ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT - 2010 YEAR IN REVIEW

January 2011

A LOOK BACK

The past year has been a busy and unprecedented year for both the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the control systems community. The most notable event was the emergence of Stuxnet, the first malware created specifically to target industrial control systems (ICS). ICS-CERT analysts and researchers across industry dissected and unraveled the malware revealing a sophisticated trail of zero-days, anti-detection, and propagation techniques.

Since Stuxnet's discovery, news outlets and bloggers have flooded cyberspace with a barrage of analysis and conjecture behind who created it and who was the intended target. While many theories abound, it is the Department's mission to remain focused on the risk mitigations and collaborate with the 18 Critical Infrastructure/Key Resource (CIKR) sectors to promote preparedness and information sharing. ICS-CERT accomplished this through sector briefings, meetings, conferences, and other engagements to meet with asset owners and operators, vendors, and federal/state/local partners to discuss concerns and mitigations for this and other threats. For many, Stuxnet signaled a paradigm shift with the ICS community, demonstrating that organizations must be operationally prepared with tools, systems, and personnel to detect malicious activity and effectively mitigate the impact to their control systems.

While Stuxnet was a dominating force in 2010, other advanced persistent threats (APT) became commonplace across industry. This uptick in activity resulted in the development of "fly-away" teams to provide onsite assistance to asset owners in response to a cyber incident. Many of these fly-away engagements were conducted in conjunction with US-CERT through the newly formed National Cybersecurity and Communications Integration Center (NCCIC pronounced 'n-kick'). The NCCIC was established by the US Department of Homeland Security (DHS) to improve communications between the private sector and government. ICS-CERT's role within the integrated NCCIC framework is to enhance DHS cyber incident response efforts and to ensure that control systems security issues are addressed.

Both the NCCIC and ICS-CERT were thoroughly put to the test during the national-level CyberStorm III exercise held in September. At its core, the exercise was intended to assess and strengthen cyber preparedness and incident response capabilities among federal, state, local, international and private sector companies. The exercise involved thousands of players from federal departments and agencies, state and local governments, twelve countries, and nearly sixty private sector companies to simulate a large-scale cyber attack on critical infrastructure. The exercise and its scenarios underscored the importance of control systems and the critical infrastructure that they operate.

This report looks back at 2010 and highlights significant activities and events affecting ICS. It also provides lessons learned and links to resources that organizations can use to help better prepare for the "next Stuxnet." ICS-CERT looks forward to 2011 as it continues this important mission to advance the state of awareness and preparedness.

STUXNET

The year 2010 was unarguably the year of Stuxnet, a sophisticated and advanced piece of malware that leveraged zero-day exploits, digitally signed certificates, and employed evasion techniques to propagate and avoid detection. The publicity surrounding Stuxnet has raised awareness within critical infrastructure organizations that may have otherwise taken several years to accomplish by normal outreach methods. It has highlighted the interdependencies and vulnerabilities that exist in legacy control system environments and demonstrated that motivated groups are interested in attacking them. Stuxnet has become a wake-up call to many that "security through obscurity" is no longer an option.

While Stuxnet will likely be studied and reported on for years to come, the salient lesson is the importance of remaining vigilant of cyber threats, employing detection mechanisms, and having an incident response plan in place to respond quickly when incidents occur.

LESSONS LEARNED

- CIKR asset owners need to employ policies concerning the use of USB drives and other removable media within the organization, particularly within the control system environment.
- Asset owners need to be better prepared to handle this level of malware by practicing defense-in-depth, developing appropriate logging procedures, practicing appropriate network monitoring, and knowing the available resources for combating this type of event.
- Timely information sharing of threats and analysis is of chief importance in empowering and protecting public and private sector partners.

ADVANCED PERSISTENT THREAT (APT) ACTORS TARGET INDUSTRY

APT actors have been reported on for some time now; however, 2010 ushered in a new uptick in APT activity affecting organizations across all CIKR sectors. These sophisticated attacks difficult to defend against and in many cases, difficult to detect and mitigate as APT actors are typically well-funded and organized. Advanced threats take advantage of the human side of cybersecurity through social engineering and phishing e-mails to entice employees to open attachments or click links that download malware to their systems. In most cases, these attacks focus on corporate espionage with the intent to gain competitive advantage in regional or global markets.

In 2010, ICS-CERT and US-CERT assisted numerous asset owners with APT-related activity. These incidents involved extensive coordination with asset owners and operators, including onsite engagements and law enforcement involvement (at the request of the organization) to identify compromised or systems of interest. While control systems are not the typical intended targets, ICS-CERT examines all pathways from the business network to evaluate if a compromise has breached the control network. ICS-CERT and US-CERT also recommend practices to help better secure the network and detect future malicious activity.

LESSONS LEARNED

- Asset owners and operators are susceptible to a variety of threat actors that appear to be increasing their activities across all sectors.

- An organization's lack of established security practices introduces more attack vectors and generally makes it difficult to detect malicious activity and perform forensic analysis.
- Spear phishing attacks are a common method of gaining footholds into corporate networks.
- Organizations need to deploy better detection measures and evaluate all connections into their control networks.

FLY-AWAY TEAMS DEPLOYED FOR ICS CYBER INCIDENTS

As mentioned, the uptick in malicious cyber activity resulted in the formation of teams that could deploy with little notice to help triage a cyber incident. Armed with toolkits, these fly-away teams were dispatched at the request of asset owners in response to actual incidents impacting ICS across various critical infrastructure sectors.

The majority of onsites involved a review of the incident details, enterprise network topologies and control systems architectures for the purpose of identifying initial infection vectors, systems of interest, and weakened areas that need strengthening. Many of the asset owners also requested law enforcement/FBI coordination to further document and protect their assets.

In certain cases, and with the approval of the asset owners involved, ICS-CERT analyzed additional information such as malware, network traffic captures, and system images for more in-depth analysis and identification of malicious activity. ICS-CERT provided follow-on reporting, mitigation measures, and access to additional resources through the US-CERT secure portal. These engagements fostered a new level of partnering and information sharing that will likely grow in 2011 and beyond.

LESSONS LEARNED

- Many asset owners reported that they were not aware of the resources available to keep them informed of current threat information or vulnerabilities to ICS.
- A common understanding of the potential impacts of cyber vulnerabilities (loss or degradation of process control, loss of sensitive information, etc.) does not exist across all CIKR sectors.
- Asset owners need to employ consistent management of privileges on their networks— who has which privileges and on which part of the network they apply for each individual.
- Forensics analysis is enhanced when the organization has established a baseline dataset for network configuration and typical traffic; this allows for more effective identification of intrusions.
- Asset owners need to develop adequate policies and procedures to educate employees and reduce the potential of unintended cyber incidents resulting from untrained workforce.

RESPONSIBLE VULNERABILITY DISCLOSURE

During 2010, ICS-CERT worked with a variety of researchers to foster responsible vulnerability disclosure with ICS vendors. Many researchers had begun viewing the control systems arena as an untapped area of focus for vulnerabilities and exploits and used their research to call attention to it. ICS-CERT, in coordination with CERT/CC and US-CERT, identified that a gap existed between the control systems research and vendor communities. ICS-CERT, CERT/CC and US-CERT were able to bridge this gap by reaching out to both parties

and acting as a conduit for information sharing and vulnerability disclosure. This process has shown excellent results for both the researchers and the vendors alike. ICS-CERT found that in most cases, vendors take security issues with their software very seriously and prefer to see them mitigated in a coordinated manner to minimize the risk to their customers.

Despite progress, some researchers continue to publicly disclose vulnerabilities without any coordination. ICS-CERT categorizes ICS vulnerability disclosure as one of two types:

- Coordinated disclosure: the researcher reports the vulnerability to ICS-CERT or the vendor and delays public disclosure until the vendor has released a patch and provided users time to apply the patch.
- Unanticipated disclosure: the researcher publicly discloses the vulnerability without notifying any coordinating groups or the vendor. In 2010, ICS-CERT saw a significant increase in the number of unanticipated disclosures of ICS vulnerabilities reported by independent researchers around the world.

ICS-CERT has coordinated vulnerability disclosures with CERT/CC, US-CERT, independent researchers, vendors, Information Sharing and Analysis Centers (ISACs) and national level CERTs throughout the world. ICS-CERT also performs testing and verification of the vulnerabilities and patches when possible. This resulted in multiple Alerts and Advisories to warn of the vulnerabilities and provide mitigation paths and resources.

LESSONS LEARNED

- Independent researchers are valuable assets for improving control system cybersecurity.
- Most ICS vendors take security issues with their software very seriously and prefer to see them mitigated in a coordinated manner to minimize the risk to their customers.
- Relationships with other national-level CERTs are as equally important for properly coordinating ICS-related vulnerabilities for protecting the install base in other countries and for communicating with vendors headquartered out of foreign regions.

USB DRIVES AND OTHER REMOVABLE MEDIA

Even before the advent of Stuxnet, ICS-CERT had begun to track a trend of removable media involved in malware infections. In one fly-away deployment, an employee had attended an industry event and used an instructor's USB to download presentation materials to the company's laptop. The USB was unknowingly infected with the Mariposa botnet and when the employee returned to the work location and plugged the laptop in, the virus quickly spread to nearly 100 systems.

ICS-CERT encourages owners and operators to review the following documents:

- ICS-CERT Control Systems Analysis Report, "USB Drives Commonly Used as an Attack Vector Against Critical Infrastructure"[a]
- ICS-CERT Advisory, "ICSA-10-238-01B—Stuxnet Malware Mitigation."[b]

a. ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-USB%20USAGE.pdf
b. ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICSA-10-238-01B.pdf

LESSONS LEARNED

- Asset owners need to evaluate the risks posed by USBs and other portable media devices and develop policies and practices commensurate with the level of risk system owners are willing to assume.

SUMMARY OF 2010 RECOMMENDATIONS

- Where practical, isolate control systems from the enterprise and from the Internet. If the control system must be connected to the enterprise system, employ a network configuration based on the defense-in-depth strategy described in the ICS-CERT publication "Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies" to firewall the control system on its own subnet.[c]
- Asset owners need to be better prepared to handle sophisticated threats by practicing defense-in-depth, developing appropriate logging procedures, employing detection measures, practicing appropriate network monitoring, and knowing the resources available to keep them informed of current threat information or vulnerabilities to ICS.
- Timely information sharing of threats and analysis is of chief importance in empowering and protecting public and private sector partners.
- An organization's lack of established security practices introduces more attack vectors and generally makes it difficult to detect malicious activity and perform forensic analysis.
- Spear phishing attacks are a common method of gaining footholds into corporate networks.
- Asset owners and operators are susceptible to a variety of threat actors that appear to be increasing their activities across all sectors.
- A common awareness and understanding of the potential impacts of cyber vulnerabilities does not exist across all CIKR sectors.
- Asset owners need to develop adequate policies and procedures to educate employees and reduce the potential of unintended cyber incidents resulting from untrained workforce.
- Independent researchers are valuable assets for improving control system cybersecurity.
- Most ICS vendors take security issues with their software very seriously and prefer to see them mitigated in a coordinated manner to minimize the risk to their customers.
- Relationships with other national-level CERTs are as equally important for properly coordinating ICS-related vulnerabilities for protecting the install base in other countries and for communicating with vendors headquartered out of foreign regions.

c. ICS-CERT, "Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies," http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

- Asset owners and operators interested in receiving alerts and advisories should request a US-CERT Secure Portal account from ICS-CERT by emailing ics-cert@dhs.gov.

ICS-CERT recommends all asset owners consider the following when configuring or expanding their enterprise and control system networks:

- Restrict control system connections to the Internet; employ firewalls where Internet connections are absolutely required
- Deploy secure remote access methods such as Virtual Private Networks (VPNs) when remote access is required to any network
- Evaluate the risks posed by USBs and other portable media devices and develop policies and practices commensurate with the level of risk system owners are willing to assume
- Employ "least privilege" and separation of duty methods when configuring security for enterprise and control systems networks
- Remove, disable, or rename any default system accounts (where possible)
- Implement account lockout policies to reduce the risk from brute forcing attempts
- Implement policies requiring the use of strong passwords[d]
- Monitor the creation of and access to administrator level accounts by third-party vendors
- Implement logging and system monitoring techniques for network devices and traffic
- Establish a baseline dataset for network configuration and typical traffic; this allows for more effective identification of intrusions.

Organizations should follow established internal procedures if any suspected malicious activity is observed and report the findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program provides numerous recommended practices[e] for control systems on the US-CERT website. Several relevant recommended practices are available for reading or downloading, including "*Developing an Industrial Control Systems Cybersecurity Incident Response Capability.*"[f]

d. NIST, http://csrc nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

e. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

f. ICS-CERT, "Developing an Industrial Control Systems Cybersecurity Incident Response Capability," http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf

STUXNET SPECIFIC RESOURCES

For more information on Stuxnet and the mitigations available, ICS-CERT recommends the following reports:

- Symantec Report "W32.Stuxnet Dossier.[g]" This comprehensive report provides a full analysis of the malware including the attack scenario and timeline, infection statistics, malware architecture, description of all the exported routines, injection techniques and anti-AV, the RPC component, propagation methods, command and control feature, and the PLC component.
- ICS-CERT Stuxnet Indicators Advisory, "ICSA-10-272-01—Primary Stuxnet Indicators.[h]" This advisory contains malware indicators that can assist with detecting the presence of Stuxnet on compromised PLCs and computers.
- ICS-CERT Mitigations Advisory, "ICSA-10-238-01B-Stuxnet Malware Mitigation.[i]" This advisory contains a summary of the mitigation measures available to protect against, identify, and remove the malware.

Organizations are encouraged to contact ICS-CERT for assistance with confirming a Stuxnet infection, diagnosing the extent of the infection, and for assistance with mitigation efforts. Organizations can call ICS-CERT at 877-776-7585 or email ics-cert@dhs.gov to report possible Stuxnet infections and to request assistance.

For Control System Security Program Information and Incident Reporting: www.ics-cert.org

g. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
h. http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf
i. http://www.us-cert.gov/control_systems/pdf/ICSA-10-238-01B.pdf