ISASecure Web Conference

Triton, Three Years After

Andrew Kling, Product Security Officer, Schneider Electric

November, 2020

ISASecure®

About the Speaker

- **Andrew Kling**
- **Industry Automation Product Security Officer**
- Andy has been developing software over 30 years across multiple industries and with Schneider Electric since 2001. Andy leads the Industry Automation business unit in cybersecurity as the Product Security Officer. He has managed many process control engineering teams, created Schneider's organization to comply with ISA/IEC 62443 standards at the process, product, and system levels and is a participating Senior member of ISA and the Global Cybersecurity.

ISA Security Compliance Institute

Agenda

- Opening Remarks
- Summary of the event
- Subsequent Data
- Product Evolution
- Industry Evolution
- Response Readiness
- CyTRICS
- General Recommendations

ISA Security Compliance Institute

Opening Remarks

- Three and a half years ago cybersecurity experts discovered the world's first known cyberattack on a safety instrumented system.
- The industry consensus is that it prompted a call to action for every industrial process and manufacturing enterprise in the era of the Industrial Internet of Things (IIoT).
- In the same manner that Stuxnet compromised a process control system, what was once considered theoretical became a real threat to every industrial safety system, everywhere in the world, no matter who designed, engineered, built or operates it.
- In this talk I will cover some of resulting changes that have taken place since that initial Triton event, as industry catches up to the cybersecurity needs of today.

Triton Event Reminder – Brief Timeline

- August 4, 2017
  - Unexplained emergency shutdown at end-user site
- Detailed investigation revealed multiple security lapses
  - Enabled sophisticated attack across DCS, SIS, workstations, etc.
  - Malware/RAT injection
- Safety system detected an anomaly
  - Took the plant to a safe state via a shutdown, as it was designed to do
- Highly targeted attack
  - This sample was not a virus that can be easily spread
  - Malware could only be successfully loaded if several conditions are present, including:
    - The site must be using specific model of controller running specific version of firmware
    - The safety network must be accessible either locally or remotely.
    - Attackers must have access to the SIS terminal or other machine connected to safety network
- Sophisticated attack vector demonstrates cause for alarm for every control system vendor and every end user

ISA Security Compliance Institute

Triton Event Summary – Malware Detection

- To gain an understanding of the prevalence of the Malware itself, signatures were shared across the cybersecurity industry
- Schneider Electric itself developed a technique to detect the presence of the malware in a running SIS.
  - The first malware detection capability in an ICS embedded device
  - After hundreds of evaluated systems there were zero indicators of compromise
  - Security tool vendors have not reported any malware detections in production systems

Triton Event Summary – Not Unique

- The attacks' sophistication demonstrates that these incidents are not unique to Triconex controllers; they could have been carried out on any industrial system.
  - In fact, in a research report published by FireEye on April 10, 2019 FireEye revealed another undisclosed site
  - The Triton malware was not present, but the attack group's signature TTPs were present
  - Up to that time, little to no information had been shared on the tactics, techniques, and procedures (TTPs) related to the intrusion lifecycle, or how the attack made it deep enough to impact the industrial processes

Triton Event Summary - 2014

Operational Since At Least 2014

- Reported by FireEye, based on an analysis of the actor’s custom intrusion tools, the group has been operating since as early as 2014.
- It is worth noting that at the time of the Triton incidents, FireEye had never before encountered any of the actor's custom tools, despite the fact that many of them date to several years before the initial compromise. This fact and the actor's demonstrated interest in operational security suggests there may be other target environments – beyond the second intrusion announced – where the actor was or still is present*
  - Reported probes of the Middle East Oil & Gas and US Electric production and distribution grids

* FireEye Report, April, 2019 - https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

Triton Event Summary - TTPs

- See FireEye Report - https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

Triton Event Summary

- In response to the creation and subsequent discovery of the malware, Schneider Electric created a first-of-a-kind tool to detect the presence of the malware in a running site (without the need to shutdown the site)
- Many hundreds of sites were visited and tested with no additional sites found to be compromised
- In addition, we have shared malware signatures with the ICS security industry. No additional Indicators of Compromise have been reported

Triton Event Summary – Industry Wake-up Call

- The global industrial process and manufacturing industry must heed this as a warning.
- Schneider Electric has many recommendations, starting with a thorough assessment of each site’s security posture.
- Schneider Electric does not speculate or participate in any attribution for the Triton attack or any subsequent attack.

Product Evolution – Triconex

- What have we done
- Remember, the Tricon product was an ancillary part of the attack, the real evolution is advances in not only our product to resist this type of attack, but across our full portfolio, across other vendors, and across the security vendors everybody has advanced as a result of the need for continuous evolution

Product Evolution – Triconex

- Security advancements, some in direct response to the malware
  - Digital signing
  - SDL practices
  - 62443-4-1 & 4-2 certification
- 11.4 release in mid-2018
  - For the Tricon CX - TS1131 secure protocol using X.509 certificates.
  - TriStation Protocol now uses sequence numbers to fight man in the middle attacks
  - MP firmware validates addresses passed as arguments on service calls.
  - The MP3009 cannot have memory protection turned off by changing the Machine State Register.
  - The application code is not writable by the application. This prevents the application from changing a program or a function.
  - The static configuration is write protected from the application.
  - A stealth Download Change is not permitted.
- Physical Security
  - Intelligent Safety Enclosure – Alarm if the MP is physically accessed
- Product Certifications, Development Process Certifications

Industry Evolution

- ISA GCA
- Mitre Att&ck Framework for ICS
- Security Vendors
- Endless presentations, research, discussion on the topic has helped get the facts out and understood
- More…

Industry Evolution

ISA Global Cybersecurity Alliance Fast Facts

- ISA Global Cybersecurity Alliance is a collaborative forum to advance cybersecurity awareness, education, readiness, and knowledge sharing
- Membership is open to any organization involved in industrial cybersecurity—end users, automation providers, system integrators, consultants, government agencies, and more
- Founding members establish priorities, but initiatives will include expanding the development and use of industry standards, creating education and certification programs, advocating for cybersecurity awareness and sensible approaches with world governments and regulatory bodies

ISA Security Compliance Institute

Industry Evolution

Objectives of the ISA Global Cybersecurity Alliance

- The objectives of the ISA Global Cybersecurity Alliance include the acceleration and expansion of standards, certification, education programs, advocacy efforts, and thought leadership. Member companies will identify and prioritize initiatives, work to proliferate adoption of and compliance with global standards, and contribute to workforce education and certification programs.
- Members of the Alliance will bring their expertise and experience together to:
- Increase thought leadership and industry-wide awareness
- Expand advocacy and outreach to governments, regulatory agencies, and stakeholder organizations around the world
- Accelerate standards development and adoption
- Share knowledge and information in an open environment
- Extend the ISA/IEC 62443 series of standards to relevant markets and develop application guides that help specific industry verticals apply the standards
- Expand compliance and prevention initiatives
- Provide best practice tools to help companies navigate the entire lifecycle of cybersecurity protection

ISA Security Compliance Institute

Industry Evolution

ISA is the Home of Industrial Cybersecurity Collaboration

- ISA developed the UN-endorsed ISA/IEC 62443 cybersecurity standards
- ISA builds training courses and certificate programs around the standards
- The Automation Federation, founded by ISA, advocates and collaborates with government agencies to advance cybersecurity initiatives
- ISASecure® provides product, system, and development lifecycle certifications
- Automation.com and *InTech* magazine deliver cybersecurity-related news and content

ISA Security Compliance Institute

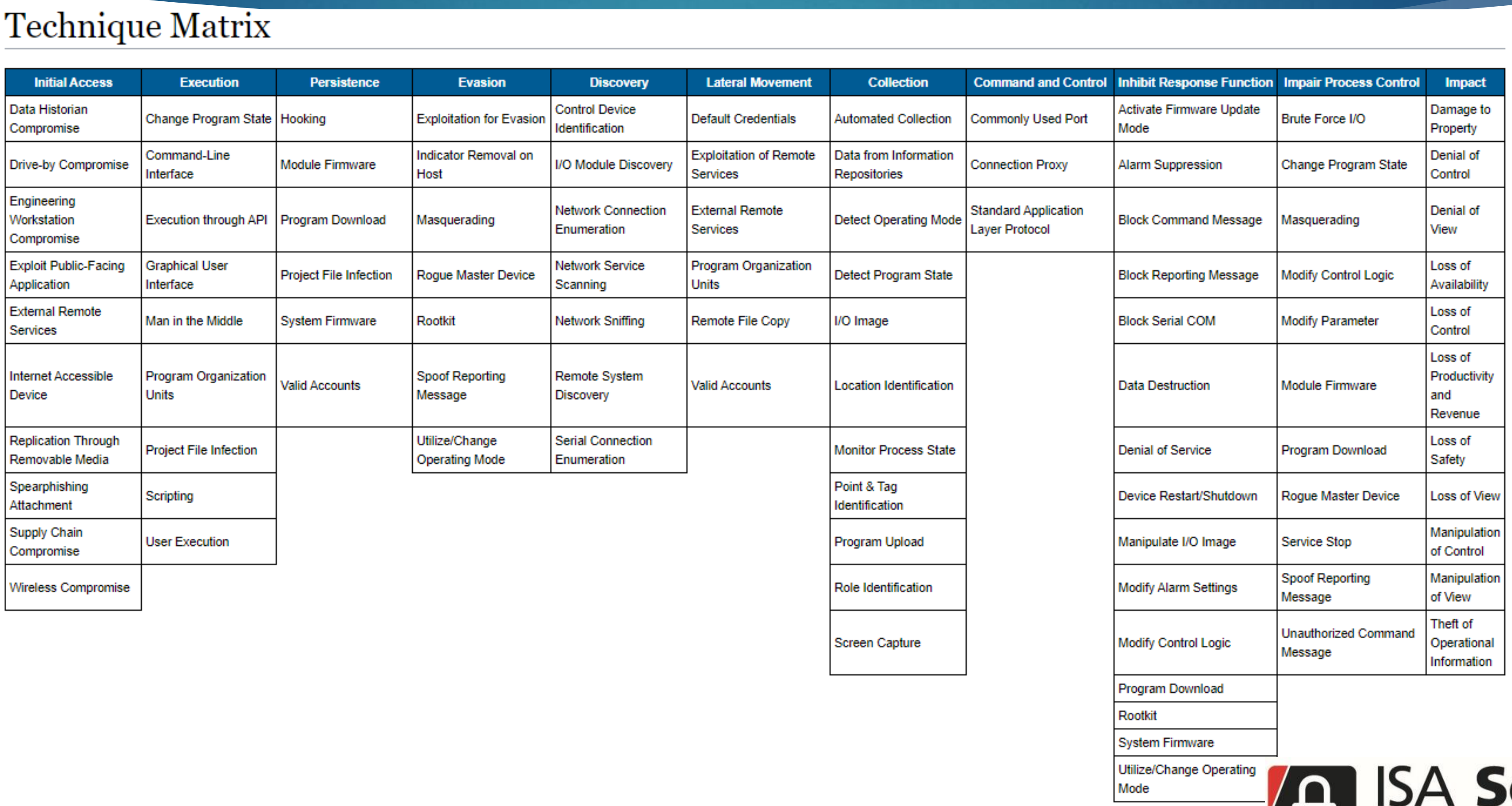
Industry Evolution – Security Tool and Service Vendors

- Many ICS-specific vendors reacted immediately to detect the malware
  - Claroty
  - Nozomi
  - McAfee

  - To name but a few
- Others continue to evolve techniques to detect TTPs as well as the malware
  - Verizon
  - Fortinet
  - Mitre Att&ck Framework for ICS (Currently using Triton as a study case)
- This evolutions are in art due to sharing, our work with partners and the industry

ISA Security Compliance Institute

Industry Evolution – Mitre Triton Study Case

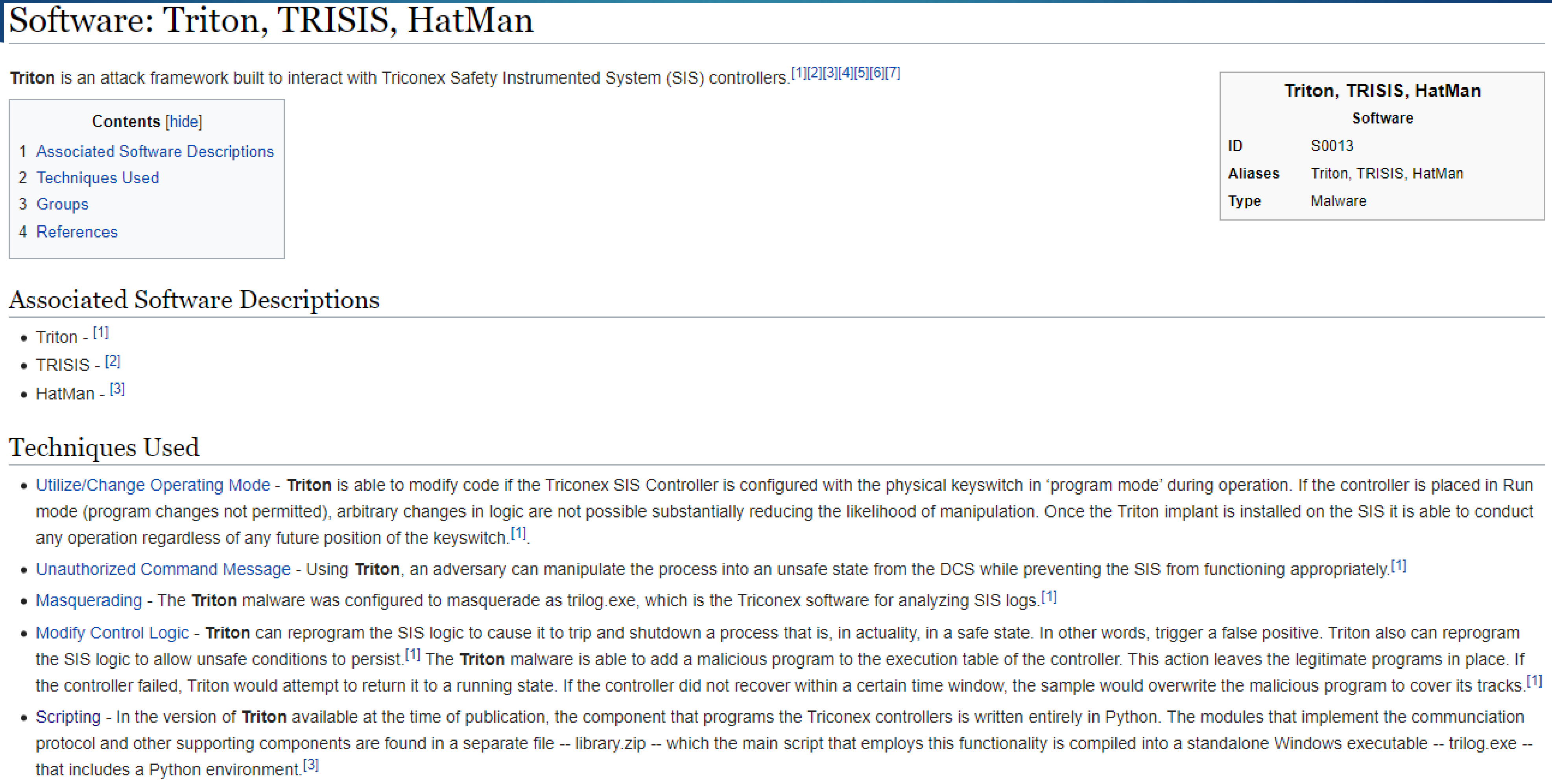


Technique Matrix

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

ISA Security Compliance Institute

Industry Evolution – Mitre Triton Study Case



Software: Triton, TRISIS, HatMan

Triton is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers.[1][2][3][4][5][6][7]

Triton, TRISIS, HatMan	
Software	
ID	S0013
Aliases	Triton, TRISIS, HatMan
Type	Malware

Contents [hide]

Associated Software Descriptions

- Triton - [1]
- TRISIS - [2]
- HatMan - [3]

Techniques Used

- Utilize/Change Operating Mode - **Triton** is able to modify code if the Triconex SIS Controller is configured with the physical keyswitch in 'program mode' during operation. If the controller is placed in Run mode (program changes not permitted), arbitrary changes in logic are not possible substantially reducing the likelihood of manipulation. Once the Triton implant is installed on the SIS it is able to conduct any operation regardless of any future position of the keyswitch.[1].
- Unauthorized Command Message - Using **Triton**, an adversary can manipulate the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately.[1]
- Masquerading - The **Triton** malware was configured to masquerade as trilog.exe, which is the Triconex software for analyzing SIS logs.[1]
- Modify Control Logic - **Triton** can reprogram the SIS logic to cause it to trip and shutdown a process that is, in actuality, in a safe state. In other words, trigger a false positive. Triton also can reprogram the SIS logic to allow unsafe conditions to persist.[1] The **Triton** malware is able to add a malicious program to the execution table of the controller. This action leaves the legitimate programs in place. If the controller failed, Triton would attempt to return it to a running state. If the controller did not recover within a certain time window, the sample would overwrite the malicious program to cover its tracks.[1]
- Scripting - In the version of **Triton** available at the time of publication, the component that programs the Triconex controllers is written entirely in Python. The modules that implement the communciation protocol and other supporting components are found in a separate file -- library.zip -- which the main script that employs this functionality is compiled into a standalone Windows executable -- trilog.exe -- that includes a Python environment.[3]

General Recommendations

- As always, keep your antivirus tools up to date and ensure you are using the latest antivirus .dat files on the engineering workstation where the TriStation terminal is installed.
- Signatures for the malware have been distributed to cybersecurity organizations. Schneider Electric has confirmed that major antivirus vendors now include the malware file’s signatures and that if detected, the antivirus tool takes action.

Response Readiness

- As shown, Schneider Electric and the ICS industry has evolved significantly. But the evolution is not over
- ICS4ICS – Are you ready for the next Triton-like incident?
  - ICS4ICS is an industry driven response for the need to improve incident response readiness
  - A program in cooperation with CISA, and the ICS GCA
  - Lead by Schneider Electric's own Megan Samford

Response Readiness

- The answer must be more than just tools or detection. The entire attack defensive posture must evolve to stop this style of attack at multiple points
  - Traditional Identify, Protect, Detect, Respond, and Recover
  - Now being extended to include Deter and Deceive

Response Readiness - Deterrence

- Deterrence is associated with the prevention of an adversary action through the presentation of a credible cost of action outweighing the adversary's perceived benefits.
- To accomplish this, we present a first-class defense in depth approach (see tradition tactics). Within the framework are techniques to deny benefits of attack (e.g. resist exfiltration) and to impose cost of attack by creating a series of strong defenses denying access. This technique is known as "Denial by Defense"
- See non-cybersecurity US Treasury and DOJ deterrence actions

Response Readiness - Deception

- **Deception** is a technology used to make any solution more resilient to attack by the creation of multiple "decoys".
- These decoys simulate real behavior, are virtual (usually), and are meant to confuse an attacker trying to sort though what is fake and what is real.

Recent Actions

- As always, Schneider Electric does not comment directly on the attribution of the attackers. However, recent actions by the US Government do bear mentioning
  - On Oct 23 The US Treasury imposed sanctions on Russia's Central Scientific Research Institute of Chemistry and Mechanics.
  - This is the group that FireEye has attributed to the Triton attacks
  - The sanctions are meant to deter similar attacks
  - These sanctions were coordinated with the US Department of Justice's indictment of six members of the Russian hacking group, Sandworm, that perpetrated the Ukrainian Blackout attacks and the creation of the NotPetya

Recent Actions - CyTRICS

- CyTRICS aims to enhance the cyber-resilience of critical operation technology (OT) components in the energy sector by identifying vulnerabilities in the digital supply chain and informing those responsible so that improvements in their design and manufacturing may take place.
- The program leverages best in class facilities and analytics at four Department of Energy national labs and strategic partnerships with technology developers, manufacturers, asset owners and operators and interagency partners for coordinated device testing and vulnerability disclosure.

Recent Actions - CyTRICS

- Current state:
  - Pilot program with Schneider Electric, protection relays
  - Lessons learned
  - Triconex testing Q1, 2021
  - Additional product prioritization and testing Q2 and on
    - Foxboro DCS
    - Modicon
    - Other vendors

ISA Security Compliance Institute

Conclusion – A Continuing Call to Action

- Ramifications of TRITON extend far beyond any one site, system and supplier
- The possibility and impact of attacks on industrial systems in the era of the IIoT are escalating
  - And they extend across industries and broader society!
- We have to evolve the security culture across the industry
- We are all responsible for cybersecurity, so we all need to take ownership
- We must tackle the hard topics such as admitting that patching is a poor response to such vulnerabilities, that a more robust approach is needed that includes application self-protection, upgrades, (real) mitigations, partners and better use of signatures

Questions