MARSH

2019

Client Briefing: Triton - The Deadly New Industrial Cyberweapon

The lines between the digital and the physical world are becoming increasingly intertwined and the effects of viruses and malware which have previously been confined to cyberspace are now having physical consequences in the real world. Concerningly, the trade-off for convenience and efficiency through the digitilisation of business operations may be personal safety and security, and we are now talking about the potential for loss of human life as a result of a cyber-attack.

Triton is the 'new kid' on the malware block. It was first spotted in 2017 when it was used against a petrochemical plant owned by Tasnee in Saudi Arabia.[1] Also known as Trisis, it has been engineered to target a specific type of industrial control system (ICS), namely the Triconex safety instrumented systems (SIS) controllers developed by Schneider Electric.[2]

The Triton malware is especially concerning as the sole purpose of the code is to, via these SIS systems, cause process shutdowns and tamper with emergency controls – in particular the failsafe functions that prevent catastrophic industrial accidents.

MARSH & McLENNAN COMPANIES

Engineered for Destruction

In the case of the Tasnee plant, the Triton hackers followed a common pattern seen in sophisticated ICS-related intrusions. They obtained a foothold in the corporate IT network and moved into segregated operational technology (OT) networks, through systems that were accessible to both network environments. The hackers then deployed malicious software in the OT that let them take over the plant's SIS systems.[3]

These physical controllers and their associated software are the last line of defense against life-threatening disasters. They are engineered to intervene if they detect dangerous conditions, returning processes to safe levels or shutting them down altogether by automatically triggering safety protections like shutoff valves and pressure-release mechanisms. Triton made it possible for hackers to take over these systems remotely.

A FireEye Mandiant investigation[4] into the Tasnee plant revealed the hackers did not steal any data; instead, they focused on moving laterally through the system and performing network reconnaissance. This could signal an increasing focus by hackers on strategic attacks of this kind in the near future.

A worst case scenario would be a Chernobyl-type disaster caused by a Triton attack – imagine a nuclear power plant having its SIS system rendered non-responsive while the temperature or pressure gauge rises beyond critical levels without any failsafes deploying . FireEye added that in a less disastrous scenario, the malware could still be used to shut down the Triconex SIS process that is in a safe state. Due to the plant not being able to safely operate without the SIS online this would subsequently disrupt plant operations until such time that the SIS could be restored to full functionality, causing widespread business interruption.

The hackers behind it, linked to a Russian IP address, are now allegedly targeting companies in other parts of the world.[5]

Industries in the Crosshairs

The industries which are most at-risk to Triton or similar types of malicious cyber-physical code are those who utilise industrial control systems to conduct business processes. These include sectors such as:

- Manufacturing
- Energy and Utility Providers
- Transport and Urban Infrastructure
- Shipping and Logistics

These are the industries in which a successful Triton attack could result in mass disruption to an organisation's operations and even the surrounding community, putting the safety of the public at risk.

Additionally, any organisation who relies on industrial control systems, or who has embedded automated or internet-connected devices into critical operating processes, may also be at risk to Triton malware and other adapted versions of this code that are designed to disrupt physical environments. The more connected equipment there is, the more targets hackers have to aim at.

Pre-Emptive Measures

Experts at places like the Idaho National Laboratory in the United States are urging companies to review all their operations in light of Triton and other cyber-physical threats, and to radically reduce, or eliminate, the digital pathways hackers could potentially use to get to critical operating technology networks.[6]

Industry-specific insurance solutions addressing the traditional gap between cyber and property insurance coverage are also being created and are steadily becoming available to more insurance buyers.

The susceptibility of industrial control systems and the destruction that malware crafted to damage these systems is a significant known exposure for infrastructure companies who are regularly targeted by malicious threat actors. These companies are actively addressing this exposure with the insurance market to create bespoke solutions, such as Cyber CAT 4.0 – a market leading Marsh cyber wording out of the US that can, as one of its many advantages, look to cover both physical and financial loss arising from a cyber event under a single insurance solution.

Cyber CAT 4.0 offers comprehensive protection, including coverages not typically available in commercial policies for cyber and technology risks, for liabilities and direct losses associated with technology failures and data breaches, and for newly emerging risks.

We recommend speaking to your Marsh broker for more information regarding how Cyber insurance can play a valuable role in managing Triton malware and cyber-physical threats of the future.

[1] Perlroth, N. and Krauss, C. (2018). A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. Nytimes.com. Available at: https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html [Accessed 6 Jun. 2019].

[2] Osborne, C. (2019). Triton hackers return with new, covert industrial attack | ZDNet. ZDNet. Available at: https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/ [Accessed 6 Jun. 2019].

[3] Osborne, C. (2019). Triton hackers return with new, covert industrial attack | ZDNet. ZDNet. Available at: https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/ [Accessed 6 Jun. 2019].

[4] Miller, S., Brubaker, N., Zafra, D. and Caban, D. (2019). TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. FireEye. Available at: https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html [Accessed 6 Jun. 2019].

[5] Cimpanu, C. (2019). FireEye links Russian research lab to Triton ICS malware attacks | ZDNet. ZDNet. Available at: https://www.zdnet.com/article/fireeye-links-russian-research-lab-to-triton-ics-malware-attacks/ [Accessed 6 Jun. 2019].

[6] Giles, M. (2019). Triton is the world's most murderous malware, and it's spreading. MIT Technology Review. Available at: https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/ [Accessed 6 Jun. 2019].

For further information, please contact your local Marsh office or visit our website at marsh.com

JONO SOO
Head of Cyber Specialty
New Zealand
e: jono.soo@marsh.com

KRISTINE SALGADO
Managing Principal – Cyber / FINPRO
t: +61 3 9603 2871
m: +61 498 046 114
e: kristine.salgado@marsh.com