Iranian Government Hackers Target US Veterans

darkreading.com/threat-intelligence/iranian-government-hackers-target-us-veterans/d/d-id/1335897

Kelly Jackson Higgins September 24, 2019

Threat Intelligence
4 MIN READ

ARTICLE
'Tortoiseshell' discovered hosting a phony military-hiring website that drops a Trojan backdoor on visitors.

September 24, 2019

Source: Cisco Talos

A nation-state hacking group recently found attacking IT provider networks in Saudi Arabia as a stepping stone to its ultimate targets has been spotted hosting a fake website, called "Hire Military Heroes," that drops spying tools and other malicious code onto victims' systems.

The so-called Tortoiseshell hacking team, which was called out last week by Symantec for a coordinated and targeted cyber espionage campaign that hops from the networks of several major IT providers in Saudi Arabia to specific customers of the providers, is also known by CrowdStrike as Iranian hacking team Imperial Kitten.

Cisco Talos researchers recently found the group hosting the "Hire Military Heroes" website, with an image from the "Flags of our Fathers" film. The malicious site prompts visitors to download an app, which is actually a downloader that drops the malware and other tools that gather system information, such as drivers, patch level, network configuration, hardware, firmware, domain controller, admin name, and other user account information. It also pulls screen size to determine whether the machine is a sandbox, according to Cisco's findings.

Tortoiseshell deploys a remote access Trojan named "IvizTech," which matches the code and features Symantec detailed in its report on the backdoor. Neither Symantec nor Cisco would tie Tortoiseshell to a specific nation-state.

It's unclear exactly how the attackers lure potential victims and whether the site is actively infecting victims at this point. Cisco Talos researchers say the creators thus far have employed weak operations security of their own, leaving behind hard-coded credentials, for instance.

"There is a possibility that multiple teams from an APT worked on multiple elements of this malware, as we can see certain levels of sophistication existing and various levels of victimology," the researchers wrote in their blog post about the threat today.

Paul Rascagneres, a researcher at Cisco Talos, says he and his team don't believe the attack is widespread, and the group is still relatively new to the APT scene.

"Tortoiseshell is not well-documented. [The research] shows that this actor is offensive for months, they create fake websites, and they probably use social engineering to send targets on these websites," he says. "We identified at least two installers, a couple of variants of the same RAT, a keylogger, and few reconnaissance tools. The toolkit of this actor is growing."

The researchers haven't pinpointed the initial infection vector, however. "[I]t could be spear-phishing or social media usage such as LinkedIn, as we saw during DNSpionage campaign," he says, referring to an attack campaign last year that used fake job websites.

CrowdStrike, meanwhile, had tagged the group as Imperial Kitten, an Iranian nation-state operation that has been operating since 2017. The group has been known to target Saudi Arabian, United Arab Emirates, and Western maritime, IT services, defense, and military veterans, notes Adam Meyers, vice president of intelligence at CrowdStrike. Imperial Kitten supports Iran's Islamic Revolutionary Guard Corps operations using tactics such as phony job recruitment, social media, and IT service provider attacks, he says.

"We have observed them active as recent as this month," Meyers says.

The malicious website is a "massive shift" for the hacking group, according to Cisco, as it's targeting a wider net of victims this way. "Americans are quick to give back and support the veteran population. Therefore, this website has a high chance of gaining traction on social media where users could share the link in the hopes of supporting veterans," the Talos team wrote in its blog post about the threat.

Jon DiMaggio, a researcher at Symantec who follows Tortoiseshell, says Tortoiseshell may be employing spear-phishing emails to lure victims.

"Assuming [Cisco Talos'] attribution is correct, it would show that another possible infection vector used by Tortoiseshell may have been spear-phishing emails," he says. "We identified a Web shell being used by the attacker indicating they may have compromised a Web server to deploy malware onto the victims' environment in the supply chain attacks, but spear-phishing is very common, and it would not be surprising to see them use more than one infection vector in various campaigns."

Related Content:

Check out The Edge, Dark Reading's new section for features, threat data, and in-depth perspectives. Today's top story: "'Playing Around' with Code Keeps Security, DevOps Skills Sharp"