Safety System Cyber Attack on Critical Infrastructure - 5 things you need to know

A successful cyber attack on a safety instrumented system (SIS) at a critical infrastructure organization in the Middle East was publicized yesterday. The attack demonstrated nation-state sophistication similar to STUXNET and the 2016 power disruptions in Ukraine, showing the ability to remove critical, industrial, fail-safe measures. Following are five things you need to know.

---

1 TRITON compromised a leading Safety Instrumented System (SIS)

The malware, initially coined “TRITON” is an industrial control system (ICS) cyber tool designed specifically to effect Schneider Electric’s Triconex Safety Instrumented System controllers, which could cause physical damage and shut down process control operations. TRITON infected an SIS engineering computer, which then changed the ladder logic on the SIS with the goal to render the SIS unable to perform its core function to take appropriate safety actions when the ICS is operating in an unsafe state. In this particular attack, the safety system tripped prematurely while the adversary was performing stealthy reconnaissance on the ICS/SIS environment, alerting the operators to an issue and causing further investigation.

SIS controllers are designed to protect the most critical assets (e.g. refinery, power plant, chemical plant, off-shore oil rig) from potentially catastrophic malfunctions. Taking out the SIS would remove well-engineered fail-safe safety measures operators rely on to prevent a significant, adverse event, such as a plant explosion. Similarly, tricking the SIS to invoke an unintended shut down when it would otherwise be unwarranted would take production off-line for months or longer, and have material operational and financial impacts. Recent

cyber incidents caused production losses resulting in write-downs of $50 million for International Paper, $300 million for Maersk Shipping, and a loss of $150 million in revenue for Merck Pharmaceuticals.

Schneider Electric's Triconex is considered to be one of the industry's best, safest, and most reliable safety systems. Compromising this system highlights that SIS controllers remain vulnerable to cyber compromise. Initial reports indicate the malware developers had specific knowledge of the industrial protocols to compromise Triconex, similar to payloads on the Industroyer malware that disrupted power grids in Kiev, Ukraine in December 2016.

2 Deep impact

Obtaining access to expensive and difficult to procure equipment, along with the time investment to study, develop, test, refine, trial, and deploy malware such as TRITON is a major undertaking. Focusing on SIS, rather than a programmable logic controller (PLC) or remote terminal unit (RTU), demonstrates the adversary is seeking maximum physical impact from a cyber attack at the time of choosing. Impacts range from halting or disrupting production for a period of time to destructive effects impacting the environment, health and safety, reputational risk, and economic loss.

3 Patient zero

While the initially-reported incident identified a Middle East-based organization, history shows advanced malware propagates after triggering via sale on the Dark Web to less-sophisticated actors looking to inflict harm against their adversaries. Examples include Stuxnet, Not Petya, WannaCry, Mirai, Black Energy, and Havex. Furthermore, other adversaries with ongoing cyber campaigns, such as DragonFly, are targeting energy company control systems and SCADA in the US, Switzerland, and Turkey. These other actors could possibly obtain and employ malware such as TRITON to achieve their own goals.

4 ISA 84 requires separation of SIS and control

ISA 84, IEC 61508 and IEC 61511 require that Control and Safety Instrumented Systems must be separate and independent in order to avoid common cause faults, minimize systems errors, and protect against cyber attacks. Control systems, such as Programmable Logic Controllers can be easily compromised.

MSi has demonstrated this on numerous occasions beginning with the DHS ICS CERT meeting in the fall of 2015. The adversary who developed TRITON could certainly compromise a PLC, move on to the SIS and carry out a successful attack. While many in the industrial safety community have robust safety programs, the reality is SIS are cyber-vulnerable. The costs of physically separating SIS and control systems can be very expensive involving new engineering, re-wiring, testing, and taking production off-line for a month or more. As such, the vast majority of SIS remain joined with the control system network. In fact, some manufacturers combine both safety and control into the same controller. A significant event linked to a safety system not in compliance with ISA 84 could lead to material loss, significant fines in the millions of dollars, company exposure to legal action, and other environmental, health and safety, and loss of production issues.

Protection requires more than visibility

The Middle East is one of the most active cyber environments on the planet, leading the world with smart cities, state-of-the-art automation, advanced robotics, and more. Companies hire the best IT cyber security vendors and deploy state-of-the-art control equipment. Despite these efforts, a sophisticated adversary can bypass these measures, gain access to “air gapped” or “protected” control system environments, and deliver malware such as TRITON. MSi believes having operational technology (OT) visibility is better than no visibility. However, visibility may not enable you to see when an attack is unfolding, let alone stop it, especially if you lack resources and technical capabilities to watch the monitoring system 24/7/365. Anti-virus is also helpful, but if the signature does not exist, then it will be difficult to detect anything unusual. TRITON was a new attack and signatures are only being developed and deployed now, after the attack took place. Where else is it embedded and waiting to launch? When will the next TRITON be launched?

The MSi Platform: Visibility and Protection

The patented MSi Platform is purpose-built for harsh industrial environments to defeat these kinds of zero day and insider attacks. MSi works with clients and trade organizations in the Energy industry to prevent Ukraine-style attacks and protect SIS compromises.

The MSi Sentinel monitors the same I/O as the SIS and validates whether the

SIS should take its safety actions. If the MSi Sentinel detects the conditions necessary for the SIS to execute its safety actions, and the SIS does not take those safety actions, the MSi Sentinel would (1) detect this situation, (2) alert the appropriate operators, and (3) allow for corrective actions to either be triggered automatically or manually.

Additionally, MSi 1 can monitor and restrict programmatic communication (versus operational communication) between ICS and SIS components. MSi 1 can restrict which hosts can access the SIS and the type of communication (i.e. protocols and commands). It can reject those changes if they come from unauthorized sources. As an SIS typically does not have frequent configuration changes, the MSi 1 can also detect when programmatic changes are being performed so operators can be alerted when unexpected changes are being made to the SIS configuration. For enhanced security, MSi 1 can block programmatic changes and be configured to only allow them during manually-controlled, authorized periods. If an attempt is made outside this specified period, then the MSi 1 will block the attempt and notify operators of this unexpected activity.

Contact us to learn how we can help

Whether your organization is just beginning to consider operational technology cyber risks and find the appropriate path to strong protection, or you are ready for immediate, advanced protection that can block malware like TRITON before impact, MSi is working with critical infrastructure companies across the spectrum.

Contact us to learn more and see how we can assist.