Warren County Veterans Service Officer's Report for November 2019

Denise A. DiResta, Director/CVSO 1340 State Route 9 Lake George, NY 12845 ☼ Phone: 518-761-6342 Fax: 518-761-7683
Email: direstad@warrencountyny.gov ~ web-site: http://warrencountyny.gov/veterans ~ FB: **WarrenCountyVeterans**

Iranian Hackers Have Set Up a Fake Jobs Website

U.S. military officials warned troops this week that Iranian hackers have set up a fake jobs website for veterans that targets service members who are considering a transition back to civilian life. A National Guard Bureau memorandum dated 2 OCT warns service members to stay away from the website called "**Hire Military Heroes**," which appears to offer them assistance finding a job outside the Defense Department via a web application that visitors are encouraged to download. However, the app actually drops malicious malware and spyware into the users' computer system, according to the document issued by the guard's Defensive Cyber Operations office.

Defense officials have determined the website targets service members close to leaving the military. Officials believe the Iranian hackers hope to gain access to Pentagon information technology systems by targeting those individuals. "They're targeting active service members looking for jobs with the promise of offering assistance for civilian employment once their service ends," the memo states. "The hackers are hoping one of their targets would use a DOD system to download and run the malware." Officials have determined the chances that the group of the hackers, known as Tortoiseshell, successfully gains access to Defense Department systems is unlikely, but nonetheless issued the guidance this week labeling the matter a high risk.

The Cisco Talos Intelligence Group, which monitors cyber threats, first warned of the website's existence last week. The group noted the website's name was "strikingly close" to that of a legitimate site run by the U.S. Chamber of Commerce aimed at assisting veterans find employment, www.hiringourheroes.org. "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," Cisco Talos researchers wrote in the analysis of the fake website. The Cicso Talos researchers characterized the use of the fake website as a "massive shift" in behavior for the Tortoiseshell group, which has been accused of hacking several Saudi Arabian IT providers during the summer.

Defense officials said the group has not gained access to DOD systems as of 4 OCT. A spokesperson said the guidance was issued this week as a precautionary matter. If downloaded, the fake application would give hackers the ability to see a variety of information in the infected system, according to Cisco Talos. "The attacker can then see information on the system, the patch level, the number of processors, the network configuration, the hardware, firmware versions, the domain controller, the name of the admin, the list of the account, etc. This is a significant amount of information relating to a machine and makes the attacker well-prepared to carry out additional attacks," the company's researchers wrote in a report.

Also Friday, Microsoft announced hackers linked to the Iranian government attempted to hack into 241 email accounts including of U.S. government officials, media members, prominent Iranian expatriates and one U.S. presidential campaign. In a blog post on the Microsoft website, Tom Burt, the company's vice president for customer security and trust, wrote four accounts had been hacked, but he declined to identify them. Microsoft identified the group responsible for the email hacks as Phosphorous. It said the attempts to gain access to email accounts occurred in August and September.

[Source: Stars & Stripes | Corey Dickstein | October 4, 2019]

https://www.stripes.com/military-warns-of-iranian-hackers-targeting-american-troops-with-fake-jobs-website-1.601787