ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT Incident Response Summary Report

2009–2011

OVERVIEW

The Department of Homeland Security (DHS) Control Systems Security Program manages and operates the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to provide focused operational capabilities for defense of control system environments against emerging cyber threats.

To accomplish this mission, ICS-CERT

- responds to and analyzes control systems related incidents,
- conducts vulnerability and malware analysis,
- provides onsite support for incident response and forensic analysis,
- provides situational awareness in the form of actionable intelligence,
- coordinates the responsible disclosure of vulnerabilities/mitigations, and
- shares and coordinates vulnerability information and threat analysis through information products and alerts.[a]

This report provides a summary of cyber incidents, onsite deployments, and associated findings from the time ICS-CERT was established in 2009 through the end of 2011. The report is divided into three main sections:

1. The first section gives a summary of incident reports and outlines major highlights for each year. Statistics are given for incident response support as well as onsite deployments. Typical incident response support consists of analysis performed in the Advanced Analytics Lab (AAL) on digital media, malware, log files, and other artifacts. Companies request analysis support from ICS-CERT to help determine the extent of the compromise and gather information about cyber attacks including the adversary's techniques and tactics. This information helps asset owners evaluate their security posture and take measures to strengthen their control systems and network security.
2. The second section examines the onsite response efforts in detail and gives a summary of each deployment. At the request of a company and when appropriate, ICS-CERT can deploy an onsite incident response team to help triage a cyber incident affecting a critical infrastructure owner/operators with the purpose of identifying threat vectors, collecting data for analysis, assisting with immediate mitigation efforts, providing cybersecurity threat briefings, and identifying future defense strategies.

a. See www.ics-cert.org for a listing of publicly available alerts, advisories, monthly monitors, recommended practices, and other resources.

3. The third section presents common findings from onsite vulnerability assessments and discusses security gaps that asset owners should address to improve the secure posture of their systems.

PROTECTING INFORMATION

Organizations submitting information to DHS regarding cyber incidents can request that their information be designated as Protected Critical Infrastructure Information (PCII) under the Critical Infrastructure Information Act (the CII Act) of 2002. Under the CII Act, information designated as PCII is protected from disclosure through a Freedom of Information Act request or through a request under a similar state, tribal, or territorial disclosure law and is protected from regulatory uses. In addition, the identity of the submitting organization is protected from disclosure to the public. ICS-CERT's practice is to use cover names for organizations it assists (such as "Energy 2" or "Transportation 3") to obfuscate their actual names.

SECTION 1: INCIDENT RESPONSE SUMMARY

Reviewing all incidents reported to and correlated by ICS-CERT from 2009[b] through 2011 provides context for the industrial control system (ICS) threat landscape during this period. Figure 1 compares all 3 years and shows the growth in reported and identified incidents impacting organizations that own and operate control systems associated with critical infrastructure.

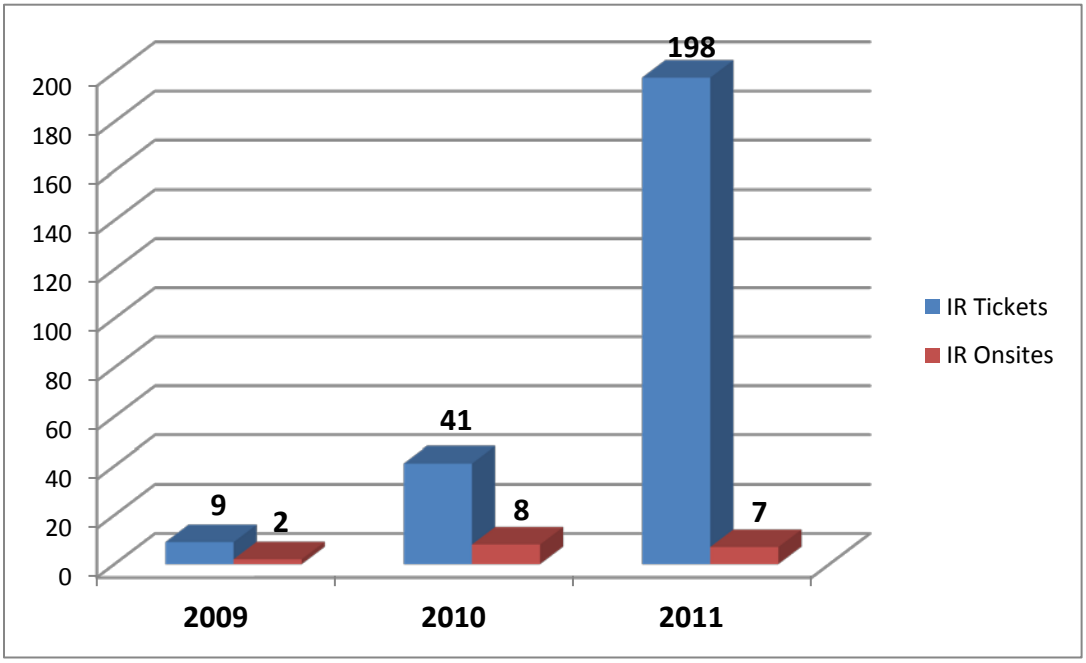

Figure 1. ICS-CERT incident response trends data.

b. ICS-CERT was formally inaugurated on November 1, 2009.

The following sections summarize the incidents reported to ICS-CERT for each year, including incident highlights, onsite deployment services, and analysis activities conducted by the team.

2009

REPORTED INCIDENTS

In 2009, ICS-CERT's inaugural year, nine incident reports were received, four were confirmed as actual incidents. Of those, two resulted in the deployment of onsite response teams. An additional two incidents involved remote analysis by the AAL to identify the threat and recommend mitigation strategies. The chart in Figure 2 illustrates the breakout of incidents by sector.

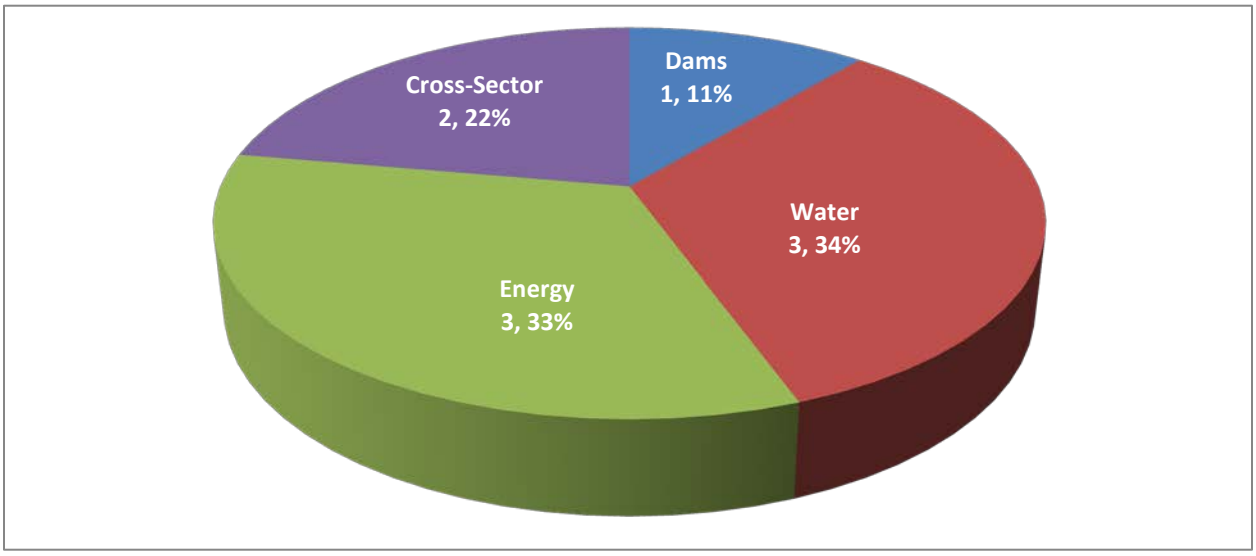

Figure 2. Incident reports by sector (2009).

2010

REPORTED INCIDENTS

Forty-one incident reports were received in 2010. Of the 41, eight resulted in the deployment of onsite response teams. An additional seven incidents involved remote analysis by the AAL. Figure 3 illustrates the breakout of incidents by sector.

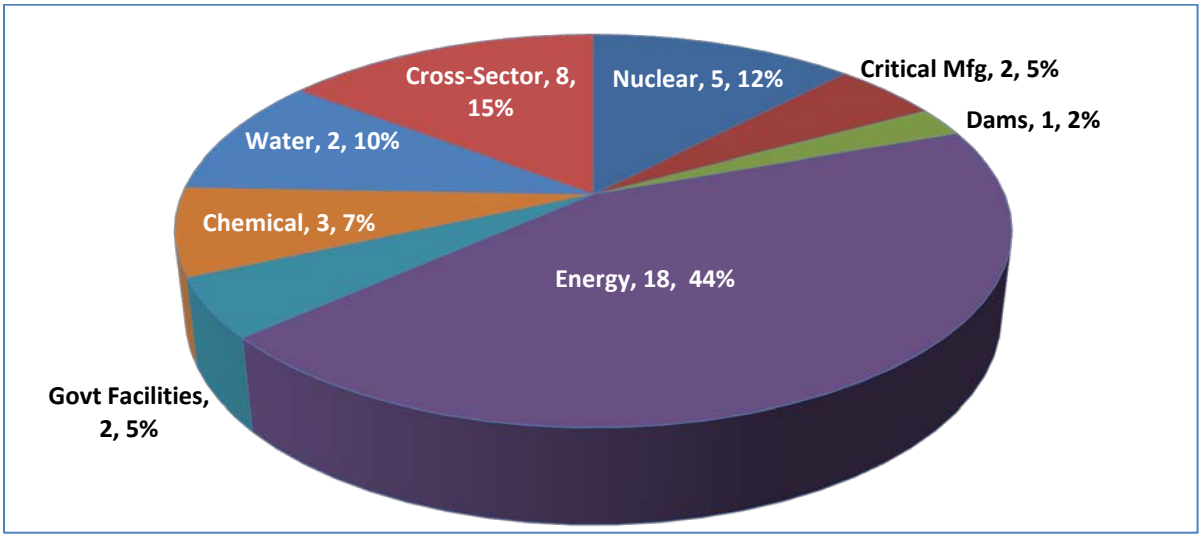

Figure 3. Incident reports by sector (2010).

ICS-CERT received multiple reports of secure shell (SSH) brute force attacks attempting to access ICS and critical infrastructure companies who operate ICS. Although this type of activity was commonly recognized in the IT sector, these incidents marked an increased awareness of the attack potential and attractiveness of targeting ICS. ICS-CERT published a report titled "CSAR-10-088-01—SSH Brute-Force Scanning and Attacks" to inform asset owners about how to identify brute force scanning and attacks, how to mitigate the risks, and when to report an incident.

Multiple spear-phishing incidents were also reported. Reports came from several sectors, but the Energy Sector accounted for two-thirds of these incidents. All the spear-phishing incidents reported to ICS-CERT involved sophisticated or advanced persistent threat actors.

Several notable threats from 2010 include:

Mariposa infections in CIKR. Defence Intelligence identified the Mariposa botnet in May 2009. Although the primary command and control (C2) infrastructure was taken down in December of that year, ICS-CERT continued to receive malware infection reports into early 2010, at least one of which resulted in an onsite incident response to determine whether the malware had breached the control system network. The operations executed by the botnet were diverse, in part because parts of the botnet could be rented by third-party individuals and organizations. Confirmed activities include denial-of-service attacks, email spam, theft of personal information, and changing the search results a browser would display in order to show advertisements and pop-up ads.[c]

Stuxnet was discovered; ICS-CERT deploys an onsite incident response team to a Stuxnet infected facility. Stuxnet, the first ever malware specifically written to target ICS, was discovered in 2010. ICS-

c. http://en.wikipedia.org/wiki/Mariposa_botnet

CERT analyzed the malware and its impacts to control systems in coordination with various government agencies, law enforcement, industry, and other organizations such as Symantec, Microsoft, CERT Bund, Siemens, and various sector ISACs (i.e., Energy, Chemical, Nuclear, Dams, Water, Transportation). ICS-CERT issued advisories with multiple updates to provide mitigation information to critical infrastructure asset owners and operators. ICS-CERT also conducted an onsite incident response deployment to a manufacturing facility infected with the Stuxnet malware and helped the organization identify all infected systems and eradicate the malware from their control system network (see page 8, "Onsite Incident Response Activities" for more details).

2011

REPORTED INCIDENTS

In 2011, ICS-CERT received 198 reports of incidents. Of those 198, seven resulted in the deployment of onsite incident response teams. An additional 21 incidents involved analysis efforts by the AAL to identify malware and techniques used by the threat actors. Figure 4 displays the sector distribution for all incidents reported in 2011. Incidents specific to the Water Sector, when added to those that impacted multiple sectors, accounted for over half of the incidents due to a large number of Internet facing control system devices reported by independent researchers.

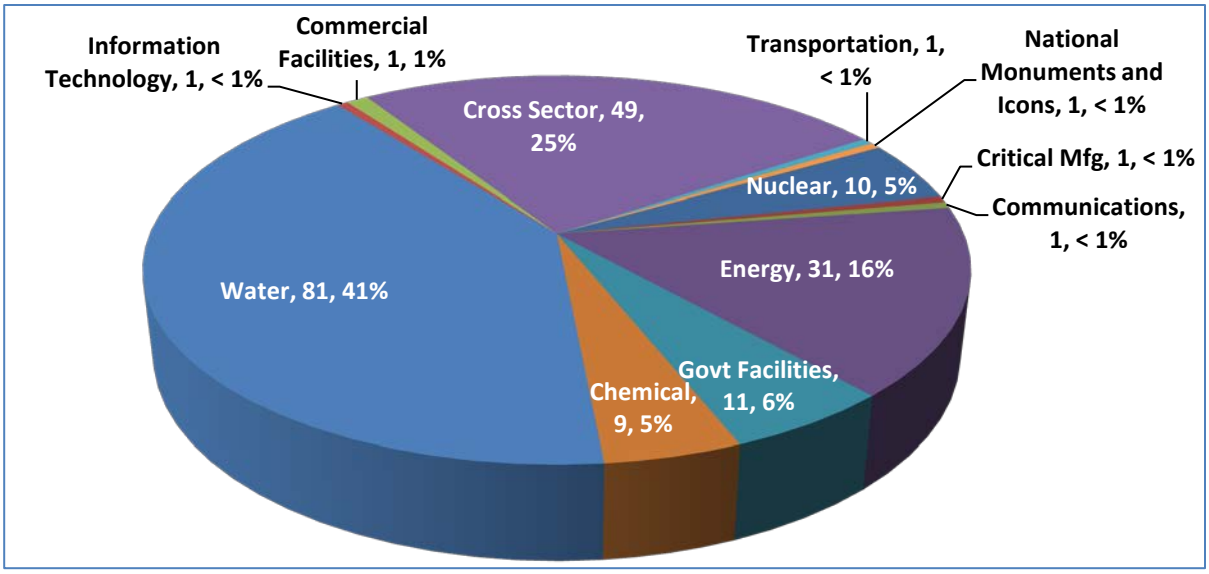

Figure 4. Incident reports by sector (2011).

Many of these Internet facing control systems employed a remote access platform from the same vendor, configured with an unsecure authentication mechanism. ICS-CERT coordinated with the vendor to mitigate the authentication vulnerability and also took on the task of identifying and notifying the affected asset owners. ICS-CERT provided them with details of the risks associated with weak boundary

protection practices and assisted with mitigation strategies. As a result, ICS-CERT published a new alert titled "ICS-ALERT-11-343-01—Control Systems Internet Accessibility" to update the public on the risk associated with Internet accessibility to control system devices.

A similar incident occurred in January 2012, in which ICS-CERT identified an organization that appeared to be compromised based on information discovered in open source forums. After analyzing the data, ICS-CERT established contact with the impacted facility owners and informed them of the open source posting of their control systems information. Facility personnel reported to ICS-CERT that they had already discovered the compromise and unauthorized adjustments to the Energy Management System control settings that had resulted in unusually warm temperatures in the facility. The organization acted quickly when they discovered the intruder and adjusted their network configuration to eliminate Internet accessibility. The organization, however, was not aware that sensitive information about their system was on the Internet or of the malicious IP address associated with the compromise.

ICS-CERT also responded to multiple incidents involving sophisticated and targeted spear-phishing campaigns against asset owners in the Nuclear, Energy, Government, and Chemical Sectors. In some cases, emails were convincingly crafted and appeared to be from corporate executives or other trusted sources in an attempt to lure users into opening malicious attachments or links. Once compromised, attackers often map out networks in order to perform a variety of functions including stealing credentials, exfiltrating sensitive information such as financial, research or operational data, and establishing multiple footholds to maintain persistent presence for future operations. In all cases, ICS-CERT works with reporting organizations to help determine if the control network was compromised and provides mitigations to detect and mitigate the activity.

Some examples include:

- ICS-CERT worked with several companies that were part of the Night Dragon[d] attacks, first publicly reported in February 2010, targeting global oil, energy, and petrochemical companies. Hackers moved deliberately through the victim's networks, trolling for sensitive data and intellectual property.
- ICS-CERT worked with several organizations impacted by the Nitro[e] attacks, where companies involved in research and development of chemical compounds and materials were the targets of sophisticated attacks. Reports indicated that the attackers gathered data from across the victim networks and moved it to internal staging servers to make data exfiltration more efficient.

These incidents highlight the activity of sophisticated threat actors and their ability to gain access to system networks, avoid detection, use advanced techniques to maintain a presence, and exfiltrate data. ICS-CERT also collaborated with the international cybersecurity community working with over 30 different countries and, in most cases, interfacing directly with the international Computer Emergency Response Teams (CERTs) to coordinate responses and reach out to affected organizations and vendors.

d. http://www mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
e. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

SECTION 2: ONSITE INCIDENT RESPONSE SUMMARY

Onsite incident response support to critical infrastructure asset owners and operators impacted by cyber incidents is an important aspect of ICS-CERT capabilities. Deploying a team onsite is always conducted at the request of the asset owner/operator and only when appropriate thresholds have been met.

ICS-CERT provided onsite support to critical infrastructure asset owners on 17 separate occasions: two in 2009, eight in 2010, and seven in 2011. In all cases, ICS-CERT performed network topology reviews while onsite, to include a thorough review of the interconnections between ICS and enterprise networks, existing security and logging mechanisms, and interviews with personnel to describe existing procedures and common practices. ICS-CERT also left asset owners with recommendations for strengthening overall cybersecurity and enhancing incident response capabilities and procedures.

INCIDENT RESPONSE GOALS

ICS-CERT performs incident response with four primary goals.

1. Provide one-on-one support to the impacted organization to characterize the nature of the attack (actors, malware, techniques, and tactics) and determine the extent of compromise.
2. Develop guidance for the impacted organization and recommend a path for recovery and future protection. ICS-CERT does not provide direct recovery services but is always available to clarify the recovery recommendations.
3. Leverage the information obtained from onsite response activities to provide situational awareness warnings and alerts to the rest of the critical infrastructure and key resources community (without attribution to the affected organization).
4. Collect threat actor indicators, techniques, tactics, and procedures to correlate with other incidents and share with National Cybersecurity and Communications Integration Center partners.

The following provides a brief synopsis of each onsite response effort by year and by impacted sector.

2009 ONSITE INCIDENT RESPONSE

Water

ICS-CERT deployed an incident response team to a municipal water treatment plant that had reported an incident that was thought to include a compromise of their control systems network. ICS-CERT obtained digital artifacts, including a hard drive from the suspected compromised host for analysis. Analysis of digital artifacts concluded that there was no targeted malicious activity against the water treatment plant's business or control systems network. The overall cyber defense and incident response capabilities at this facility were low, and ICS-CERT provided recommendations and resources for hardening its security posture and enhancing its response capabilities.

Energy

An electric utility detected a suspicious cyber event and requested support from ICS-CERT. ICS-CERT performed memory forensic analysis and provided onsite support. The analysis concluded that the network had not been compromised as initially expected. ICS-CERT conducted a thorough network topology review and provided recommendations for implementing better detection mechanisms.

2010 ONSITE INCIDENT RESPONSE

Energy

ICS-CERT deployed an incident response team to an Energy Sector organization that was targeted by a spear-phishing email campaign, which was successful in compromising and exfiltrating data from the enterprise network. The ICS-CERT incident response team performed network traffic analysis, both live and historical, to identify additional machines that may have been involved. In total, ICS-CERT analyzed 11 drives from the affected organization that were suspected as compromised as a result of logged DNS queries to known bad domains. Analysis of the drives produced indicators of a rootkit, malware specific to the victim's network, and characteristics of a known and sophisticated threat actor, all of which supported the premise that this had been a targeted attack. The suspected attack vector was spear-phishing, and ICS-CERT believes that it is highly likely that data were exfiltrated from this organization's network. ICS-CERT provided extensive indicators for use by the organization to identify, mitigate, and eradicate the threat.

Nuclear

ICS-CERT deployed an onsite incident response team in response to an incident in the Nuclear Sector resulting from the presence of crimeware on the enterprise network. The team evaluated six 6 hard drives while on site and found indicators of malware related to the Mariposa botnet. The infection occurred when an employee attended an industry event and used an instructor's universal serial bus (USB) flash drive to download presentation materials to a laptop. The USB drive was infected with the Mariposa botnet and when the user connected the laptop to the corporate network upon returning to work, the virus spread to over 100 hosts on the enterprise network. ICS-CERT, in conjunction with the company, identified all infected computers and provided recommendations for eradicating the virus from their network. ICS-CERT confirmed that the compromise did not impact control processes or operations.

Interestingly, interviews with the employee revealed that other nuclear industry personnel had also used the same infected USB drive at the industry event and their laptops were likely infected as well. ICS-CERT obtained the instructor's name, contacted him to inform him of the infected drive, and requested a list of attendees for notification purposes. The instructor declined the offer and said that he would reach out to the entities himself to inform them of the malware. Unfortunately, ICS-CERT was not able to verify if the companies were ever contacted and to what extent they may have been impacted.

Manufacturing

ICS-CERT deployed an incident response team to a critical manufacturing organization after receiving a report of an intrusion by a sophisticated threat actor into the organization's enterprise network. While onsite, ICS-CERT identified infected systems, obtained log files, and provided mitigation strategies to the organization. Through analysis, ICS-CERT determined that the source of the compromise appeared to be a sophisticated threat actor, based on analysis of the path and mechanism of the initial entry point and indicators found on the hard drive images. The entry point was a spear-phishing email with specific and highly relevant content for that organization and a malicious .zip file attachment. Exfiltration of data from the organization was suspected, but due to the lack of available logging, was unable to be confirmed. The compromise did not impact control processes and operations.

Energy

ICS-CERT deployed an incident response team to an electric utility after receiving a request from support from the organization. This utility requested onsite support during a scheduled outage to review its control system and enterprise network architecture, identify potential vulnerabilities, and recommend mitigation strategies for an improved security posture. The utility had noted anomalous activity on its network, but had already completed the initial stages of incident management and had begun to perform the root cause failure analysis necessary to guide business and architectural improvements to its various network environments. This organization possessed mature cybersecurity capabilities and maintained a high level of preparedness to respond to a cyber incident. ICS-CERT provided an in-depth architectural review and threat assessment of the incident after the incident had been contained and provided the utility with additional recommendations.

Energy

ICS-CERT deployed a team to an oil and gas company after they identified compromised hosts on its network that were communicating to malicious IP addresses as a result of a malware infection. The company received several spear-phishing emails to a number of internal recipients, and indications showed that the spear-phishing emails were opened by multiple recipients. ICS-CERT and US-CERT coordinated a joint onsite incident response and analysis effort. The spear-phishing email included a .zip attachment containing a .chm file, compressed binary Help files (that display results information via HTML), and exploitation code. Extensive analysis indicated that the compromise was limited to the enterprise network and did not extend to the control system network and process operations. ICS-CERT and US-CERT analyzed their network topology and provided recommendations for mitigating the sophisticated intrusion as well as enhancing their overall security posture.

Manufacturing

ICS-CERT deployed an incident response and analysis team to a critical manufacturing facility infected with the Stuxnet malware. ICS-CERT deployed a team of analysts to the facility and confirmed the presence of Stuxnet on all their engineering workstations as well as several other machines connected to their manufacturing control systems network. The malware was verified to be the same as the one previously analyzed in ICS-CERT's malware laboratory. ICS-CERT worked with the asset owner to

develop and implement a multi-staged Stuxnet removal process, customized for their network, and confirmed that the infection had been eradicated prior to leaving. ICS-CERT also left the facility with procedures and mechanisms for detecting and removing any future Stuxnet infections.

Energy

ICS-CERT deployed an incident response and analysis team to an energy sector organization to review an incident relating to a sophisticated threat actor and potential data exfiltration from its network. The organization had experienced a series of spear-phishing attacks against their users and they were able to detect and monitor the resulting intrusion and the exfiltration of data. The organization had a mature security posture which enabled them to quickly contain the incident. The onsite response team helped perform a defensive gap analysis of the network using known threat indicators. ICS-CERT verified that the organization's containment strategy addressed the potential attack pathways and provided technical recommendations for detecting and mitigating future attacks.

Energy

ICS-CERT deployed an incident response and analysis team to an Oil and Gas company after the organization reported that a series of spear-phishing emails targeting members of their organization. It was suspected that information was being exfiltrated. During this onsite response effort, the ICS-CERT team met with the organization to support mitigation efforts from the incident. The organization had begun the initial stages of incident management and ICS-CERT assisted the organization in evaluating their network topology, understanding the threat, examining logs for indicators of further compromise, and discussion of the findings and relevant defensive strategies for mitigating the threat and improving their overall security posture.

2011 ONSITE INCIDENT RESPONSE

Water

ICS-CERT deployed an incident response team to a water organization that reported a compromise of its remote terminal server. The ICS-CERT incident response team performed throughout analysis of the infected host and of the associated malware. Analysis concluded that an infection of the remote terminal server had occurred and that the infection was non-targeted and consistent with crimeware, not a sophisticated threat. Further analysis of logs confirmed this finding as the logs showed that the infected host had been communicating with known crimeware hosts. The ICS-CERT team worked with the organization to identify the scope of the incident and the most probable points of entry, allowing the organization to develop a more effective strategy for mitigating future attacks and strengthen its remote log-in practices.

Energy

ICS-CERT deployed an incident response team to a bulk electric power organization that had been the victim of a broader spear-phishing campaign against the nuclear/energy sectors. ICS-CERT analyzed multiple digital artifacts, including three malware samples and detected evidence of a sophisticated threat

actor; the point of entry appeared to have been an employee opening a PDF attachment of a spoofed industry-specific newsletter, which contained the malware. Following execution, a non-malicious PDF was presented to the user. Command and control was positively identified as part of this analysis and ICS-CERT provided indicators and mitigation strategies to this organization to detect further infections on their network and take appropriate defensive measures to combat the threat. The recommendations given to this organization also included security recommended practices and mitigation techniques specific to the threat actors.

Government

ICS-CERT deployed an incident response team to a government facility after a malfunction of a PLC controlling backup generators at one of their facilities. This partial loss of backup power affected non-vital services. The ICS-CERT incident response team performed a security assessment of the government facility's control systems network and collected log files and other digital artifacts for further analysis. ICS-CERT confirmed through analysis that there was no evidence of a cyber incident that resulted in the malfunction of the PLC and the resultant impact to non-vital services. ICS-CERT provided the government facility with recommend practices to enhance their security posture.

Government

A government organization requested support from the ICS-CERT to investigate suspicious cyber activity involving their internally-managed building management control systems. ICS-CERT provided on-site support and conducted analysis detected no evidence of malicious cyber activity. The response team provided guidance and recommendations on best practices to improve their cyber security posture for defense against future cyber threats.

Energy

ICS-CERT deployed an incident response team to an electric utility that had been targeted by a broader spear-phishing campaign. ICS-CERT conducted analysis on three suspected malicious PDF files provided by the organization. From this analysis, ICS-CERT determined that two of the PDF files were known malicious and made requests to known malicious domains. However, post- analysis of digital artifacts and interviews with utility personnel, including the targeted employee uncovered that all attempts were unsuccessful. ICS-CERT provided the organization with indicators to detect compromise based on analysis of the malicious email, and the utility determined that their network had not been compromised.

Water

ICS-CERT deployed an incident response team to a water utility that appeared to have evidence of an unauthorized login to their control systems network. Initial reporting indicated that a pump had failed as result of changes made in the control systems environment. ICS-CERT conducted analysis and interviews with the organization (and their support contractors) and determined that the unauthorized login was in fact an authorized user logging into the control system while on personal business in a foreign country for legitimate business purposes. The owner confirmed this as legitimate system access. Further analysis of the network logs and telemetry data on the control systems network found no evidence of an unauthorized

login, malicious intrusion, or compromise. ICS-CERT also provided recommendations to the water utility on methods of improving the security of remote access to their controls system.

Because of the media attention given to this incident, ICS-CERT later published a report in coordination with the asset owner.

Chemical

ICS-CERT deployed an incident response team to a chemical industry organization that had reported anomalous activity on its network. The ICS-CERT incident response team analysis of its systems found two suspicious files running in memory. ICS-CERT examined network logs for evidence that company hosts had communicated with malicious IP addresses during the timeframe surrounding the infection period and found indicators of compromise in several locations on the network. Based on the indicators discovered, ICS-CERT concluded that a sophisticated adversary compromised multiple machines and uploaded tools onto the network. Review of the network topology showed that the organization had a flat network and lacked other defensive technologies for a secure system. ICS-CERT provided recommendations for improving the network defensive posture and the architecture of their network. ICS-CERT recommended that the organization continue to use improved defensive technologies to continue to evaluate the full extent of the compromise and eradicate the attacker from the network.

SECTION 3: COMMON FINDINGS

This section summarizes key metrics from onsite deployments and common findings from incident response events.

KEY METRICS FROM ONSITE DEPLOYMENTS

An analysis of the onsite deployment events provides some key findings regarding the threat environment, methods of detection, and incident response activities. These findings highlight areas for improvement in protecting control systems networks.

THREATS

The most common infection vector for network intrusion was spear-phishing emails with malicious links or attachments. Spear-phishing accounted for 7 out of 17 incidents. At least one incident involved an infection from a removable USB device.

Sophisticated threat actors were present in 11 of the 17 incidents, including the actors utilizing spear-phishing tactics to compromise networks. These threat actors were responsible for data exfiltration in several cases, which seems to have been the primary motive for intrusion. No intrusions were identified directly into control system networks. However, given the flat and interconnected nature of many of these organization's networks, threat actors, once they have gained a presence, have the potential to move laterally into other portions of the network, including the control system, where they could compromise critical infrastructure operations.

In 12 of 17 cases, implementation of security recommended practices, such as login limitations and segmenting networks with properly configured firewalls, could have deterred the attack, significantly reduced the time to detect the attack, or at least reduced the impact of the incident.

DETECTION

Properly developed and implemented detection methods are the best strategy to quickly identify intrusions and implement mitigation and recovery procedures. Most of the organizations to which ICS-CERT responded were not prepared with adequate detection techniques. In 3 of the 17 onsite responses, the asset owners had been notified of the event or intrusion by external organizations. In two additional cases, the incident had been identified by a hired third party (consultant or integrator). For one asset owner, server administrators identified unusual activity that led to the discovery of a phishing compromise. Equipment failure was responsible for two reported incidents that led to the deployment of onsite response teams. The following statistics from the 17 incidents highlight the value of using detection capabilities to identify a compromise.

Ten organizations could have detected the intrusion by using ingress/egress filtering of known bad IP addresses or domain names.

In seven incidents, file indicators were used by the incident response team to confirm the compromise and identify the threat.

In three incidents, traffic was observed to known bad IP addresses or domain names, allowing the response team to identify the threat actor.

RESPONSE

In three cases, ICS-CERT responded with onsite deployments to incidents and determined that the attacks were not targeted at the asset owner. In the other onsite response situations, the infection vector could not be determined. Several common issues or concerns emerged during these incident responses. Many organizations did not have sufficient logging capabilities enabled and were unable to provide valuable log data for analysis. In some cases, the forensic images that were sent to the AAL for analysis were created long after the event occurred. By then, important timestamps had been overwritten and a reliable timeline could not be established. Similarly, running antivirus scanning after an intrusion can overwrite timestamps. ICS-CERT has developed guidance for preserving forensic data and provides this information (*ICS-CERT Incident Handling Brochure*) during incident response efforts to help network administrators preserved forensic data for analysis. Updates are posted to the ICS-CERT web page at http://www.ics-cert.org.

COMMON FINDINGS—ALL INCIDENTS

Through analysis of the findings from the onsite incident response events, the incident reports, and the results from over 150 onsite assessments using the CSET,[f] ICS-CERT has identified common trends in operational security gaps in control systems environments. These findings can be broken down into three major categories:

1. People
2. Process
3. Technology.

The following sections summarize the most common cybersecurity gaps associated with each of these categories.

PEOPLE

An organization's personnel can contribute to cybersecurity gaps when they 1) lack understanding of the overall security risk to control systems, 2) do not consider the technical and security impacts of inadequate security policies or implementation thereof, and/or 3) lack the cybersecurity skills needed to provide protection of its network against cyber attacks. In other words, personnel may not believe the

f. Cyber Security Evaluation Tool (CSET), http://www.us-cert.gov/control_systems/satool.html

threat is credible, or they don't see themselves as a target, or they lack the knowledge and capabilities to implement adequate protective measures.

Cybersecurity gaps can occur when personnel at all levels of an organization do not clearly understand security risks to the control systems environment. This includes management, IT operations, security operations, process operations, control systems, and incident response operations. Until critical infrastructure organizations see themselves as probable targets and gain an understanding of the threat actor capability to penetrate, avoid detection, and maintain a presence on their networks, they will not make the necessary investments in cybersecurity. To address this gap, ICS-CERT strives for improved information sharing and outreach efforts by continually providing situational awareness to the ICS community in the form of alerts, advisories, and briefings.

Cybersecurity gaps also can occur when personnel have an insufficient understanding of the technical impacts of inadequate security policies. Organizations often fail to develop common technical and security standards for the IT and control systems components of their environments. Without such standards, it may be impossible to create an effective security posture. Organizations should integrate business requirements and technical needs when developing security strategies. Changing default user names and passwords on vendor equipment and placing ICS remote logon sites behind firewalls with VPN protection are two examples of policies that are readily implemented and will significantly improve an organization's security posture.

Gaps in the necessary cybersecurity skills can result from limited resources and funding or from a lack of understanding of security needs in relation to the organization as a whole. The primary reasons for this gap in skill mix often include the following:

- Failure to perform risk and consequence analyses of a successful cyber attack and develop a business case for investing in cyber security
- Failure to hire individuals or a team dedicated to perform security operations for the organization as a whole
- Failure of organizations that have identified cybersecurity subject matter experts to allocate enough time and training to fulfill the role at the required level
- A lack of situational awareness regarding cyber threats and inadequate polices to guide the implementation and maintenance of technical security solutions, such as policies for managing removable media or guidance for personnel to spot and defend against threats from spear-phishing attacks
- Failure to consider technical administration of control systems and corporate IT networks as a core business function that crosses all business silos. This limits communication among technical administrators, business owners, and technology end users, resulting in gaps relating to how the technology is designed, procured, and secured.

PROCESS

An organization's processes can result in cybersecurity gaps for the following reasons.

- Lack of or insufficient incident response planning or processes to prevent or inhibit cyber events, detect intrusions, and preserve forensic data for analysis and recovery strategies.
- Lack of policies or processes for moving security operations from a tactical level to a core business competency across business functions (i.e., IT operations, security operations, process operations, control systems).
- Lack of or insufficient security strategies and policies necessary to develop adequate security maturity throughout the organization. This also includes a clear policy addressing removable media, particularly when and where its use is allowed within the organization.
- Lack of minimum functional and security standards necessary to develop the following:
  - Adequate functional IT operational requirements and best practices
  - Necessary security operations strategy and technical architecture
  - Adequate control systems and process operations security requirements plan
  - Adequate training and qualification of personnel.

TECHNOLOGY

An organization's technology can result in cybersecurity gaps for the following reasons.

- Control systems environments risk assessments do not identify or prioritize most significant technical risks and potential impacts to operations that would support the business case for investing in cybersecurity.
- Lack of security management framework, which results in an inconsistent tactical security posture at each of the following levels:
  - Lack of network segmentation, both physically and logically.
  - Network segmentation using firewalls is a network design approach that offers a number of security advantages to an organization.
  - It involves separating a network into smaller functional networks that can than restrict the extent at which an intruder can easily move laterally through the network.
- Patch Management
  - Lack of adequate patch management policies and practices to address known vulnerabilities and ensure up-to-date protection of common cybersecurity threats.
  - Organizations should also develop test environments to assess possible impacts of patches prior to implementation in the operating environment.

  - Lack of configuration management policies and practices to ensure changes to the network topology are tracked and assessed for impacts to security.

- User access controls
  - Allowing uncontrolled user logons across network segments
  - Uncontrolled network access by vendors
  - Default user name and passwords not changed in applications, etc.
- Network communications
  - Insufficient ingress/egress traffic filtering due to lack of a functional network baseline
  - Network architecture not adequate for security needs
- Firmware
  - Embedded systems do not support incremental security changes
- Operating system
  - Lack of integrated security expertise (control systems, sec ops, IT ops, process) prohibit development of compensating controls
  - Lack of systems development life cycle (SDLC) by vendor, integrator, or operator prevents adequate security controls from being implemented.

GOING FORWARD

ICS-CERT and the ICS community have worked together successfully to identify and mitigate malicious cyber activity in critical infrastructure assets, but much remains to be done. As discussed, reports from various organizations enabled ICS-CERT to analyze incident data from their networks and create an overall view of the incidents in progress. This would not have been possible without the active cooperation of the reporting organizations. ICS-CERT encourages ICS companies to report cyber incidents for tracking, correlation, and support.

Sophisticated and targeted cyber intrusions against ICSs across multiple critical infrastructure sectors continue to increase. ICS-CERT developed guidance (ICS-TIP-12-146-01) to provide basic recommendations for owners and operators of critical infrastructure to mitigate the impacts of cyber attacks and enhance their network security posture.

In 2012, ICS-CERT continues to provide situational awareness information about the emerging threats and incident response services to assist with mitigation and recovery efforts.

For more about ICS-CERT incident response activities and to learn more about recommended security practices for ICSs, visit http://www.ics-cert.org or contact ICS-CERT at ICS-CERT@hq.dhs.gov.