What's a SCADA?
Or, The First Salvo in the Cyberwar?

On Wednesday, April 13, 2022, a headline from Wired.com caught my eye, "**Feds Uncover a 'Swiss Army Knife' for Hacking Industrial Control Systems**." The first paragraph seemed almost like security essay boilerplate.

> **MALWARE DESIGNED TO target industrial control systems like power grids, factories, water utilities, and oil refineries represents a rare species of digital badness. So when the United States government warns of a piece of code built to target not just one of those industries, but potentially all of them, critical infrastructure owners worldwide should take notice.**

I would suggest that if the article is about a **CISA press release concerned about malware that could cripple many different critical industries**, then you put that fact in the lead.

> **The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) device.**

A Supervisory Control And Data Acquisition (SCADA) device is a very specific piece of networking hardware that acts as a controller between a set of industrial controls and the computers that manage those controls. The CISA press release explained the malware in question can exploit the vulnerabilities of SCADA devices to perform attacks on Windows based systems within the targeted network.

> **The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising and maintaining full system access to ICS/SCADA devices, APT actors could elevate privileges, move laterally within an OT environment, and disrupt critical devices or functions.**

We don't usually think that the gears and dials and other instruments in an industrial plant are open to computer malware attack. Yet, here we have a real world example how the network has no boundary, as a first principle of Zero Trust.

The FBI made the first announcement of a type of malware that had been used by state actors associated with Russia. This malware, dubbed **TRITON**, had been used in prior industrial attacks. **March 24, 2022, the FBI issued an alert** warning **"that the group responsible for the deployment of TRITON malware against a Middle East–based petrochemical plant's safety instrumented system in 2017, the Russian Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), continues to conduct activity targeting the global energy sector."** The FBI release went on to state **"TRITON was malware designed to cause physical safety systems to cease operating or to operate in an unsafe manner. Its potential impact could be similar to cyberattacks previously attributed to Russia that caused blackouts in Ukraine in 2015 and 2016."**

Specifically, among the vulnerable industrial controls are those manufactured by Schneider Electric. Anyone who has ever been around any commercial electrical installation is familiar with the name, Schneider Electric.

> **TRITON malware targeted the Schneider Electric Triconex safety instrumented system (SIS),which is used to initiate safe shutdown procedures in the event of an emergency. TRITON malware affected Triconex Tricon safety controllers by modifying in-memory firmware to add additional programming, potentially leading to damage of a facility, system downtime, and even loss of life should the SIS fail to initiate safe shutdown procedures. Schneider Electric addressed the vulnerability (with the Tricon model 3008 v10.0-10.4) when version 11.3 of the Tricon controller was released in June 2018; however, older versions of the controller remain in use and are vulnerable to a similar attack. As a result, the FBI is alerting the ICS community of continued activity by this group and requests that any indicators of potential compromise be reported to the FBI.**

Discovery of the variant believed to now be in the wild was attributed to security company, Mandiant. The **April 13, 2022**, press release put out by Mandiant coincided with, and complimented that, of CISA. Mandiant now calls this new strain of malware designed to attack industrial controls, **INCONTROLLER**. **Guess that says it all, huh?**

> **In early 2022, Mandiant, in partnership with Schneider Electric, analyzed a set of novel industrial control system (ICS)-oriented attack tools—which we call INCONTROLLER (aka PIPEDREAM)—built to target machine automation devices. The tools can interact with specific industrial equipment embedded in different types of machinery leveraged across multiple industries. While the targeting of any operational environments using this toolset is unclear, the malware poses a critical risk to organizations leveraging the targeted equipment. INCONTROLLER is very likely state sponsored and contains capabilities related to disruption, sabotage, and potentially physical destruction.**

Schneider Electric has also put out its own bulletin, dated April 13, 2022. The manufacturer did not in any way deny or try to obfuscate the real threat its products are currently under and the danger those devices represent. Schneider was also direct about what could be the consequences. The malware could deceive the rest of the systems into accepting the malware as the system controller, and as such could do or take whatever actions the actual controller could initiate or perform.

> **If the framework is used against one of the targeted devices, it would allow for use of the same standard features as the programming tool or Modbus client or OPC-UA client. Any action that can be performed by an attacker using a legitimate programming tool or modbus client can likewise be performed using the framework. Other than that, we have not identified any weakness or vulnerability being exploited. Depending on the features utilized in the framework and the security features configured on the device, an attacker can perform actions such as:**
>
> **• Perform a network scan to discover the device**
>
> **• Change the IP address to communicate with the framework or make the device unreachable**
>
> **• Send Modbus frame (standard or proprietary)**
>
> **• Automate connection to PLC in order to bruteforce the password using standard programming protocols • Upload and download files (configuration, firmware, application, receipes, etc)**
>
> **• Execute denial of service attacks to force the user to authenticate again or make the device unreachable**
>
> **• Perform read & write to OPC-UA server**

Schneider Electric is imploring its customers to patch their devices NOW!

The malware also exploits long known vulnerabilities in another piece of industrial software, known as **CODESYS**. The **PIPEDREAM** industrial malware leverages known vulnerabilities in CODESYS. **July 21, 2021, The Hacker News**, reported on the vulnerabilities of CODESYS

> **The flaws can be turned "into innovative attacks that could put threat actors in position to remotely control a company's cloud OT implementation, and threaten any industrial process managed from the cloud," the New York-headquartered industrial security company Claroty said in a report shared with The Hacker News, adding they "can be used to target a cloud-based management console from a compromised field device, or take over a company's cloud and attack PLCs and other devices to disrupt operations."**

A team of security researcher have been tracking the new variant of this attacker since the beginning of this year. **"Dragos CEO Robert M. Lee attributed the malware to a state actor dubbed CHERNOVITE, assessing with high confidence that the destructive toolkit has yet to be employed in real-world attacks, making it possibly the first time "an industrial cyber capability has been found *prior* to its deployment for intended effects."**

> **"Capabilities to reprogram and potentially disable safety controllers and other machine automation controllers could then be leveraged to disable the emergency shutdown system and subsequently manipulate the operational environment to unsafe conditions," Dragos cautioned.**

So, by any other name, whether PIPEDREAM or TRITON or INCONTROLLER, this malware strain has proven itself to be quite dangerous. **"INCONTROLLER [aka PIPEDREAM] represents an exceptionally rare and dangerous cyber attack capability," Mandiant said. "It is comparable to Triton, which attempted to disable an industrial safety system in 2017; Industroyer, which caused a power outage in Ukraine in 2016; and Stuxnet, which sabotaged the Iranian nuclear program around 2010."**

A cyberattack on the power grid in Ukraine had been recently thwarted, as was reported by **The Hacker News, also April 13, 2022. "The attackers attempted to take down several infrastructure components**

of their target, namely: Electrical substations, Windows-operated computing systems, Linux-operated server equipment, [and] active network equipment," the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) said in a statement."

Since early February, researchers tracked "**three new threat groups targeting industrial control systems**." And it is now believed that the intended targets for these cyberattacks **Liquid Natural Gas facilities through out North America**.

Now, obviously this is not an attack on the personal computers readers of this blog use. But all of our systems require power to function. Moreover, when we consider how technology, not necessarily considered to be "computer technology", is now leveraged to launch hopefully unsuccessful attacks on systems at the periphery of the Internet, the logic of Zero Trust and its concept of no boundary to the network, makes great sense. Furthermore, it clearly stands out as a warning that all those vulnerable and exploitable IoT devices, and out of date routers, that this blog and smarter security professionals than me, rail against.

In the 60s, it was said either "You are part of the solution. Or you are part of the problem." What is clear right now is that critical problem before all of us is this: **Will those small industrial operators patch their systems before those systems are exploited? And someone's grandmother can't heat her home**.

Back to Top

Gerald Reiff

Back to Top **next post (TBA) →**