A Trend Micro Research Paper

The SCADA That Didn't Cry Wolf

Who's Really Attacking Your ICS Equipment? (Part 2)

Kyle Wilhoit

(Trend Micro Forward-Looking Threat Research Team)

Contents

Introduction

"Who's Really Attacking Your ICS Equipment?" presented a thorough outline of a honeynet specifically developed to catch attacks against industrial control systems (ICS).[1] The devices featured in the paper were external facing and riddled with vulnerabilities commonly found plaguing ICS equipment worldwide.

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 and SCADA systems is going to become even more prevalent.

In this paper, we looked at who are continuing to attack external-facing ICS devices and why. It also features a more robust honeynet architecture that we developed and deployed worldwide over a period of several months. This paper intends to describe not only attack statistics but also show the robust attribution framework we utilized. Finally, it also contains more in-depth analysis of the threat actors and their possible motivations behind attacks.

ICS: Past and Present

Over the past 30 years, SCADA devices with varying functions have been deployed nearly everywhere in the world. SCADA devices' history is rooted on distribution applications like power and water pipelines, which need to gather remote data through unreliable or intermittent low-bandwidth or high-latency links.[2] While SCADA devices have had very successful deployments worldwide, they suffer one primary oversight—lack of security implementation.

The current state of SCADA deployments does not vary much from 30 years ago. While technological advancements have been made to these, they have not improved in terms of information security. From software development to server deployment, information security is often an afterthought in SCADA environments. Despite several documented security issues in relation to SCADA devices, little has been achieved in the past 10 years to help secure them. SCADA deployment has consistently risen. Lack of information security implementation and advancements in SCADA technology have dramatically increased security risks worldwide with likely far-reaching consequences.

1 Kyle Wilhoit. (2013). "Who's Really Attacking Your ICS Equipment?" Last accessed June 27, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf.

2 Wikimedia Foundation, Inc. (July 10, 2013). *Wikipedia.* "Industrial Control System." Last accessed July 29, 2013, http://en.wikipedia.org/wiki/Industrial_control_system.

Worldwide SCADA Deployment Considerations

While SCADA deployment variances are seen worldwide, one of the biggest changes in deployment methodologies is related to cloud-based deployment considerations. Several security concerns related to cloud-based SCADA deployment have been published worldwide and these considerations should be closely monitored.[3] In addition to cloud deployments, we should also consider the industry types and countries that utilize SCADA devices. Enterprises in China, for instance, largely use SCADA devices in the manufacturing industry. In the United States, SCADA devices are most utilized in the building automation and manufacturing industries. Finally, in Japan, SCADA devices are most utilized in the automotive industry.

Many countries are starting to develop and implement standards to secure SCADA environments. The United States, for instance, has come up with the National Institute of Standards and Technology (NIST) Special Publication 800-82 and IEC 62443.[4] Japan, which has a robust automotive industry, meanwhile, adheres to IEC 62443. The country's Information-Technology Promotion Agency (IPA) is also starting to implement the Embedded Device Security Assurance Certification Program with provisions for SCADA devices.[5]

ICS Risks and Threats

Risks and threats to SCADA devices are now becoming common. Many of the risks surrounding SCADA device use are related to the use of HMI and data historians. Data historians are used to record trends and historical information about industrial processes for future reference.[6] HMI use, meanwhile, can also be plagued by traditional web application vulnerabilities like SQL injection and cross-site scripting (XSS) bugs. HMIs can also be affected by traditional server-side vulnerabilities. If an HMI, for instance, runs on a Windows® Server® 2003, an attacker could locate unpatched vulnerabilities to exploit and, therefore, gain access to the HMI. HMI threats are likely to be introduced via connections from an insufficiently secure demilitarized zone (DMZ) or business network to a secure SCADA environment. Setpoints, which are deviation checks, ensure that specific control is maintained within a controlled segment. For instance, a thermostat for home heating would have a high setpoint for high temperature and a low one for low temperature. If the low setpoint is triggered by a very low ambient temperature, the heating unit will automatically turn on. Compromising an HMI in any fashion can open communications to a secure area and result in modifications to setpoints or controls that are similar in nature.

3 Kyle Wilhoit. (2013). "SCADA in the Cloud: A Security Conundrum?" Last accessed July 29, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-scada-in-the-cloud.pdf.

4 Keith Stouffer, Joe Falco, and Karen Scarfone. (June 2011). "Guide to Industrial Control Systems (ICS) Security." Last accessed July 29, 2013, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf; Tom Phinney. "IEC 62443: Industrial Network and System Security." Last accessed July 29, 2013, http://www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf.

5 ISA SECURE. (April 15, 2013). "Establishment of ISASecure Japanese Scheme and Publication of ISASecure Embedded Device Security Assurance Certification Program Specifications in Japan." Last accessed July 29, 2013, http://isasecure.org/News-Room/Press-Releases/Establishment-of-ISASecure-Japanese-Scheme-and-Pub.aspx.

6 Wikimedia Foundation, Inc. (July 10, 2013). *Wikipedia.* "Operational Historian." Last accessed July 29, 2013, http://en.wikipedia.org/wiki/Operational_historianhistorian.

In addition to HMI-related risks and threats, threats to the data historian should also be considered. A data historian functions as a centralized database for logging all process information within an ICS environment. If an attacker gains access to a data historian that sits in the DMZ or business network, for instance, he would be granted access (i.e., can include Read or Read/Write access) to possibly many secure systems. The attacker would be presented with a wealth of information, ranging from historical data on processes and/or commands to statistical data. In some environments, a data historian also functions as a "clearinghouse" for some commands issued to programmable logic controller (PLC) devices. If an attacker gains access to a data historian, he can also issue man-in-the-middle (MiTM) commands that modify legitimately issued ones.

Publicized ICS Attacks

While many ICS attacks have been publicized, many more have not been disclosed and even those that are made public are not clearly understood. The table below shows just some ICS or critical infrastructure attacks that have been publicized and their locations.[7]

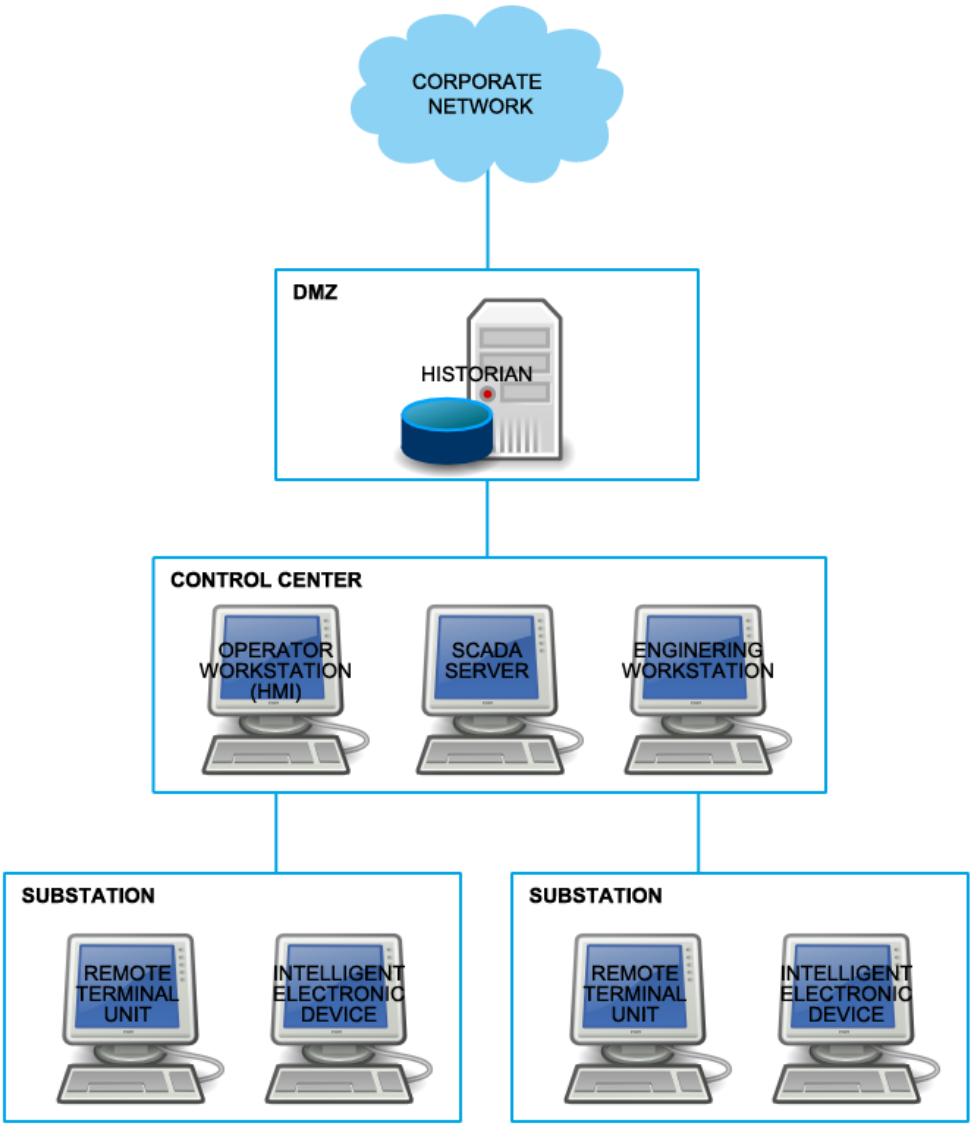
7 *Dancho Danchev's Blog—Mind Streams of Information Security Knowledge*. (October 5, 2006). "SCADA Security Incidents and Critical Infrastructure Insecurities." Last accessed August 1, 2013, http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html; Kevin Poulsen. (September 3, 2003). *The Register.* "U.S. Warns Nuke Plants of Worm Threat: If There Was Ever a Place That Needed AV Protection…." Last accessed August 1, 2013, http://www.theregister.co.uk/2003/09/03/us_warns_nuke_plants/; John Leyden. (January 11, 2008). *The Register.* "Polish Teen Derails Tram After Hacking Train Network: Turns City Network into Hornby Set." Last accessed August 1, 2013, http://www.theregister.co.uk/2008/01/11/tram_hack/; Shelby Grad. (December 1, 2009). *L.A. Now.* "Engineers Who Hacked into L.A. Traffic Signal Computer, Jamming Streets, Sentenced." Last accessed August 1, 2013, http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html; William J. Broad, John Markoff, and David E. Sanger. (January 15, 2011). *The New York Times.* "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." Last accessed August 1, 2013, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0; John E. Dunn. (November 14, 2011). *Techworld.* "Mystery 'Virus' Disrupts New Zealand Ambulance Service: Malware Sends Operators Back to Manual Communication." Last accessed August 1, 2013, http://news.techworld.com/security/3318106/mystery-virus-disrupts-new-zealand-ambulance-service/; John Leyden. (June 25, 2013). *The Register.* "North and South Korea Hit by Cyber-Blitz on Korean War Anniversary: Official Nork Portals Knocked Offline, South Korean Prez, and PM also KO'd." Last accessed August 1, 2013, http://www.theregister.co.uk/2013/06/25/korean_war_anniversary_ddos_attacks/.

Publicized ICS Attacks		
Year	**Incident**	**Location**
2000	Sewage-processing plant attack by a former employee	Maroochy, Australia
2003	Nuclear power plant system was disabled via the Slammer worm	Ohio, USA
2008	Train derailment due to hacking	Lodz, Poland
2009	Traffic signal system hacked	LA, California, USA
2010	Stuxnet worm destroyed uranium centrifuge operations	Natanz, Iran
2011	Ambulance service disrupted via a malware infection	New Zealand
2013	Banking and broadcasting services were disrupted	South Korea

While almost all attacks against ICS environments are digitally instigated (i.e., launched online), many remain undisclosed or categorized as "classified" by government agencies and incident response teams. Several attacks remain undisclosed as well because many engineers are unable to differentiate between a cyber attack and a hardware or software failure. If a device in a SCADA network stops functioning, for instance, many engineers simply replace the defective device without investigating the reason for the malfunction. Many do not understand what cyber attacks are as well nor do they want to affect production requirements and so just replace defective devices and carry on as usual.

Traditional Honeypot Deployments

When referencing honeypot deployments, it is very important to understand how a traditional ICS environment looks.



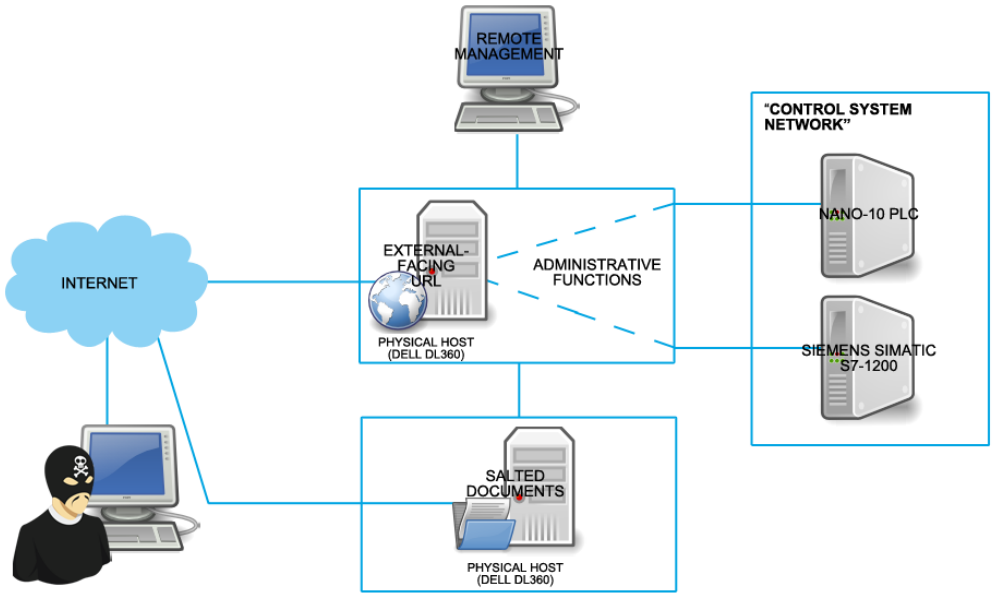
As shown above, no security devices or protocols appear to be in place. While some ICS environments do contain these measures, most do not have such preventative controls.

Original Honeypot Deployment

"Who's Really Attacking Your ICS Equipment?" featured an external-facing honeypot deployment stationed in the United States, which was specifically designed to attract targeted attacks. The honeypot architectures were of two distinct types—high and low interaction.

The first honeypot was a high-interaction one, which imitated the activities of a physical ICS device.

ORIGINAL HIGH-INTERACTION HONEYPOT



Apart from high-interaction honeypots, we also used a low-interaction architecture. Low-interaction honeypots can be characterized as "traps used to simulate the services provided by a production system." These honeypots use very little resources and allow multiple instances to be virtually spun up if desired.

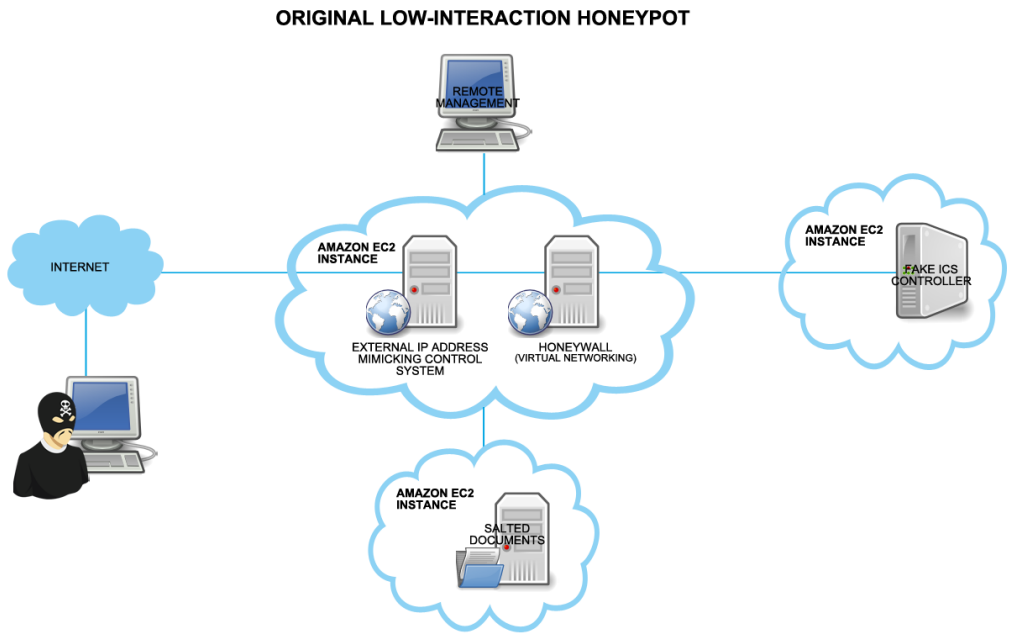
New Honeypot Architecture

While the original honeypot deployment was successful and garnered accurate results, we wanted a bigger data sample to better represent the global perspective. So, a more robust virtualized environment that could be deployed in a matter of minutes anywhere in the world was created. Traditionally, municipal water districts, even worldwide, have very little control over the systems that run water supplies. These systems are traditionally rarely secure, which is why they were ideal for these purposes.

The first challenge in rearchitecting the honeypot solution was to create a believable, fully mimicked version of a virtualized ICS environment. To accomplish this, newly created tools and already-existing toolsets were utilized across multiple virtualized environments.

The second challenge was to create a full-featured service emulation module, which was also accomplished via the utilization of newly created and already-existing tools and scripts.

Other challenges included attack attribution. Attributing attacks using IP addresses is very inconsistent and provides little value to an organization that wants to know who attacked it. As such, each of the honeypots utilized in the architecture used a module called "The Browser Exploitation Framework (BeEF)," which helped attribute attacks to a particular attacker or group of attackers.[8]

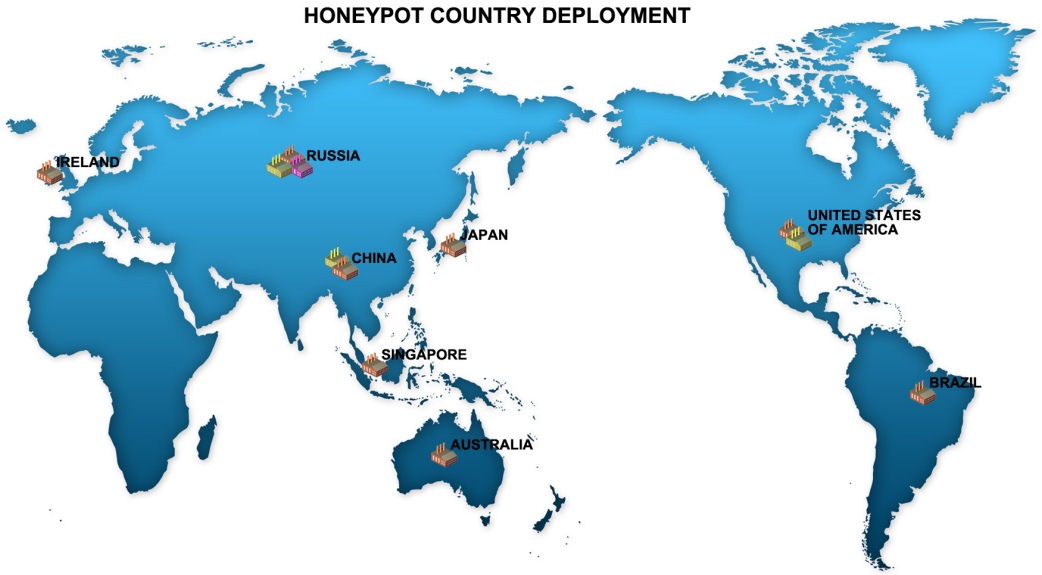


When looking at the new honeypot architecture, each section should be seen as a "module" that independently operates from the others. Many of these modules operate on a single virtual machine, except the human-machine interface (HMI), which operates on a logically separated virtual instance. In addition, the PLC device with which the HMI interacts is also logically separated from the other devices.

8 *BeEF*. Last accessed August 13, 2013, http://beefproject.com/.

New Honeypot Deployment

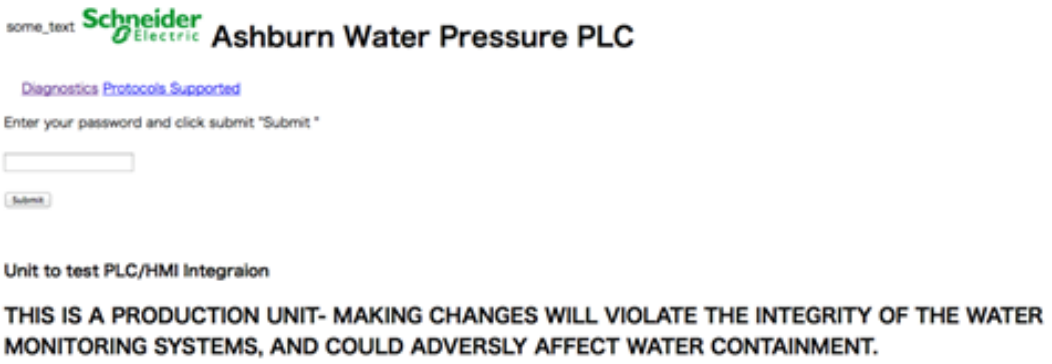
In order to gather realistic targeted attack scenario data worldwide, we had to virtualize and make a more robust honeypot architecture. We then focused on multiplying and expanding the number of honeypots to turn the architecture into a honeynet. A honeynet is generally a network of honeypots that is traditionally distributed geographically. In this case, however, all of the honeypots worked separately and did not communicate with one another. Segregation ensured that no cross-communication contamination could occurs in the event an attacker compromises a single honeypot on the honeynet.



The diversity of the countries where the honeypots were deployed helped generate a great number of attacks.

Honeypot Country Deployment	
Honeypot Location	**Number Deployed**
China	2
Japan	1
Russia	3
Australia	1
USA	2
Ireland	1
Brazil	1
Singapore	1
Total	**12**

In addition to deploying honeypots worldwide, all of the text in the honeypot deployments was localized. This was a difficult task that required the assistance of research colleagues familiar with the languages and local customs in the honeypot location.



Sample main web page of a honeypot instance

Sample HMI page

ICS Device Reconnaissance

Determining how attackers perform reconnaissance on ICS devices is very similar to how they target other systems like Windows servers. Many of the attackers who targeted the honeynet first searched on ShodanHQ's website for specific search terms.[9] The most common search terms used were "SCADA" and "Modbus," followed by "Simatic+HMI," "Simatic+S7," and "HMI."

Apart from using ShodanHQ's site, the attackers also ran numerous port scans for reconnaissance purposes. These port scans were typically ran on the first 1024 ports within the honeypots. Depending on their interests, the attackers expanded their port scanning selection. It appeared that the attackers did not commonly perform "slow scanning" (i.e., scanning at a very slow rate to reduce getting noticed). Many of the attackers scanned ports in clusters, which made them very easy to locate and find. This could likely be due to many system and firewall administrators not closely monitoring logs.

Another reconnaissance method we identified had to do with utilizing common text-based-sharing platforms like Pastebin and Pastie. While we did not see the honeypots mentioned in any post, we did see compilations of other ICS devices on these sites.

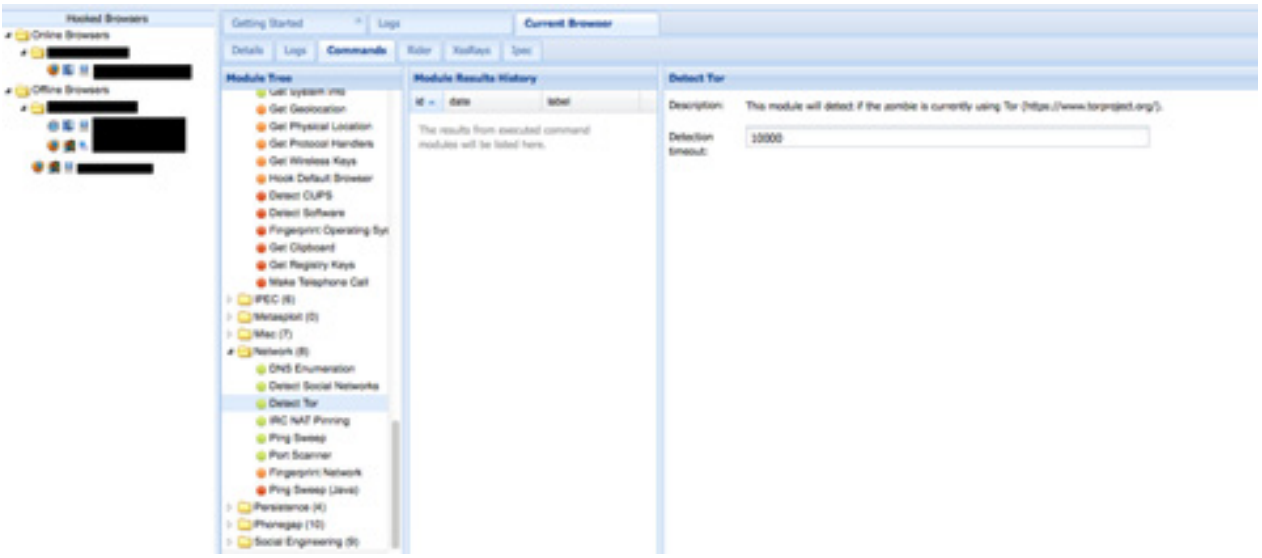
Attribution Framework

Determining an attacker's location based on the IP source address of incoming connections is inconclusive. Attackers often use anonymizers like Tor to change their source IP addresses.[10]

To help fight attribution-related issues, an excellent framework—BeEF—was used. While the use of this framework could be unreliable by nature; when used properly, it allows security researchers and analysts to more effectively attribute attacks in greater detail.

9 *SHODAN*. (2013). Last accessed July 30, 2013, http://www.shodanhq.com/.
10 The Tor Project, Inc. *Tor.* Last accessed July 3, 2013, https://www.torproject.org/.

BeEF, as a framework, can actively run scripts on a victim's browser every time he accesses a certain web page. A BeEF injectable script was embedded into a web page that could only be accessed using secure credentials stored in the honeypot environment. The page was in the honeypot architecture, behind a secure area. As such, a potential victim must access the page inside the secure area in the honeypot for his browser to be affected. So, if an attacker compromises website authentication, BeEF would run the script to help determine his geographical location and obtain other statistical data.



Sample BeEF administration portal

Within BeEF, the *get physical location* module will retrieve geographical location information based on neighboring wireless access points using commands encapsulated within a signed Java applet. The *get system info* module will, meanwhile, pull system information using an unsigned Java applet. The data obtained includes operating system (OS) details, number of processors, NIC names, and IP addresses, along with other details. Finally, the *detect Tor* module will detect if the machine used runs Tor.

Apart from BeEF, several other attribution methods and internal tools were used. While we are unable to disclose what these methods are, it is certain that the correlation between BeEF and the internal tools we used can effectively determine an attacker's physical location.

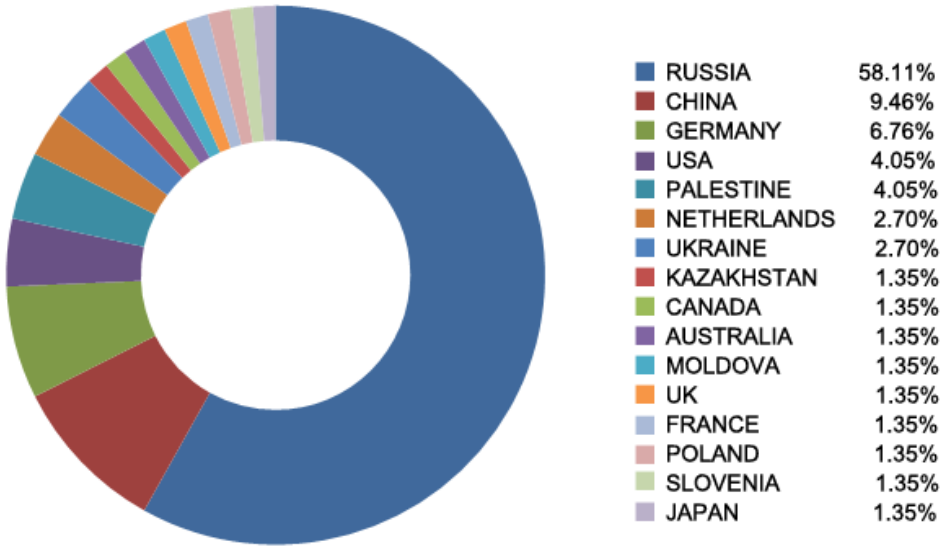
Attacks

ICS attackers can often be compared with traditional targeted attackers. We have seen ICS attackers engage in many of the same steps targeted attackers take prior to staging attacks. Many perform reconnaissance not just on their target IP addresses but also on the netblock where the devices are hosted, which is traditionally seen in a /24 network. This stage typically involves port scanning of surrounding subnets. The attackers also perform fingerprinting on devices to ascertain their OSs, if possible, along with other identifiable information. Moreover, they traditionally identify vulnerabilities at this stage. Once access to devices is gained, persistence and lateral movement were also observed in roughly 70% of the attacks. In addition, data exfiltration is commonly seen. In one particular instance, we observed the exfiltration of perceived virtual private network (VPN) configuration files leaving a compromised server.

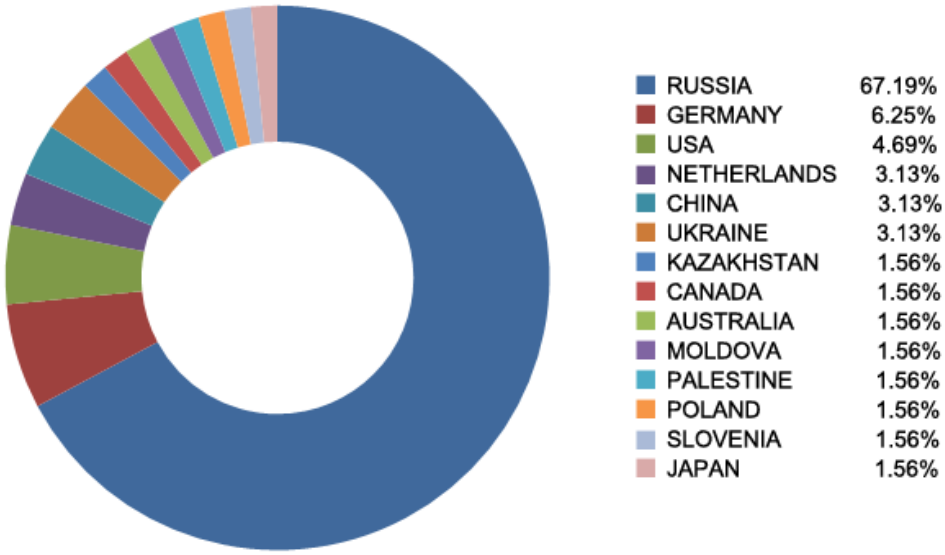
Over a period of three months, several attacks took place. Some were even able to compromise the entire operation of an ICS device. While many would consider an attack to be any type of drive-by or automated attack (e.g., "mass" SQL injection), we only accounted for attacks that were considered targeted in nature (i.e., showed that a reasonable amount of reconnaissance was carried out prior to engaging in fingerprinting or the actual attack).

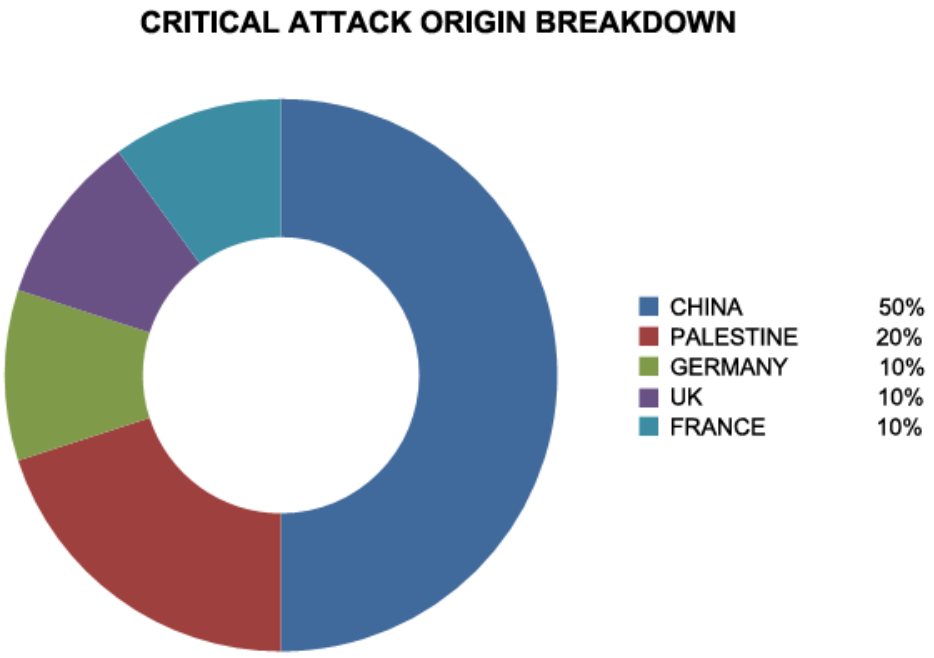
From March to June 2013, we observed attacks originating in 16 countries, accounting for a total of 74 attacks on seven honeypots within the honeynet. Out of these 74 attacks, 11 were considered "critical." When we refer to attacks as critical, we mean those without established motivations but can cause the catastrophic failure of an ICS device's operation. Likewise, attacks considered noncritical cannot cause a catastrophic failure but should they continue, can. These types of attacks can take the form of a distributed denial-of-service (DDoS) attack, for instance.

ATTACK ORIGIN BREAKDOWN



NONCRITICAL ATTACK ORIGIN BREAKDOWN





More details on how the attacks are broken down by type are shown in the following table.

Attack Origin and Type Breakdown			
Country	Type		Total
	Critical	Noncritical	
Netherlands	0	2	2
China	5	2	7
Germany	1	4	5
Kazahkstan	0	1	1
Canada	0	1	1
USA	0	3	3
Australia	0	1	1
Moldova	0	1	1
Ukraine	0	2	2
UK	1	0	1
France	1	0	1
Palestine	2	1	3
Poland	0	1	1
Slovenia	0	1	1
Japan	0	1	1
Russia	0	43	43
Total	**10**	**64**	**74**

More details on the attacks, specifically what steps the attackers took and how they were classified, are shown in the following table.

Attack Activity and Classification Breakdown		
Honeypot Location	**Activities**	**Classification Based on Alert Triggered**
USA	Modbus traffic modification attempt Water pump central processing unit (CPU) fan speed modification HMI access Spear-phishing attack	Unauthorized access attempt SCADA system modification
Japan	Access to the *statistics.php, diagnostics.php,* and *protocols.php* pages Spear-phishing attempt Modbus traffic modification attempt HMI access	Unauthorized access attempt Information disclosure
China	Access to the *statistics.php, diagnostics.php,* and *protocols.php* pages HMI access Setpoint modifications	Unauthorized access attempt Information disclosure SCADA system modification
Brazil	Access to the *statistics.php, diagnostics.php,* and *protocols.php* pages HMI access	Unauthorized access attempt Information disclosure
Singapore	Attempted access to the *diagnostics.php* page Water pump CPU fan speed modification	Unauthorized access attempt Information disclosure SCADA system modification
Ireland	Access to the *statistics.php, diagnostics.php,* and *protocols.php* pages	Unauthorized access attempt Information disclosure

Attack Activity and Classification Breakdown		
Honeypot Location	**Activities**	**Classification Based on Alert Triggered**
Australia	Access to the *statistics.php, diagnostics.php,* and *protocols.php* pages HMI access	Unauthorized access attempt Information disclosure
Russia	Malware exploitation attempt Access to the *statistics.php, diagnostics.php,* and *protocols.php* pages	Malware exploitation attempt—malware not known Unauthorized access attempt Information disclosure

Out of the 11 critical attacks, six generated Snort alerts. Two rules were triggered within Snort—*Unauthorized Read Request to a PLC* and *Unauthorized Write Request to a PLC*. These rules traditionally issue alerts when an unauthorized Modbus client attempts to read or write information from a PLC or SCADA device. Both rules usually indicate that ICS network reconnaissance is occurring—the first step in ICS network exploitation.

Based on the attacks that occurred and the Snort signatures triggered, we determined that the alerts were generated during reconnaissance rather than when the actual attacks were carried out.

In addition to these attacks, we also tracked repeat or similar IP addresses or netblocks perform attacks. One interesting statistic involved attacks against three separate honeypots that were geographically disparate. Among these, two separate /24 netblocks with five unique IP addresses performed attacks. Referrers from ShodanHQ queries as well as port scans, OS fingerprinting, and automated vulnerability assessments were also seen.

Many of the attacks involved attempted exploitation of the HMI in addition to modifying Modbus protocol traffic. The HMI in the honeynet environment would be perceived as a gateway to the ICS environment. When the attackers attempted to modify the HMI, they were looking for SQL injection and cross-site request forgery (CSRF) vulnerabilities. SQL injection is a code injection technique that exploits security vulnerabilities in an application, often targeting the backend database. Likewise, CSRF attacks refer to a type of malicious exploitation of a website by transmitting unauthorized commands from a user that the site trusts. Attackers also often attempted to log in to secure areas using default credentials. Dictionary attacks (i.e., use brute force by nature) against an HMI were also commonly seen. As such, HMIs with no lockout mechanisms can allow attackers to attempt multiple logins with little effort and no repercussions.

Attackers who targeted Modbus traffic, meanwhile, attempted to modify and execute valid commands issued by the HMI to the PLC. Because Modbus sends traffic in cleartext without requiring authentication, it is a ripe target for attackers looking to compromise ICS environments.

Automated Attacks

While this paper focuses on targeted attacks, we also tracked automated attacks like SQL injection attacks. The sheer number of automated attacks was surprising. For the entire honeynet during the sample timeline, 33,466 automated attacks were recorded for which 1,212 unique IP addresses were used. While we do not perform attribution or any other type of statistical analysis on these attacks, we do monitor and keep base numbers for comparison purposes.

Interesting Japan-Related Attack

While most of the attacks against the honeypots were interesting, a few were especially notable. One of these was the attack against a Japanese honeypot. Reconnaissance on the honeypot was performed via a conventional ShodanHQ search. The attackers located the honeypot by entering the query, "SCADA country: Japan." Executing this search allowed them to ascertain the honeypot's IP address and perform two remote port scans.

The first port scan was performed on the first 1024 ports. These are often scanned first because they are considered "common" ports. After seeing port 502 (i.e., Modbus port) open, they then continued to scan all of the 65,535 ports. The attackers did not perform a common "slow scan," which would make detection more difficult to do for an astute system administrator. Instead, they scanned all ports at once, thus attracting a lot of attention.

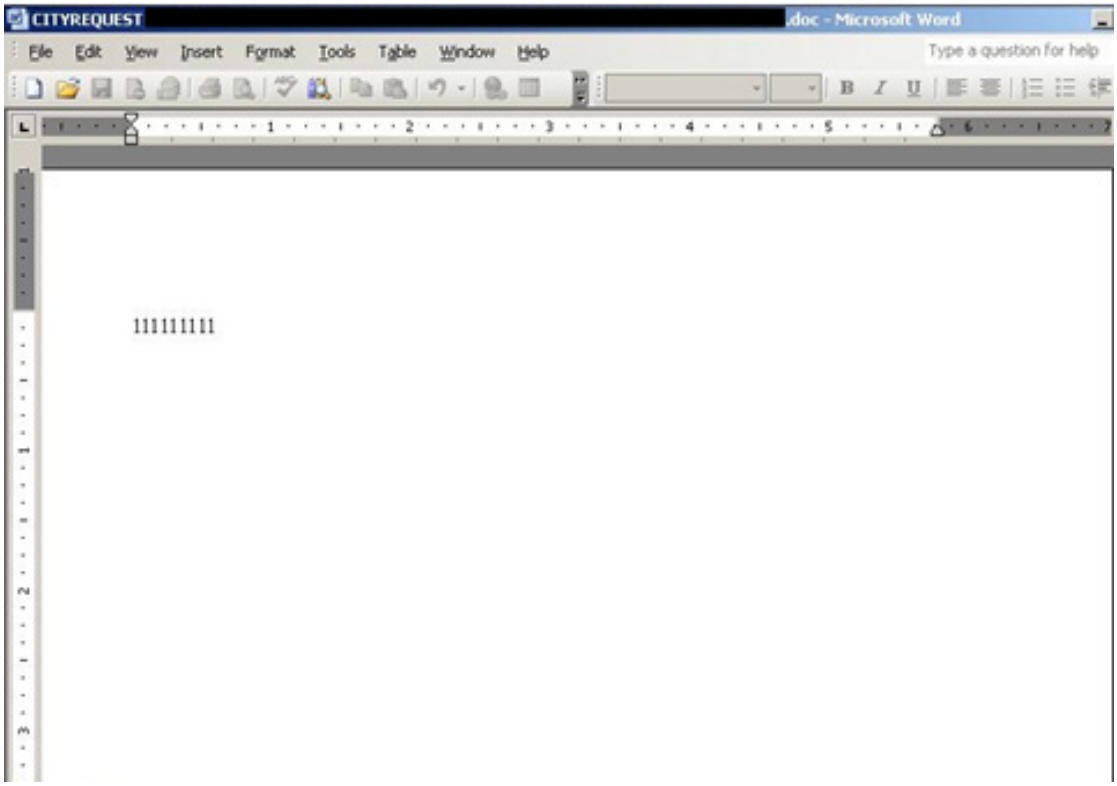
After scanning the ports of a target device, the attackers immediately attempted to access the HMI, which was secured with default user name and password combinations. After trying out several combinations in a seemingly manual fashion, the attackers successfully gained access to the secure HMI area. From there, they attempted to read and modify the Modbus traffic while trying to access the Windows Server 2003 at the same time.

After an unsuccessful attempt to read Modbus traffic, the attackers quickly started to modify the setpoint settings of the honeypot HMI. They modified the device's pump pressure as well as water temperature. After modifying these setpoints, they then scheduled a task—pump shutdown—which effectively disabled water pumping at the time set. After accomplishing this task, they immediately logged out and ceased all activities related to the honeypot and/or Windows server.

Interesting Targeted Attacks

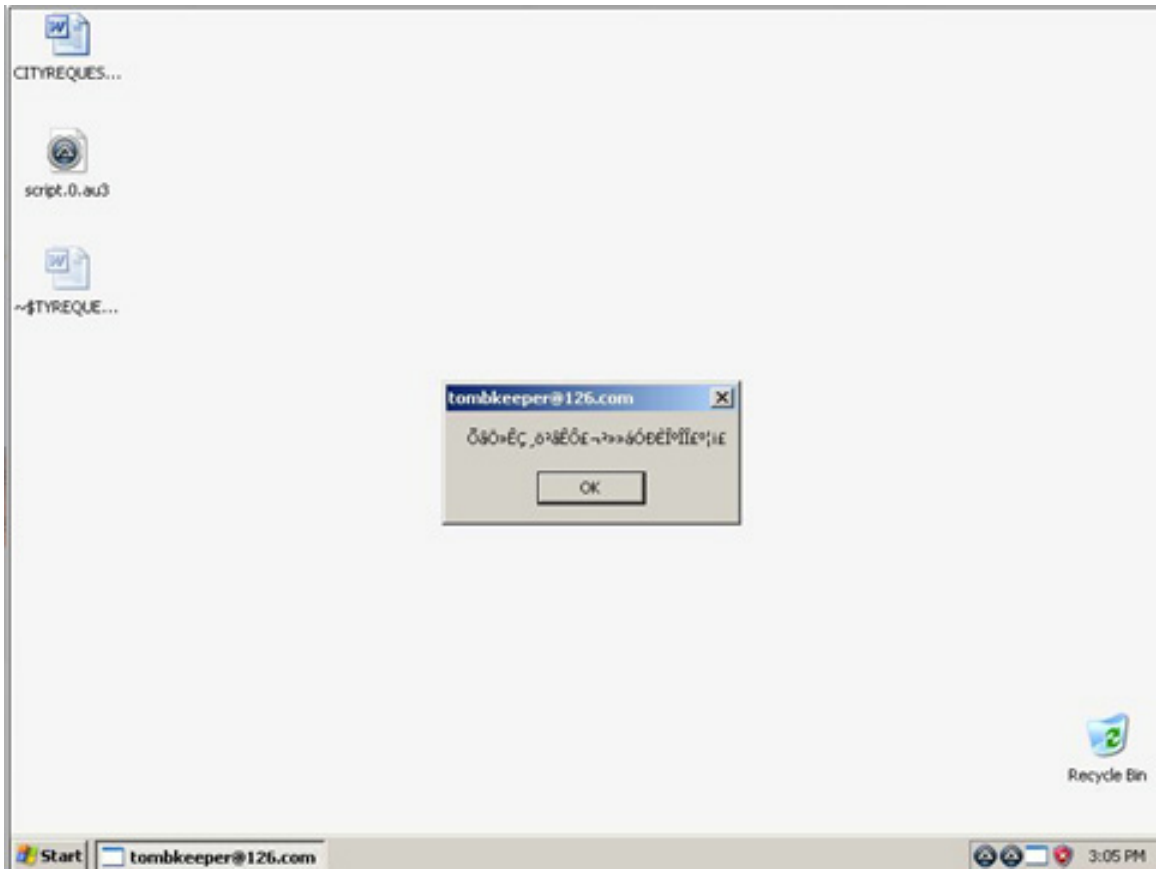
In the course of conducting research, we observed a highly targeted attack against a honeypot based in the United States in December 2012. Although this targeted attack took place prior to the period covered in this paper, March to June 2013, and has only been briefly discussed in "Who's Really Attacking Your ICS Equipment?," it will be discussed in greater detail here.

The targeted attack, like many others seen today, began with a phishing message sent to an email address provided on the website of the honeypot that was compromised. The email address closely mimicked a valid one that a city government would normally have. The phishing email had an attachment named *"CITYREQUEST.doc."*



Screenshot of *CITYREQUEST.doc* when opened

Opening the attached document opens a decoy document with little text defined. It also quickly and automatically closes then displays a dialog box containing unidentifiable text.



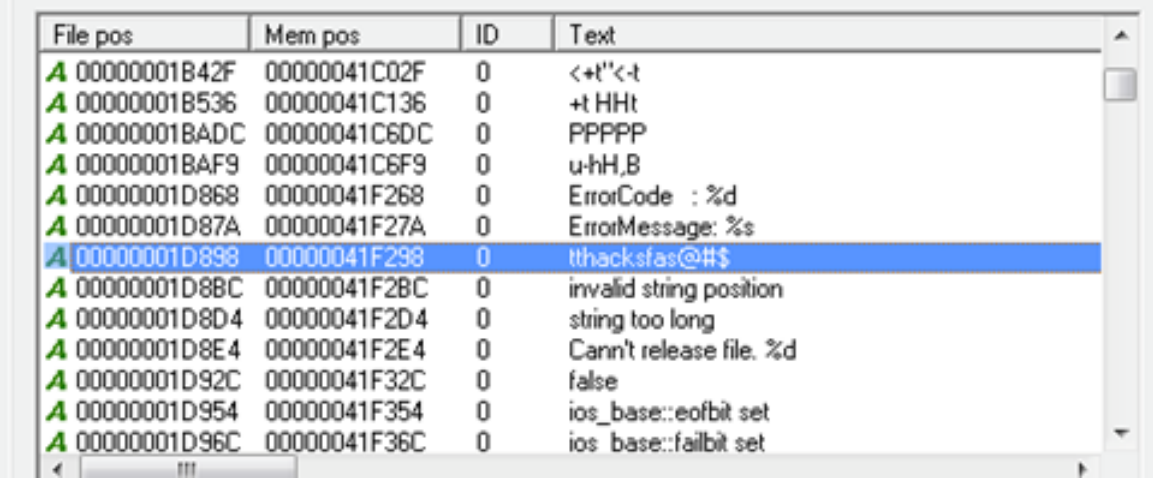
Dialog box that pops up after the document is closed

Clicking "OK" sends out several beacons to command-and-control (C&C) servers in China and the United States. The action also leads to the dropping of two files—*ai.exe* and *gh.exe*.

Gh.exe is a standard password hash dump file. When executed using the command line, you must run the "-w" switch to dump all of the hash's files. This is a standard functionality to maintain persistence and laterally move throughout a target network, seen in many targeted attacks.

Ai.exe, meanwhile, was more interesting. As soon as its strings were first dumped, we were able to identify its origin as a common piece of malware known as "HACKSFASE."[11]

11 Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." Last accessed July 4, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.



File pos	Mem pos	ID	Text
00000001B42F	00000041C02F	0	<+t"<-t
00000001B536	00000041C136	0	+t HHt
00000001BADC	00000041C6DC	0	PPPPP
00000001BAF9	00000041C6F9	0	u-hH,B
00000001D868	00000041F268	0	ErrorCode : %d
00000001D87A	00000041F27A	0	ErrorMessage: %s
00000001D898	00000041F298	0	tthacksfas@#$
00000001D8BC	00000041F2BC	0	invalid string position
00000001D8D4	00000041F2D4	0	string too long
00000001D8E4	00000041F2E4	0	Cann't release file. %d
00000001D92C	00000041F32C	0	false
00000001D954	00000041F354	0	ios_base::eofbit set
00000001D96C	00000041F36C	0	ios_base::failbit set

String showing HACKSFASE

```
User name or Password input wrong.
Domain Name input wrong.
The Remote Machine input wrong.
tthacksfas@#$
ERROR! Cannot connect to %s\IPC$.
%s\ADMIN$
```

Additional HACKSFASE reference

Further analysis of *ai.exe* yielded several switches that could be used to interface with it.

```
< ai.exe –d1 (Domain) –c1 (Compare IP) –s (Service) >
```

Example of a command structure for *ai.exe*

```
%SystemRoot%\System32\svchost.exe -k netsvcs
svchost.exe
%s\admin$\system32\
Port Number is wrong.
The Service describe is wrong.
-des
The Service display is wrong.
-dis
You must input dll name.
You must input services name.
-c2
you must choose at least one compare IP address.
-c1
The second dns name input wrong.
-d2
You must choose at least one dns name.
-d1
```

Code showing HACKFASE strings

The attackers' execution of *ai.exe* also led to data exfiltration, which began roughly three hours after *CITYREQUEST.doc* was opened. The items exfiltrated by the attackers include the Security Accounts Manager (SAM) database, VPN configuration files, and some additional configuration details like hostname, IP address, and location.

The attackers also sent a litany of commands via the server, many of which appeared to be for lateral movement purposes. Several "pings" and "traceroutes" to default gateways and adjoining networks were noticed. Also seen were many "arp" commands to look for communication patterns. Moreover, shared drives and folders were mounted and local host-based firewalls and antivirus software were disabled. Strikingly, the attackers used basic anti-forensic techniques like deleting prefetch data on Windows instances.

In traditional targeted attacks, these commands typically mean that the attackers are looking to maintain persistence in and laterally move throughout the target network.

Attack Statistics and Motivations

Attributing attacks is often very difficult to do. Accurately ascertaining who attacked your device is a daunting task and will only provide you a small subset of possible motivations. Determining motivations is also very difficult to do, as attackers would nearly never reveal their real intentions.

Most attack attribution attempts begin with determining the attackers' country of origin. Doing this will also help us ascertain their motivations. If Country A, for instance, is interested in copying Country B's ICS device deployment methodology then it is possible to derive Country A's motivation behind the attack.

As shown by data from the honeynet, many of the attacks targeted deployments in Russia. It is, however, also clear that most attacks originated in the same country. In fact, roughly 58% of the total number of attacks targeted deployments in Russia. The "cannibalistic" nature of attacks can easily be confirmed by looking at the honeypot data. Each honeypot deployed within Russia used a Russian IP address. Russian IP addresses launched noncritical attacks against the Russian honeypots a total of 43 times.

Among the critical attacks across the honeynet, five or 50% originated in China. It is interesting to note that we recorded four IP addresses from China launch attacks. These four IP addresses also resided in two /24 networks.

When attempting to determine possible motivations, we should also consider the type of attack that ensued. If an attack was targeted in nature, for instance, but did not compromise the operation of a target ICS device, the attackers' motivation could be espionage or information gathering. If an attack, however, compromised the operation of a target ICS device, depending on how badly it was affected then the motivation could be considered destructive in nature.

Among all of the attacks seen across the architecture from December 2012 to May 15, 2013, we can accurately say that at least 15 were targeted in nature and aimed to gather information, spy on the target, or compromise the target's operation. At least 33 attacks appeared to be destructive in nature and aimed to halt the operation of a target ICS device. These could be attacks of happenstance, wherein the attacker just happened to come across the honeypot, or targeted. But establishing the motivation behind these 20 attacks was more difficult to do. We did not consider "accidental" attacks, as counting such and proving they happened is difficult to do. An accidental attack can occur when an attacker with a nondestructive motive accidently causes a critical or destructive attack against a target ICS infrastructure.

We did not consider or account for attacks of happenstance as well. These attacks occur when someone searching ShodanHQ's site, for instance, happens to see an external-facing ICS device and decides to attack it. While many of the attacks we saw started out with ShodanHQ queries, we cannot accurately say if these were accidental or targeted in nature without additional details like port scans.

Conclusion

It is not possible to determine how often attacks against true Internet-facing ICS devices occur but we can say that attacks against unprotected or semi-protected ICS devices happen on a regular basis. The ICS device threat landscape constantly changes at a seemingly rapid pace. Attacks against ICS devices are occurring and simply ignoring this issue will not make the problem disappear.

As with any security problem, using a multitier approach is the best solution. Heeding the recommendations in "Who's Really Attacking Your ICS Equipment?" and implementing the following controls can help your organization thwart ICS attacks:

- **Implement a USB and external media lockdown:** A surprising number of ICS attacks start out from an infected USB drive. As such, do not allow the use of USB drives and provide Read/Write access to any external media on any ICS device.
- **Use proactive protection:** While many oppose the use of intrusion prevention system (IPS) or any sort of proactive protection on an ICS network, doing so can help thwart lateral movement. Not all networks can support proactive protection though, so use this only when applicable.

- **Whitelist applications:** In any ICS environment, it is important to not only know what applications are present, it is also imperative to control what are installed. Application whitelisting alleviates much of the stress involved in using application control. Application whitelisting only allows approved applications to be installed on a control network. This reduces the overall likelihood of vulnerability exploitation, in addition to minimizing the amount of communication that originates in a "protected" ICS network.

- **Classify data:** Knowing what data resides in or traverses an ICS network is very important in understanding the risks losing it can pose to an environment. Classifying data into "highly confidential," "confidential," and/or "open access" can help ensure that important and confidential documents do not make their way out of your ICS environment. Doing the same thing to information that comes in to the environment should enhance protection as well.

- **Follow a standard:** While many standards do not cover necessary topics many security experts would consider crucial, some ICS standards are very useful. Following the National Institute of Standards and Technology (NIST)—the U.S. government's ICS standards body—standards is a great starting point to get your ICS network in order.

- **Red team often:** While many are opposed to "red teaming" or penetration testing on networks or applications on an ICS network, research has proven that this often helps lower vulnerability counts and ensures that vulnerabilities are addressed. Performing red teaming on a quarterly basis, for instance, will help ensure that vulnerabilities are patched in a timely fashion.

- **Manage vulnerabilities:** Similar to red teaming, vulnerability management will also help ensure that vulnerabilities, especially critical ones, are patched. Introducing a vulnerability scanner and manager to your ICS infrastructure will help lower your vulnerability count and drive awareness of the issues plaguing your ICS environment.

Appendix

The following map and table show additional details regarding the attack types launched against each particular honeypot deployment.

COUNTRY ORIGIN AND ATTACK TARGETS

Overall Attack Matrix								
Origin	Target							
	Brazil	Russia	USA	Ireland	Singapore	China	Japan	Australia
Netherlands	N/A	2 NC	N/A	N/A	N/A	N/A	N/A	N/A
China	N/A	1 NC 3 C	N/A	1 C	N/A	1 NC 1 C	N/A	N/A
Germany	N/A	4 NC 1 C	N/A	N/A	N/A	N/A	N/A	N/A
Kazahkstan	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
Canada	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
USA	N/A	2 NC	N/A	N/A	N/A	1 NC	N/A	N/A
Australia	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
Moldova	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
Ukraine	N/A	2 NC	N/A	N/A	N/A	N/A	N/A	N/A
UK	N/A	N/A	N/A	N/A	N/A	1 C	N/A	N/A
France	N/A	N/A	N/A	N/A	N/A	1 C	N/A	N/A
Palestine	N/A	1 NC	N/A	N/A	N/A	1 C	1 C	N/A
Poland	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
Slovenia	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
Japan	N/A	1 NC	N/A	N/A	N/A	N/A	N/A	N/A
Russia	N/A	43 NC	N/A	N/A	N/A	N/A	N/A	N/A

Note: "N/A" stands for "not applicable"; "NC" stands for "noncritical"; "C" stands for "critical"

References

- *BeEF*. Last accessed August 13, 2013, http://beefproject.com/.
- *Dancho Danchev's Blog—Mind Streams of Information Security Knowledge*. (October 5, 2006). "SCADA Security Incidents and Critical Infrastructure Insecurities." Last accessed August 1, 2013, http://ddanchev.blogspot.com/2006/10/scada-security-incidents-and-critical.html.
- ISA SECURE. (April 15, 2013). "Establishment of ISASecure Japanese Scheme and Publication of ISASecure Embedded Device Security Assurance Certification Program Specifications in Japan." Last accessed July 29, 2013, http://isasecure.org/News-Room/Press-Releases/Establishment-of-ISASecure-Japanese-Scheme-and-Pub.aspx.
- John E. Dunn. (November 14, 2011). *Techworld*. "Mystery 'Virus' Disrupts New Zealand Ambulance Service: Malware Sends Operators Back to Manual Communication." Last accessed August 1, 2013, http://news.techworld.com/security/3318106/mystery-virus-disrupts-new-zealand-ambulance-service/.
- John Leyden. (January 11, 2008). *The Register*. "Polish Teen Derails Tram After Hacking Train Network: Turns City Network into Hornby Set." Last accessed August 1, 2013, http://www.theregister.co.uk/2008/01/11/tram_hack/.
- John Leyden. (June 25, 2013). *The Register*. "North and South Korea Hit by Cyber-Blitz on Korean War Anniversary: Official Nork Portals Knocked Offline, South Korean Prez, and PM also KO'd." Last accessed August 1, 2013, http://www.theregister.co.uk/2013/06/25/korean_war_anniversary_ddos_attacks/.
- Keith Stouffer, Joe Falco, and Karen Scarfone. (June 2011). "Guide to Industrial Control Systems (ICS) Security." Last accessed July 29, 2013, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.
- Kevin Poulsen. (September 3, 2003). *The Register*. "U.S. Warns Nuke Plants of Worm Threat: If There Was Ever a Place That Needed AV Protection…." Last accessed August 1, 2013, http://www.theregister.co.uk/2003/09/03/us_warns_nuke_plants/.
- Kyle Wilhoit. (2013). "SCADA in the Cloud: A Security Conundrum?" Last accessed July 29, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-scada-in-the-cloud.pdf.
- Kyle Wilhoit. (2013). "Who's Really Attacking Your ICS Equipment?" Last accessed June 27, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf.

- Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." Last accessed July 4, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
- Shelby Grad. (December 1, 2009). *L.A. Now*. "Engineers Who Hacked into L.A. Traffic Signal Computer, Jamming Streets, Sentenced." Last accessed August 1, 2013, http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html.
- *SHODAN*. (2013). Last accessed July 30, 2013, http://www.shodanhq.com/.
- The Tor Project, Inc. *Tor*. Last accessed July 3, 2013, https://www.torproject.org/.
- Tom Phinney. "IEC 62443: Industrial Network and System Security." Last accessed July 29, 2013, http://www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf.
- Wikimedia Foundation, Inc. (July 10, 2013). *Wikipedia*. "Industrial Control System." Last accessed July 29, 2013, http://en.wikipedia.org/wiki/Industrial_control_system.
- Wikimedia Foundation, Inc. (July 10, 2013). *Wikipedia*. "Operational Historian." Last accessed July 29, 2013, http://en.wikipedia.org/wiki/Operational_historianhistorian.
- William J. Broad, John Markoff, and David E. Sanger. (January 15, 2011). *The New York Times*. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." Last accessed August 1, 2013, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey to the Cloud

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