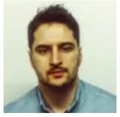
FBI says an Iranian hacking group is attacking F5 networking devices

zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/

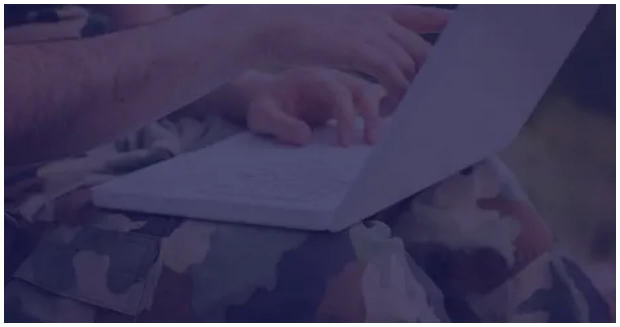
Home Innovation Security

Sources: Attacks linked to a hacker group known as Fox Kitten (or Parisite), considered Iran's "spear tip" when it comes to cyber-attacks.



Written by Catalin Cimpanu, Contributor on Aug. 9, 2020 iran-cyber.png

Special feature



A group of elite hackers associated with the Iranian government has been detected attacking the US private and government sector, according to a security alert sent by the FBI last week.

While the alert, called a Private Industry Notification, didn't identify the hackers by name, sources have told *ZDNet* that the group is tracked by the larger cyber-security community under codenames such as **Fox Kitten** or **Parisite**.

Iran's cyber operations "spear tip"

A former government cyber-security analyst, now working for a private security firm, called the group as Iran's "spear tip" when it comes to cyber-attacks.

He described the group's primary task as having to provide an "initial beachead" to other Iranian hacking groups — such as APT33 (Shamoon), Oilrig (APT34), or Chafer.

To reach its goals, Fox Kitten primarily operates by attacking high-end and expensive network equipment using exploits for recently disclosed vulnerabilities, before companies had enough time to patch devices. Due to the nature of the devices they attack, targets primarily include large private corporations and government networks.

Once the hackers gain access to a device, they install a web shell or backdoor, transforming the equipment into a gateway into the hacked network.

According to reports published by cyber-security firms ClearSky and Dragos earlier this year, Fox Kitten has been using this modus operandi since the summer of 2019, when it began heavily targeting vulnerabilities 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)

FBI warns of new attacks targeting F5 BIG-IP devices

The FBI notification sent out to the US private sector last week says the group still targets these vulnerabilities, but Fox Kitten also upgraded its attack arsenal to include an exploit for CVE-2020-5902, a vulnerability disclosed in early July that impacts BIG-IP, a very popular multi-purpose networking device manufactured by F5 Networks.

The FBI doesn't call the group by its public names, but makes references to their past attacks against Pulse Secure VPNs and Citrix gateways, and also warns companies that once the hackers gain access to their networks, they are very likely to provide access to other Iranian groups, or monetize networks that aren't useful for espionage by deploying ransomware.

FBI officials also warn that this group isn't targeting any particular sector, and any company running a BIG-IP device is likely to be targeted.

While the FBI asked US companies to patch their on-premise BIG-IP devices to prevent successful intrusions, FBI officials also shared details about a typical Fox Kitten attack, so companies can deploy countermeasures and detection rules. These details are similar to what ClearSky detailed in their February 2020 report.

"Following successful compromise of the VPN server, the actors obtain legitimate credentials and establish persistence on the server through webshells. The actors conduct internal reconnaissance post-exploitation using tools such as NMAP and Angry IP scanner. The actors deploy Mimikatz to capture credentials while on the network, and Juicy Potato for privilege escalation. The actors create new users while on the network [...]"

The actors use several applications for command and control (C2) while exploiting victim networks, including Chisel (C2 tunnel), ngrok, Plink, and SSHNET (reverse SSH shell). When tracking suspected C2 activity, the FBI advises that C2 activity with ngrok may be with external infrastructure associated with ngrok."

Two confirmed victims

But while the FBI alert doesn't say it, sources have told *ZDNet* that Fox Kitten attacks against BIG-IP devices have been successful.

A security researcher working for a US cyber-security firm told *ZDNet* that the FBI sent out the PIN alert last week after agents were called to investigate two successful intrusions where Fox Kitten hackers managed to breach US companies.

Due to non-disclosure agreements, the source could not identify the two companies, nor could they confirm these are the same "two compromises" mentioned in a similar alert sent out by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA) on July 24.

Either way, Iran's state-sponsored hacking groups aren't the only threat actors that have targeted the BIG-IP vulnerability.

Multiple hacker groups began exploiting this bug within two days after details and proof-of-concept exploits became public, and in recent weeks, an exploit for the BIG-IP bug has even been spotted part of a Mirai-based DDoS botnet.