3-ABC News-Researchers

We’ll notify you here with news about

Turn on desktop notifications for breaking stories about interest?

OffOn

Researchers discover another ongoing cyberattack using NSA hacking tools

Adylkuzz predates WannaCry, uses NSA exploit to mine for cryptocurrency.

By PETE MADDEN

May 17, 2017, 1:35 PM

• 4 min read

Number of cyberattack victims in Europe not rising as feared: Europol

A spokesperson from Europol said the attack appears to have been stabilized.

Kacper Pempel/Illustration/Reuters/File

— — Cybersecurity researchers have identified a second ongoing global cyberattack that has quietly hijacked hundreds of thousands of computers around the world, including many in the United States, for a massive cryptocurrency mining operation.

While investigating the WannaCry ransomware attacks, researchers at the cybersecurity firm Proofpoint stumbled upon another “less noisy” form of malware called Adylkuzz that, the firm says, has likely generated millions of dollars in cryptocurrency for the unknown attackers.

According to Ryan Kalember, the senior vice president for cybersecurity at Proofpoint, the attack employed the same hacking tools developed by the U.S. National Security Agency (NSA) and leaked to the public by the hacker group Shadow Brokers in April to exploit vulnerabilities in the Microsoft Windows operating system.

"I would say the real-world impact of this attack is going to be more substantial than WannaCry," *[Worry]* Kalember told ABC News. "Ransomware is painful, but you can restore operations relatively quickly *[Hope]*. Here, you have a huge amount of money landing in some bad people's hands. That has geopolitical consequences. *[Worry]*"

The firm is still working to establish attribution for the attacks, but Kalember pointed out that North Korean-backed Lazarus Group – the same hacker group linked to the WannaCry attacks – launched a similar cryptocurrency mining attack in late 2016.

Microsoft released a pair of patches to address the vulnerability exploited by both WannaCry and Adylkuzz, but the firm says computers that adopted those patches after being infected would remain compromised, and networks that have not adopted those patches would remain exposed.

Proofpoint identified Adylkuzz attacks dating back to May 2, which would predate the WannaCry attacks, making Adylkuzz the first known widespread use of the leaked NSA hacking tools. It remained undetected for so long, Kalember says, because its impact on users is far less noticeable than ransomware.

"It takes over your computer, but you probably don't notice anything other than that the system runs really slow," *[Worry]* Kalember said. "Your computer might be mining cryptocurrency for some very bad people." *[Worry]*

The theft itself is also more subtle. While the WannaCry attack spread ransomware to extort payments in Bitcoin , the Adylkuzz attack created a botnet that steals processing power to mine for Monero, another form open-source cryptocurrency that boasts of being "secure, private, [and] untraceable."

According to John Bambenek of Fidelis Cybersecurity, who confirmed the existence of a second virus using NSA tools to mine for cryptocurrency, Monero has largely supplanted Bitcoin as the preferred cryptocurrency of cybercriminals. Law enforcement officials have become more adept at tracking transactions through Bitcoin's public ledger, he said, while records of Monero transactions remain "highly obfuscated."

"It's made it extremely attractive for cybercriminals," *[Worry]* Bambenek told ABC News. "There are a handful of people still hanging on to Bitcoin, but the center of gravity is moving in Monero's favor."

When reached for comment, Riccardo Spagni, one of the seven members of Monero's "core team," acknowledged that some people use Monero for nefarious purposes but said that the cryptocurrency's stewards "choose not to get involved in protracted debates about what people are using Monero for, much as we find it disinteresting to discuss how criminals are using U.S. dollar cash notes, or the Internet, or kitchen knives."

"We do not condone Monero's use in outrightly criminal acts," Spagni told ABC News, "nor do we believe we are in a position to stop anyone from doing so or build a system that is even capable of detecting what it is being used for and making some sort of moral judgement."

Cybercriminals appear to appreciate that policy. Monero was recently adopted by AlphaBay, one of the most prominent darknet markets to emerge following the disruption of the Silk Road, where users can purchase illicit goods, such as illegal drugs, under the cloak of anonymity.

"Monero is really ugly stuff," Kalember said. "You're not using it for anything good. You can't use Monero to go buy groceries."