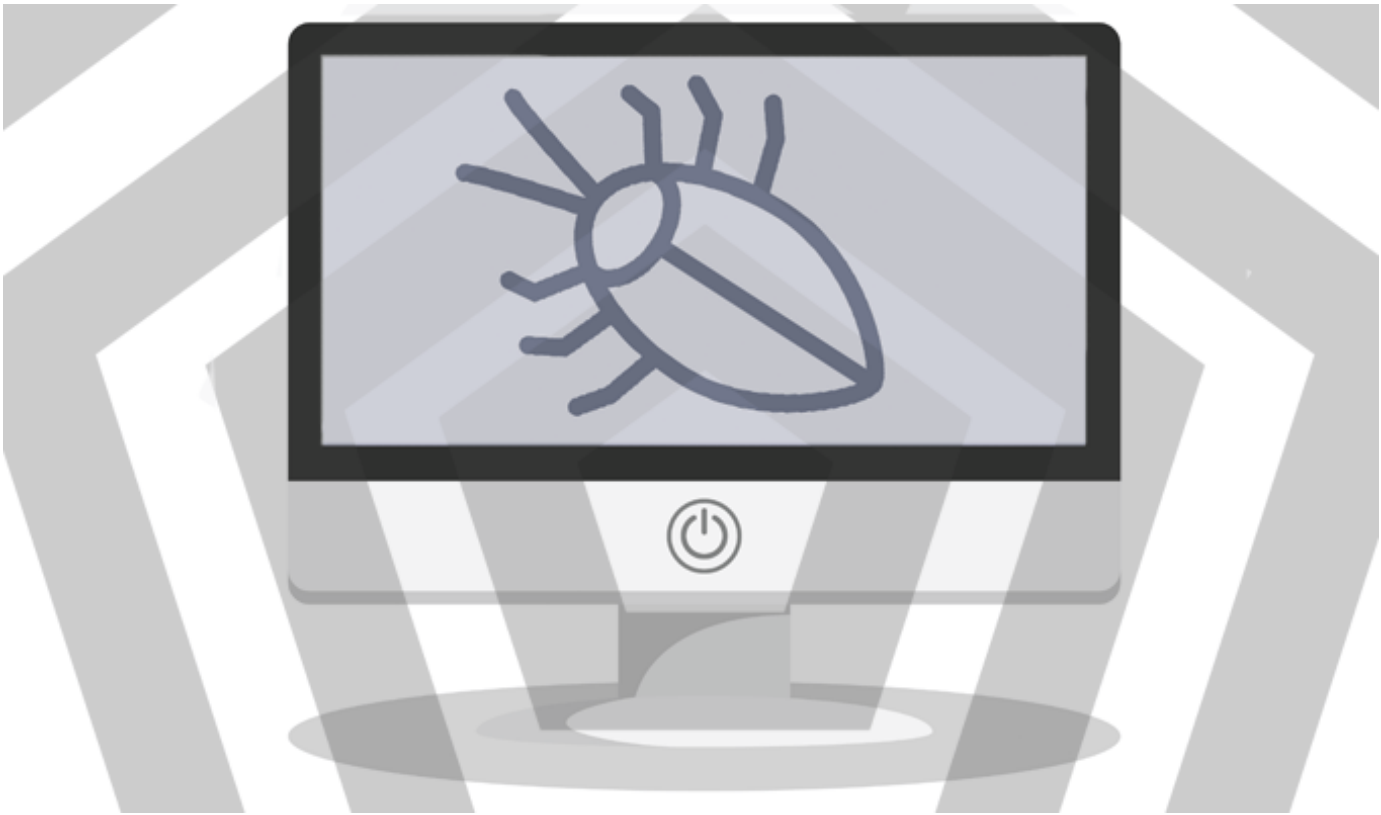
Pentagon Draws Back the Veil on APT Malware with Sudden Embrace of VirusTotal

Author:
Tara Seals

November 8, 2018 / 4:56 pm



Two samples have already been added to the malware zoo, indicating a new openness from the federal government when it comes to cyber.

The Pentagon has suddenly started uploading malware samples from APTs and other nation-state sources to the website VirusTotal, which is essentially a malware zoo that's used by security pros and antivirus/malware detection engines to gain a better understanding of the threat landscape.

The Cyber National Mission Force (CNMF), which is under the auspices of the U.S. Cyber Command, posted its first malware samples to VirusTotal on Monday, after opening its account there. It also set up a "malware alert" Twitter feed to go along with the new effort. No advanced announcement of a new initiative accompanied the move, which is unusual for government entities.

"Recognizing the value of collaboration with the public sector, the CNMF has initiated an effort to share unclassified malware samples it has discovered that it believes will have the greatest impact on improving global cybersecurity," CNMF said in a brief statement.

The first two samples are files called rpcnetp.dll and rpcnetp.exe, which are both detected as dropper mechanisms for what was formerly known as the Computrace backdoor trojan, often associated with the Russia-based APT28/Fancy Bear group.

"The particular pair of samples, Computrace/LoJack/Lojax, is actually a trojanized version of the legitimate software 'LoJack,' from a company formerly called Computrace (now called Absolute). The trojanized version of the legitimate LoJack software is called LoJax or DoubleAgent," a spokesperson from Chronicle told Threatpost.

Releasing such samples is a bold move for a Department of Defense that has long kept its cyber-activities and knowledge very close to the vest, according to Tom Kellermann, chief cybersecurity officer at Carbon Black.

"This is a huge leap forward for the cybersecurity community," he told Threatpost. "For too long, the U.S. has over-classified cyber- threat intelligence. This empowers the cybersecurity community to mobilize on clandestine threats in real time, thus aiding the U.S government in protecting and securing American cyberspace."

John Hultquist, director of intelligence analysis at FireEye, noted that the malware disclosure may exist somewhat in a vacuum, thanks to the counterintelligence operations that undoubtedly are tied to any sample released by CNMF.

"It remains to be seen exactly how this new initiative will unfold, but what is striking about this initiative is it lacks many of the contextual elements of the name-and-shame strategy," he noted, via email. "Whereas that strategy involves a tremendous amount of context which has to be scrutinized throughout the government, this initiative could be less encumbered by those considerations. There will undoubtedly still be a strategy behind these disclosures, since disclosures always have consequences for intelligence operations, but their simplicity may allow for simpler, faster action, something government has historically struggled with."

And indeed, this could lessen the impact of the initiative, Kellermann told us.

"It's important to consider that malware samples are only a part of the overall defense equation," he said. "A truly robust cybersecurity posture means we have a deeper understanding of attacker TTPs – the specific behaviors attackers use to avoid detection,

move laterally and counter incident response. Sharing both malware samples and TTPs across industries creates true situational awareness and allows for all to participate in a collective defense against adversaries."

Yet others were feeling cynical about the effort. "Rest assured that they won't be submitting their own offensive samples. And they won't be submitting bespoke samples that were crafted to target them except for well after the fact so as not to tip their hand to the attacker," Oliver Tavakoli, CTO at Vectra, told Threatpost. "It's just something of a watershed moment as in 'even Pentagon realizes the value of sharing malware samples and threat intel.' Beyond that – it's meh."

Many other researchers were simply pleased at the idea of building a broader knowledge base. "The announcement by U.S. Cyber Command signals a new level of collaboration among public- and private-sector actors and will broaden the VirusTotal knowledge-base, further enhancing VirusTotal's role as signature aggregator and benchmark for malware detection engines," said William Weinberg, director of Comodo Cybersecurity's corporate communications.

Mukul Kumar, CISO and vice president of Cyber Practice at Cavirin, meanwhile told us that he thought it was an "excellent move."

It "speaks to the need for additional information-sharing," he told Threatpost. "As hackers are still on the 'offense,' the combined vendor and intelligences communities must look for new, creative ways to multiply forces. There should be a secure means of distributing this threat data, though not at the expense of usability."

Government Malware

Recently-Patched Adobe ColdFusion Flaw Exploited By APT

The critical vulnerability, which was patched earlier in September, has put ColdFusion servers at risk.

November 9, 2018

Threatpost News Wrap Podcast for Nov. 9

The Threatpost editors break down the top news stories from this week.

November 9, 2018

Pentagon Ex Program to I Systems

The news come was called out f its weapons syst

October 25, 2018

DISCUSSION

Leave A Comment

Write a reply...

Your name

Your email

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

Send Comment

I'm not a robot

reCAPTCHA
Privacy - Terms

This site uses Akismet to reduce spam. Learn how your comment data is processed.

EDITOR'S PICKS

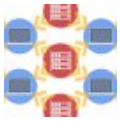
WordPress Flaw Opens Millions of WooCommerce Shops to Takeover

WordPress Flaw Opens Millions of WooCommerce Shops to Takeover

November 7, 2018 1

Rapidly Growing Router Botnet Takes Advantage of 5-Year-Old Flaw

November 7, 2018 2



ThreatList: Despite Fraud Awareness, Password Reuse Persists for Half of U.S. Consumers

November 6, 2018

Samsung, Crucial's Flawed Storage Drive Encryption Leaves Data Exposed

November 6, 2018 2

U.S. Elections True Test for Facebook's Disinformation Crackdown

November 6, 2018