IBM Security

Security attacks on industrial control systems

How technology advances create risks for industrial organizations

Managed Security Services Research Report

IBM

Click here to start ▶

Contents

Executive overview

Those of us living in developed industrialized nations tend to take modern-day conveniences for granted. Take a typical end-of-workday scenario. You disembark from a train that arrived on schedule. You flip a light switch to illuminate your home. You turn on the tap and clean water flows freely. It all happens routinely, without a hiccup. Now imagine a world where the delivery of sustained services is interrupted. Suddenly there's no clean water. Electric power disappears. The effects of such failures can be disastrous, putting your personal safety and that of millions of others at immediate risk. That's why governments and private institutions all over the world are increasingly focused on the threat to industrial control systems.

About this report

This report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources including event data, activity, and trends sourced from tens of thousands of endpoints managed and monitored by IBM for Managed Security Services accounts around the globe.

Contents

Our post-industrial societies reinvent themselves every day. Advances in the delivery of power and water systems may go unnoticed by the consumer, but over the past 25 years big industry has gradually embraced the digital age in the cause of making their production environments much more stable and efficient. Programmable logic controllers (PLC) developed for control of industrial equipment and processes are now largely implemented across the globe and are used extensively in almost all industrial processes. In many ways that's good news, but it is bad news too. Chaos can result when these electronic systems are compromised, so they are highly prized targets for threat actors everywhere. Stories of sabotage are frequently headline news.

In this paper we look at the history of industrial control systems (ICS), the susceptibility of these systems to certain attacks, and how the systems can be defended.

Types of industrial control systems

An industrial control system (ICS) is a computer-based system that monitors and controls physical industrial processes.

SCADA (supervisory control and data acquisition) is a system operating with coded signals over communication channels to provide control of remote equipment, typically using one communication channel per remote station. SCADA is a type of ICS.

A distributed control system (DCS) is a control system for a process or plant, with control elements distributed throughout the system.

Evolution of SCADA architecture and attacks

Many threat vectors can be used to target a modern SCADA system. One is unauthorized access to the control software, whether by human access or through changes induced intentionally or accidentally by virus infections and other software threats residing on the control host machine. Another threat vector is packet access to the network segments hosting SCADA devices. In many cases the control protocol lacks any form of cryptographic security, allowing an attacker to control a SCADA device by sending commands over a network. SCADA users often assume that having a virtual private network (VPN) offers sufficient protection, unaware that security can be bypassed quite easily with physical access to SCADA-related network jacks and switches. Industrial control vendors suggest approaching SCADA security like data security, with a defense-in-depth strategy leveraging common IT practices.

Reviewing the evolution of SCADA architecture allows organizations to understand the current and past attack landscape (see Figure 1). Malware was not a threat to first-generation "monolithic" systems because they weren't connected to other systems; an attacker would have needed authorized physical access to tamper with them. Second–generation, "distributed" architecture took the once isolated SCADA system and distributed it across multiple stations connected via a LAN. During this period security was often an afterthought. Further complicating matters was the non-standardization of network protocols. Even a security-savvy system supervisor would have needed an understanding of the proprietary network protocols to determine proper configuration of the SCADA system. Lack of security awareness opened the door for SCADA malware. As an example, in 1982 an unknown Trojan program remotely inserted into SCADA system software caused a massive natural gas explosion along the Trans-Siberian pipeline.

SCADA users often assume—incorrectly—that a virtual private network (VPN) can offer sufficient protection for control systems.

Contents

Targeted malware attacks against SCADA systems grew with the third, networked generation of SCADA architecture, which allows the system to control devices that are separated geographically and attached to more than one local area network, called a process control network (PCN). In 1999, a Trojan program installed in the pipeline system of a Russian oil corporation disrupted the control of gas flows for several hours. In 2003, the Sobig virus infected a railroad company's computer system, shutting down signaling, dispatching and other systems and causing train delays. That same year, the infamous Slammer worm tried to slow down the network in a nuclear power station. In 2004 the Sasser worm targeted two airlines and one rail transportation company, delaying or cancelling flights and trains.

While opening a whole new world for industry, third-generation architecture also kept a backdoor open for dark-side entities. In 2009, the Conflicker Work grounded an airline's whole fleet. The same year, McAfee reported that a combination of social engineering and cyber attacks using Trojans, remote control software, and other malware targeted many big oil and gas companies.

While the adoption of the fourth generation of industrial technology—the Internet of Things (IoT)—allows organizations to significantly reduce cost and improve maintenance management, it also opens SCADA systems to new security risks. Since the discovery of Stuxnet, the susceptibility of SCADA to cyber attacks is getting more attention not only from researchers but also from attackers. In 2014, Havex and BlackEnergy began circulating as the new ICS threats on the block. Both take advantage of a Windows vulnerability and use command & control (C&C) channels to control SCADA systems. Most recently hackers attacked a German steel mill to prevent shutting down a blast furnace, causing damage reported as "massive." Such incidents point to a growing trend. According to one report, SCADA attacks increased by a factor of more than six between 2012 and 2014, a rise of 636 percent in just two years.

Disclosure of vulnerabilities targeting ICS systems, a large portion of them buffer overflow vulnerabilities, is also trending upward. Buffer overflow occurs when a program or process tries to store more data in temporary storage than it can hold. While many buffer overflow issues result in denial of service, some could allow remote code execution, thus enabling an attacker to completely take over the vulnerable process. In terms of industrial control systems, this means that an attacker could obtain full control of critical infrastructure.

Contents

IBM Security

ICS historical timeline

1982

Uncorroborated report of a Trojan program inserted into SCADA system software that caused a massive natural gas explosion along the Trans-Siberian pipeline in 1982.

2000

The Maroochy Shire sewage control system in Queensland Australia attacked by former contractor resulting in release of sewage. These attacks highlight the need to manage and promote the security and protection of critical infrastructure.

2003

First ICS controllers with embedded web server are developed.

January - The "Slammer" worm disabled the computerized safety monitoring system at the Davis-Besse nuclear power plant in Ohio. The worm entered the plant network via a contractor's infected computer connected via telephone dial-up directly to the plant network, thus bypassing the firewall.

August - The Blaster worm infected the communication system of a US railway company. The dispatching and signaling systems were affected and all passenger, freight traffic and morning commuter traffic in the Washington, DC area had to be stopped for about half a day.

December - The IT staff at a French chemical company noticed that the Advanced Process Controls (APC) servers were getting slower and slower. Investigators found Nachi (AKA Welchia) virus on 8 APCs (running Windows 2000) and disconnected these servers from the production network for 5 hours.

2004

DHS Control Systems security program managed by the Idaho National Laboratory implements cyber security test bed focused on critical infrastructure.

2005

North American Electric Reliability Corporation (NERC) establishes security requirements and measures for compliance and monitoring for ICS systems.

August - Zotob worm infects 13 US auto plants causing shutdowns and delays.

2006

March - First SANS SCADA Security Summit.

IBM

Contents

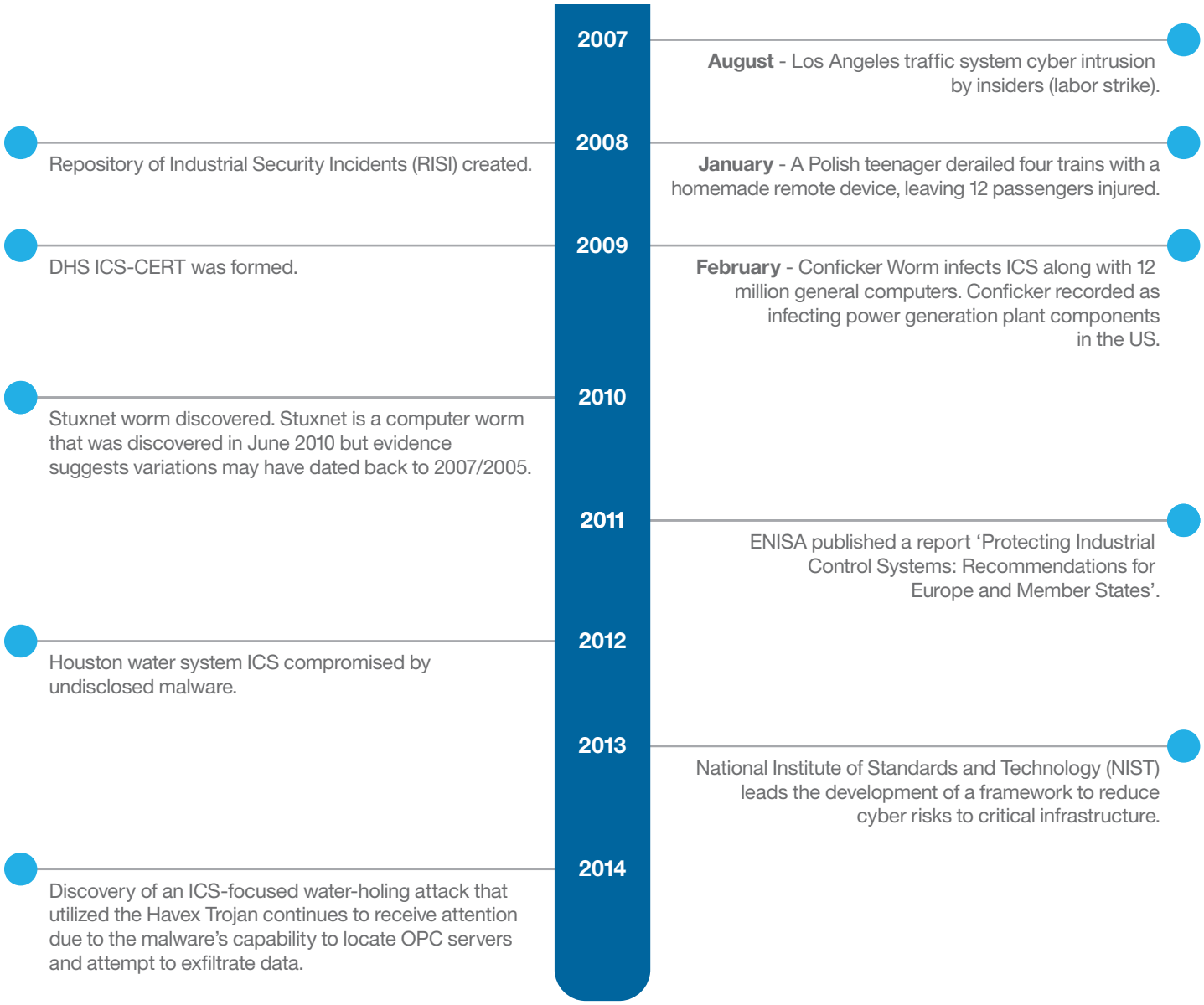

Figure 1. Critical attacks on ICS resources across industries

Contents

ICS attack statistics

As stated in a report from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT),[1] "The energy sector led all others again in 2014 with the most reported incidents…Also noteworthy in 2014 were the incidents reported by the Critical Manufacturing Sector, some of which were from control systems equipment manufacturers."

The ICS community is a target for sophisticated threat actors for a variety of reasons, including economic espionage and reconnaissance. Actor types identified in the ICS-CERT report included hacktivists, malicious insiders and criminals. In many cases there wasn't enough data to identify the threat actors.

Dell, the source of the 636 percent figure cited previously, reported that it saw worldwide SCADA attacks increase from 91,676 incidents in January 2012 to 163,228 in January 2013 and 675,186 in January 2014[2]. The Open-Source Vulnerability Database (OSVDB) shows that through the end of 2014, more than 85% of all ICS vulnerabilities have been disclosed since 2011, the year following the discovery of Stuxnet.

ICS attacks on the rise

IBM Managed Security Services (MSS) has been tracking ICS attacks. Figure 2 illustrates a major increase in ICS-based alerts over a three-year period ending August 30, 2015. IBM's figures align with those of other cyber security organizations.

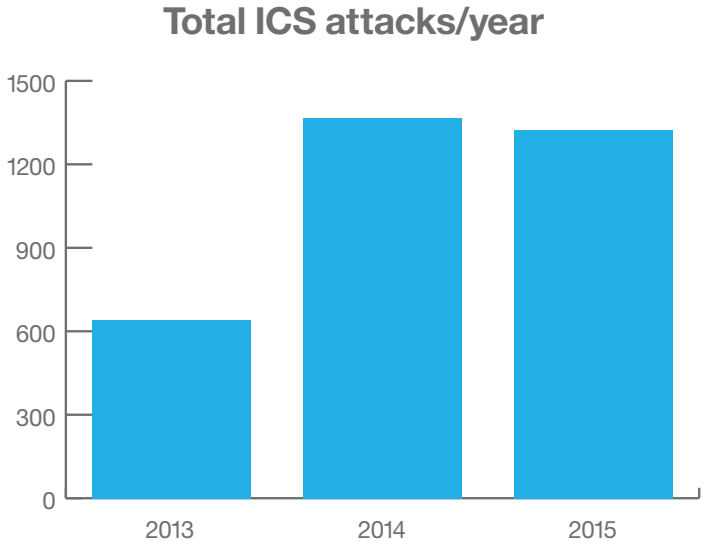

Figure 2. The number of ICS attacks tracked by IBM Managed Security Services from January 1 2013 to August 30 2015

Attack metrics

According to IBM MSS attack data, the United States leads all other countries by a large margin as the origination point of ICS-based attacks (see Figure 3). The data tells us nothing about the motives behind the attacks, but we know that hacktivist groups have been largely responsible.

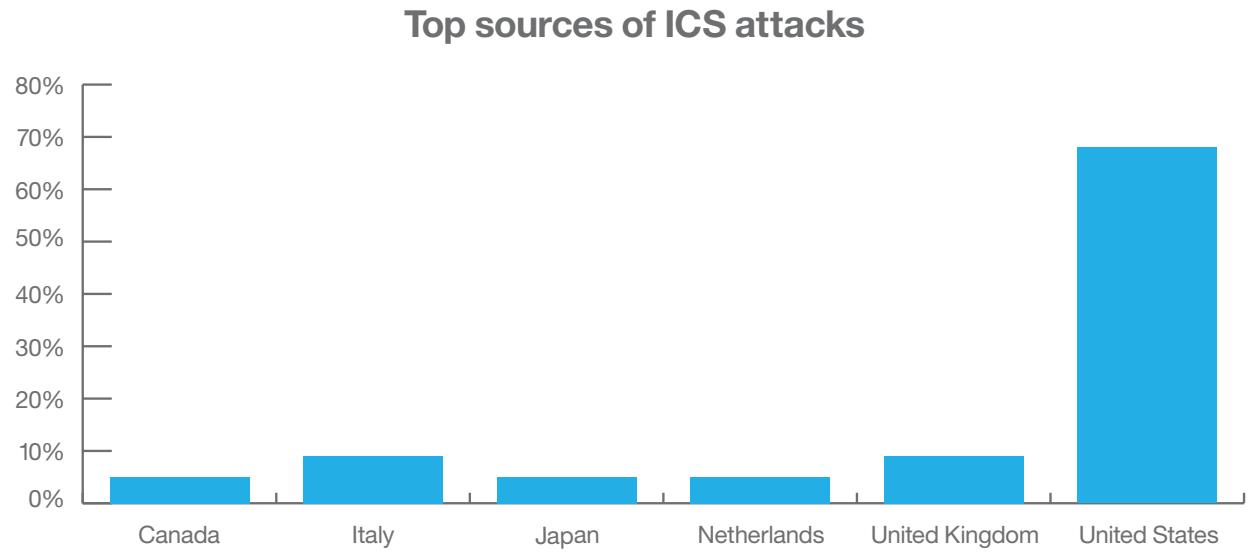

Figure 3. The source countries of ICS attacks, based on IBM Managed Security Services data collected January 1 to August 30 2015

Contents

A report issued by the Department of Homeland Security via the ICS-CERT[3], states that:

"[H]acktivist groups are evolving and have demonstrated improved malicious skills. They are acquiring and using specialized search engines to identify Internet-facing control systems, taking advantage of the growing arsenal of exploitation tools developed specifically for control systems. In addition, individuals from these groups have posted online requests for others to visit or access the identified device addresses.

"Asset owners should take these changes in threat landscape seriously and should not assume that their control systems are secure or that they are not operating with an Internet-accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet-facing devices, weak authentication methods and component vulnerabilities."

IBM MSS data shows that Canada, the US and the UK were attacked most frequently during the past year, followed closely by Israel, Hungary and Denmark (see Figure 4). A report from a major security firm[4] says that this is "due to the fact that SCADA systems are simply more common in these countries and also more likely to be part of networks connected to the Internet."

Asset owners should not assume that their control systems are secure or that they are not Internet accessible.

Contents

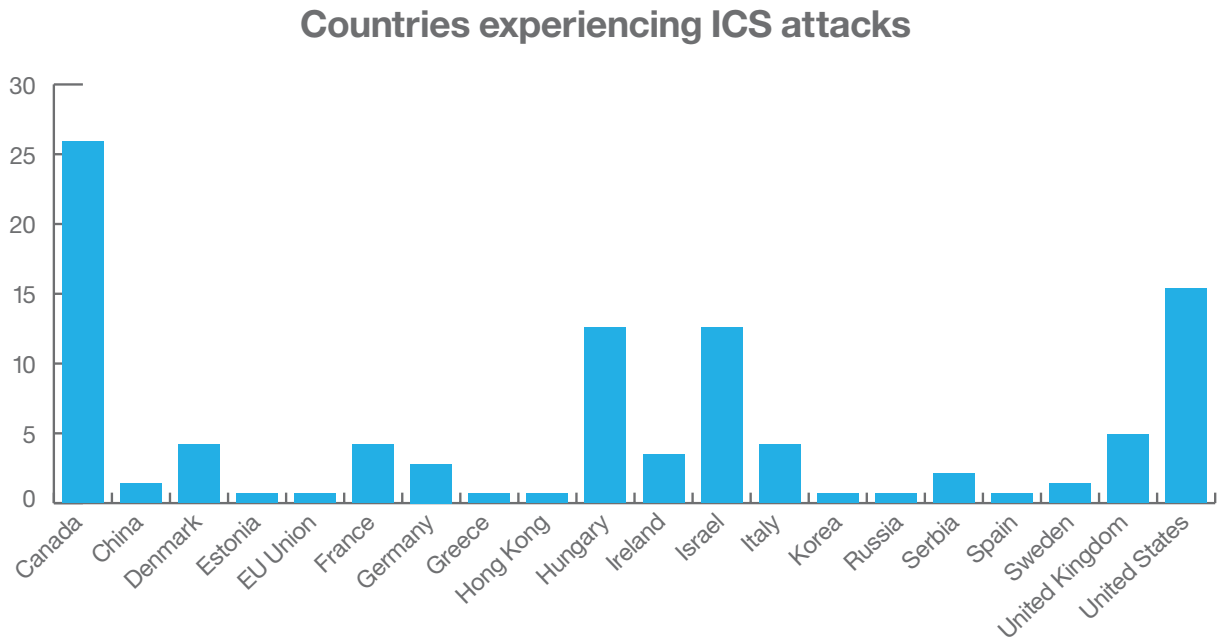

Figure 4. Countries experiencing ICS attacks, based on IBM Managed Security Services data collected January 1 to August 30 2015

Contents

Key SCADA attack methods

ICS software is often deployed on old equipment that would be difficult to replace without disrupting critical processes, with the result that installing patches and upgrades is often avoided despite the obvious security benefits. That makes ICS systems highly prized targets because they offer attackers an opportunity to wreak a lot of havoc once they've taken control. Below we look at the top attack vectors used against ICS systems.

Buffer overflows

According to a 2014 report by a major security firm[5], buffer overflow, which occurs when a program or process tries to store more data in temporary storage than it can hold, is the most widely used attack method against ICS systems, accounting for 25 percent of attacks[6].

Spear phishing

The threat vector represented by Stuxnet and similar types of malware introduced through the use of USB sticks has now been diminished by the standard practice of locking down USB ports. Currently, one of the main threats to ICS is also one of the most prominent attack vectors overall, spear phishing. An attacker simply does his social media homework on an employee of a large industrial company and baits the person to open an attachment, for example by sending an email that appears to be a Human Resources communication prompting the individual to review a benefit plan. Perhaps the attacker knows that the victim is a systems administrator with access to the target company's critical ICS systems.

Once the attachment has been executed, the damage is in motion and the attacker gains a foothold. Phishing is now the primary mode of injecting malware into an ICS. A comprehensive IBM MSS research report on the perils of phishing can be downloaded from the IBM website.

Contents

SQL injection

SQL injection remains one of the most potent attack vectors across multiple applications because there are so many entry points. There are four main types of SQL injection:

- First-order attack—the attacker enters a malicious string and causes the modified code to be executed immediately
- Second-order attack—the attacker injects persistent storage (such as a table) which is normally a trusted source, and the attack is carried out by a second activity
- Lateral injection—the attacker manipulates the function To Char() by changing environmental variables
- Blind injection—the attacker launches SQL injection attacks that don't require error messages to be returned and are more focused on vulnerable applications.

Input fields on web applications are major injection entry points. Search fields are also used to send injection attack strings. To thwart these attacks, expected characters need to be defined and anything outside of that range rejected. These are called "check constraints"—rules that define acceptable column values for row data within a table. They can validate the integrity of one or multiple columns, and you can also use multiple constraints within a single column. If the data being inserted or updated violates the check constraint, the database will not allow the operation.

Complex applications can have many entry points, making it very difficult for a developer to enforce rules. All possible forms of input must be tested to check whether the application sufficiently validates the data before using it. Although input validation and check constraints are vital components of a defense-in-depth strategy, they aren't infallible.

Using stored procedures is just as important. Stored procedures are a group of SQL statements that perform a particular task, with SQL code for a stored procedure defined and stored in the database itself, then called from the application. The benefits of using stored procedures are performance gains from precompiled execution, reduction in client/server traffic, and security controls enhanced by granting users permissions on the stored procedures instead of database tables.

Contents

Distributed denial of service (DDoS)

ICS systems require dedicated and separated communication channels and separated networks for inter-system communications. ICS system distributed denial of service (DDoS) attacks may remotely shut down the power at key sites, interrupting secured physical communication links by signal jamming surveillance cameras or even flight-control signals. A growing trend in historical incidents suggests that DDoS attacks against ICS will continue to rise.

A survey by the Center for Strategic and International Study (CSIS)[7] states that distributed DoS attacks were "particularly severe" in the energy/power and water/sewage sectors, where attacks were usually aimed at computer-based operational control systems like SCADA.

Access controls

Vulnerabilities exist in almost all off-the-shelf applications. That's the reality security professionals have to live and deal with daily. One of the most exploited entry points, however, is plain old access controls, so hardening ICS applications to prevent unauthorized access should always be an element in ICS deployments. Often attackers attempt brute-force entry to ICS networks by remotely leveraging default login credentials that can give them complete access to the ICS infrastructure.

Weak passwords can be an open invitation to attack. In April 2014, the ICS-CERT published a report about a large public utility that was successfully infiltrated primarily because of weak passwords. "ICS-CERT validated that the software used to administer the control system assets was accessible via Internet-facing hosts. The systems were configured with a remote access capability, utilizing a simple password mechanism; however, the authentication method was susceptible to compromise via standard brute forcing techniques."[8]

Contents

Types of popular ICS malware

Several popular pieces of malware have enjoyed success against ICS. Since Stuxnet was first observed, more and more ICS malware has been discovered and analyzed, mostly backdoor/Trojans targeting Windows and ICS software in an attempt to modify the ICS configuration file, gather information and control the entire system. Most of these types of malware try to compromise ICS systems by injecting themselves into the network through a phishing email or a drive-by download via a compromised website. Stuxnet is spread primarily by USB drive.

Hackers can find your ICS online

The ERIPP[9] and SHODAN[10] search engines can be leveraged to search for Internet-facing ICS devices and have made it easier than ever for attackers to identify potential targets. ICS-CERT has issued an advisory warning the ICS community of these tools[11].

Increasing interest in Internet-accessible ICS devices has been shown by a variety of threat actors, including hacktivist and anarchist groups notorious for publicly posting the IP addresses to various ICS systems. Their individual members post online requests for others to visit or access the identified device addresses.

ICS system owners are encouraged to query these search engines, using the vendor product, model and device version to determine if their IP address block is found. If system owners find ICS devices using these tools, they should remove them from direct or unsecured Internet access as soon as possible.

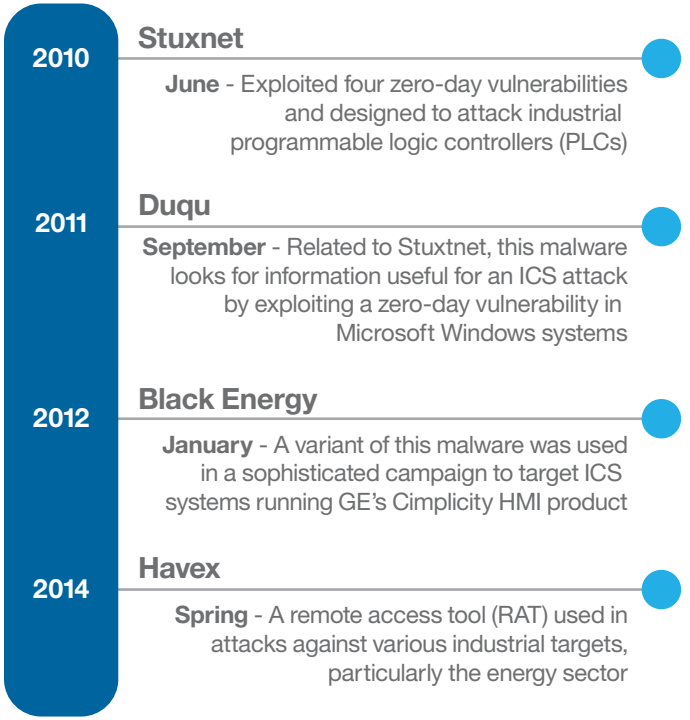

Figure 5. Common ICS malware and the dates of first observation

Finding the attackers looking for you

Later in this paper we discuss defense mechanisms you can use to harden your ICS systems. First, though, we note the availability of Conpot ICS/SCADA Honeypot, an open-source tool that, by mimicking a fully Internet-available ICS system, lets you capture the IP addresses of potential attackers for immediate blacklisting. The developer's website explains further:

"Conpot is a low interactive server side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend. By providing a range of common industrial control protocols we created the basics to build your own system, capable to emulate complex infrastructures to convince an adversary that he just found a huge industrial complex. To improve the deceptive capabilities, we also provided the possibility to server a custom human machine interface to increase the honeypots attack surface. The response times of the services can be artificially delayed to mimic the behavior of a system under constant load. Because we are providing complete stacks of the protocols, Conpot can be accessed with productive HMI's or extended with real hardware."[12] *[SIC]*

An open-source "honeypot" tool available online can mimic an ICS system, letting you capture the IP addresses of potential hackers.

Contents

Securing Your ICS resources

Define your ICS

Document the ICS network infrastructure and all components, applications, databases and connections critical to your ICS system. Perform a baseline security analysis for ongoing risk management and set corresponding security requirements.

Establish security roles, responsibilities and authorization levels for IT, management, administrative staff and third-party users.

Protect the perimeter

Block or remove any unnecessary or unauthorized networks that have access to your ICS systems, including unsecured disk drives, USB ports, and wireless connections or links to third-party networks.

Create a demilitarized zone (DMZ) to isolate ICS systems on protected segments, segregating them from the rest of the network. Allow no direct connections.

Maintain updated defenses

Develop and deploy defense-in-depth security solutions such as unified threat management and next-generation firewalls to protect against single-point-of-failure compromises.

Implement defenses including intrusion prevention, anti-malware, content filtering and application-intelligent firewalling. Be sure that your security services are continually updated with the latest signatures and patches.

Strengthen access controls

No outside entity should be able to reach your ICS network unless you invite them. Develop and deploy rules for access control and sharing of data, applications and resources. Define, deploy and monitor all the external secure access connections you need for business users, remote maintenance and third parties.

Develop and deploy policy-based access criteria that limit access privileges to authorized personnel only. Keep a current list of access accounts, check logs at established intervals, and frequently review and renew all credentials that have enhanced access. Employ access authentication at the gateway to prevent unauthorized backdoor access.

Harden remote access

The growing number of mobile, wireless and widely distributed networks presents a greater potential for unauthorized remote access. Secure all remote access over virtual private networks (VPNs) using point-to-point IPSec or clientless secure socket layer (SSL) technology.

Contents

Harden ICS features

Many ICS applications come with automated features, for example remote maintenance, that can create their own security hazards by introducing vulnerabilities for unauthorized access or intrusion attacks. Disable all features that aren't required. Team with your ICS vendor to identify which features can be disabled safely without violating support agreements, interrupting service or causing downtime.

Monitor logs for incidents

Develop and deploy monitoring and logging solutions for all ICS critical applications and infrastructure. Record incidents and assess alerts concerning the ICS system status. Use proactive measures to prevent attacks and avoid service interruptions.

Third-party solutions offering real-time display of all network traffic within ICS applications are widely available. They enable faster response to threats.

Change control and configuration management

Manage and document all configuration changes and back them up frequently to limit disruption and delays in case of ICS restarts.

Regular audits

Conduct a complete system integrity check every three to six months. Check the event logs for incidents to confirm that technological safeguards documentation, procedures and access controls are current and maintained.

Periodically assess audit results and correct any anomalies to keep your security posture at a high level.

Recovery preparedness

ICS systems are high-profile targets. They need to be backed up regularly and capable of quick recovery should an adversary take them offline. Develop and deploy contingency processes and procedures to ensure business continuity and disaster recovery for ICS critical systems.

Intrusion detection

Intrusion detection and prevention system (IDPS) signatures exist across multiple vendors. Although IDPS is not a one-stop system for preventing ICS system attacks, this technology is necessary in your network environment to help defend against network layer and application layer attacks. A full list of vendor signatures is available for download as a separate document[13].

Contents

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud and mobile. Our Critical Infrastructure Security Services provide expert consultants who can help you deploy the National Institute of Standards and Technology (NIST) Cybersecurity Framework to protect your critical infrastructure. We can assess your industrial controls against a security baseline, recommend improvements and develop a plan to help enhance your security program. IBM Security Strategy and Planning consultants can help you define a strategy and develop an IT security plan to better manage risk across your organization. IBM Identity and Access Management Services help you strengthen protection of your ICS resources against unauthorized access. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Contents

About the author

David McMillen, Senior Threat Researcher, IBM Managed Security Services. David brings more than 25 years of network security knowledge to IBM. David began his career at IBM over 15 years ago as a member of the core team that created the IBM Emergency Response Service, which eventually grew and evolved into IBM Internet Security Systems.

As an industry-recognized security expert and thought leader, David has a rich background in IT security. He thrives on identifying threats and developing methods of solving complex problems. His specialties are intrusion detection and prevention, ethical hacking, forensics, and analysis of malware and advanced threats. As a member of the IBM Managed Security Services Threat Research Team, David takes the intelligence he has gathered and quickly produces tangible remedies that can be implemented within a customer's network on IBM's own proprietary threat detection engines.

David became interested in security in the 1980s, when he owned and operated one of the first companies to offer penetration and vulnerability testing. As the Internet's footprint grew, it became clear to him that there was a new challenge on the horizon: protecting data. David next worked with IBM Business Partner WheelGroup (later acquired by Cisco), where he helped develop the NetRanger IDS intrusion detection system and NetSonar, a vulnerability scanner. David also assisted with the development of the very first IBM intrusion detection system, BillyGoat. David has subsequently developed several other security-based methods and systems that have been patented by IBM.

Contributor

Bo Li, Threat Researcher, IBM Managed Security Services

Contents

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

For more information on security services, visit:
ibm.com/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

[1] https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

[2] https://threatpost.com/dell-threat-report-claims-100-percent-increase-in-scada-attacks/112241

[3] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-046-01A

[4] http://www.businesswire.com/news/home/20150413005064/en/Dell-Annual-Threat-Report-Sheds-Light-Emerging#.Vehhjk3bLs1

[5] https://threatpost.com/dell-threat-report-claims-100-percent-increase-in-scada-attacks/112241

[6] http://www.hstoday.us/single-article/cyber-attacks-against-scada-systems-doubled-in-2014-says-dell-threat-report/ae81a11c6c44f731bfd5ff8ab6f26c88.html

[7] http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf

[8] https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

[9] http://beta.eripp.com/

[10] http://www.shodanhq.com/browse/tag/scada

[11] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-046-01A

[12] http://www.conpot.org/

[13] https://portal.mss.iss.net/mss/html/en_US/support_resources/documents/ICS_SCADA_signatures_supplemental.xls

Contents

IBM Security

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2015

IBM

SEL03046-USEN-00