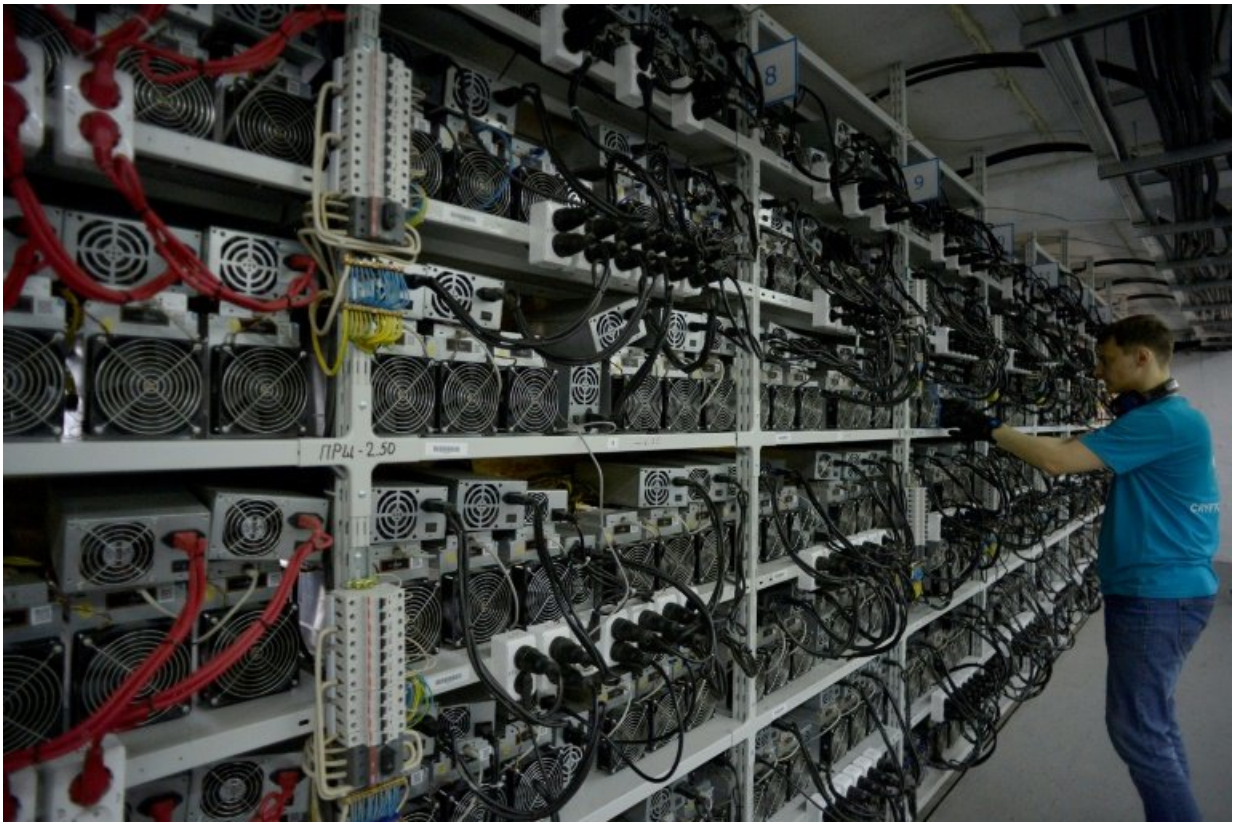
NSA leak fuels rise in hacking for crypto mining: report

September 19 2018



A new report says hackers have used a leaked US government software tool to step up illicit mining of cryptocurrencies like bitcoin and monero

Illicit cryptocurrency mining has been surging over the past year, in part due to a leaked software tool from the US National Security Agency,

researchers said Wednesday.

A report by the Cyber Threat Alliance, an association of cybersecurity firms and experts, said it detected a 459 percent increase in the past year of illicit crypto mining—a technique used by hackers to steal the processing power of computers to create cryptocurrency.

"Activity has gone from a virtually non-exist issue to one that almost universally shows up at the top of our members' threat lists," said a blog post by Neil Jenkins, chief analytic officer for the alliance.

One reason for the sharp rise was the leak last year by a group of hackers known as the Shadow Brokers of "EternalBlue," software developed by the NSA to exploit vulnerabilities in the Windows operating system.

"A patch for EternalBlue has been available for 18 months and even after being exploited in two significant global cyberattacks—WannaCry and NotPetya—there are still countless organizations that are being victimized by this exploit, as it's being used by mining malware," Jenkins wrote.

The rise in hacking coincides with growing use of virtual currencies such as bitcoin, ethereum or monero, which are not regulated by any government and are created through solving complex computing problems.

While some cyptocurrency mining is legitimate, hackers have discovered ways to tap into the processing power of unsuspecting computer users to illicitly generate currency.

Jenkins said the rise in malware for crypto mining highlights broader cybersecurity threats.

"Illicit mining is the 'canary in the coal mine' of cybersecurity threats," he said. "If illicit cryptocurrency mining is taking place on your network, then you most likely have worse problems and we should consider the future of illicit mining as a strategic threat."

Hackers can generate gains and use cryptocurrency for other malicious purposes such as purchasing other kinds of malware tools on the "dark web," according to the report.

The researchers said 85 percent of illicit cryptocurrency malware mines monero, with bitcoin representing eight percent.

"Although monero is significantly less valuable than bitcoin, several factors make this the cryptocurrency of choice for malicious actors," the report said.

Monero, according to the report, offers more privacy and anonymity, "which help malicious actors hide both their mining activities and their transactions using the currency," the researchers said.

"Transaction addresses and values are obfuscated by default, making tracking monero incredibly difficult for investigators."

Citation: NSA leak fuels rise in hacking for crypto mining: report (2018, September 19) retrieved 16 April 2024 from https://techxplore.com/news/2018-09-nsa-leak-fuels-hacking-crypto.html