



---

# ANATOMY OF AN ATTACK

## Industrial Control Systems Under Siege

RESEARCH by TrapX Labs

---

Authored by: TrapX Labs – A Division of TrapX Security, Inc.

Date: August, 2017

## Table of Contents

Notice

About Anatomy of an Attack

Executive Summary

Industrial Control Systems – A Legacy of Sophisticated Attacks

New Case Studies from TrapX Security Operations Center

Case Study #1 – Global Pharmaceutical Manufacturer

Case Study #2 – Paper Products Manufacturer

Case Study #3 – Tubing, Pipe and Sheet Metal Manufacturer

Case Study #4 - Water Treatment and Waste Processing Company

Case Study #5 – Power Plant

The Specific Threat to Industrial Control Systems (ICS/SCADA)

Understanding the Attack Vectors

Inside Industrial Control Systems

Industrial Control System Architecture

Industrial Control Systems Operations

Evolution of Functionality Increases Vulnerability to Attack

Industrial Control System Protocols

Recreating an Attack – The Aurora Vulnerability Attack Vector

Conclusions

Recommendations

About TrapX Security

Find Out More – Contact Us Now

Trademarks

## Notice

TrapX Security reports, white papers, and legal updates are made available for educational purposes and to provide general information only. Although the information in our reports, white papers and updates are intended to be current and accurate, the information presented therein may not reflect the most current developments or research.

Please note that these materials may be changed, improved, or updated without notice. TrapX Security is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

## About Anatomy of an Attack

The Anatomy of an Attack (AOA) Series highlights the results of our research into current or potential critical information security issues. The AOA series is a publication of TrapX Laboratories. The mission of TrapX Labs is to conduct critical cyber security experimentation, analysis and investigation and to bring the benefits back to the community at large through AOA publications and rapid ethical compliance disclosures to manufacturers and related parties.

The TrapX Labs knowledge base benefits significantly from information on advanced malware events shared with us by the TrapX Security Operations Center (TSOC). Uniquely this TSOC threat analysis includes very deep intelligence on advanced persistent threats (APTs) provided by our global interactions with customers and partners, both commercial and government.

## Executive Summary

The 2003 the Northeast Blackout consisted of a series of power outages that stretched across eight states and further into Canada. This outage was so extensive that it took close to two days to restore power to the more than 50 million people impacted. In total, the event contributed to at least 11 deaths and cost over \$5+ billion.

The reaction from industry and public utilities was to implement sweeping changes to ensure business resiliency and continuity. A major part of these changes was to enable the remote monitoring and control of important power and manufacturing subsystems previously closed off from the internet. Unfortunately, by solving one problem, manufacturers have in fact exposed themselves to another. Critical infrastructure which was historically shielded due to isolation from the internet is now at significant risk for cyber-attack. Embedded supervisory control and data acquisition (SCADA) systems often use out of date operating systems and present an easy target to attackers.

Over the past few year's attackers have exploited this opportunity, and as documented in our Anatomy of an Attack (AOA) report, have compromised a wide variety of manufacturing control systems. This report documents five case studies which show how cyber attackers could gain access to manufacturing and utility facilities. We also detail the progression of the attacks which in some cases disabled operations for an extended period. In one of our case studies, losses were catastrophic with the impacted entity suffering losses of over 800,000 euro per day.

This report will explain how the attacks happen, and once established, how the attackers can extend these command and control points to breach the institution's records, blackmail and extort funds, or worse, disable ongoing operations of the facility over an extended period.

Over the past five years, cyber security has become a top corporate issue within the manufacturing industry for chief executive officers, their executive teams and the board of directors. Manufacturing sector companies, despite seeing a reduction in attacks and security incidents in 2016 still experienced some of the most serious and compromising attacks at a rate estimated as almost 40 percent higher than the average across all industries. Per one report manufacturing was the third most attacked sector in 2016.<sup>1</sup>

Industrial control systems (ICS) are the prime target for cyber attackers seeking to compromise the manufacturing base and public utilities. The legacy of old embedded Microsoft® operating systems provide attackers a well-protected safe harbor from which to launch their attack and establish "backdoors" to compromise the enterprise. Attackers have proven that they can successfully work through a multi-layer cyber defense, strict user access policies, links filtered through corporate network firewalls, and even air-gapped perimeter defenses.

In the final analysis, strategies that attempt to defend the perimeter, whether through physical means or policy are insufficient to provide the comprehensive defense that critical infrastructure demands. Attackers will get through. It is imperative therefore that manufacturers find new and innovative ways to detect ICS attackers early, mitigate the effects of their attack, and then defeat them.

**Tom Kellermann, CEO of Strategic Cyber Ventures, Global Fellow for the Wilson Center and advisor to the International Cyber Security Protection Alliance (ICSPA)**

In contrast, another report examined the risk factors the 10-K filings of the largest 100 publicly traded U.S. manufacturers. Approximately 92% of manufacturers share significant concern about cybersecurity concerns up

---

<sup>1</sup> IBM 2017 X-Force Threat Intelligence Index

from approximately 44% percent from 2013. 91% of manufacturer's further have concerns about related operational infrastructure risk, which relies heavily upon information systems and related network infrastructure.<sup>2</sup>

Manufacturing information technology and information security personnel are not surprised by these revelations. The manufacturing sector has been vulnerable for years and continues to experience a high rate of disruptive and financially costly attacks. Many of these have not been disclosed to the public. An earlier 2015 report by Dell Security<sup>3</sup> noted that the reported attacks on supervisory control and data acquisition systems had climbed by over a factor of five from 2012 to 2014.

It is a conclusion of this report that the majority of industrial control systems deployed across the many thousands of power plants and manufacturing facilities globally are all susceptible to the cyber-attacks documented in this report. This report also supports our conclusion that attackers will successfully breach ICS networks, even with the best perimeter, endpoint, intrusion detection and defense in depth cyber defense strategy. We also find that socially engineered attacks, the failure of "air gaps" and failure of policy directed security are common themes. This is certainly the case as you review our actual case studies. Many industrial networks are near "air gapped" and isolated to some extent from other internal networks. Consider that it only takes one connection point to an outside network (through a USB stick, a repairman's laptop, a quick plug-in of a manager's laptop into another network) to result in a potentially catastrophic industrial emergency.

The clear theme that emerges is that industrial control systems need a more comprehensive strategy for dealing with persistent targeted attacks. The probability of breach in these cases over time is high. Manufacturers can benefit best from a strategy that detects the breach and then mitigates the impact. Deception technology has proven that it can deceive and detect these advanced attackers once they have penetrated perimeter cyber defenses and then enabling the security ecosystem and/or the security operations team to shut down the attack promptly so that normal operations can be removed.

Finally, we present our analysis and recommendations for minimizing the risk associated with an industrial control system attacker and our ideas towards best practices for design, implementation and system life management of these facilities.

---

<sup>2</sup> <https://www.bdo.com/insights/industries/manufacturing-distribution/2016-bdo-manufacturing-riskfactor-report>

<sup>3</sup> <https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf>

## Industrial Control Systems – A Legacy of Sophisticated Attacks

Industrial control systems are part of our key infrastructure. Industrial control systems are at the center of all our manufacturing and process control systems around the globe. Industrial control systems are embedded everywhere within our power plants, chemical manufacturing, food and beverage process plants, automotive, aerospace, pharmaceutical, water and wastewater management systems and many other types of critical industrial processes.

The typical power plant or manufacturing facility is replete with internet connected systems and computer controlled controllers. These devices are also connected to other electronic systems that are part of the control process. This creates a highly connected ecosystem that brings the most vulnerable devices together and exposes it to this to invading cyber attackers.

Attackers may be standalone operators, part of larger organized crime syndicates, nation states or even terrorist organizations. Some attackers are interested in seizing control of the manufacturing process so they can extort funds for economic gain. Other attackers are focused on the theft of intellectual property. Finally, there are those attackers that want to deliver attacks in an attempt to cripple critical infrastructure and cause physical harm to personnel in proximity to these attacks.

It is the informal observation of TrapX Labs that this final group of attackers are active, preparing research and creating back-door pivot points so that these attacks can be initiated at a later date. These attackers know that industrial control systems have a legacy of uncorrected cyber vulnerabilities. They know that a successful cyber-attack on ICS can uniquely result in physical harm to people and resources in the affected area.

Imagine a horrendous crisis such as the industrial accident which happened in Bhopal, India and exposed over 600,000 people to the toxic gas methyl isocyanate.<sup>4</sup> Perhaps as many 15,000 people died as a result of this attack. Now imagine an attack of the same magnitude being initiated remotely, by a cyber attacker, using one of the manufacturing facilities that belong to your business.

On September 10, 2015 during testimony before the House Select Committee on Intelligence, James R. Clapper, the Director of National Intelligence stated for the record that, “Politically motivated cyber-attacks are now a growing reality, and foreign actors are reconnoitering and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary’s intent became hostile.” Clapper further noted that “cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures ... actors successfully compromised the product supply chains of at least three ICS vendors such that customers downloaded malicious software (“malware”) designed to facilitate exploitation directly from the vendors’ websites along with legitimate software updates...”<sup>5</sup>

Anecdotal evidence suggests that the great majority of attacks go unreported. In general, companies are only required to report data breaches as required by local data breach laws, compliance requirements and which generally involve the theft of money, personal data or related payment information. Government entities have widely varying commitments to public disclosure. Breaches are bad news and almost always have a negative effect on business fundamentals. In the absence of compliance driven disclosure, many enterprises decide not to disclose information about the attack.

As we have observed, many cyber attackers tend to use generic cyber attack tools and standard malware. They may use a well developed socially engineered attack but in the end, rely on standard attack vectors. They may target manufacturing directly but do not demonstrate or utilize any special knowledge of the industrial process control systems.

A second and emerging group of cyber attackers is more concerning. These cyber attackers are highly sophisticated and demonstrate an advanced knowledge of both information technology systems as well as the industrial control

---

<sup>4</sup> <https://www.theatlantic.com/photo/2014/12/bhopal-the-worlds-worst-industrial-disaster-30-years-later/100864/>

<sup>5</sup> <http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf>

systems architectures and the manufacturing processes they support. Some of them understand how to program the various PLM controllers and subsystems. These are the most threatening.

We need to learn from history. The trends and sophistication of attackers have been building for many years. Industrial control systems have been a high-value target of choice. The cyber security experts that read this report are likely very familiar with these known attacks.

#### Stuxnet - 2011

Stuxnet is perhaps the most famous and recent attack on industrial control infrastructure.<sup>6</sup> It is believed that one or more governments developed the Stuxnet worm to sabotage and delay Iran's nuclear program. Stuxnet was designed to target the PLC controllers that directly controlled the approximately 7,000 centrifuges used to process uranium within Iran's atomic research facilities. Stuxnet relied on the use of outdated operating systems and certain specific versions of Siemens® control software.

The Stuxnet attack was extremely successful. The attack supposedly damaged over 20% of Iran's nuclear centrifuges and set their programs back well over a year. Imagine, in the worst case, the centrifuges spinning out of control, breaking, and spreading radioactive material within the local area. It is important to note that Stuxnet worked via infected USB drives. As the internal network, the Siemens PLC's and the centrifuges were "air-gapped" to protect activity, the plan for the propagation of the attack was carefully targeted to several contractors that regularly visited the facility. Then the use of USB drives would propagate the intended attack to the internal networks. Note that Stuxnet was designed to cause no harm unless you had a very specific model of Siemens PLC and the associated software. In short, it was targeted and designed to destroy Iran's nuclear program.

#### Duqu - 2011

Duqu is another very sophisticated and advanced attack discovered in late 2011 that seems to be related to the Stuxnet worm. The Budapest University of Technology and Economics in Hungary wrote a report and named the threat Duqu.<sup>7</sup> Duqu seeks information that could be useful in attacking industrial control systems but still, no example has been found yet with ICS specific attack code. Initially, Duqu appears to be non-destructive as the visible structures are trying to gather information. However, upon review of the structure of Duqu, it could clearly deliver a special payload used to propagate almost any type of attack.

According to McAfee<sup>8</sup>, one of Duqu's primary activities is to acquire digital certificates and the private keys that support them from attacked computers to help future malware payloads infiltrate. Duqu uses a pixel jpeg file and encrypted dummy files as containers to smuggle stolen data to its command and control center. Security experts are still analyzing the code to determine what information these communications contain. Research suggests that the original malware automatically removes itself after 36 days which would make it very hard to detect upon forensic inspection.

#### German Steel Plant - 2014

In 2014 a major steel plant in Germany was the target of a sophisticated attack which resulted in significant damage to plant operations. This attack was reported by the German Federal Office for Information Security (BSI).<sup>9</sup> Many of the details of the attack including the nature and type of malware used, the identity of the company and more have been withheld by the German Federal Office for Information Security report.

This advanced attack was combined with the use of social engineering and spear fishing to gain access to the corporate networks of the steel plant. Using links between the corporate networks and the production industrial control system networks, the attackers were able to penetrate the networks involved with manufacturing and process

---

<sup>6</sup> <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

<sup>7</sup> <http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf>

<sup>8</sup> <http://www.mcafee.com/us/about/duqu.aspx>

<sup>9</sup> <https://translate.google.com/translate?hl=en&sl=de&u=https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html&prev=search>



control. Production lines experienced long shutdowns due to the attack and in particular, this attack caused damage to the central plant blast furnace which resulted in very significant damage to the plant.

#### The Legacy of ICS Attacks

The key takeaway from this section of the report is a reminder that Stuxnet has forever changed the rules of engagement. Cyber-attacks can be used successfully against ICS to inflict physical damage and injury to personnel. Cyber-attacks against ICS can support important strategic objectives in time of war or in preparation for future war. Cyber-attacks against ICS are a likely cornerstone of an asymmetric warfare strategy where millions of dollars invested can counter billions invested by an opponent in traditional military programs and deployment. For all of these reasons and more ICS systems within the industry and the public utility infrastructure are moving to the center of the bullseye for attackers.

## New Case Studies from TrapX Security Operations Center

Five important case studies from the TrapX security operations center are reviewed in this section. Our 4th and 5<sup>th</sup> case studies were documented very recently in 2017 and remain under ongoing investigation. These case studies were selected because we believe they serve to highlight unexpected problems with ICS cyber defense. All of the customers involved were generally surprised by the presence of the ongoing ICS attack, by the attack vector chosen, and by their existing cyber suites failure to detect any of the ongoing breach activities in a timely way.

### Case Study #1 – Global Pharmaceutical Manufacturer

Our first manufacturing case study focuses on a global pharmaceutical company that uses automation to produce their products, package them and then collects them for shipment. Assets included a very large network of industrial control systems (ICS) and additional components which run their manufacturing processes end to end. Prior to our involvement, this manufacturer was unaware of sophisticated malware infection or advanced persistent threats. The customer had an industry suite of cyber defense products supported by an almost relatively closed or partitioned network. There were several limited network connections back to the corporate network.

TrapX DeceptionGrid™ was installed within their industrial control system infrastructure near the supervisory control and data acquisition (SCADA) console. The TrapX sensors generated ALERTS and identified malicious activity.

This network worm attacked the network by scanning randomly generated IP addresses on port 445. Once a connection was established, the worm sent exploit code to the target computer. If the computer is running a Windows OS the exploit code caused the computer to download a copy of the worm using TFTP protocol which then ran on the exploited computer. The malicious code then connects to an IRC server to receive commands, which can include retrieving system information, downloading more malicious files, executing them using HTTP and then carefully removing the original worm malicious code.

Our security operations center began a forensic investigation to understand how the malware was able to penetrate this critical and secure network. We determined that the source of the infection was one of the ICS vendor personnel that had arrived on-site to provide maintenance and upgrade various servers. Our research determined that an “Air-Gap” was compromised and broken. Notwithstanding the rigorous security protocols mandated by the pharmaceutical manufacturer, ICS vendor personnel plugged an infected USB memory stick into an Outage Restoration Management Suite server (ORMS) for the upgrade process. This was spreadable malware and it infected the server and then spread to ICS devices running windows OS as well as the deception technology traps which provided the initial detection of the attack.

The analysis of the malware enabled the security operations center to create a network IOC (an indication of compromise). Using this IOC we found two additional SCADA console PCs that were also compromised. To make matters worse, it was determined that the defense in depth suite that was deployed in certain areas was not placed on the console PCs as this asset was categorized as “critical” and for this reason, it was felt that the security software might lead to unexpected variations in behavior or performance.

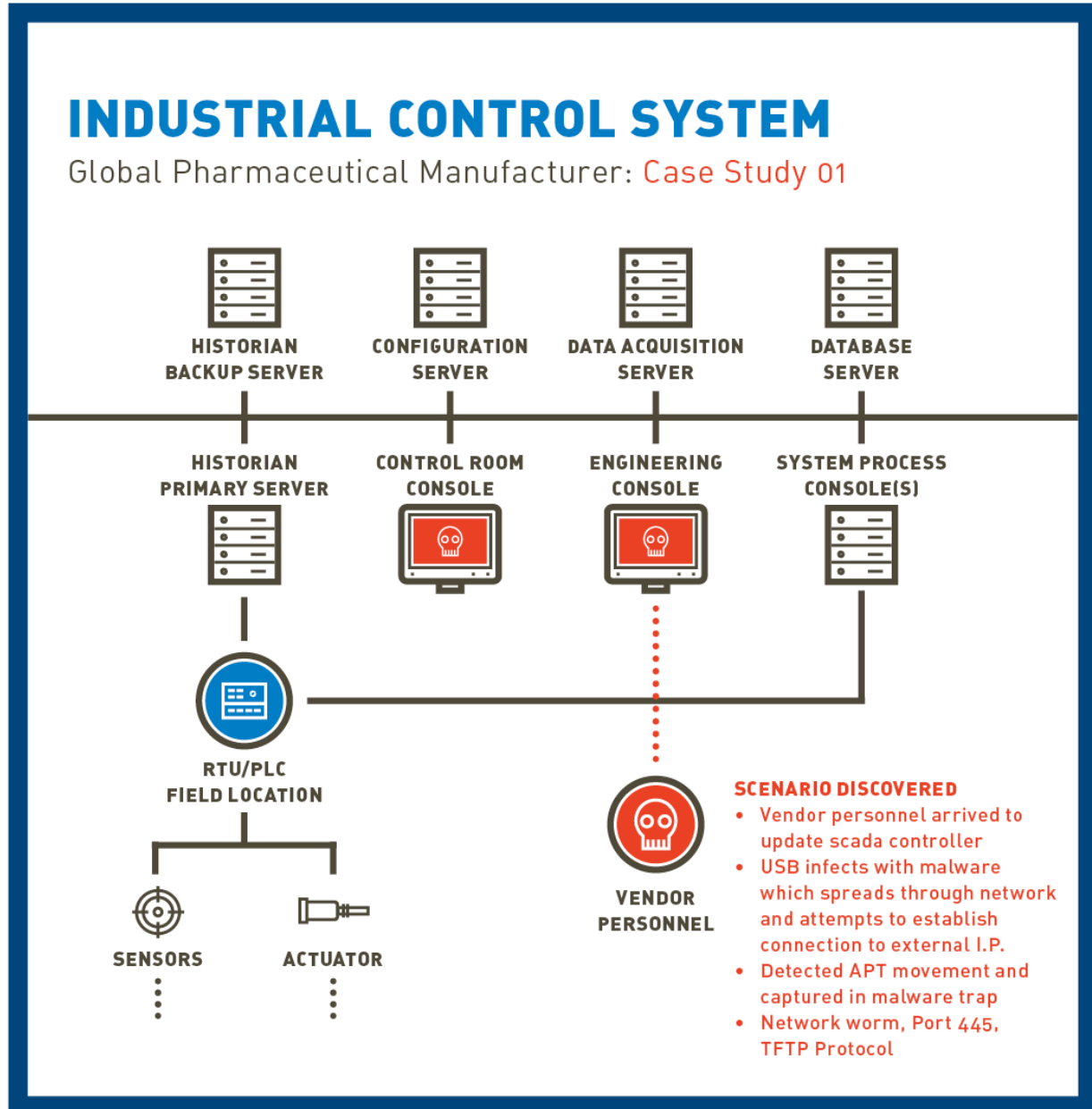
The customer coordinated with TrapX and ICS component vendors to determine the impact of the attack and then to re-provision the software in all of the affected components.

#### Threat Description:

- MD5 - 7a67f7a8c844820c1bae3ebf720c1cd9
- Second stage Infection method : tftp://x.x.x.x/a3048.exe
- Payload file name : a3048.exe

Conclusions from this case study include:

- “Air Gaps” continue to be breached by media such as USB memory.
- Deception technology works to enhance network visibility and provide attacker identification in sensitive ICS environment that can not be protected by classical security solutions.
- Best practice includes the creation of a process that checks and clean files that come from external sources by running them on a standalone computer that runs anti-virus (AV) software that includes at least 5 of the leading AV engines .



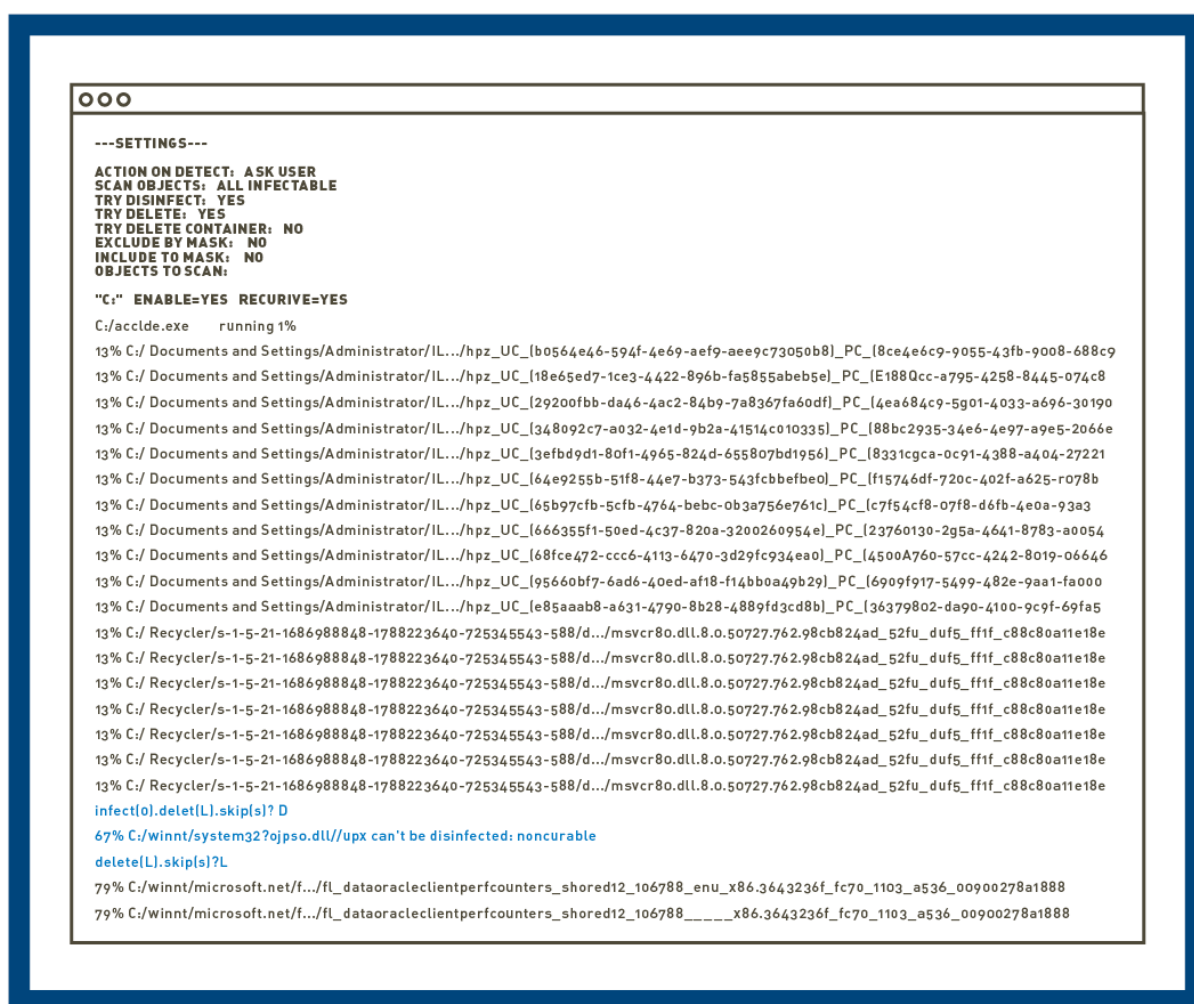
Copyright 2015 TrapX Security, inc.

**Figure 3 – Industrial Control System Infrastructure for a Global Pharmaceutical Manufacturing Company – Case Study 1**

## Case Study #2 – Paper Products Manufacturer

Our second manufacturing case study centers on a paper products manufacturer that uses automation to process the paper pulp, produce the paper into several products, then collect and package them for bulk shipments. Assets included a network for industrial control systems (ICS) and additional modules integrated with their manufacturing processes. The customer had an industry suite of cyber defense products including firewalls, network intrusion detection, endpoint security, anti-virus and more. There were multiple network connections between the ICS and the corporate networks.

TrapX DeceptionGrid™ was installed within corporate information technology and within the SCADA infrastructure close to the management consoles. ALERTS pointed to directed lateral movement that came from a server which managed the industrial production floor. This server controlled the machine that was in charge of the automated movement of raw materials on the industrial floor. This server was connected to corporate information technology assets, the SCADA network and the external Internet.



Copyright 2015 TrapX Security, Inc.

### Screen Capture 1 - Malicious Code Identified in Paper Manufacturer SCADA Networks

It should be noted that this paper manufacturing facility operated on a 24-hour basis, 7 days per week. Shortly after installation, TrapX deception technology found several types of malware activity. We detected connections between

malware command and control in the internal server to botnets within the Dark-Net network. The deception technology traps detected the same server attacking the SCADA network trying to exploit the SMB protocol. The server was running defense in depth software (specifically Trend Micro® AV) which in this instance did not detect the attack.

We participated in a forensic investigation with the engineer on the manufacturer cyber security team and observed:

- The SCADA management server has access to the internet and runs an outdated version of AV software.
- The server was infected from web surfing (large amount of web cache was found).
- The malware started spreading across the network and use SMB exploit. Once the exploit was successful the second stage payload was loaded using http connection from the primary infected machine.
- The management server that was infected and started the spreadable vector infected several manufacturing devices running windows XP and also several Deception Trap sensors.
- Each infected machine tried to connect to a C&C server that was part of the Tor network using port 443.

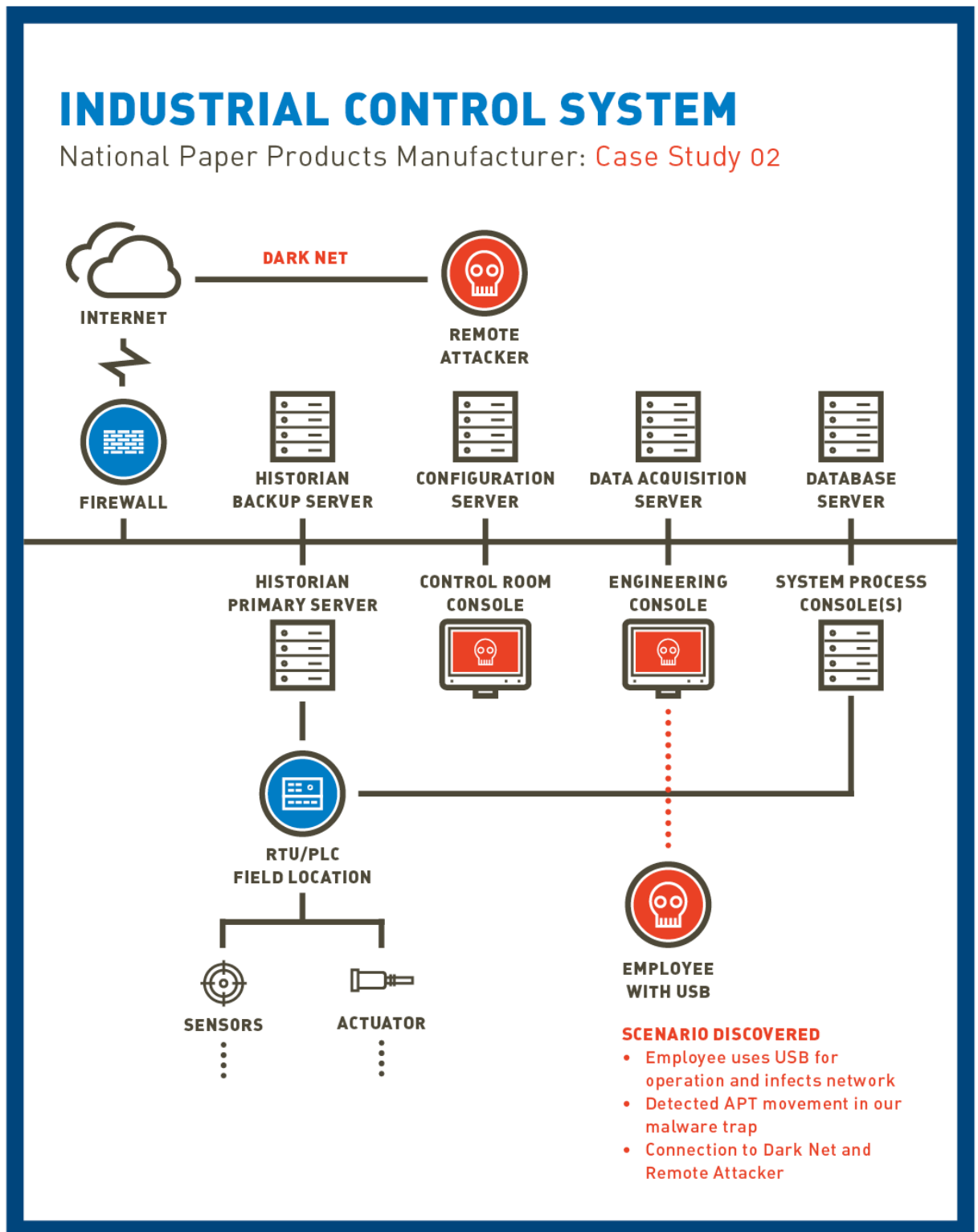
#### Threat Description:

- MD5 - 0e0f1ced3b52d51ff1056e2aab715848
- Second stage Infection method : <http://x.x.x.x:7059/hspmr/> / <http://x.x.x.x:2049/ssrxoz> (the string gets change on each infected machine)
- C&C server IP - 195.22.26.231, 192.58.105.7, 37.0.124.119
- Screen capture 1 shows the threat inside the primary infected machine (scada management).

#### Conclusions from this case study include:

- Best practice suggest strongly that the industrial production floor should be isolated from the internet and the rest of the corporate network.
- ICS management system that allows the vendor to install AV software should be frequently maintained so that the most recent signature & software updates are applied.
- As before, deception technology works to enhance network visibility and provide attacker identification in sensitive ICS environment that can not be protected by classical security solutions.

- Review your playbook on incident response – these sorts of attacks on the production line will surely stop the production process for potentially extended periods of time.



Copyright 2015 TrapX Security, Inc.

**Figure 4 – Industrial Control System Infrastructure for a Global Pharmaceutical Manufacturing Company – Case Study 2**

## Case Study #3 – Tubing, Pipe and Sheet Metal Manufacturer

Our manufacturing case study focuses on one of the largest manufacturers of steel products to include tubing, pipe and sheet. Assets included a very large network for industrial control systems (ICS) and the necessary supervisory control and data acquisition (SCADA) components which run their manufacturing processes end to end. The customer had a large industry suite of cyber defense products which included a firewall, anti-virus suites, multiple intrusion detection software products, endpoint security and other software. The software on the SCADA networks was manufactured by Siemens, a well respected vendor and supplier of this technology.

OOO				
SVCHOST.EXE	93	3236	C:\Windows\System32	C:\Windows\System32\Svchost.exe -lc Hp212
SVCHOST.EXE	93	2336	C:\Windows\System32	C:\Windows\System32\Svchost.exe -lc Hp212
SVCHOST.EXE	93	1792	C:\Windows\System32	C:\Windows\System32\Svchost.exe -lc Metsvcs
SYSTEM	92	4		
WMIPVSE.EXE	61	5840		
SQLEXPRESS.EXE	58	1932	C:\Program Files\Microsoft Sql Server\Mss...	"C:\Program Files\Microsoft Sql Server\Mssql\Binn\Sqlserver.exe" - Swt
CUSS.EXE	57	1104	\\?\C:\Windows\System32	C:\Windows\System32\Csrss.exe Objectdirectory=\Windows Shared Section=100
RTHDOP.EXE	53	2552	C:\Windows	C:\Windows\svrthdcp.exe
WMIPVSE.EXE	53	276	C:\Windows\System32\Wbem	
OPCIDASERVER.EXE	52	4824	C:\Program Files\Siemens\Simatic.net\Op...	C:\Program Files\Siemens\Simatic.net\Opc2\Bin\Opcidaserver.exe" Embedded
SCORE57.EXE	52	4584	C:\Program Files\Siemens\Simatic.net\Op...	C:\Program Files\Siemens\Simatic.net\Opc2\Bin57\Score57.Exe
TEAMVIEWER.EXE	52	4604	C:\Program Files\TeamViewer\Version8	C:\Program Files\TeamViewer\Version8\TeamViewer.exe
EXPLORER.EXE	52	2256	C:\Windows	C:\Windows\Explorer.exe
WINLOGON.EXE	52	1128	\\?\C:\Windows\System32	Winlogon.exe
TV.W32.EXE	49	5556	C:\Program Files\TeamViewer\Version8	
SIMNETPNPMAN.EXE	49	484	C:\Program Files\Siemens\Simatic.Net\Sa...	C:\Program Files\Siemens\SimaticNetCom\simnetpnpman.exe
SYSEBMDATLOGGER.EXE	49	1004	C:\Program Files\GeSiTsell	C:\Program Files\GeSiTsell\Systemdataalklogger.exe
CBLMINTERFACE.EXE	49	2024	C:\Program Files\CobianBackup11	C:\Program Files\CobianBackup11\cbinterface.exe-service
TEAMVIEWER_SERVICE.EXE	49	2476	C:\Program Files\TeamViewer\Version8	C:\Program Files\TeamViewer\Version8\TeamViewer_Service.exe
SVCHOST.EXE	49	2236	C:\Windows\System32	C:\Windows\System32\Svchost.exe -k imgsvc
OPC-UA.DISCOVERYSERVER.EXE	49	2632	C:\Program Files\CommonFiles\OPC Found	C:\Program Files\CommonFiles\OPC Foundation\UA\v1.0\Bin\opc.Ua.Discovery
SPOOLSV.EXE	49	608	C:\Windows\System32	C:\Windows\System32\spoolsv.exe
CLIENT32.EXE	49	1072	C:\Program Files	C:\Program Files\NetSupport\NetSupportManager\Client32.exe
CBSERVICE.EXE	49	1188	C:\Program Files	C:\Program Files\CobianBackup11\cbservice.exe

Copyright 2015 TrapX Security, inc.

TrapX deception technology malware traps were installed both within the standard information technology network and the SCADA networks. It should be noted that the SCADA networks and the information technology networks were physically isolated from each other.

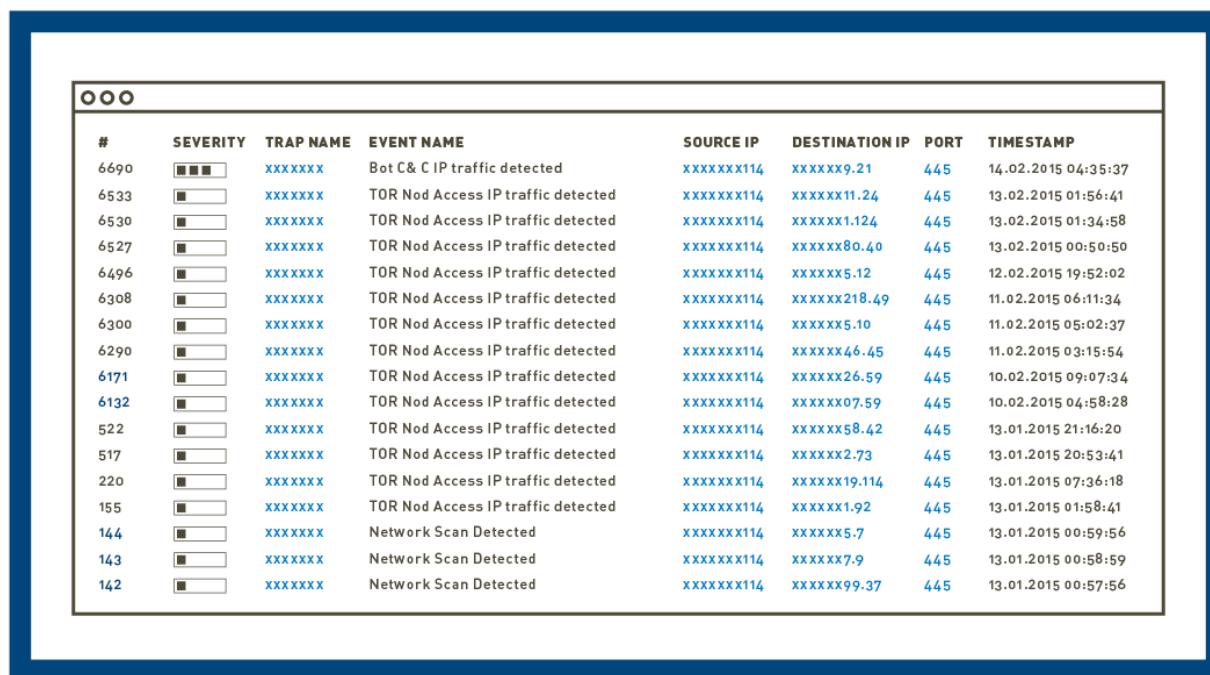
Deception technology was also installed in the SCADA network. Deception technology also monitored the egress traffic on the SCADA network that was used for vendor support only in case of emergency.

We noted that an internal PC was connected to several botnet C&C networks within the Dark-Net. The PC that was attacking the SCADA network was also trying to exploit the SMB protocol.



In the screenshot below we can see that the infected machine was trying to access the darknet network (using TOR) and in the same time we see internal scanning to identify additional potential windows host targets.

Once the attacker malware identifies more active assets, it then tries to inject malware using SMB (port 445), one of several MB exploits and the pass the hash (PTH) technique.



#	SEVERITY	TRAP NAME	EVENT NAME	SOURCE IP	DESTINATION IP	PORT	TIMESTAMP
6690	■■■	XXXXXX	Bot C & C IP traffic detected	XXXXXX114	XXXXXX9.21	445	14.02.2015 04:35:37
6533	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX11.24	445	13.02.2015 01:56:41
6530	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX1.124	445	13.02.2015 01:34:58
6527	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX80.40	445	13.02.2015 00:50:50
6496	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX5.12	445	12.02.2015 19:52:02
6308	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX218.49	445	11.02.2015 06:11:34
6300	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX5.10	445	11.02.2015 05:02:37
6290	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX46.45	445	11.02.2015 03:15:54
6171	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX26.59	445	10.02.2015 09:07:34
6132	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX07.59	445	10.02.2015 04:58:28
522	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX58.42	445	13.01.2015 21:16:20
517	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX2.73	445	13.01.2015 20:53:41
220	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX19.114	445	13.01.2015 07:36:18
155	■	XXXXXX	TOR Nod Access IP traffic detected	XXXXXX114	XXXXXX1.92	445	13.01.2015 01:58:41
144	■	XXXXXX	Network Scan Detected	XXXXXX114	XXXXXX5.7	445	13.01.2015 00:59:56
143	■	XXXXXX	Network Scan Detected	XXXXXX114	XXXXXX7.9	445	13.01.2015 00:58:59
142	■	XXXXXX	Network Scan Detected	XXXXXX114	XXXXXX99.37	445	13.01.2015 00:57:56

Copyright 2015 TrapX Security, inc.

## Screen Capture 2 - Connection to Botnet Command and Control IP Addresses

The forensic investigation determined that an engineer that maintained and operated the SCADA infrastructure used his laptop to work on both the IT and the SCADA networks. He would connect to one network, disconnect and then connect to the other. The laptop was infected in the IT network and then used his laptop, when connected to the SCADA, to launch an attack.

The malware was successful in hiding from the corporate AV software. Several AV scans provided no additional information answer so our forensics team captured deep memory dumps to support additional investigation .

The memeory dump shows us that the SVCHOST.EXE was the service that create the malicous network connection. The malware was injected into a legitimate process to camouflage and hide ongoing malicious activities.

You can see in the screenshot below the malicous connection that was detect by the NIS sensor trigger from the SVCHOST.EXE process.

## Screen Capture 3 - Laptop Running Siemens Software

PROCESS NAME	PID	PATH	STATE	CREATED	LOCAL IP ADDRESS	LOC	REMOTE IP ADDRESS	RE.	PROTOCOL
svchost.exe	1792	C:\WINDOWS\System32	Unknown	xxxx 2015 05:43:54	xxx.xx.x.x.xxx	123	.*	0	UDP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1509	xxxxx31.32	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1505	xxxxx12.24	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1502	xxxxx60.6	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1525	xxxxx29.62	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1507	xxxxx28.49	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1495	xxxxx8.112	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1480	xxxxx5.60	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1489	xxxxx65.117	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1483	xxxxx6.119	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1518	xxxxx7.18	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1484	xxxxx3.5	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1494	xxxxx27.21	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1492	xxxxx127.107	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1490	xxxxx9.83	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1286	xxxxx3.19	1900	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1511	xxxxx10.47	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1519	xxxxx214.31	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	1476	xxxxx104.95	445	TCP
svchost.exe	1792	C:\WINDOWS\System32	Established		172.16.1.114	103	xxxxx102.42	445	TCP

Copyright 2015 TrapX Security, Inc.

#### Screen Shot 4v - SVCHOST.EXE Infected by Malware and Connected to Botnet

Since the malware was not detected and the SCADA infrastructure had far less protection. The potential for damage was considerable.

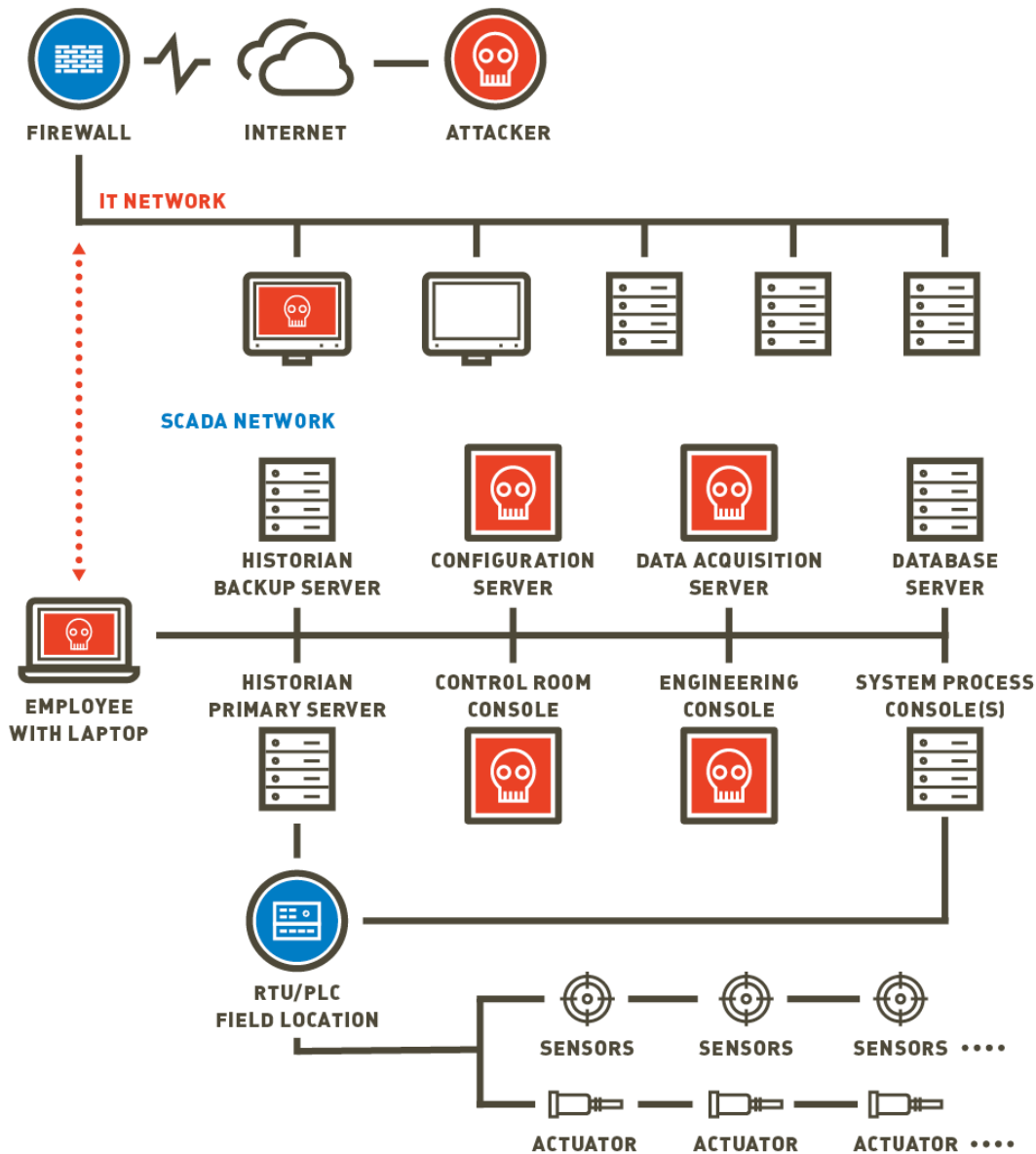
This is yet another classic case where even physical isolation did not provide insurance that cyber attack will not harm critical infrastructure. In our case if the SCADA system was shutdown the economic loss was approximately 800,000 Euro's every day.

Conclusions from this case study include:

- Implement a wide mix of deception technology traps in both the SCADA and information technology networks for the best visibility and protection. Assume air gaps will be breached. Prepare accordingly.
- Install additional SCADA console PCs in the console area to eliminate the need to bring an additional external laptop.
- Files and software that was to be brought into the network will go through an additional, extensive security check on standalone isolated workstations.
- The company web policy filter was modified to avoid downloading PE32 files.

# INDUSTRIAL CONTROL SYSTEM

Tubing, Pipe and Sheet Metal Manufacturer: Case Study 03



Copyright 2015 TrapX Security, Inc.

Figure 5 – Industrial Control System for a Tubing, Pipe and Sheet Metal Manufacturing–Case Study 3

## Case Study #4 - Water Treatment and Waste Processing Company

Our 4th case study focuses on a large international provider of water treatment and waste processing services. The attackers used the DMZ server as a pivot point to compromise the internal network. This case study is particularly interesting as the defenders rapidly identified multiple major attacks against several of their plants. These ongoing breaches and the related attacker activity were previously unidentified by their perimeter defenses and other standard cyber defense software.

Their assets include a very large industrial control systems (ICS) infrastructure and the necessary supervisory control and data acquisition (SCADA) components which manage and run their processes. These systems are distributed among multiple plants distributed globally. The waste processing company has a comprehensive set of cyber defense products which included advanced 2nd generation firewalls, anti-virus suites, multiple intrusion detection software products, SIEM, 2nd generation endpoint security, machine learning and analytics software and more.

Deception “traps” were emulations of standard servers, workstations, switches, and various process control devices to include PLC controllers and more.

The security operations team received alerts in the network DMZ (a physical or logical subnetwork that bridges internal networks from untrusted networks such as the internet) that protected other internal infrastructure. These alerts came from several Traps camouflaged as workstations and servers deployed within the network. These alerts and subsequent investigation determined:

- The connection attempts absolutely came from a server in the DMZ.
- Investigation found this DMZ server was breached as a result of misconfiguration that allowed RDP connections.
- Investigation found this server was breached and controlled from several IP's which were connected to political hacktivists hostile to the plant.

## Case Study #5 – Power Plant

Our 5th, most compelling, and most very recent case study focuses on a power plant under attack earlier this year. This case study is particularly interesting as the defenders rapidly identified a major attack against the plant.

The power plant critical assets include a very large industrial control systems (ICS) infrastructure and the necessary supervisory control and data acquisition (SCADA) components which manage and run their processes. The plant is considered critical national infrastructure and subject to scrutiny and oversight by the responsible national security agency. Policies and procedures were in place so that the ICS infrastructure was to be isolated and “air gapped” from the standard information technology resources. This was considered to be a high security installation.

The CISO involved had decided to bring in deception technology, primarily to protect the standard information technology resources from ransomware attacks. The deception technology was also distributed within the ICS infrastructure. Deception “traps” were emulations of standard servers, workstations, switches, and various process control devices to include PLM controllers and more.

Almost immediately, the security operations team received several alerts that indicated a breach to the systems within the critical infrastructure plant operations. Their immediate investigation concluded:

- A device in the process control network was attempting to interact with the deception traps which were camouflaged as PLM controllers.
- This appeared as an active attempt to map out and understand the exact nature of each PLM controller within their network.
- This device was normally closed, but was supporting outside communications as a vendor performing maintenance failed to close the connection after maintenance. This opened the process control network to potential attackers.
- The information being gathered was exactly the type needed to disrupt plant activity and potentially cause great damage to ongoing plant operations.
- Major changes to security controls for the plant are under review and implementation. This attack remains under investigation.

## The Specific Threat to Industrial Control Systems (ICS/SCADA)

Industrial control systems are the center of the bullseye for nation states and terrorists that wish to cause great harm through the use of cyber-attacks. It seems obvious that a single cyber-attack could undermine the safety of millions of individuals and compromise their security and well-being.

To put the risk in context, as of August 2016, there are approximately 7,658 operational power plants in the United States.<sup>10</sup> Power plants include many types of generators which may include nuclear, hydro-electric, coal-burning and more. Each of these plants will likely have one or more generators, and some generators will use more than one type of fuel. Nuclear plants are by far the most potentially dangerous and sensitive. As of June 1, 2015, there are approximately 438 operational nuclear power plants around the world with another 67 under construction.<sup>11</sup> The United States has the largest number of plants at 99, followed by France with 58 and the United Kingdom at 16. All of these are now targets for ongoing directed cyber-attacks.

Other industries that are heavy users of industrial control systems generally have complex manufacturing processes or need to manage the distribution of chemical or gas flows via distributed pipelines. This includes aerospace, automotive, pharmaceutical, petrochemical and chemical manufacturing systems. These major manufacturers would suffer substantial losses if their assembly lines were shut down, or worse, damaged. Raw materials would be lost, employee time would be wasted, important customer commitments might be missed, and certainly, financial performance would be impacted. Those that deal with petrochemicals, chemicals and extensive pipeline distribution systems also have the same potential for a cyber-attack to compromise the physical safety of people over a broad geographic area.

These industrial control systems remain under a steady barrage of attacks. Homeland Security, the National Cybersecurity and Communications and Integration Center has put out a report for the ICS-CERT Year in Review for 2014.<sup>12</sup> This report provides information about the attacks that are reported and groups them by type of attack. They find attackers using tactics to include:

- Unauthorized access of internet-facing ICS/SCADA systems;
- Exploitation of zero-day vulnerabilities in control devices and software;
- Propagated malware infections within air-gapped control system networks;
- SQL injection via exploitation of web application vulnerabilities;
- Network scanning and probing;
- Lateral movement between network zones;
- Targeted spear-phishing<sup>13</sup> campaigns; and
- Strategic website compromises such as a watering hole<sup>14</sup> attack.

Attackers of industrial control systems tend to be political in nature, since they target operational capabilities within power plants, factories, and refineries, rather than financial account information. This sets the stage for one or more potentially major disasters in the future.

Take the energy industry, which includes the nation's energy grid. According to the Department of Homeland Security (DHS), approximately 59% of investigated cyber incidents from October 2012 to May 2013 occurred within the energy sector. Many of these attacks targeted energy companies to include power and utility companies. The nation's energy sector is composed of government and private entities working together. Certain government

---

<sup>10</sup> U.S. Energy Information Administration website - independent statistics and analysis

<sup>11</sup> <https://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm>

<sup>12</sup> [https://ics-cert.us-cert.gov/sites/default/files/documents/Year\\_in\\_Review\\_FY2014\\_Final.pdf](https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf)

<sup>13</sup> Spear phishing is a targeted email scam with the sole purpose of obtaining unauthorized access to sensitive data. In contrast, phishing scams use broad widely dispersed attacks. Spear phishing instead hones in on a specific group or organization.

<sup>14</sup> Water hole attacks, are engineered to anticipate the websites routinely used by targeted entity personnel. For example, if the primary target is an industrial control system within a power plant, they could attack and place malware clandestinely on a website that provides current news within the target industry.

agencies are responsible for protecting key infrastructure such as the energy grid, but the energy itself is actually generated by private industry.

“Out of all of the critical infrastructure sectors reporting attacks, the most vulnerable to attacks is the energy sector,” as Michael Gomez of KPMG, a tech firm that offers cybersecurity advice to the energy industry, as cited in The Hill newspaper. “Not any single sector within the energy industry is outside the scope of recent cyberattacks.”<sup>15</sup> All of the refineries, pipelines, petroleum distillation plants and the control room components that operate and manage the power grid are all digital and hence at greater risk for attack. Cyber attackers have the potential to inflict devastating attacks to our U.S. power grid that could easily cost \$1 trillion or more.<sup>16</sup>

The United States Computer Emergency Readiness Team maintains an industrial control systems cyber emergency response team (ICS-CERT). ICS-CERT frequently publishes reports for both government and industry and works closely with various government agencies to coordinate activity, spread information about attacks, better understand weaknesses and deficiencies and then suggest best practices to deal with these problems head-on.<sup>17</sup>

ICS-CERT has distributed alerts to provide timely notification concerning threats with a potential for impact on critical infrastructure computing networks. For example, ICS-CERT has disclosed that some models of one particular PLC (programmable logic controllers) used in industrial control systems contain multiple controllers that use embedded passwords to grant remote access. The manufacturer has produced a fix for this but this is just one of many hundreds of similar problems. The PLC in ICS networks are directly connected to sensors and actuators that provide data to control highly critical and important components. In many instances, the default passwords are hard-coded into the Ethernet controllers these systems use to command the devices so that administrators can gain remote access to the equipment.

This vulnerability is broadly distributed today. Shodan®, a search engine for the internet of things devices, can reveal the location of thousands of similar controllers where the terms “embedded password” are clearly visible.

Hard-coded passwords appear to be a common deficiency found in many industrial control systems. Critical industrial control systems operate the machinery within dams and floodgates, oil refineries, water and waste treatment plants. In all of these cases, unauthorized access would likely be considered a national security threat as it would affect the operation of these critical infrastructure components.

## Understanding the Attack Vectors

The cyber threats faced by corporate information technology networks also impact industrial control system infrastructure. A significant majority of industrial control system breaches start with their connection to servers and computing resources within the corporate information technology network.

Stuxnet, once again, is the harbinger for a new world of complex and innovative attack vectors. Stuxnet, as we know, was said to have exploited multiple zero-day vulnerabilities to launch a worm-based attack. USB memory sticks were used to manually spread the attack, jump the “air gap” and then enable the corruption of the centrifuge control operations. Stuxnet demonstrated a very detailed knowledge of how the PLC’s worked within the industrial control systems so as to sabotage them completely.

Our research has demonstrated what other studies have suggested. Key vulnerabilities are well known, visibly documented and the source of compromise many times. These include:

- Existing documented ICS controller and software vulnerability and exposure;
- Connections with the internal corporate networks to the ERP and/or financial systems;
- Use of unapproved software applications on ICS workstations and servers;
- Failure of “air gaps” through the use of USB drives to load infected maintenance software;
- Contractors that visit the installations may unknowingly bring infected devices;

---

<sup>15</sup> <http://thehill.com/policy/technology/209116-cyber-threats-put-energy-sector-on-red-alert>

<sup>16</sup> <http://www.utilitydive.com/news/lloyds-cyber-attack-on-us-power-grid-could-cost-1-trillion/402454/>

<sup>17</sup> <https://ics-cert.us-cert.gov/>



- Employees that violate policies with respect to workstations within the ICS network and then access infected websites or participate in other high-risk exposure; and,
- Social engineering that creates a compromise using one or more of the above attack vectors.

## Inside Industrial Control Systems

The industrial controls system market is quite large. In 2014 this market was estimated at \$58 billion and is expected to grow to \$81 billion by 2021.<sup>18</sup> Leading manufacturers that participate in this market include Siemens AG® (Germany), ABB Ltd® (Switzerland), Omron Corp® (Japan), Emerson Electric Co® (U.S.), Rockwell Automation, Inc.® (U.S.), Honeywell International, Inc.® (U.S.), Alstom SA® (France), General Electric Co (U.S.), Yokogawa Electric Corporation (Japan), Schneider Electric SE (France) and others.

Industrial control systems (ICSs) are deployed in the majority of major manufacturing facilities and utilities on a global basis. Within the United States, while some of these are operated by the Federal Government, it is estimated that over 90% are privately owned and operated.<sup>19</sup> ICS systems control a variety of industrial processes using networks and management software. Their control capabilities allow them to coordinate and manage remotely connected devices based upon sensor data, operational status and internal algorithms.

Industrial control system (ICS) is a very general term and refers to a broad category of control systems that include control and data acquisition (SCADA) systems, programmable logic controllers (PLC) and distributed control systems (DCS):

- SCADA generally refers to systems that span a large geography. Examples of this include gas pipelines, water systems, power systems and more. Programmable logic controllers and distributed control systems evolved within various industries, each with a more specialized purpose.
- PLC's are usually rack mountable computers used to automate industrial processes such as assembly lines and manufacturing processes. The automotive industry has traditionally been a heavy user of PLCs. Within a PLC software applications control and monitor analog and digital inputs (and outputs) which, in turn, provide a continuous stream of state information used to then adjust the ongoing processes.
- DCS control systems are used for broad-scale processes that need central control and monitoring. These systems often exist in large hierarchies that can span many thousands of sensors and control points.

Industrial Control Systems vendors are followed by many hundreds of documented vulnerabilities that are now freely available on the Internet from various sources. The vulnerabilities include backdoors, lack of authentication and encryption, and weak password storage schemes that would allow attackers to gain access to the systems and then compromise them. The security vulnerabilities make it possible to send inappropriate commands to the system components in order to stop them, to distort readings from sensors connected to them, and to interfere with specific critical processes controlled by them, such as the opening and closing of valves, actuators, relays and servos.

Industry common wisdom suggests that ICS networks are usually separate from corporate information technology networks. Based upon TrapX Labs investigation, this conclusion appears to be false. Data from the ICS networks is required within corporate networks so interconnections, a constant source of vulnerability, exist. It is very typical to have connections between the ERP application on the corporate network and the ICS networks. "In conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks and in some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment" per the May 2011 Testimony of National Cybersecurity and Communications Integration Center Director Sean McGurk.<sup>20</sup>

<sup>18</sup> <http://www.transparencymarketresearch.com/pressrelease/industrial-controls-market.htm>

<sup>19</sup> <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>

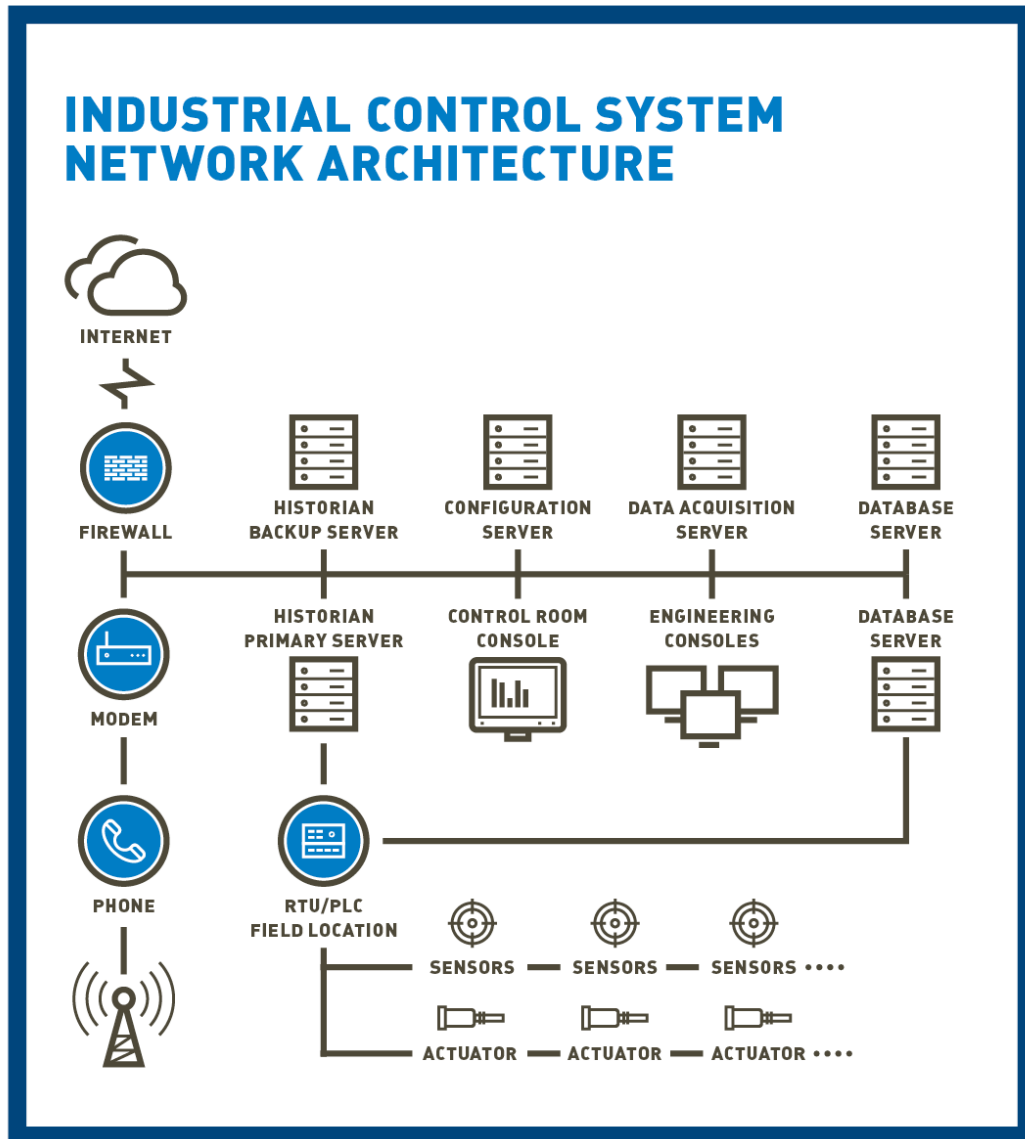
<sup>20</sup> <http://www.dhs.gov/news/2011/05/26/written-testimony-nppd-house-oversight-and-government-reform-subcommittee-national>



ICS systems are also much harder to maintain than traditional corporate networks. They may be difficult to access and often operate in more extreme environmental conditions. They may have operating systems that are old and out-of-date, are missing updates or have other known deficiencies. Installed cyber-security software may be inadequate as many of the ICS components cannot be scanned or monitored easily. Updates cannot be done via a network so the manual process of delivering updates for the cyber-security software is cumbersome, slow and also a source of malware introduction. Finally, they are so complex that often software updates are withheld because the managers fear the introduction of problems that could halt ongoing operations. Many managers consider these installations “turnkey” and “purpose built” and, if possible, would like to avoid any software updates at all unless absolutely required to maintain ongoing operations.

### Industrial Control System Architecture

ICS components include processors that provide for sensors (which understand the state of various components, measurements) and actuators (which can respond to changes in state to affect operations). The historian servers record the data from the production components and network which allow this data to be utilized by the corporate network financial systems and ERP systems. A large distributed architecture can be represented this way:



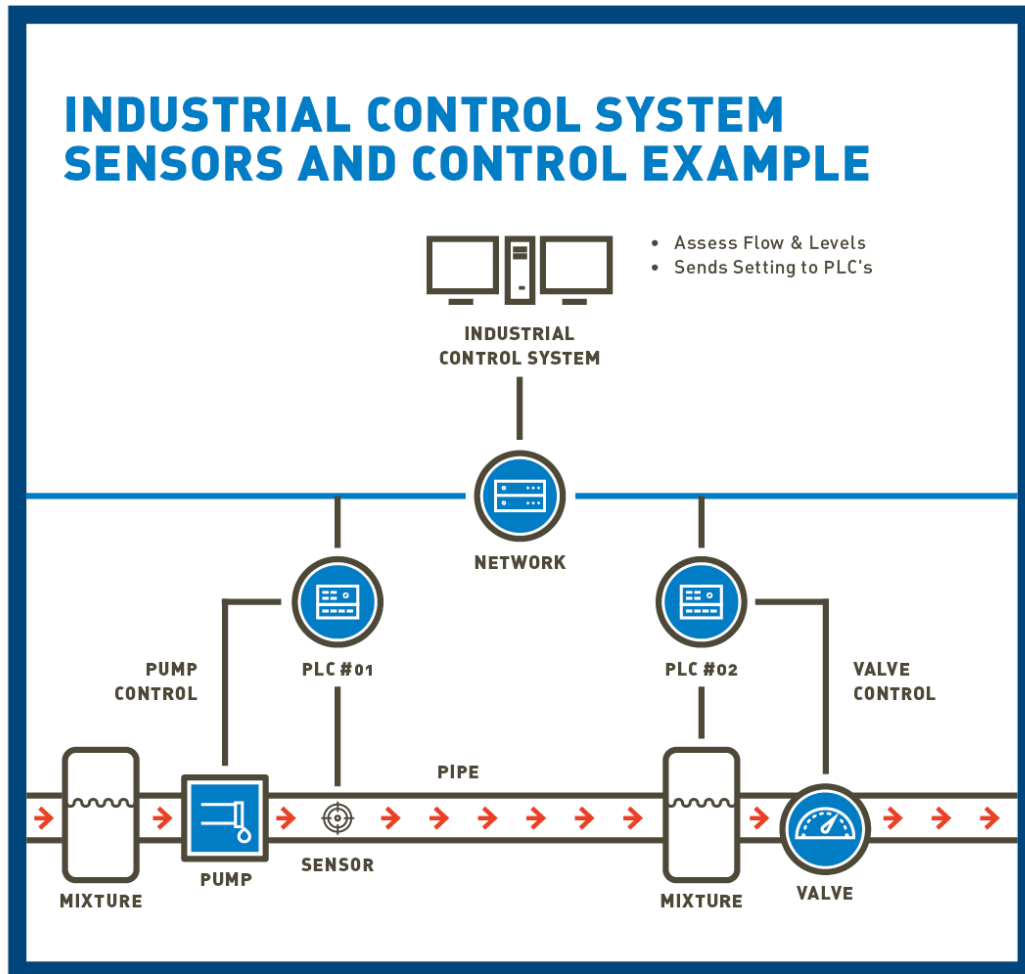
Copyright 2015 TrapX Security, Inc.

**Figure 1 – Industrial Control System Network Architecture**

## Industrial Control Systems Operations

Here, in Figure 2, we illustrate an example of how the industrial control system works at a detailed level. You can see the direct link between computer driven controls, and mechanical devices such as valves, servos and switches. It is easy to understand how ICS process management activity can be disturbed by an attacker which would rapidly result in cessation of operations.

In Figure 2, you can see PLC #01 monitoring flow by gathering measurements from an embedded sensor. This sensor is embedded in the pipe coming from a primary storage vessel containing volatile chemicals. The flow is then modulated and controlled by the pump control which PLC #01 also controls. This flow continues into a secondary storage vessel. Based upon various measurements within the storage vessel, the valve may be directed to open so that portions of the volatile chemical mixture flow through the pipe into the next manufacturing process.



Copyright 2015 TrapX Security, Inc.

**Figure 2 – Industrial Control System Sensors and Control Example**

A typical plant or utility has hundreds to sometimes thousands of complex interrelated processes all depending on the correct, timely and accurate operation of the ICS components. Now you can understand the risk associated with an attack and the potential for extreme damage and physical harm. If one of these actuators was set to a wrong reading, as in the Stuxnet attack, the potential for damage and injury may be very high.

## Evolution of Functionality Increases Vulnerability to Attack

Over time, two big evolutionary changes resulted in a convergence of functionality which has made these different ICS platforms look more alike, and, substantially increased the vulnerability of these systems to sophisticated cyber attackers and some of the attacks documented in our case studies.

The first evolutionary change over time was the replacement of hard-wired hardware boards, with purpose resident software, to general purpose microprocessor utilizing more general libraries of digital to analog control software. This, in turn, continued to the use of full commercial operating systems like Microsoft® XP utilizing standard networking protocols. Today many of these systems still use embedded versions of Windows® XP, Windows 7, Windows 2000. Existing systems retain these older operating systems and often the system managers have no clear roadmap for a more current and secure operating system.

The second major change was the evolution from proprietary systems that hardwired devices together using vendor specific protocols to a highly interoperable environment using standard Ethernet and TCP-IP protocols. These systems often have external access points to the standard corporate information technology networks from within the firewall. Security designers have unfortunately depended on the integrity of firewalls and signature scanning software to protect these networks and this has not been enough.

The legacy of this technology today is the continued production use of obsolete and highly vulnerable Microsoft operating systems such as Windows XP, Windows 7 and Windows 2000. Many of these control systems have even older operating systems and lifetimes in excess of twenty years.<sup>21</sup> These operating systems remain wide open to the most common cyber-attacks. They are no longer updated or patched and provide an open pivot point for the successful attacker. This reduction in isolation has resulted in an increase in the nature and type of potential threats to operations. New wireless devices increase the risk from attackers that may be in close proximity to the network and devices.

Malware propagating through the corporate network is often found and eliminated. However, the same malware once spread into the ICS network, has a greater chance of not being found, undetected by endpoint security or antivirus (signature based) cyber defense, and comfortably located in one of the processors running the older Microsoft operating systems.

## Industrial Control System Protocols

ICS networks make use of many proprietary protocols that have known vulnerabilities. Each ICS protocol presents specific additional opportunities for attacker breach.

MODBUS is an application-layer supervisory communication protocol between devices across buses or networks. It provides almost no security against unauthorized commands or data integrity. An attacker with connectivity and the ability to emulate the MODBUS protocol can support several different attack vectors that can shut down ICS operations.

DNP3 (Distributed Network Protocol) is a communication protocol used primarily between components in electric utilities. DNP3 does not support encryption or basic authentication. Common DNP3 attacks can get in the middle of

---

<sup>21</sup> <http://www.controleng.com/single-article/are-microsoft-technologies-still-best-for-process-control-systems/eba959613f8b0a8c24ffde31227d768f.html> Systems using old VAX/VMS technology from Digital Equipment Corporation are only today being replaced.

communications to change, distort or stop DNP3 messages. Once again, with potentially large impact to ongoing ICS operation.

Beyond MODBUS and DNP3 there is a multitude of additional vendor specific protocols being used in ICS systems throughout the world.<sup>22</sup> As noted earlier, once a system is in production there is strong resistance to making changes or upgrading software. The most common tactic for cyber protection is to “air gap” the network and attempt to physically isolate it from cyber threats and other interference. As we have seen in the case of Stuxnet, and as we shall see in our case studies, these attempts to protect networks by using “air gaps” are still not enough.

---

<sup>22</sup> [https://en.wikipedia.org/wiki/List\\_of\\_automation\\_protocols](https://en.wikipedia.org/wiki/List_of_automation_protocols)

## Recreating an Attack – The Aurora Vulnerability Attack Vector

Beyond the case studies we present in this report, the TrapX Labs team felt that a review of the Project Aurora vulnerability attack vector would better serve as a reminder of the existing, ongoing and very basic risks within the industrial control system environment.

In 2007 the Idaho National Laboratory very quietly ran the Aurora Generator Test to demonstrate how a cyber-attack could physically damage the electric grid. The experiment was initially designated as unclassified and but for “official use only.” On September 27, 2007, CNN published an article based on the information and video DHS released to them. Later, on July 3, 2014, the Department of Homeland Security released many of the documents related to the Aurora Vulnerability experiment as part of a FOIA request.

The experiment used a computer software program to rapidly open and close a diesel generator's circuit breakers. This was done out of phase from the rest of the grid such that it caused shock to the system and ultimately caused an explosion and extreme damage to the generator. This attack vector is referred to as the Aurora Vulnerability.

The Aurora Vulnerability attack vector is especially dangerous because most of the power grid still supports protocols that were designed without much security in their basic architecture. More explicitly, they often don't support authentication, the lack of which enables any attacker to communicate with the device, control it and then use the Aurora Vulnerability attack vector to destroy it.

The failure of one generator could cause broad spread outages. The potential for cascading failure of the entire power grid is also possible such as happened in the 2003 and 2012 blackouts in the northeastern United States.<sup>23</sup> In the normal course of service, there may be no repercussions to taking one of the generators out of service for an extended period of time. Often these power generators are custom built for each installation such that it might take months or even more than a year to repair it or replace it. During that window, additional attacks and failures could potentially lead to a cascading failure.

Researchers acquired a 2.25 MW generator and connected it to the test substation directly. In order to damage the generator, the researchers used a carefully constructed cyber-attack to open and close the breakers out of sync. Each time the breakers were actuated and closed, the powerful torque from the synchronization caused the generator to shake itself apart. This eventually caused components from the generator to come loose and fly off. Some parts of the generator landed as far as 80 feet away from the generator. This also generated considerable noise and smoke consistent with a series of explosions.

The generator was destroyed in approximately three minutes. The researchers assessed damage from each phase of the attack and hence the attack moved slower than it would have in a real situation. A real cyber-attack would have destroyed the generator much faster.

---

<sup>23</sup> <http://wimnet.ee.columbia.edu/wp-content/uploads/2014/01/CU-EE-2014-01-20.pdf>



**Image 1 - Destruction of a 2.25 Megawatt Generator by Cyber-Attack**

You can download the video file in .wmv format from the government FOIA response here:

<https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/#file-23387>

This shows the generator shaking itself apart, smoking and suffering severe damage and trauma. You can also watch it in this article on CNN where the video may still be embedded:

<http://www.cnn.com/2007/US/09/26/power.at.risk/>



## Conclusions

The manufacturing sector and the industrial control systems which they use remain highly vulnerable to advanced cyber attackers. Historically there has been a balance between what was possible in documented known exploits and the expertise required to truly use those vulnerabilities. The cognoscenti of the cyber defense world, industrial control systems and government will tell you that the planning of a major attack requires that the knowledge of the traditional cyber attacker be coupled with expertise in specific industrial control system components and software systems. Even with that expertise, to plan and deliver a debilitating attack, the attacker must have knowledge of the specific industrial control system vendor components used, and as much detail as possible on the process control flow. The more the attackers know about the process control flow, the more they can plan an effective attack.

Aurora showed that damaging attacks can be generated perhaps with less detailed domain knowledge of the installation. Penetration by targeted malware can still cause considerable damage with more generalized attack strategies such as, “open every valve.”

In the final analysis, it is clear to our team that Stuxnet is the change agent that has enabled very new thinking in terms of what is possible. Nation states and other bad actors are researching vulnerabilities within major manufacturer facilities, the power grid and other key infrastructure. They may not be leveraging the detailed knowledge of these vulnerabilities now, but we feel it is possible they are researching and cataloging key information and perhaps quietly placing the footprints within targeted ICS networks to leverage this knowledge at a later time.

Moshe Ben Simon, Founder and Vice President, TrapX Security

At a more tactical level, we are concerned with day-to-day operations. We see several themes visible in our security operations center and our customer base:

- There are very few true “air gapped” systems. Most ICS systems seem to have more than one connection to the corporate network infrastructure.
- Management for ICS networks has believed that the firewalls on corporate networks serve to keep malware out of the enterprise networks and therefore out of the ICS networks. Corporate networks and the commercial defense in depth suites that currently defend them are easily compromised. This has become very evident in the past few years. Defense in depth suites are failing at an increasing rate to protect standard information technology infrastructure, let alone critical and potentially physically dangerous industrial control systems.
- “Air gaps” are better than not but do not guarantee the safety of the ICS network. Data from our security operations center shows that these strategies fail. This is a common theme visible within the installations reviewed by our security operations team and TrapX Labs personnel. Social engineering targeted towards your personnel or those of your vendors and suppliers can jump the “air gap.” All it takes is one successful compromise to bring down or damage your ICS network.
- Policies do not guarantee safe operation either. Employees, well intended or not, do not always follow corporate guidance to protect the ICS network.
- Inside attacks by rogue employees can be most unpredictable. In one of our case studies, the rogue employee was a manager within the information technology team.
- Thousands of internet industrial control system which represent viable targets for attackers are exposed to the internet directly. The internet of things (IoT) search engine SHODAN, and other data mining techniques make it relatively easy to assemble targets by individual manufacturer, type of facility, embedded passwords and more.
- The continued use of embedded or default passwords is a huge problem in the legacy installed base of ICS components. Many internet controllers within PLCs are still in operation with embedded passwords and

represent yet another easy target of choice for potential attackers. Once again, you can search SHODAN to find these directly.

- The vulnerabilities and zero-days associated with industrial control systems constitute a very long list. Respectfully submitted, some manufacturers are slower to remediate issues than they would like and from time to time may have trouble keeping up. They did not plan to fund cyber security experts to go to market in the control systems space. Yet now they have deep security operations teams discovering vulnerabilities and issuing fixes on a 24 x 7 basis.
- In the past few years, some manufacturers have often chosen instead to release a newer product that eliminates the major known vulnerabilities. In contrast, the installed base of older revision components left within the ICS networks, either without known “fixes” installed because the customer does not want to make the investment, or just without available “fixes” because the manufacturer has moved forward, is quite large. Consider these highly vulnerable ICS systems stay in place for 5 to 10 years. A much longer systems life than for traditional information technology assets.
- Old standard operating systems such as Windows 7, Windows XP, and Windows 2000 are widely distributed within the global ICS production base. These operating systems are out of date and there are no current fixes for many known attack vectors. They are targets of choice for attackers.
- Specialized operating systems in use with ICS (e.g., QNX, OSE, and VxWorks) have similar problems to those faced Windows but perhaps are at lower risk by the supposition, that at least for the short term, attackers with detailed knowledge of these operating systems are relatively few in number.
- Many ICS network administrators try to deploy and run components of modern defense in depth suites of software. Depending on the age of the ICS systems, and the original manufacturers, we find there are often nodes within the ICS network that run target operating systems, but that does not work in conjunction with the deployment of standard cyber defense. For various reasons, some of these endpoints and servers cannot be scanned.
- Maintenance of cyber defense can be much more difficult and time-consuming in ICS networks. Consider some ICS networks are in inhospitable environments (temperature, location, physical packaging, exposed to the environment, etc.). Without external network connections updates to even anti-virus software must be walked in and manually installed. Yet another opportunity for an attack to penetrate the infrastructure using a DVD or USB device.

So, are core industrial control systems at increasing and greater risk?

We believe the answer is absolutely YES for both public utilities and major commercial manufacturing. Standard and out-of-date operating systems and the broad-scale deployment of networks have opened up these systems to more risk than ever. Attackers are motivated and nation states are investing far more dollars in understanding what vulnerabilities exist and how to best exploit them. Socially engineered “air gap” breaches and spear fishing attacks exploit human nature to grant the attacker access.

Finally, standard defense-in-depth cyber-defense, if it can be deployed completely and correctly within critical ICS networks, is not working much of the time. Attackers will penetrate the ICS networks. Your strategy must now assume the attackers will obtain network and system access, and instead focus on how to find them quickly (reduce the time to breach detection), successfully break the attack and then recover full operations of the ISC network quickly and effectively.

## Recommendations

Deploy a broad cyber defense strategy within your ICS networks. Administer it separately. Consider automation such to support security updates via automation using file distribution servers. Consider new techniques such as deception technology that deploy on the assumption that your network perimeter will be breached so that you can quickly detect successful attackers, break their attacks, and then promptly restore operations within your facilities.

**Yuval Malachi, Founder and Vice President, TrapX Security**

TrapX Labs believes there are concrete steps that can be taken to further minimize risk and ensure the integrity of operations within your facility. These include:

- Review your vendors and systems. Determine if you are upgrading all of your ICS components on a regular basis to manufacturer's specifications for cyber defense. Insure that all patches and updates are applied promptly. Senior management understanding and oversight of the procedures for this update are required.
- In the event that patches and updates are not available, such as in the case of ICS networks using older Microsoft operating systems, plan to migrate to new technology. It is a necessary cost of business to do so.
- Implement "air gaps" wherever possible to reduce your risk profile. Minimize to the greatest extent possible the use of USB memory sticks and DVD drives.
- Assume at some point this "air gap" will be breached and plan your response accordingly. New best practices using new technology such as deception can help even protect isolated networks by detecting attackers that have jumped the "air gap."
- Engage a tiger team to review software updates once a quarter prior to installation in the production network. Make sure your team has tools to read and analyze both static and dynamic memory dumps as a routine course-of-business process.
- Critical installations, such as a nuclear plant, fall under U.S. Nuclear Energy Institute (NEI) NEI-08-09 guidance. Rule NRC-5.71 eliminates all interactive remote user access to nuclear generator control system networks. All ICS networks should consider the benefits of using the NEI-08-09 guidance where applicable to protect non-nuclear infrastructure.
- Isolate ICS systems from corporate information technology networks. Do not allow any direct connections between the two. That includes network connections, laptops, memory sticks - absolutely nothing.
- Implement policies that severely limit the use of the ICS networks for anything other than essential operations. Minimize accessibility to ICS workstations and monitors with external Internet browser access. Assume these policies will fail and plan accordingly.
- Minimize activity within ICS systems to only essential operations and "white list" the files required for operation of these systems. This can work in conjunction with "black list" technologies such as anti-virus software. Recognize that "white lists" can be researched and corrupted by an advanced persistent threat. Plan accordingly.
- Utilize products with "signed software" to minimize hidden attacks. Signing is a cryptographic technique that preserves the integrity of the executable software environment and makes it difficult to substitute or add files with malware.
- Research and eliminate all embedded passwords or default passwords in your production network. If these are outside of your control plan to choose new components as soon as possible. Wherever possible implement two-factor authentication.
- Develop a plan for comprehensive authentication to access every node and function within your networks. Utilize two factor authentication within your ICS networks to the greatest extent practical.

- Major facilities should hire at least two (2) independent trusted external security services vendors to do an annual security audit and comprehensive red-team penetration test. Listen carefully to them and follow their recommendations. Contrast their recommendations.
- Review plans for disaster recovery driven from a major cyber-attack. This should be part of your top level corporate or enterprise disaster planning. Consider rapid and detailed steps to newly provision damaged systems and restart operations.

## About TrapX Security

TrapX Security is a leader in deception based cyber security defense. Our solutions rapidly detect, analyze, and defend against zero day and advanced attacks in real time. DeceptionGrid® provides automated, highly accurate insight into malware and malicious activity unseen by other types of cyber defense. We create a proactive security posture, fundamentally changing the economics of cyber defense by shifting the cost to the attacker. The TrapX Security customer base includes Forbes Global 2000 commercial and government customers around the world in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries.

## Find Out More – Contact Us Now

TrapX Security, Inc., 1875 S. Grant St., Suite 570 San Mateo, CA 94402

+1-855-249-4453

[www.trapx.com](http://www.trapx.com)

For sales: [sales@trapx.com](mailto:sales@trapx.com)

For partners: [partners@trapx.com](mailto:partners@trapx.com)

For support: [support@trapx.com](mailto:support@trapx.com)

## Trademarks

TrapX, TrapX Security, DeceptionGrid and all logos are trademarks or registered trademarks of TrapX in the United States and in several other countries.

Other trademarks are the property of their respective owners.

© TrapX Software 2015. All Rights Reserved.