An Attack on a U.S. Water Treatment Facility Makes the Case for a More Comprehensive ICS Solution

Gartner COOL VENDOR 2020™

Abstract: A recent attack on an American water treatment facility shows that while private industry and the federal government are rapidly improving the quality and richness of shared threat intelligence, the automated tools and systems used to protect critical networks are unable to make practical use of the information to prevent intrusions. Until now. Trinity Cyber has invented an active sensor that combines a new and extremely accurate approach to detection with technology that can interfere with command and control traffic and actively strip or edit malware and remote code execution from Internet sessions in line. The breakthrough in engineering represents a dramatic evolution in active network security, and the ability of this technology to insulate critical infrastructure will be one of its most important applications.

In early 2021, unidentified cyberattackers gained access to the control system of a U.S. drinking water treatment facility in Pinellas County, Florida. The attackers used a remote access program to access a control system and instructed it to increase the amount of sodium hydroxide in the drinking water, from 100 parts per million to 11,100 parts per million.[1] Fortunately, the attack occurred during business hours and a supervisor actually saw the attempt to tamper with the chemical controls, as a cursor operated by the remote intruder moved across the screen and changed settings. The supervisor was able to intervene to prevent a calamity.

In the days that followed, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a joint advisory highlighting the attack and recommending mitigation measures to other water and wastewater treatment system operators across the country.[2] The ease of gaining access and the magnitude of the consequences narrowly avoided in this incident highlights our vulnerability and adds one more log to the growing signal fire from critical infrastructure operators beckoning for help.

> *"We have to help all these critical infrastructures as much as we can 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?"*
>
> ***Damon Small, who works with oil and gas companies.***
> ***(CNN 02/21)***

The same old answers will not suffice.

Current security solutions lack the ability to operationalize rich, contextual information about adversary tactics. To achieve better security, a new approach is necessary. Before Internet traffic enters or leaves any network containing sensitive information or digital controls, it must be staged in a stateful manner, fully parsed and thoroughly interrogated up to the application layer for the presence of exploits and known techniques for hiding and delivering those exploits—and this must occur outside the network being defended, for the network might be compromised already. This work must be performed by hardware and software that is not connected to the open Internet.

Most of today's existing cybersecurity appliances are connected to both the open Internet and the network they are trying to defend. This leaves the vulnerable to attacks from outside or inside the network being defended.

The trade-off has led to compromises in security.

The status quo in cybersecurity relies on layers of necessary but insufficient automated controls and manual incident response. Meaningful automated prevention has not previously been available due to practical business and technological limitations. These limits

[1]https://www.cnbc.com/2021/02/08/hacker-tried-to-taint-florida-citys-water-with-lye-sheriff-says.html
[2]https://us-cert.cisa.gov/sites/default/files/publications/AA21-042A_Joint%20Cybersecurity%20Advisory_Compromise%20of%20U.S.%20Water%20Treatment%20Facility.pdf

have placed network performance in tension with network security for the past decade. Roughly stated, network security tools have self-imposed limitations that result in cursory inspections of Internet traffic using algorithms to guess which traffic might be bad based on previously identified indicators of compromise. It has not been previously feasible to look deeply into the fully assembled content of an Internet session for the actual presence of exploitive conditions.

The existing approach adds value, but misses a lot of malicious activity and produces a large volume of false alerts. A significant amount of a cybersecurity team's time is spent responding to these false alerts. According to a recent article from BitDefender.com, "On average, the typical organization wastes anywhere between 424 hours and 286 hours per week on false positives."[3] On average, that's 15 minutes out of every hour. These tools need to improve. It has not been previously feasible to look deeply into the fully assembled content of an Internet session for the actual presence of exploitive conditions. Until now.

Trinity Cyber developed technology that can provide truly preventive controls at line rate speed—and it represents the next evolution in Intrusion Prevention Systems (IPS). The technology can thoroughly, deeply, and precisely interrogate **and modify** full session network traffic at line speed, averaging a sub millisecond processing latency. In other words, every Internet session can be fully staged, parsed, and inspected in flight, at line speed (not in a sandbox) in a manner that combines the best attributes of network perimeter security with the depth, accuracy, and fidelity of application layer endpoint security. Malicious content can be removed, altered, or replaced without interrupting customer business operations or arming the hacker with feedback.

In the case of the Pinellas County water treatment facility, many cybersecurity professionals have blamed the facility operator for still running Windows 7, a dated operating system for which Microsoft ended support a year earlier. We heard similar reactions to the 2017 WannaCry attack that took advantage of Windows XP, a then 16-year-old operating system that was issued its last service pack in 2008. Millions of users were still using it.

Reality is not so cut and dried for industrial control systems.

There are often numerous difficulties associated with changing operating systems. Especially for systems running industrial control systems. The software supporting those controls is often written for a specific version of specific operating systems. Changing one can necessitate changing all, which can be a costly proposition. And that's just one system at one facility. The hidden and often inconvenient truth behind many successful cyberattacks is that many critical infrastructure operators have limited options when it comes to upgrading their systems—and the bad guys know it.

But what if we could neutralize the threats facing these outdated systems and buy critical infrastructure operators additional time to plan, resource, and execute costly upgrades?

At Trinity Cyber, we understand the attackers' models and the techniques and have the ability to reach into each network session and counter those techniques. We go beyond blocking the simple things like malicious IP addresses or files that have made their way to deny lists. Instead, we remove the actual artifact that seeks to exploit a vulnerability. We remove the code used to control the malware that an adversary may have already installed. We apply a safety critical approach and add a critical preventive control.

While this sounds simple and intuitive, it is extraordinarily complex. To provide this level of real-time mitigation, Internet sessions must be decoded, parsed, and fully interrogated to the depth necessary to see these techniques. Infected areas across multiple stages of attack have to be neutralized, while simultaneously reconstructing the protocols and file contents in near real time. While this may seem impossible, it's not. It requires a team of innovators, engineers, analysts, and mission-driven professionals with decades of experience in advanced parallel processing, switching, and load balancing for America's most critical networks. It can be done—and Trinity Cyber is the ***only*** company capable of doing it today.

> *"Over 70% of the industrial control system (ICS) vulnerabilities disclosed in the first half of 2020 were remotely exploitable through a network attack vector, industrial cybersecurity company Claroty reported on Wednesday."*
> ***(SecurityWeek, August 2020)***

[3]https://businessinsights.bitdefender.com/every-hour-socs-run-15-minutes-are-wasted-on-false-positives

Clear benefits:

- ✓ Elite technicians, malware analysts, and reverse engineers operate our highly performant technology on the customer's behalf, allowing us to offer a capability run by experts in expert mode. The results are impressive and the benefits scale exponentially.
- ✓ This approach significantly increases network security with a near zero false detection rate.
- ✓ The technology performs a deeper inspection faster and more accurately than IPS alone, and does more than just block threats; it sanitizes corrupted traffic with automated responses that include replacing or altering files, code segments, and protocol fields in flight.
- ✓ It provides protection for customer networks and security appliances independent of the systems or composition of the protected network. Heterogeneous networks with uneven patching schedules gain significant value.
- ✓ When added to high-end, widely used firewalls equipped with threat prevention, Trinity Cyber always identifies additional threats and on average detects and prevents 30% more. These numbers go up significantly for threats hidden within Microsoft Office documents, which are arguably one of the most common source of data breaches and one of the most difficult to accurately detect.
- ✓ An extremely low false detection rate of less than one-tenth of 1% means that cybersecurity teams using Trinity Cyber will spend less time chasing meaningless events and more time securing enterprises—saving considerable time and money

SPECIAL NOTE:
For networks affected by the SolarWinds exploitation

- The SolarWinds Orion compromise was a sophisticated supply chain attack. The adversary who carried out the attack had access to production source code and the ability to surreptitiously insert malicious logic into that code before it was digitally signed and provided out to customers by SolarWinds as a seemingly legitimate software update. This clever and sophisticated method made it impossible for any SolarWinds customer to have been able to detect the attack.
- The adversary designed this attack such that once a customer installed the SolarWinds Orion software update, a backdoor was created with system administrator, privileged access that allowed the adversary to download and install whatever they wanted. Given that it is widely believed that the adversary is a foreign government's Intelligence Service, and they have enjoyed full, highly privileged access for more than six months, they own everything—or at least everything they care about. This includes user accounts, PII, servers, IT infrastructure, and security software and appliances.
- As a result, any customer of SolarWinds Orion must assume that a foreign government has widespread, persistent access to and control of their networks. The hackers abandoned long ago the infrastructure and static indicators associated with the initial backdoor delivered with the attack. Removing SolarWinds Orion does not address what has likely already been installed in their networks by the adversary.
- While long-term remediation tasks are being performed, immediate steps can and should be taken to thoroughly and accurately inspect bi-directional, full-session network traffic.
- Because the security appliances on corrupted networks also could be compromised, traffic inspection of this sort must be performed outside the network, in line (not in a sandbox) and out of band in a manner that can detect and neutralize command and control traffic, remote code execution, exfiltration of data, and embedded malicious code. Trinity Cyber's technology was designed from the ground up to operate in this manner and can detect and prevent network threats that Next Generation Firewalls and IPS cannot—including command and control traffic within protocol fields and file content.

As public and private sector entities consider new security approaches and deploy passive detection capabilities instrumented at the Internet facing ingress and egress points of critical infrastructure networks, they should consider Trinity Cyber's active capability designed to complement existing tools and to make operational (practical) use of rich threat intelligence to deeply interrogate network traffic, uncover and thwart entire attack family methods and techniques.

Two practical use case examples follow.

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.[4] 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 the attacker has gained access to a sensitive system, they can cause significant damage to both electronic and physical systems.

The report goes on to highlight a specific attacker that leverages a Citrix vulnerability (CVE-2019-19781) to target North American electric and 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 if 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—giving us unparalleled flexibility to detect both scanning activity as well as remote exploitation attempts. By combining this logic, we can find 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 matter. Trinity Cyber responds differently depending on which CVE and stage is inherently detected—ranging from modification of HTTP content, to providing non-vulnerable responses to awaiting attackers. Having options to maneuver or act against these various stages provides flexibility and enables business operations to continue. This approach protects the perimeter of the IT network, which if compromised, could be used as a pivot into non-Internet connected ICS networks.

[4]https://www.dragos.com/year-in-review/#section-report

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 in a Microsoft Office document, called Object Linking and Embedding (OLE) objects. This depth of interrogation is sometimes performed by anti-virus 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 we also remove the executable content in flight independent of the specific code or specific file that housed the code, rendering the entire technique inert. All of this inspection and removal of code occurs in line, in flight, before the content reaches its destination in less than a millisecond.

What does this mean for a user? Trinity Cyber completely removes ***the use*** of the tactic by an advanced adversary independent of the specific malicious code hidden in the Office document without impacting Microsoft Office's functionality. In other words, adversaries can develop many variants of code to perform a vast array of malicious deeds based on one particular method of exploitation. ***Trinity Cyber creates conditions necessary to protect against every variant of the method used by the adversary, independent of the specific code.***

THE TAKEAWAY

With Trinity Cyber, there is an additional approach to insulate critical infrastructure networks from advance persistent threats. Trinity Cyber is designed to complement passive detection capabilities instrumented at network ingress and egress points with active capabilities designed to deeply interrogate network traffic so as to uncover and thwart entire attack family methods and techniques.

Additionally, as the federal government's information sharing capabilities continue to expand, public and private sector entities can further empower these systems through an intelligence sharing program with the government. This symbiotic relationship would create an advanced public-private threat intelligence sharing construct that could empower the United States to protect its critical infrastructure backbone at these protected enclaves.

The Trinity Cyber form factor exists in the major Internet hubs at Equinix data centers and is deployed on premises to large, critical customer sites. Traffic moves to and from Trinity Cyber infrastructure at Internet Layer 2. All development, command, and control, as well as client-specific (or derived) data, exists in an out-of-band, private, Suite B encrypted network.

Passive and active sensors also can be physically positioned such that a relatively few number of systems could service a relatively large number of critical facilities—all receiving the same expert-level protection within protected security enclaves.

Trinity Cyber possesses the only capability that can interrogate Internet sessions to the depth necessary to identify attack methodologies in flight. Moreover, detection is coupled with real-time action designed to neutralize attack methods and make critical vulnerabilities operationally irrelevant. As the new administration contemplates which actions take priority in addressing the vulnerabilities of our nation's critical infrastructure, Trinity Cyber's commercial capabilities must be part of the active solution. Empowered by sensitive threat intelligence delivered through an advanced public-private sharing construct, we can begin to make terrifying events like the Pinellas County water treatment facility a thing of the past.

 trinitycyber.com

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