in a report today, Crowdstrike says that Pioneer Kitten has also been spotted selling access to some of these compromised networks on hacking forums, since at least July 2020.

Crowdstrike believes the group is merely trying to diversify its revenue stream and monetize networks that have no intelligence value for Iranian intelligence services.

Classic targets of Iranian state-sponsored hacking groups usually include companies and governments in the US, Israel, and other Arabic countries in the Middle East. Targeted sectors have usually included defense, healthcare, technology, and government. Anything else is most likely out of scope for Iranian government hackers, and very likely to be made available on hacking forums to other gangs.

Today, the biggest customers of "initial access brokers" (like Pioneer Kitten) are usually ransomware gangs.