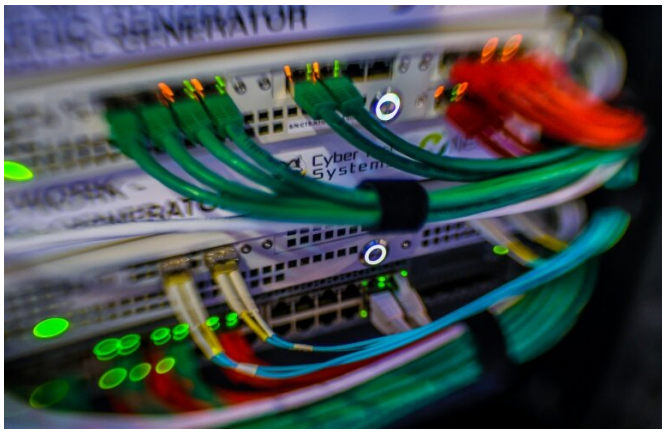
Warning issued on industrial plants as 'Triton' hack resurfaces

12 April 2019



Security researchers say they have discovered new activity by hackers using malware called "Triton" that can target industrial control systems including oil and gas facilities

Security researchers this week confirmed that they spotted new activity by hackers using "Triton" malware capable of doing real-world damage to oil, gas or water plants.

The security firm FireEye said in a blog post Wednesday that it had identified and was "responding to an additional intrusion by the attacker behind Triton at a different critical infrastructure facility."

It did not disclose details regarding the target.

FireEye urged oil, gas, water and other facilities with industrial control systems to ramp up defenses and vigilance for Triton activity on their networks.

A study of the hackers' arsenal indicated they may have been in action since early 2014, avoiding detection for years.

FireEye said that Triton hackers were refining the ability to damage industrial plants when they unintentionally caused the shutdown in 2017 that got them noticed.

"The targeting of critical infrastructure to disrupt, degrade, or destroy systems is consistent with numerous attack and reconnaissance activities carried out globally by Russian, Iranian, North Korean, US, and Israeli nation state actors," FireEye said in a blog post.

"Triton" tactics employ custom hacking tools to snake through plant networks to reach operating systems that control safety mechanisms, according to analysis that followed its initial discovery in late 2017 after it inadvertantly stopped processes at an oil plant in Saudi Arabia.

In an update last year, FireEye expressed confidence that the Triton activity was "supported by" the Central Scientific Research Institute of Chemistry and Mechanics, which it described as a Russian government-owned institution in Moscow.

FireEye described Triton as one of a limited number of publicly identified malicious software families aimed at industrial control systems.

"It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016," FireEye said in an earlier blog post.

"Triton is consistent with these attacks, in that it could prevent safety mechanisms from executing their intended function, resulting in a physical consequence."

APA citation: Warning issued on industrial plants as 'Triton' hack resurfaces (2019, April 12) retrieved 6 May 2021 from https://techxplore.com/news/2019-04-issued-industrial-triton-hack-resurfaces.html