US Cyber Command issues alert about hackers exploiting Outlook vulnerability

By Written by Catalin Cimpanu, ContributorContributor July 2, 2019 at 1:06 p.m. PT

Archived: 2026-04-05 15:59:02 UTC

See als

-

US Cyber Command has issued an alert via Twitter today about threat actors abusing an Outlook vulnerability to plant malware on government networks.

The vulnerability is CVE-2017-11774, a security bug that Microsoft patched in Outlook in the October 2017 Patch Tuesday.

The Outlook bug, discovered and detailed by security researchers from SensePost, allows a threat actor to escape from the Outlook sandbox and run malicious code on the underlying operating system.

Outlook vulnerability previously used by Iranian hackers

The bug was privately reported by SensePost researchers in the fall of 2017, but by 2018, it had been weaponized by an Iranian state-sponsored hacking group known as APT33 (or Elfin), primarily known for developing the Shamoon disk-wiping malware.

At the time, in late December 2018, ATP33 hackers were deploying backdoors on web servers, which they were later using to push the CVE-2017-11774 exploit to users' inboxes, so they can infect their systems with malware.

"Once the adversary has legitimate credentials, they identify publicly accessible Outlook Web Access (OWA) or Office 365 that is not protected with multi-factor authentication. The adversary leverages the stolen credentials and a tool like RULER to deliver [CVE-2017-11774] exploits through Exchange's legitimate features," the FireEye report said.

The attacks leveraging the CVE-2017-11774 vulnerability came at the same time that reports surfaced about new sightings of the infamous Shamoon disk-wiping malware -- another hacking tool developed by the APT33 group.

No connection was ever proved at the time about links between FireEye's APT33 report and Shamoon deployments.

However, Chronicle Security researcher Brandon Levene has told *ZDNet* in an email today that the malware samples uploaded by US Cyber Command appear to be related to Shamoon activity, which took place around January of 2017.

Three of the five malware samples are tools used for the manipulation of exploited web servers, Levene said, while the other two are downloaders which utilized PowerShell to load the PUPY RAT -- most likely on infected systems.

Levene told *ZDNet* that if the observation of CVE-2017-11774 together with these malware samples holds true, this sheds some light on how the APT33/Shamoon attackers were able to compromise their targets.

When Shamoon attacks happened in the past, Levene said that it had been highly speculated that spear-phishing was involved, but not a lot of information around the initial infection vectors was published other than the FireEye report, which speculated on the infection vectors, rather than provide indisputable evidence.

Increased Iranian hacking activity

US Cyber Command's Twitter account doesn't issue alerts about financially-motivated hacker crews targeting the US, and is focused on nation-state adversaries only. All in all, the malware samples shared by US Cyber Command today link the new attacks the agency is seeing to old APT33 malware samples -- most likely deployed in new attacks against US entities.

While US Cyber Command has not named APT33 by name, Levene has, as well as Palo Alto Networks (on Twitter), and FireEye (on Twitter [1, 2] and in private conversations with *ZDNet*).

The US Cyber Command tweet also comes after Symantec warned about increased activity from APT33 back in March.

Furthermore, two weeks ago, CISA, the Department of Homeland Security's cyber-security agency, also issued a similar warning about increased activity from Iranian threat actors, and especially about the usage of disk-wiping malware such as Shamoon, APT33's primary cyber-weapon.

Besides analyzing malware that hits the US government network, the US Cyber Command is also in charge of offensive cyber operations. Two weeks ago, the DOD agency launched a cyber-attack aimed at Iran's rocket and missile system after the Iranian military shot down an expensive US surveillance drone. With Iranian hackers

targeting government networks and the US hitting back, you could say the two countries are in the midst of a very silent and very unofficial cyberwar.

And as a side note, Levene has also pointed out that this is the first time that US Cyber Command has shared non-Russian malware via its Twitter account. The agency started publishing malware samples on VirusTotal and issuing Twitter alerts last fall, deeming it a faster way of spreading security alerts about ongoing cyber-attacks and putting the US private sector on notice.

> USCYBERCOM has discovered active malicious use of CVE-2017-11774 and recommends immediate #patching. Malware is currently delivered from: 'hxxps://customermgmt.net/page/macrocosm' #cybersecurity #infosec
>
> — USCYBERCOM Malware Alert (@CNMF_VirusAlert) July 2, 2019

Article updated on July 3 with additional confirmations from FireEye and Palo Alto Network linking the malware shared on Twitter by US Cyber Command to Iranian hacking group APT33.

The world's most famous and dangerous APT (state-developed) malware

Related government coverage:

- NASA hacked because of unauthorized Raspberry Pi connected to its network
- US wants to isolate power grids with 'retro' technology to limit cyber-attacks
- Report shows failures at eight US agencies in following cyber-security protocols
- US launches cyber-attack aimed at Iranian rocket and missile systems
- Germany to publish standard on modern secure browsers
- Germany and the Netherlands to build the first ever joint military internet
- How Estonia became an e-government powerhouse TechRepublic
- Sri Lanka blocks social media after deadly Easter explosions CNET
