Trend Micro Incorporated
Research Paper
2013

Who's Really Attacking Your ICS Equipment?

By: Kyle Wilhoit

LEGAL DISCLAIMER

Contents

Introduction

Industrial control systems (ICS) are devices, systems, networks, and controls used to operate and/or automate industrial processes. These devices are often found in nearly any industry—from the vehicle manufacturing and transportation segment to the energy and water treatment segment.

Supervisory control and data acquisition (SCADA) networks are systems and/or networks that communicate with ICS to provide data to operators for supervisory purposes as well as control capabilities for process management. As automation continues to evolve and becomes more important worldwide, the use of ICS/SCADA systems is going to become even more prevalent.

ICS/SCADA systems have been the talk of the security community for the past two years due to Stuxnet, Flame, and several other threats and attacks. While the importance and lack of security surrounding ICS/SCADA systems is well-documented and widely known, this research paper illustrates who's really attacking Internet-facing ICS/SCADA systems and why. It also covers techniques to secure ICS/SCADA systems and some best practices to do so.

What Do Typical ICS Deployments Look Like?

A typical deployment often has a segregated SCADA network that is either connected via a firewall or air-gapped from the Internet. As in most ICS deployments, firewalls are a rarity, so please keep in mind that a firewall is not shown in the following diagram for this reason. There was also no mention of firewalls throughout the analysis.

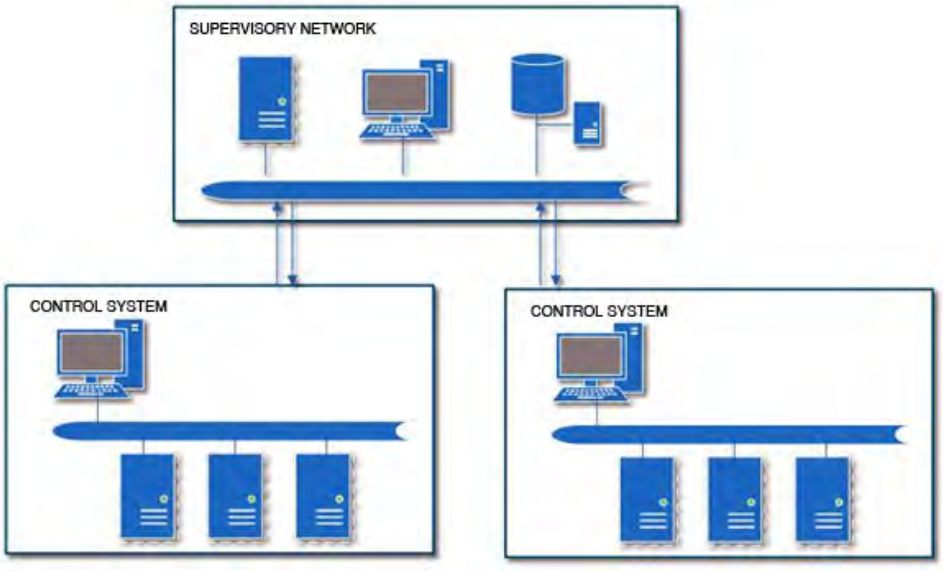


FIGURE 1: Simple ICS/SCADA system deployment

How ICS/SCADA Systems and IT Systems Differ

ICS/SCADA and IT system security, while similar in function, greatly differ in terms of priority. These systems, unfortunately, have different ideas as to what security is and how to stay secure. Each system type has unique uptime requirements, risk-avoidance tactics, architectures, goals, and performance requirements.

IT system security's first priority is typically known to protect data and help employees continue working without being interrupted. ICS/SCADA system device security, on the other hand, is known to focus on protecting the reliability of data without affecting productivity. Because of unique differences, securing ICS/SCADA systems must also be treated uniquely and approached with care.

Security After the Fact

Security in an ICS/SCADA network is often considered "bolt-on" or thought of "after the fact." When these systems were first brought into service more than 20 or so years ago, security was typically not a concern. Many of them, at that time, were not even capable of accessing the Internet or connecting to LANs. Physical isolation addressed the need for security.

However, as things changed over time, most of these systems' purposes have been reestablished, along with the way they were configured. A system that used to only be accessible to a single computer next to a conveyor belt became accessible via the Internet, with very little hindrance.

Internet-Facing ICS/SCADA Systems, Why So Insecure?

Disturbing evidence recently surfaced to prove the insecurity of ICS/SCADA devices. More importantly, this trend of insecurity continues to grow as more and more devices are connected to the Internet.

Through the power of the Internet, one can easily perform some Google-dorks searches and find embedded systems that are exposed to the web, some of which have been so since 2010 or even earlier.

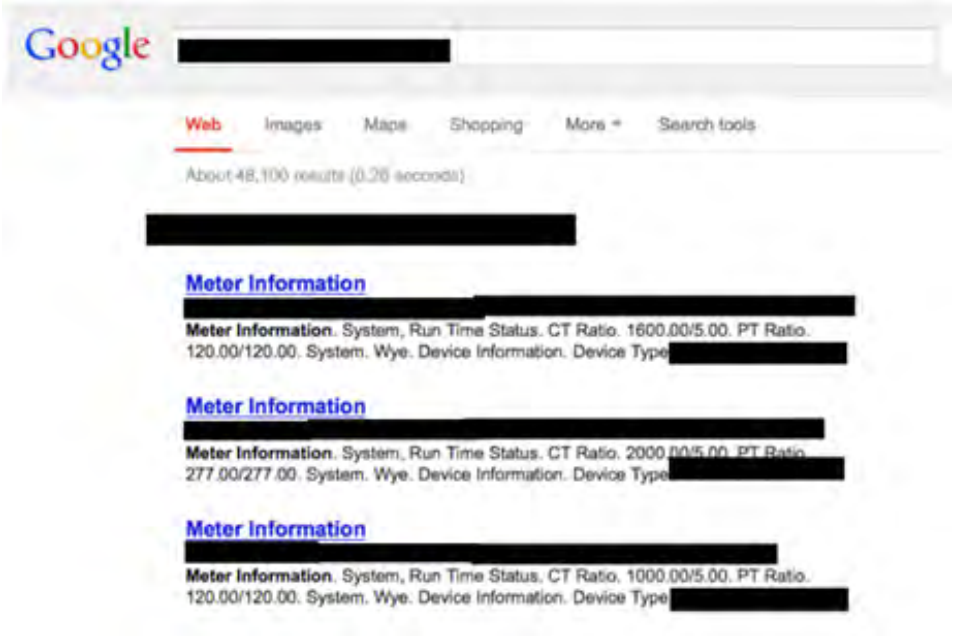


FIGURE 2: Google-dorks search showing ICS/SCADA systems

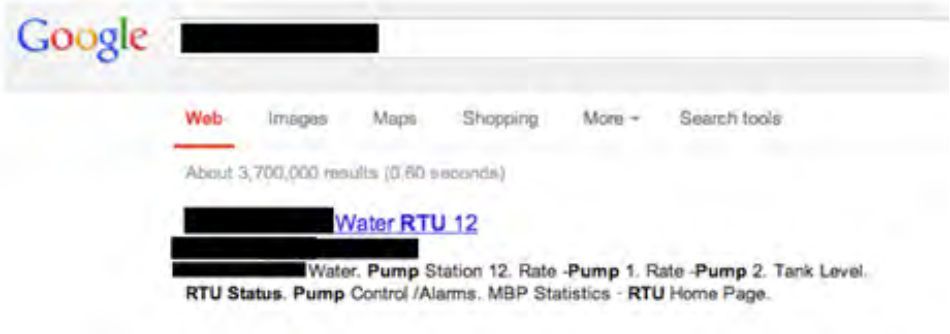


FIGURE 3: Google-dorks search that easily located a water-pumping station

Unfortunately, at the time of testing, these devices were not only Internet facing, they did not have security mechanisms to prevent unauthorized access as well. We contacted the companies in question and law enforcement agencies, which are in the process of remedying our findings.

Google-dorks searches can help identify machines but attackers use another popular site—Pastebin—to distribute their findings. A disturbing trend that is starting to pop up on Pastebin involves posts containing data on ICS/SCADA devices like IP addresses and other identifiable information.

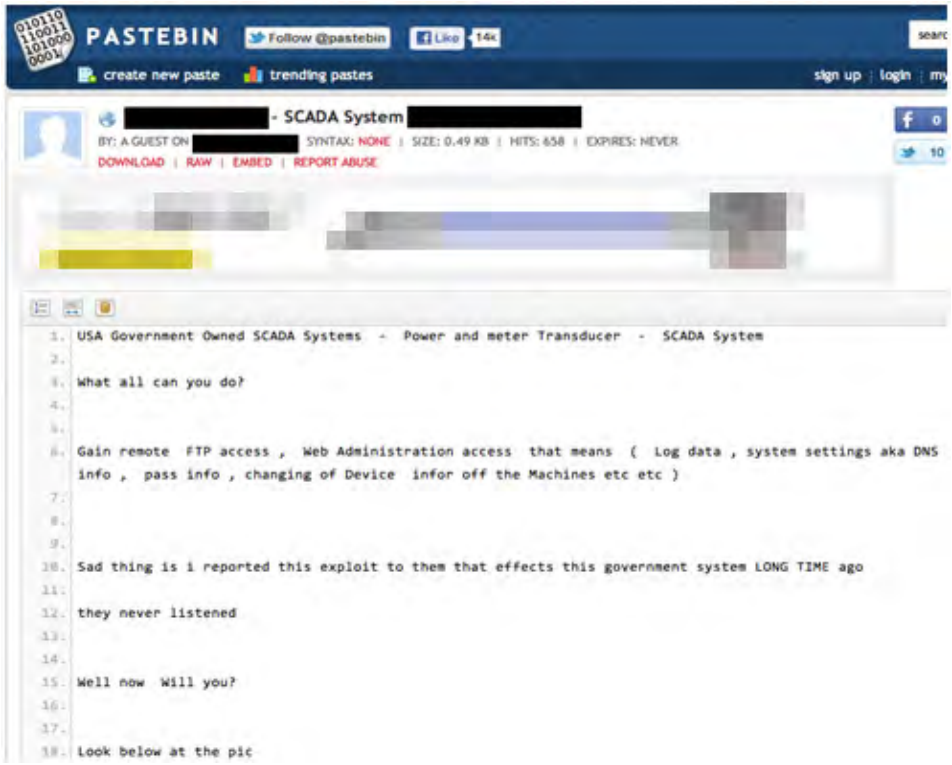


FIGURE 4: Pastebin post listing down ICS/SCADA device information

ICS/SCADA Systems Are Always Attacked, Right?

While Flame, Duqu, and Stuxnet were garnering media coverage, we set out to find samples to see what they were really targeting and via what method. Without knowing if Internet-facing ICS/SCADA systems were attacked, we set out to develop a honeypot architecture that would emulate several types of ICS/SCADA devices and mimic those that are commonly Internet facing. The honeypots had traditional vulnerabilities found across similar systems, showcasing a very realistic honeypot environment.

The objective of the honeypot deployment is to assess who/what is attacking Internet-facing ICS/SCADA devices and why. In addition, this research set out to identify if the attacks performed on these systems were targeted, by whom, and for what purpose.

There has been constant debate in the information security world surrounding the validity of ICS/SCADA system-related incidents and attacks. According to recent research conducted by ICS-CERT, in 2012 alone, 171 unique vulnerabilities affecting 55 different ICS vendors were found.[1]

The honeypot architecture design uses a combination of high-interaction and pure-production honeypots. A total of three honeypots were created to ensure that we cover as much of the target surface as possible. All three honeypots were Internet facing and used three different static Internet IP addresses in different subnets scattered throughout the United States. A high-interaction honeypot imitates the activities of the real systems it mimics. As such, a programmable logic controller (PLC) system running on a virtual instance of Ubuntu hosted on Amazon EC2.

This cloud-based Amazon EC2 instance was configured as a web page that mimics that of a water pressure station. This web server was simply an Apache web server with custom-developed web pages to mimic the exact functions of a PLC system.

The tools to aid analysis on the honeypot included snort, honeyd (modified to mimic common SCADA protocols), tcpdump, and several others to help monitor the system.[2] In addition to network monitoring on the honeypot, local log files were also sent to a central syslog server to ensure that logs were kept intact.

1 http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf
2 https://www.snort.org/; http://www.honeyd.org/

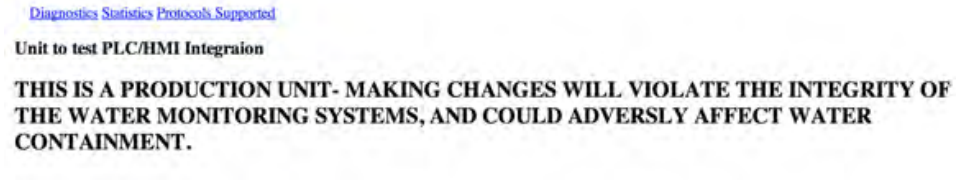


FIGURE 5: Web page hosted on the high-interaction honeypot and exposed to the Internet

The traditional web server hosting the page that appeared to be a control station for water pumps could also emulate port 502 or Modbus, FTP, and HTTP services.

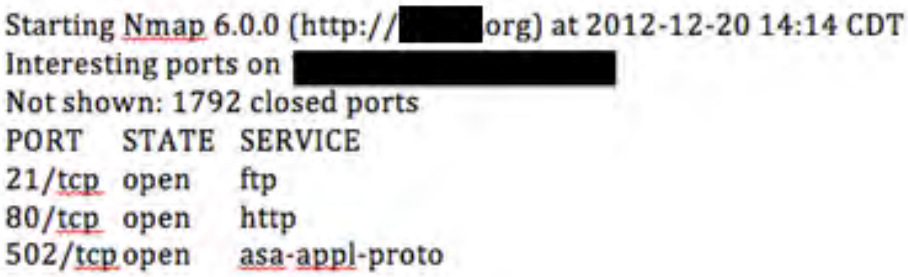


FIGURE 6: Port scan showing open ports on the high-interaction honeypot

In addition to the high-interaction honeypot, we also used a pure-production honeypot, which was hosted on a Dell DL360 server running PLC software programs and a web server.

A pure-production honeypot is a physical server created to be a mirror of a real production system of the same type. In this case, the server mimicked the function of a human machine interface (HMI). This server, when modified, hypothetically modified a PLC connected to the HMI.

FIGURE 7: Screenshot showing a pure-production honeypot hosted on a Dell DL360 server

Finally, an actual PLC device called a "Nano-10" from Triangle Research was utilized.[3] This PLC device in our honeypot environment could also be considered a pure-production honeypot. It was set up to mimic temperature controllers in a factory and had temperature, fan speed, and light settings that could be modified. The PLC was set with default login credentials, as is a common practice when using PLC systems, and had a password-protected administration section that also had default credentials. All of the settings were set to defaults with no modifications of any sort, leading attackers to believe the PLC system is a newly deployed device that has not been configured yet.

Modifying the settings of this device would physically alter the PLC system, which would mimic a catastrophic change to a SCADA system on the back end.

Architecture

In sum, two types of architecture were utilized in the honeypot design. The first was a high-interaction honeypot, which could be characterized as a trap that imitates the activities of a production system. Often, as in the case of the ICS honeypot, this runs on a production system in its entirety with service emulation occurring.

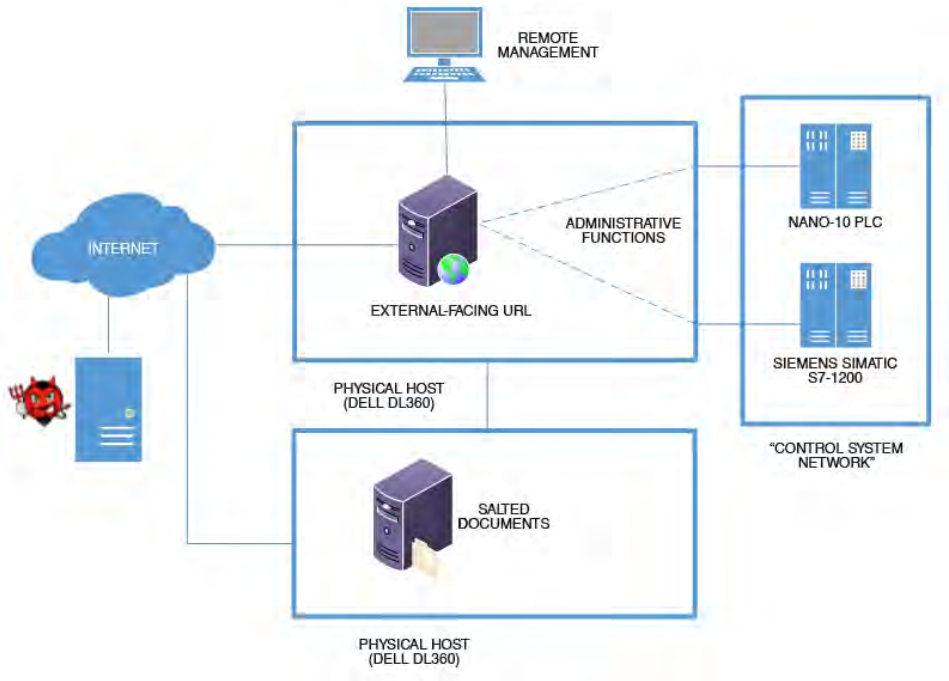


FIGURE 8: High-interaction honeypot architecture

3 http://www.tri-plc.com/nano10.htm

In addition to high-interaction honeypots, the ICS honeypot also utilized a low-interaction honeypot. Low-interaction honeypots could be characterized as traps used to simulate the services provided by a production system. These honeypots utilize very little resources and allow multiple instances to be virtually spun up, if desired.

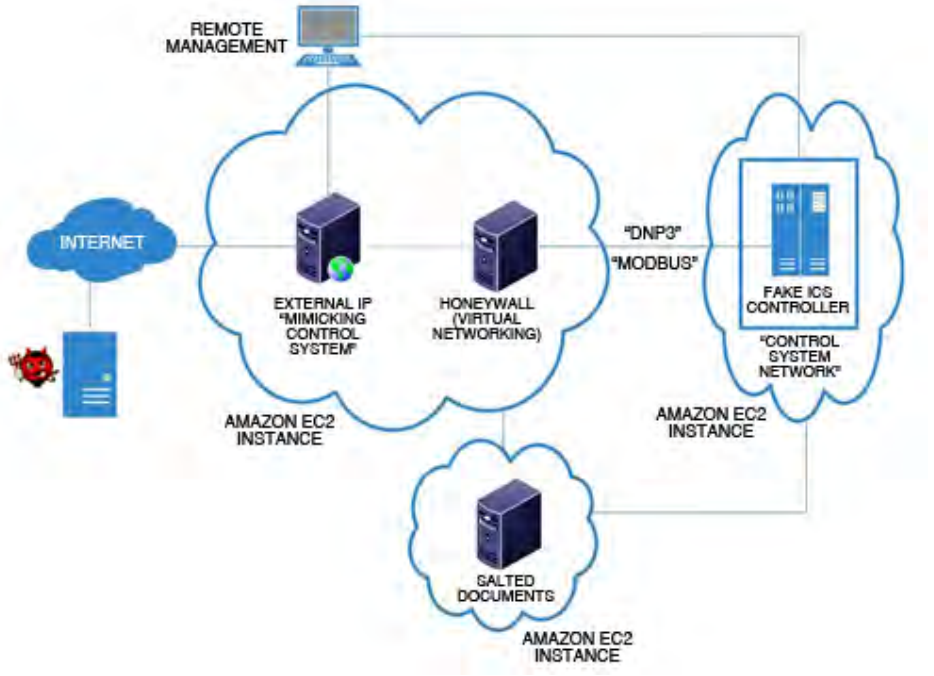


FIGURE 9: Low-interaction honeypot architecture

Findings and Metrics

Before going into the metrics and findings of the three honeypots, we need to define what we consider an "attack." We will not report based on port scans, automated attack attempts like SQL injection or other automated attacks that are typically considered "drive-by" attacks.

We define an attack as anything that may be deemed a threat to Internet-facing ICS/SCADA systems. This includes unauthorized access to secure areas of sites, modifications on perceived controllers, or any attack against a protocol specific to ICS/SCADA devices like Modbus. In addition to classifying these attempts as "attacks," we also consider any attempt to gain access or cause an incident to the server in a targeted fashion "attacks."

When the honeypots were launched, we seeded the devices in several fashions. First, we optimized the sites for searches and published them on Google to make sure they garnered attention. In addition to seeding on Google, we also named the servers "SCADA-1," "SCADA-2," and so on. We also made sure that the other honeypot settings would be seeded on devices that were part of HD Moore's Shodan Project.[4] This would enable motivated and targeted attackers to easily find the servers.

It took only 18 hours to find the first signs of attack on one of the honeypots. While the honeypots ran and continued to collect attack statistics, the findings concerning the deployments proved disturbing. The statistics of this report contain data for 28 days with a total of 39 attacks from 14 different countries. Out of these 39 attacks, 12 were unique and could be classified as "targeted" while 13 were repeated by several of the same actors over a period of several days and could be considered "targeted" and/or "automated." All of these attacks were prefaced by port scans performed by the same IP address or an IP address in the same /27 netblock.

In sum, China accounted for the majority of the attack attempts at 35%, followed by the United States at 19% and Lao at 12%.

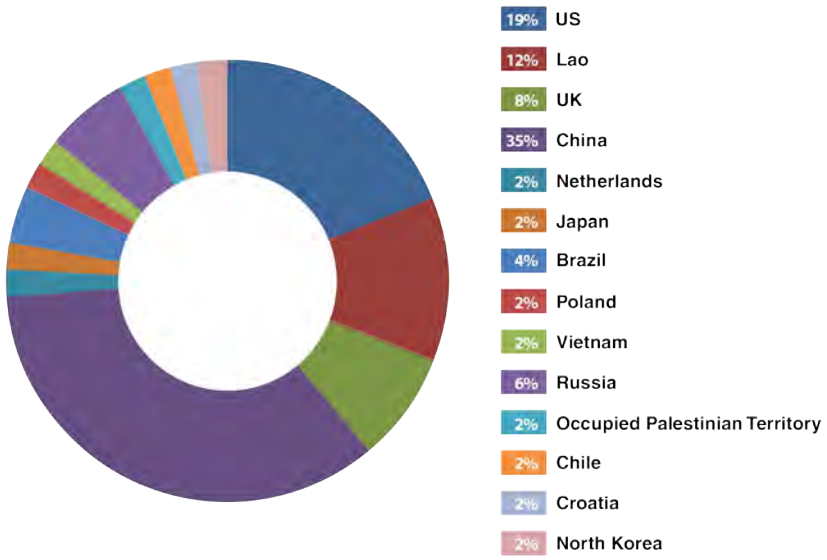


FIGURE 10: Country breakdown indicating the number of attack attempts

4 http://www.shodanhq.com/

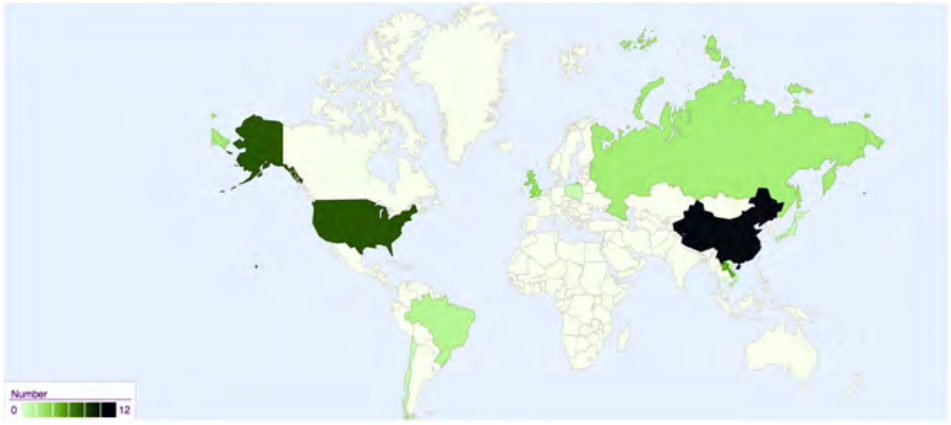


FIGURE 11: Heat map showing where most of the targeted attacks came from

Even more concerning than the number of legitimate attacks was the number of repeat offenders. The country with the greatest number of repeat offenders was Lao, closely followed by China. These repeat offenders often came back at dedicated times on a 24-hour basis and attempted to not only exploit the same vulnerabilities present on the devices but also attempted additional exploitation if they did not succeed with prior attempts. This shows that these particular actors were likely interested in gaining access to the devices or causing further damage/exploitation.

In addition to the many attacks seen on the honeypot environment, there was also a surprising number of malware exploitation attempts on the servers. Utilizing the popular malware honeypot, Dionaea, four samples were collected over the testing time frame, two of which have not been seen in the wild as they had unique MD5 checksums. Trend Micro is currently analyzing these pieces of malware to determine their functionality.

Country	Attack Type	Attack Classification
United States	Unauthorized access attempt to diagnostics.php, attempted Modbus traffic modification, modification of the CPU fan speed on the water pump	Unauthorized access attempt, unauthorized modification attempt, information disclosure
United Kingdom	Attempted modification of the diagnostics.php page	Modification of the php on the site
Lao	Attempted access to the diagnostics.php page, modification of the CPU fan speed on the water pump	Unauthorized access attempt, information disclosure, modification of the SCADA system
China	Access to the statistics.php, diagnostics.php, and protocols.php pages; spear-phishing attempt; Modbus traffic modification attempt	Unauthorized access attempt, information disclosure

Country	Attack Type	Attack Classification
Netherlands	Attempted Modbus traffic modification, modification of the CPU fan speed on the water pump	Unauthorized access attempt, modification of the SCADA system
Japan	Access to the statistics.php, diagnostics.php, and protocols.php pages	Unauthorized access attempt, information disclosure
Brazil	Attempted Modbus traffic modification	Unauthorized modification attempt
Poland	Attempted access to the diagnostics.php page	Unauthorized access attempt, information disclosure
Russia	Attempted malware exploitation; access to the statistics.php, diagnostics.php, and protocols.php pages	Malware exploitation attempt—malware not known, unauthorized access attempt, information disclosure
Vietnam	Attempted malware exploitation	Malware exploitation attempt—common malware—TROJ_MEREDROP.II and WORM_ATAK.A
North Korea	Access to the statistics.php, diagnostics.php, and protocols.php pages	Unauthorized access attempt, information disclosure
Chile	Attempted access to the diagnostics.php page	Unauthorized access attempt, information disclosure
Occupied Palestinian Territory	Attempted access to all of the secure areas of the site, attempted Modbus traffic modification	Unauthorized access attempt, information disclosure

TABLE 1: Attack attempt breakdown[5]

5 http://about-threats.trendmicro.com/Malware.aspx?language=au&name=TROJ_MEREDROP.II; http://about-threats.trendmicro.com/us//archive/malware/WORM_ATAK.A

Snort Findings

While the honeypot environment continued to gather statistics, so did the Snort instances running on each device. Snort, a popular intrusion detection system (IDS), has great subsets of ICS rules included in its default rule releases in addition to custom rules that were created on the fly to accommodate for attack attempts. In the case of the honeypot environment, we utilized Digital Bond's IDS rules.[6]

The top Snort alert generated in the honeypot environment was Modbus TCP non-Modbus communication on TCP port 502. This rule is triggered when an established connection utilizing Modbus is hijacked or spoofed to send other commands or attacks to a different device.

In addition to generating this alert, the following two rules were also triggered:

- Unauthorized Read Request to a PLC
- Unauthorized Write Request to a PLC

These rules are traditionally triggered when an unauthorized Modbus client attempts to read or write information from or to a PLC or SCADA device. Both of these rules traditionally indicate that ICS network reconnaissance is occurring—the first step in ICS network exploitation.

The sources of all three alerts were the United States, Russia, and China, respectively. Out of these countries, China and Russia generated all three alerts while the United States generated two out of the three. The attacks were generated in a fashion that did not indicate drive-by scan attempts. Each of the three alerts was generated in single instances and by separate IP addresses with no other port scan activities from the said IP addresses, indicating that they were targeted in nature.

Recommendations

Fortunately, there are compensating controls that can help ensure that ICS/SCADA devices don't end up listed on sites like Pastebin or easily found via Google searches.

6 http://www.digitalbond.com/tools/quickdraw/

There are some very basic configuration and architectural considerations that can help prevent remote access to trusted ICS resources from occurring in this fashion. Most of these recommendations are based on "baking in" your security as ICS are architected and deployed. Future discussions will include ways to "bolt on" security for these systems and networks.

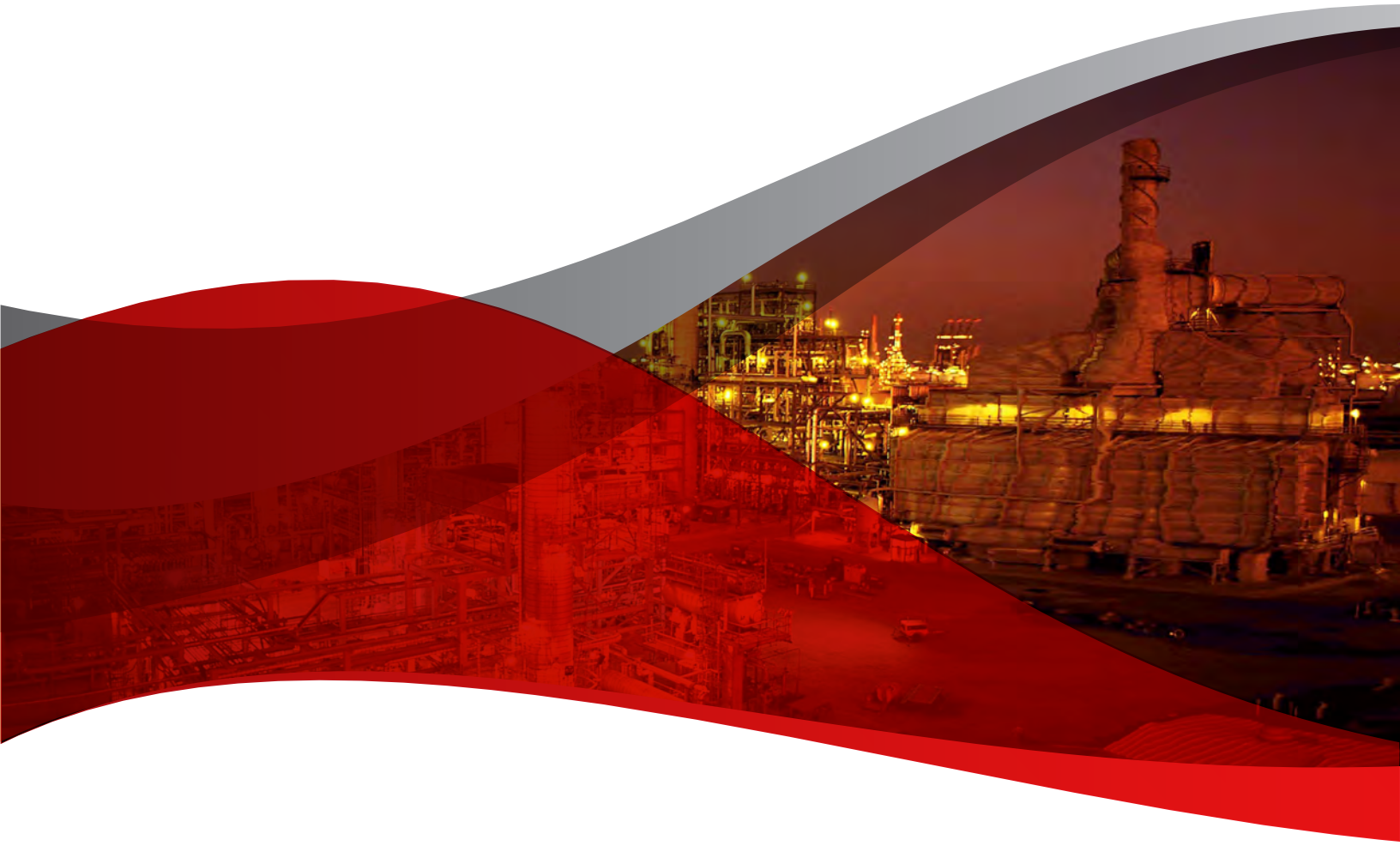
- Disable Internet access to your trusted resources, where possible.
- Make sure your trusted resources have the latest patches and that you diligently monitor when new patches/fixes are released.
- Use real-time anti-malware protection and real-time network scanning locally on trusted hosts and where applicable. (Some PLC systems cannot support anti-malware products because of the fragile nature of ICS protocols.)
- Require user name/password combinations for all systems, including those that are not deemed "trustworthy."
- Set appropriately secure login credentials. Do not rely on defaults.
- Implement two-factor authentication on all trusted systems for any user account.
- Disable remote protocols that are insecure like Telnet.
- Disable all protocols that communicate inbound to your trusted resources but are not critical to business functionality.
- Control contractor access. Many ICS/SCADA networks utilize remote contractors, and controlling how they access trusted resources is imperative.
- Utilize SSL/TLS for all communications to web-based ICS/SCADA systems.
- Utilize network segmentation to secure resources like VES systems, ICS, and SCADA devices. See a great write-up on network segmentation at http://www.tofinosecurity.com/blog/controlling-stuxnet---no-more-flat-networks-please-lets-embrace-security-zones.
- Control access to trusted devices. For instance, for access to a segmented network, use a bastion host with access control lists (ACLs) for ingress/egress access.
- Improve logging in on trusted environments in addition to passing logs to SIEM devices for third-party backup/analysis.
- Develop a threat modeling system for your organization. Understand who's attacking you and why.

Conclusion

As you can see, Internet-facing ICS are readily targeted. Until proper ICS security is implemented, these types of attack will likely become more prevalent and advanced or destructive in the coming years. This research paper was a first foray into the attacks that are performed on Internet-facing ICS.

The attack sources nor the attackers' motives were not discussed. Continued research will focus on motives, sources, delivery techniques, and increasing sophistication.

We expect attack trends to continue in the ICS arena, with possible far-reaching consequences. With continued diligence and utilizing secure computing techniques, your ability to deflect and defend against these attacks will help secure your organization.



TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud