Industrial Control System Cyberattack Highlights Importance of Defeating Attacker Tactics, Techniques and Procedures (TTPs)

Gartner
COOL VENDOR 2020

Abstract:

New and automated capabilities are needed to defeat attacker tactics, techniques and procedures (TTPs) and protect industrial control system (ICS) infrastructure. Trinity Cyber has invented technology that focuses on identifying and defeating attacker TTPs in network traffic. We deliver dramatically increased security for ICS customers with a true threat prevention capability that significantly enhances existing intrusion prevention systems (IPS), automates and scales existing managed detection and response (MDR), performs content disarm and reconstruction (CDR) inline and at line rate speed (not in a sandbox) and reduces strain on security operations center (SOC) resources. Trinity Cyber's breakthrough technology edits network traffic inline, bidirectionally, to make threats disappear. A recent attack on a U.S. water treatment facility illustrates the importance and application of this new technology.

In 2021, cyberattackers gained access to the supervisory control and data acquisition (SCADA) system of a drinking water treatment facility in Pinellas County, Florida. A remote access program was used to increase the amount of sodium hydroxide (aka lye) in the drinking water from 100 parts per million to 11,100 parts per million, putting thousands of innocent people at risk.[1] Fortunately, the attack occurred during normal business hours. A watchful supervisor physically observed the attempt to adjust the chemical controls, as a cursor operated by the remote intruder moved across the screen and changed settings. Corrective intervention occurred immediately, and a calamity was averted.

Following this attack, the FBI, Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA) and Multi-State Information Sharing and Analysis Center issued a joint advisory highlighting the attack and recommending mitigation measures to other water and wastewater treatment system operators across the country.[2]

> "We have to help all these critical infrastructures … knowing we don't have the benefit of closing down at 5 o'clock every day. How do you upgrade these things and make a system that might have been deployed two or three decades ago—how do you make it resilient against 21st-century attacks?"[3]
>
> **DAMON SMALL** / NCC Group

The importance of improving the security of ICS infrastructure is recognized not only within the industry but also as a national government priority. In July 2021, the Biden administration issued a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems that emphasized that "deploying systems and

technologies that can monitor control systems to detect malicious activity and facilitate response actions to cyber threats is central to ensuring the safe operations of these critical systems."[4] In addition, President Joe Biden held a cybersecurity summit with leading technology companies at the White House in August 2021, where several commitments and initiatives were announced as "part of a broader Biden administration effort to prioritize cyberattacks as a national security and economic threat."[5]

There Is a Better Way

While the attack in Pinellas County was physically observed and stopped while underway, there is a much more effective and comprehensive way to protect ICS infrastructure. Trinity Cyber has invented new technology that:

- Detects attacks, threats and malware using a new and better approach
- Edits network traffic inline to make threats disappear
- Prevents cyberattacks to ensure safe operation of critical ICS systems and business continuity

Current security solutions lack the ability to operationalize rich, contextual information about adversary tactics, techniques and procedures. For instance, existing intrusion detection systems, intrusion protection systems (IPS) and network detection and response (NDR) technologies all have shortcomings in exposing and preventing threats where they actually exist deep within network sessions. Attackers who implement common techniques such as obfuscation, encoding and complexity within files and protocols as part of their attack can and do successfully penetrate the existing cybersecurity infrastructure that has been deployed.

Even when these technologies successfully identify threats, they often cannot or struggle to prevent the attack. Often, they disrupt business continuity, increase alert fatigue and generate excess noise for SOC teams who are already struggling to keep pace. As recently reported by BitDefender.com, "On average, the typical organization wastes anywhere between 424 hours and 286 hours per week on false positives."[6]

Trinity Cyber's Premise

Trinity Cyber's premise is straightforward: Every Internet session can and should be fully staged, parsed and inspected inline (not in a sandbox) in context, before it enters or leaves a customer's control. At the same time, automated processes must be run to remove or alter

malicious content from files and protocol fields at speed and scale to affect the outcome in the favor of the customer. This must be performed without introducing noticeable latency or degrading the customer's Internet experience.

TTPs Are Key to Threat Prevention

Trinity Cyber's technology focuses on attacker TTPs and protects ICS customers from entire classes of actual malware, command and control (C2), remote exploits, drive-by downloads, and in-the-wild malicious threats and techniques that are commonly missed by traditional detect-and-respond systems.

Example Threats Prevented by Stopping TTPs

Attack Type	Trinity Cyber Protection
IoT botnets (Mirai, Hajime, etc.)	Our focus on TTPs prevents delivery and spread of their binary payloads
Malicious Microsoft documents, including those with the latest MSHTML Zero Day as well as many others	Our ability to inspect, sanitize and rebuild Microsoft documents down to their "DNA" before users receive them is unmatched in the industry
PrintNightmare exploits vulnerability in Windows Print Service, allowing remote code execution on any server/workstation with print spooler enabled	Our ability to inspect and meaningfully contextualize traffic neutralizes this threat and others similar to it
Password-protected, encrypted WannaCry ransomware	Deep, full session inspection to discover hidden payloads and disguised extensions that thwart other network defenses. Our understanding of context, including the way a document is delivered and how it is presented, allows us to easily find malicious payloads with extreme accuracy and precision
Revil, aka Sodin or Sodinokibi, is prevalent today and is considered one of the most frequently used ransomware binaries	Our focus on TTPs identifies ransomware through design methods found in the code, versus the comparatively straightforward and less reliable simple file comparison or delivery domains used by other technologies today
Protection against attacks targeting Microsoft systems and software before a patch is available (such as Microsoft Exchange RCE, aka CVE-2021-26854)	As part of Microsoft's Active Protections Program, we detect new exploitations against Microsoft systems/software and protect our customers early, before patches have been released. This helps keep our customers protected and ensures networks are protected between patch release and remediation
MageCart, a criminal gang that steals payment and other information by inserting hard-to-find code into legitimate websites	We scan every script on every web page a customer visits. Malicious scripts are detected and transformed or removed to enable secure, uninterrupted browsing by the user

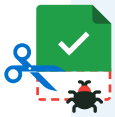
A Closer Look at Trinity Cyber

In a system segregated from the Internet, Trinity Cyber's technology establishes every session at rest, pairing the request and response. Trinity Cyber then fully inspects all Internet traffic at the application layer before it enters or leaves a customer's control by staging, parsing and deeply examining it inline (not in a sandbox). Our patented technology then removes obfuscation that is often challenging for other security technologies and parses protocol fields and files, down to their sub-objects. With this contextually rich view of the session as well as its protocols and payloads, Trinity Cyber exposes the exploitive conditions employed by the adversary—not indicators of compromise, but the actual conditions. We then match responses and neutralize threats inline, in both directions. All of this is performed on average in less than a millisecond and with a *near zero false positive rate.*

Actions Beyond Block and Alert

Trinity Cyber created a new set of actions/automated responses beyond block and alert that prevent attacker TTPs as well as specific threats. Rather than reacting to indicators, these advanced capabilities against threats provide ICS customers real power to prevent attacker techniques, methods and strategies *before they compromise a network.*

These powerful actions can be classified into three categories:



Remove:
The ability to make attacks disappear from network sessions without interrupting the traffic itself, as if the attack never existed. This is useful against threat vectors such as malware delivery, command and control and remote code exploits.

Modify:
The ability to transform attacks from damaging into benign at the file and the protocol levels inside network sessions. This is useful against threat vectors such as scanning, exploitation of unpatched applications and data exfiltration.

Replace:
The ability to swap malicious content for benign (without tipping off attackers). This is useful against threat vectors such as malware beaconing and other techniques that many ransomware gangs employ.

Lessons from Pinellas County

In the case of the Pinellas County water treatment facility, many cybersecurity professionals have pointed to the facility operator running Windows 7, a dated operating system (OS) for which Microsoft ended support a year earlier. Similar reactions were heard in 2017 in response to the WannaCry attack that took advantage of Windows XP, a then 16-year-old operating system that issued its last service pack in 2008. Even after the attack, millions of users continued to operate Windows XP systems. The operational reality of simply migrating to a modern OS on all computer systems is not always feasible or straightforward to implement.

> "Over 70% of the industrial control system (ICS) vulnerabilities disclosed in the first half of 2020 were remotely exploitable through a network attack vector."[7]
> **SECURITYWEEK** / August 2020

There are often numerous challenges associated with migrating from one operating system to another, and this is particularly true for industrial control systems. The software supporting these control systems is often written for a particular version of a specific operating system, and changing one may require changing all at each and every facility. The associated testing and deployment for these kinds of upgrades can pose significant challenges, not to mention cost and budget constraints. The inconvenient truth behind many successful cyberattacks is that many critical ICS operators have limited options when it comes to upgrading their systems—and attackers know it and exploit it.

Alternatively, what if threats facing these outdated systems could be prevented with a new technology that provides ICS operators additional time to plan, resource and execute patch cycles and upgrades?

Trinity Cyber Flagship Service

Trinity Cyber's breakthrough technology is available as a Flagship Service that operates outside the customer's traditional security perimeter. It functions as a transparent, bidirectional, store-and-forward proxy and inspects all network traffic before it enters or leaves a customer's control in real time, with session-level awareness. Our deep inspection examines the entire session, parses out individual protocols and file types, and even decodes and decompresses objects to expose attacker TTPs and threats.

Virtually instantaneously as threats are exposed, Trinity Cyber triggers automated actions to remove, modify or replace malicious content from files and protocol fields at speed and scale to prevent attacks and protect ICS customer traffic and infrastructure. This is all executed seamlessly in less than a millisecond and with a near zero false positive rate. Every action comes with a detailed telemetry record about the threats and actions taken—something that can also be consumed via a flexible application programming interface (API).

Secure ICS Networks With a Powerful New Technology

Trinity Cyber's Flagship Service is offered as a fully managed service delivering clean traffic and safe connections to the Internet:

- An inline **IPS** product and automated **MDR** capability that combine to deliver **clean traffic**
- **Content disarm and reconstruction** capability performed inline with **no latency**
- **Preventive controls** that reduce manual incident response and **increase operational efficiency**
- Extensible **threat intelligence** that allows ICS customers to protect **all of their systems**
- **Bidirectional controls** that enable ICS customers to achieve targeted **data loss prevention**
- Preserved **forensic data** to greatly improve **incident response and remediation**
- Advanced **threat hunting** and 24/7/365 technical support to **reduce strain on SOC teams**

We've designed our managed service specifically to speed adoption, minimize operational complications and deliver value as quickly as possible. The Flagship Service is managed by some of the most skilled cybersecurity professionals in the industry with decades of experience managing and operating the most sensitive and demanding networks in both the public and private sectors. Our experts extend the security capabilities of infrastructure operators by leveraging a cutting-edge new technology along with decades of experience and expertise in combating and defeating the most sophisticated nation state adversaries.

Cybersecurity Technology	Flagship Service Feature	Flagship Service Function	ICS Customer Benefit
Intrusion prevention system (IPS) and automated managed detection and response (MDR)	Deep inspection of full sessions bidirectionally coupled with automated response actions edit network traffic inline and make threats disappear	Prevents attacks coming from/ going to a customer network before threats can interact with customer infrastructure	Clean network traffic bidirectionally for uninterrupted, secure business operations
Intrusion prevention system, managed detection and response and content disarm and reconstruction (CDR)	Discovery of TTP threats (one to many) inflight with simultaneous automated response actions; modify, remove and replace are used to edit the contents of network traffic to make threats disappear at average latency of < 1ms	Prevents attacks before threats interact with customer infrastructure, significantly reduces need for manual incident response and lets SOC teams focus on high-priority incidents	Significantly reduced need for manual incident response and greater productivity from SOC resources
Threat intelligence and forensic data	Descriptions of actions taken, threat descriptions and associated metadata provided and available	Actions taken, threat descriptions and associated metadata can be collected, combined and analyzed with data from other cybersecurity infrastructure components	Detailed descriptions of defeated threats deliver transparency, yield insights and potentially initiate actions on other security infrastructure elements. Enriched threat intelligence for SOC team analysis
Managed detection and response	Continuous development and refinement of formulas increases security and available to customers via updates	All customers benefit from the development, refinement and sharing of formulas increasing security against new threats	Enables customers to protect other cybersecurity infrastructure and allows it to perform better/in a more scalable way
Data loss prevention (DLP)	Prevents attacks attempting to enter or coming from customer networks to achieve DLP, including C2 threats; lens and aperture is wider and more accurate	Bidirectional automated preventive control capabilities prevent both infiltration and exfiltration of data	Customers achieve their DLP targets
SOC team operations and productivity	24/7/365 support	Customer SOC teams are ”virtually extended” by team of Trinity Cyber security experts providing expertise and guidance	24/7 tech support reduces strain on customer SOC teams
Threat hunting	Advanced threat hunting/deep inspection of full session and protocols	Going beyond log analysis into content analysis of full session traffic	Advanced threat hunting; discovery of new and emerging threats

Putting It All Together

The following use cases are two examples that highlight the impact and importance of Trinity Cyber's Flagship Service for ICS customers:

CITRIX VULNERABILITY USE CASE

According to the Dragos 2020 ICS Cybersecurity Year in Review report, one of the top two techniques used by adversaries to gain access to control systems is spear phishing.[8] There are three key phases of any adversary's activity—reconnaissance, access and control. Before acquiring access to a specific system in the control network, the adversary will typically perform some form of reconnaissance to identify a vulnerability that can be exploited. The information gleaned from the reconnaissance will inform how access to the target system can be achieved. Once access is gained, the attacker delivers malware that provides remote control of the target system. Once access to a sensitive system has been acquired, the attacker can cause significant damage to both electronic and physical systems.

The report highlights a specific attacker that leverages a Citrix vulnerability (CVE-2019-19781) to target North American electric oil and gas entities. Identifying this vulnerability will propel many security professionals to focus on patching that system and installing sensors within the network to identify whether an intrusion has already taken place—all necessary but time-consuming work. Time is what gives the adversary the advantage. To assess whether a facility has the vulnerable Citrix version, the adversary performs reconnaissance on the target system by sending a request for a file using a technique called "directory traversal." Allowing directory traversal is the heart of this vulnerability—enabling an adversary to get to wherever they need on the server, whether it is authorized or not. If the Citrix server is vulnerable, it will respond to such a request with a "200 OK" approval notification, signaling to the adversary that the system is vulnerable to CVE-2019-19781. This vulnerability ultimately leads to remote code execution for the adversary.

Trinity Cyber detects attempts to exploit Citrix servers by analyzing HTTP request and response traffic at the session level—providing unparalleled flexibility to detect both scanning activity as well as remote exploitation attempts. By combining this logic, we uncover the full range of threat vectors that face vulnerable Citrix infrastructure from unauthenticated access and remote code execution. Within an attack on a Citrix server, stages are especially important. Trinity Cyber responds differently depending on which common vulnerabilities and exposures (CVE) and stage is inherently detected—ranging from modification of HTTP content to providing invalid non-vulnerable responses to

awaiting attackers. The advanced modify, remove and replace actions we provide (beyond block/alert) provide options to maneuver or act against these various stages as well as enable critical ICS business operations to continue.

LOOKBACK MALWARE USE CASE

In another example, the Dragos report highlights an adversary who leverages LookBack malware, a modular framework of malicious executables designed to enable further control and persistence. LookBack campaigns abuse macro functionality inside Microsoft Office documents. LookBack decodes these modules using a utility that validates stored certificates. Once delivered to a victim system, macros that are enabled by an unsuspecting user trigger this same utility to deploy multiple LookBack modules.

Detecting this threat requires deep file examination of the complex internal proprietary containers within a Microsoft Office document, called Object Linking and Embedding (OLE) objects. This depth of interrogation is sometimes performed by antivirus software once a file has already been downloaded. Even with this deep level of host-based interrogation, the content of legitimate-looking certificates is ignored by most antivirus software. This condition enables adversaries to sneak executable content into the body of legitimate-looking certificates. Trinity Cyber not only detects the executable content within legitimate-looking certificates buried within OLE objects but also removes the executable content in flight independent of the specific code or specific file that housed the code, rendering the entire technique inert. All inspection and removal of code occurs inline before the content reaches its destination in less than a millisecond, keeping users and network assets safe—and adversaries guessing.

Conclusion

There is a renewed focus on securing ICS infrastructure from within the industry as well as the federal government. An opportunity to dramatically increase ICS infrastructure security is now possible with a technology breakthrough that makes threat prevention achievable. Trinity Cyber's Flagship Service, managed by the most skilled cybersecurity professionals in the industry, is a "security multiplier" for ICS customers to protect, automate, scale and boost the performance and capabilities of existing security infrastructure and assets such as IPS, MDR, CDR, DLP, threat intelligence, threat hunting and SOC operations.

The Pinellas County water treatment attack is a cautionary example of the importance and necessity of protecting ICS infrastructure in a new and more effective way by preventing attacks. Trinity Cyber's breakthrough technology and Flagship Service make threat prevention attainable to dramatically increase ICS security and complement existing security infrastructure.

Endnotes

1. "Hacker Tried to Taint Florida City's Water with Lye, Sheriff Says," CNBC, Feb. 8, 2021.
2. "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," CISA, Feb. 11, 2021.
3. "Florida Water Hack Highlights Risk of Remote Access Work Without Proper Security," CNN, Feb. 13, 2021.
4. "Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure," White House Fact Sheet, July 28, 2021.
5. "Biden Tells Top CEOs at White House Summit to Step Up on Cybersecurity," Washington Post, Aug. 25, 2021.
6. "Every Hour SOCs Run, 15 Minutes are Wasted on False Positives," Bitdefender Business Insights Blog, September 2, 2019.
7. "Over 70% of ICS Vulnerabilities Disclosed in First Half of 2020 are Remotely Exploitable," SecurityWeek, Aug. 19, 2020.
8. "ICS Cybersecurity Year in Review," Dragos, Feb. 24, 2021.

Trinity Cyber

Gartner
COOL
VENDOR
2020

© 2022 Trinity Cyber, Inc. CONFIDENTIAL AND PROPRIETARY

Trinity Cyber was named a Cool Vendor in Gartner's Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., Sept. 30, 2020.

The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

trinitycyber.com