ICS-CERT MONTHLY MONITOR

April 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

Contact Information

For any questions related to this report or to contact ICS-CERT:

E-mail: ics-cert@hq.dhs.gov

Toll Free: 1-877-776-7585

For Control Systems Security Program (CSSP) Information and Incident Reporting:

http://www.ics-cert.org

INCIDENT RESPONSE ACTIVITY IN MARCH

GAS PIPELINE CYBER INTRUSION CAMPAIGN

In March, ICS-CERT identified an active series of cyber intrusions targeting natural gas pipeline sector companies. Various sources provided information to ICS-CERT describing targeted attempts and intrusions into multiple natural gas pipeline sector organizations. Analysis of the malware and artifacts associated with these cyber attacks has positively identified this activity as related to a single campaign with spear-phishing activity dating back to as early as December 2011. Analysis shows that the spear-phishing attempts have targeted a variety of personnel within these organizations; however, the number of persons targeted appears to be tightly focused. In addition, the e-mails have been convincingly crafted to appear as though they were sent from a trusted member internal to the organization.

ICS-CERT has issued an alert (and two updates) to the US-CERT Control Systems Center secure portal library and also disseminated them to sector organizations and agencies to ensure broad distribution to asset owners and operators. ICS-CERT Alerts are intended to provide early warning indicators of threats and vulnerabilities for the community to act upon quickly. While ICS-CERT strives to make as much information publicly available as possible, the indicators in these alerts are considered sensitive and cannot be disseminated through public or unsecure channels. ICS-CERT will continue to issue updates as new information is uncovered.

ICS-CERT is currently engaged with multiple organizations to provide remote and onsite analytic assistance to confirm the compromise, extent of infection, and assist in removing it from networks. ICS-CERT does NOT recommend enabling the intrusion activity to persist within networks and has been working aggressively with affected organizations to prepare mitigation plans customized to their current network security configurations to remove the threat and harden networks from re-infection.

In addition, ICS-CERT recently conducted a series of briefings across the country to share information related to the intrusion activity with oil and natural gas pipeline companies. These briefings provided additional context of the intrusions and mitigations for detecting and removing the activity from networks. ICS-CERT will continue to work with private sector and government partners to respond to this and other cyber threats.

Combating sophisticated attacks are challenging for any company and therefore, ICS-CERT is working with partners to evaluate a more strategic and layered approach to detecting and mitigating these threats. ICS-CERT is also preparing additional mitigation information that will be released in an upcoming Advisory. Until then, ICS-CERT continues to recommend Defense-in-Depth practices and educating users about social engineering and spear-phishing attacks. Organizations are also encouraged to review ICS-CERT's Incident Handling Brochure for tips on preparing for and responding to an incident.

Asset owners/operators who would like access to the portal or to the alerts can contact ICS-CERT at ics-cert@dhs.gov. Alternatively, they can work with their sector Information Sharing and Analysis Center (ISAC) or sector source for cyber alerts and information sharing to obtain the ICS-CERT Alerts.

In this particular campaign, reporting organizations enabled ICS-CERT to analyze the data and create an overall view of the activity in progress. This would not have been possible without the active cooperation of the reporting organizations, so ICS-CERT commends those involved and requests continued private sector reporting whenever possible. ICS-CERT provides secure portal access to critical infrastructure asset owners and government agency personnel who are tasked with protecting critical infrastructure.

RISK MANAGEMENT PLAN FOR THE ELECTRICITY SECTOR—A SUMMARY

The Department of Energy (DOE) collaborated with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC) to release a second draft of the Electricity Sector Cybersecurity Risk Management Process (RMP) guideline. According to DOE, RMP has been designed to provide a consistent, repeatable, and adaptable process for the Electricity Sector that will help organizations proactively manage cybersecurity risk.

RMP was designed with the idea that the process should scale for use at organizations of any size and that cybersecurity risk management should be driven by the business needs of the company. Furthermore, the group responsible for creating RMP identified foundational concepts regarding technical security efforts, which are core to the success of enterprise cybersecurity risk management planning:

- The belief that cybersecurity risk is not just a technology problem but a business risk with the potential to cause any number of critical business impacts
- The idea that cybersecurity risk cannot be eliminated but must be managed through informed decision-making
- The need to incorporate cybersecurity risk management into the organizational enterprise risk management program.

Risk Management Model:

The RMP model represents a fairly standard strategic approach to breaking down business responsibilities for enterprise risk management. Responsibility for risk management is divided into three different business layers and their associated areas of business functionality:

- Organization—responsible for executive leadership
- Mission and business process—responsible for business management
- Information technology (IT) and industrial control system (ICS) teams—responsible for systems management.

The RMP model addresses a number of areas in which lack of clarity or attention can significantly impede enterprise risk management efforts. Use of such common roles in the RMP facilitates the integration of cybersecurity risk management into existing enterprise risk management programs as does the focus on aligning technical security needs with business operations and requirements. The RMP is very clear about the level of engagement required by people at each tier and how insufficient support disrupts the timing and sequence of critical, programmatic workflow.

Risk Management Life Cycle

The four stages of the risk management life cycle described in the RMP are also commonly defined steps in enterprise risk management programs.

- Framing—provides a framework by which technical risk to critical IT and ICS assets can be put into context with business and organizational needs, ensuring future risk identification and prioritization are considered holistically
- Assessment—is the primary process by which risks to business are identified and prioritized
- Response—defines how to address risk based on impact and risk tolerance rather than technical urgency
- Monitoring—completes the business improvement loop by ensuring the risk response addressed cybersecurity risk as planned.

RMP comprehensively addresses what each tier, or group in the risk management model, is responsible for during the individual stages of the risk management life cycle. The use of consistent work flow descriptions, i.e., the inputs, activities, and outputs, throughout the life cycle sections allows for consistency throughout RMP planning and implementation. Where inputs, activities, and outputs are called out, the RMP provides thorough explanation of what they are, how they fit into the RMP, and why they are significant.

Conclusion

DOE and its partners have done an excellent job of organizing and presenting the strategic tasks necessary to either integrating cybersecurity risk into existing risk management processes or creating a risk management function specific to cybersecurity. The clear and consistent mapping between the risk model and life cycle provides enough strategic planning information to make the pitch for leveraging RMP an easy one to enterprise risk management stakeholders. And, given its strategic focus, the RMP could be easily modified for use in other critical sectors as well as the electrical.

FROM THE TRENCHES–AN ICS TABLETOP EXERCISE

The conference room was heating up 3 months ago on a cold January day as law enforcement, a county emergency planner, and the staff for a small municipal utility dealt with cyber attacks on the utility's power generation, water, and wastewater control systems. Fortunately for the 25 participants, this was only a test; actually, it was table top exercise facilitated by Control Systems Security Program (CSSP) staff. The exercise tested the municipality's cybersecurity incident response plan with the specific objectives to:

- Test the staff's understanding of the policies and procedures for handling a cyber incident
- Review the effectiveness and suitability of the policies and procedures
- Evaluate coordination with federal, state, and local government
- Identify gaps and mitigations to the cyber response plan
- Educate–if it just doesn't look right–report it.

The facilitators, with the exercise play book in hand, released a series of "injects" or story lines throughout the day. The injects were designed to test the utility's response to internal and external cyber attacks on its control systems. The facilitators followed up with probing questions to generate discussions on how the participants would handle the topic at hand. A variety of subjects were covered, including the traditional cybersecurity issues of access control, remote access, perimeter defenses, logging, and auditing. The exercise also covered noninformation technology subjects. For example, one of the injects produced conversations on the human resources policies and procedures for dealing with an employee suspected of an internal cyber attack. Another inject forced the agency to think about recommended practices for handling local and national media coverage caused by disruption of services because of the cyber attack.

The participants then held "hot washes" that highlighted key points and takeaways following the completion of each scenario. The notes and hot washes were used by the utility's staff to develop an action plan.

Was it worth it? According to both the utility's security and safety specialists who were responsible for coordinating the exercise, it definitely was. As a result of the exercise, utility staff will review and update policies and procedures, mitigate identified security gaps, strengthen cyber defenses, and provide more cybersecurity training for the staff. But perhaps the most valuable benefit of the exercise was that it jump-started crucial conversations and interactions between stakeholders that will undoubtedly lead to a more secure environment for their ICSs.

According to the security specialist, "The tabletop was a way for us to put our heads together and collaborate on how we would handle specific, realistic cybersecurity incidents. With the expertise of the DHS CSSP staff that created the scenarios and injects, we were forced to work together and talk through what we are doing already and where we have more work to do. Incident response is critical. During a real incident, you don't want to discover major gaps in policy/procedure and/or technology tools. In addition, the collaboration that occurred during the day of the tabletop helps us all to understand the roles and responsibilities that each of us have in situations such as those we worked through for the tabletop exercise. My hope is that we could do a tabletop exercise like this on a recurring basis so that the participants continue to improve our incident response capabilities and security posture. Lastly, the tabletop gives everyone the opportunity to build relationships with DHS CSSP, FBI, state/local law enforcement and others; which is a huge win. If - or more likely when- an incident is going down, that is not the time I want to be introducing myself for the first time to the people who are equipped to help us get through it as quickly and efficiently as possible."

Are you interested in conducting a table top exercise to test your organization's response to a cyber attack on your ICS? If so, here are a few tips for organizing the exercise:

- Identify the goals and objectives for the exercise, for example testing an incident response plan
- Develop relevant and realistic scenarios and injects to achieve those goals and prepare a situation manual or play book documenting the scenario
- Prepare briefing slides for guiding the participants through the exercise
- Generate a facilitator handbook that provides instructions to guide the facilitator during the exercise, capture information and document action items, and develop an Action Report/ Plan
- Invite all crucial stakeholders to the exercise including technical and nontechnical staff and managers
- Select a facilitator that will draw out comments from all participants and a scribe who will capture the key points of the exercise.

Want to learn more?

- Homeland Security Exercise and Evaluation Program (HSEEP) website information on establishing an exercise program for all types of disasters https://hseep.dhs.gov/pages/1001_HSEEP7.aspx
- Tabletop Exercises for Incident Response Plans Under NERC Reliability Standard CIP-008¾Good resource for setting up a cyber table top exercise http://www.us-cert.gov/control_systems/icsjwg/presentations/fall2010/Simon%20-%20Tabletop%20Exercise%20Webinar.pdf
- Creating Cyber Forensics Plans for Control Systems–CSSP Recommend Practices http://www.us-cert.gov/control_systems/practices/documents/Forensics_RP.pdf
- Developing an Industrial Control Systems Cybersecurity Incident Response Capability–CSSP Recommended Practices http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf

If you have questions or want more information on conducting a table top exercise for your ICS please contact us at cssp@hq.dhs.gov.

a. CSSP Recommended Practice, http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf, website last accessed April 17, 2012.

PLANNING FOR A CYBER INCIDENT?

The best cyber defense mechanisms cannot prevent all cyber incidents. Even with well-trained staff, properly configured firewalls, current antivirus systems, and a solid network, a cyber attack could still be successful. Therefore, proper planning and preparation are invaluable to respond to and recover from a cyber incident.

Organizations without an existing incident response capability should consider establishing one. To aid control systems owners and operators, the CSSP has prepared a *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*.[a]

Even without a detailed and complete response plan, organizations can familiarize themselves with some basic concepts and actions that will make for a more effective incident response if and when a cyber compromise occurs.

Detection of Compromise

The ability to detect and identify the source and analyze the extent of a compromise is crucial to rapid incident response, minimizing loss, mitigating exploited weaknesses, and restoring services. Detecting an incident early limits or even prevents possible damage to control systems and reduces the level of effort required to contain, eradicate, recover, and restore affected systems.

Many tools are available to assist with the detection of network and system compromises. Network traffic analysis tools, intrusion detection systems (IDSs), antivirus systems, and real-time log analysis (including security information and event management [SEIM] systems) combine to aid in detecting malware, intrusion attempts, policy violations, exploitation, and component failure.

ICS-CERT releases indicators of compromise, when available, to assist critical infrastructure asset owners and operators in the detection of compromise by known attackers. In addition, ICS-CERT provides analytic services to companies requesting support in response to an incident. ICS-CERT is able to analyze hard drives, log files, malware, and other artifacts and provide detailed indicators/analysis reports to assist organizations in detecting and mitigating malicious activity.

The following different types of indicators are commonly provided by ICS-CERT through analysis and reports:

- IP addresses
- Domain names
- Web browser user agent strings
- File hashes
- File names
- E-mail addresses
- E-mail subject lines.

Using this information, network administrators should be able to identify which internal hosts have communicated with which IP addresses or domains and what type of traffic was generated. Domain Name Service (DNS) queries, e-mail activity, and the presence of specific files on systems are all detection capabilities that asset owners are encouraged to develop.

Preserving Forensic Data

Other critical components of incident response are forensic data collection, analysis, and reporting. These elements are essential to preserving important evidence. To avoid the loss of essential forensic data, the following activities should be conducted:

- Keep detailed notes of what is observed, including dates/times, mitigation steps taken/not taken, device logging enabled/disabled, and machine names and IP addresses for suspected compromised equipment.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a machine from the network you suspect is compromised.
- Capture forensic images of the system memory and hard drive prior to powering down the system.
- Avoid running antivirus software "after the fact" as the antivirus scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.
- Avoid making changes to the operating system or hardware, including updates and patches, as they will overwrite important information about the suspected malware.

Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts. Control system environments have special needs that should be evaluated when establishing a cyber forensic plan. ICS-CERT recommends the following source on Control System forensics:

- Recommended Practice: Creating Cyber Forensics Plans for Control Systems, Department of Homeland Security, 2008.[b]

Reporting and Coordination

When an incident is suspected, working with ICS-CERT can enhance an organization's ability to detect and understand the problem. CSSP and ICS-CERT encourage organizations to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Reporting both suspected and known incidents assists ICS-CERT with tracking and correlation against other incidents.

b. CSSP Recommended Practice, www.uscert.gov/control_systems/pdf/Forensics_RP.pdf, website last accessed April 17, 2012.

CSSP NEWS

Join ICS-CERT on the US-CERT Secure Portal

One of the best kept secrets in the critical infrastructure world is the existence of the US-CERT secure portal, a web-based platform that provides a mechanism for secure, unclassified information exchange between government agencies and the private sector asset owners and operators that comprise the nation's critical infrastructure.

The portal includes many subcompartments for different stakeholder groups. Of those, the Control Systems Center (the CS compartment) is the place where ICS-CERT publishes sensitive but unclassified documents related to critical infrastructure cybersecurity (alerts, advisories).

The portal includes a library, secure messaging, and a number of other collaboration tools. The ICS-CERT organization makes significant use of both the Library area and the Secure Messaging system.

Library

ICS-CERT regularly publishes advisories and alerts of special interest to ICS asset owners and operators to the portal Library.

ICS-CERT maintains a portal library folder specifically for "Advisories and Reports" and another folder specifically for the ICS-CERT "Weekly Digest" product (only available through the portal Library).

Secure Messaging

Secure messaging is particularly helpful for asset owners who want to transmit sensitive data to ICS-CERT, whether vulnerability-related or for incident-related analysis. ICS-CERT also uses the Secure Messaging system to notify all active CS compartment members when posting a new product to the Library and/or to the public website.

ICS-CERT encourages U.S. asset owners and operators to join the CS compartment of the US-CERT secure portal. Simply send an email message with your name, e-mail address, and company or agency affiliation to:
ics-cert@hq.dhs.gov.

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-12-068-01 - Solar Flare Alert"

Alert "ICS-ALERT-12-065-01 - xArrow Multiple Vulnerabilities"

ADVISORIES

Advisory "ICSA-12-081-01 - Invensys Wonderware System Platform Buffer Overflows"

Advisory "ICSA-12-088-01 - Rockwell Automation FactoryTalk RNADiagReceiver-DOS vulnerability"

Advisory "ICSA-12-083-01 - Ecava IntegraXor ActiveX Directory Transversal"

Advisory "ICSA-12-079-01 - Microsoft Remote Desktop Protocol Memory Corruption Vulnerability"

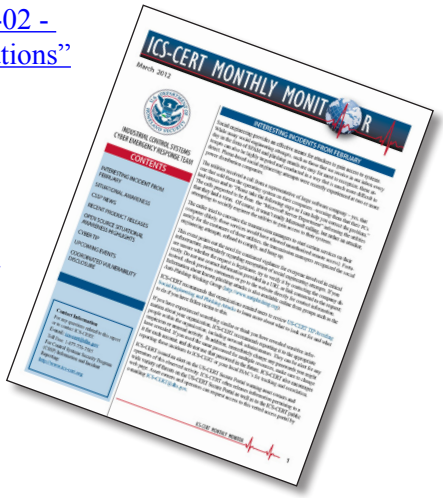
Advisory "ICSA-12-032-01 - GE Proficy Historian ihData-Archiver"

Advisory "ICSA-12-032-03 - GE Proficy Portal"

Advisory "ICSA-12-032-02 - GE Proficy Plant Applications"

OTHER

The ICS-CERT Monthly Monitor March 2012 issue includes highlights of activities from February 2012.



OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

ICS-CERT compiles this section from multiple resources including current events as disclosed on websites, blogs, mailing lists, and at conferences. ICS-CERT does not endorse the opinions or comments stated in these articles, nor has the US Department of Homeland Security (DHS) independently verified the technical information included. The links provided were confirmed at the time of data capture. ICS-CERT is not responsible for broken or nonfunctioning URLs.

Cybersecurity Bill: Vital Need Or Just More Rules?
2012-03-22
The Homeland Security Department's Control System Security Program facilities in Idaho Falls, Idaho, are intended to protect the nation's power grid, water, and communications systems. U.S. security officials and members of Congress are convinced a new law may be needed to promote improved cyber defenses at critical facilities.
http://www.npr.org/2012/03/22/149099866/cybersecurity-bill-vital-need-or-just-more-rules

U.S. Nukes Face Up to 10 Million Cyber Attacks Daily
2012-03-20
The head of the National Nuclear Security Administration says America's nuclear weapons face a massive number of cyber attacks every day, and are calling for a budget increase in order to enhance security.
http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily

To hackers, government users are phish in a barrel
2012-03-19
Government networks are being targeted increasingly by hacktivists, nation-states and other malefactors, and the most common means of successful attacks, by a wide margin, is phishing.
The United States Computer Emergency Readiness Team, which collects security incident reports from federal, state and local government agencies, processed 107,655 incident reports in 2011, 43,889 of them involving federal agencies.

And more than half of those reports — 55,153, or 51.2 percent — came from phishing, which has become hackers' favorite way of getting a foot into the door of a network.
http://gcn.com/articles/2012/03/19/phishing-goverment-cyber-attacks-us-cert.aspx
http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf

Effects of Geomagnetic Disturbances on the Bulk Power System
2012-03-16
Understanding the effects of GMD (geomagnetic disturbance) on bulk power systems and the ability of the industry to mitigate their effects are important to managing system reliability.
http://www.nerc.com/files/2012GMD.pdf

New Interest in Hacking as Threat to Security
2012-03-13
During the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago.
http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html

Ron Ross on Revised Security Controls
2012-03-13
"The fundamentals of cyber security - I call it the physics of security - don't change over time," National Institute of Standards and Technology Senior Fellow Ron Ross says in a video interview with Information Security Media Group. "How we apply those controls ... is a little bit different, but the same fundamentals."
NIST last month published a draft of Special Publication 800-53 Revision 4: Security and Privacy Controls for the Federal Information Systems and Other Organizations, which was written by a team of institute computer scientists led by Ross
http://www.govinfosecurity.com/articles.php?art_id=4572
http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

Feds Simulate Crippling Cyber Security Attack On NYC Electricity
2012-03-08
Senators and agencies participate in exercise, which simulated how the government might respond in the event of a cyber attack on New York's electricity supply during a summer heat wave.
http://www.informationweek.com/news/government/security/232602280

RSA 2012: Aging industrial control systems increasingly vulnerable to cyber attack
2012-03-07
Aging industrial control systems that run US critical infrastructure are at increasing risk of cyber attacks, warned Donald Purdy, chief cyber security strategist at CSC and former cyber official at the Department of Homeland Security (DHS).

"These are older systems so they are harder to control. And for convenience and cost savings, people have connected them to the internet in order to control them from remote locations. So this is almost a perfect storm in terms of vulnerability because the nation is so dependent on these systems," Purdy said in an interview with Infosecurity at last week's RSA Conference in San Francisco.
http://www.infosecurity-magazine.com/view/24384/

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

NIST fills some gaps in smart-grid standards
2012-03-05
The National Institute of Standards and Technology has added 22 technical standards in its updated roadmap for smart-grid interoperability and security.
http://gcn.com/articles/2012/03/05/nist-smart-grid-framework-update.aspx

The Bright Side of Being Hacked
2012-03-04
Despite the arrests of dozens of suspected members of Anonymous and its offshoots worldwide, it is far from diminished. Nor have most of its corporate targets been irreparably damaged by the attacks.

Rather, what Anonymous has done, experts said at the big RSA computer security conference here last week, is raise the alarm about the unguarded state of corporate computer systems.
http://www.nytimes.com/2012/03/05/technology/the-bright-side-of-being-hacked.html

DHS, Not NSA, Should Lead Cyber security, Pentagon Official Says
2012-03-01
In the midst of an ongoing turf battle over how big a role the National Security Agency should play in securing the nation's critical infrastructure, a Defense Department official asserted on Wednesday that the military's controversial intelligence agency should take a backseat to the Department of Homeland Security in this regard.

"Obviously, there are amazing resources at NSA, a lot of magic that goes on there," said Eric Rosenbach, deputy assistant secretary of Defense for Cyber Policy in the Department of Defense. "But it's almost certainly not the right approach for the United States of America to have a foreign intelligence focus on domestic networks, doing something that throughout history has been a domestic function."
http://www.wired.com/threatlevel/2012/03/rsa-security-panel/
http://gcn.com/articles/2012/03/02/cyber-eye-nsa-oversee-domestic-cybersecurity.aspx

Security to Industry: Time to Wake Up
2012-02-29
The past two years have been a real wakeup call for the industrial automation industry. For the first time ever there is proof the industry has been the target of sophisticated cyber attacks like Stuxnet, Night Dragon and Duqu.

After the realization of targeted attacks came the next step and that was a huge number of security vulnerabilities exposed in industrial control products and regulatory agencies are demanding compliance to complex and confusing regulations. Cyber security has quickly become a serious issue for professionals in the process and critical infrastructure industries.
http://www.isssource.com/security-to-industry-time-to-wake-up/
http://www.isssource.com/wp-content/uploads/2012/02/022912WP-7-Steps-to-ICS-Security-v1.0.pdf

Tracking Down Advanced Threats In Your Network
2012-02-29
If you had an advanced attacker in your network, would your security team know it? At the RSA Conference, HBGary's Greg Hoglund shared four ways to defend against pernicious attacks
http://www.darkreading.com/advanced-threats/167901091/security/security-management/232601808/

Device Hacking Continues: Medtronic, Others 'Lacked Foresight'
2012-02-29
These high-profile hacks of medical devices by Jack and Radcliffe, for example, certainly make for gripping presentations and stories. But they've also proven to be extremely polarizing. On the positive side, they help to initiate change, applying ample pressure on manufacturers to examine potential security vulnerabilities and address them for next-generation devices. They also help the companies in identifying some of these vulnerabilities.

On the other side of the coin, however, they are causing unnecessary public panic among some insulin pump users despite a low likelihood of a hacking event actually occurring. Furthermore, this glamorization of medical device hacking could potentially have the effect of actually inspiring a real-world medical device hacking attempt. Critics even go so far as to admonish the professional hackers for providing a blueprint of sorts and ideas for maliciously breaching device security.
http://www.qmed.com/mpmn/medtech-pulse/device-hacking-continues-medtronic-others-lacked-foresight

We Want to Hear from You

A key aspect of our mission is providing relevent and timely cybersecurity information products and services to ICS stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we cn work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to ics-cert@hq.dhs.gov.

UPCOMING EVENTS

May

ICSJWG Spring Conference
May 7–10, 2012
Hyatt Regency Savannah
Savannah, Georgia
Conference Information
Registration

ICSJWG Conference Training
Introductory Training: Introduction to Control Systems Cyber Security (Course 101, 8 Hours)
May 10, 2012
Hyatt Regency Savannah
Savannah, Georgia
Course Description
Registration

International Community Advanced Training: Control Systems Cyber Security Advanced Training and Workshop (1 week)
May 14-18, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

NESCO Town Hall Security Risk Management Practice for Electrical Utilities
May 30–31, 2012
New Orleans Marriott
New Orleans, Louisiana
Contact Info: Abbie Trimble, abbie@ energysec.org
http://nescotownhall2012.eventbrite.com/

NERC CIP Compliance Training
May 24–10, 2012
Newark Liberty International Airport Marriott
Newark, New Jersey
Contact Info: Abbie Trimble, abbie@ energysec.org
http://cipcompliance-newark.eventbrite.com/

June

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop (1 week)
June 18-22, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

July

NERC CIP Compliance Training
July 12, 2012
Minneapolis Airport Marriott
Minneapolis, Minnesota
Contact Info: Abbie Trimble, abbie@ energysec.org,
http://cipcompliance-minneapolis.eventbrite.com/

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop (1 week)
July 16-20, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

October

NERC CIP Compliance Training
October 25, 2012
SpringHill Suites, Las Vegas Convention Center
Las Vegas, Nevada
Contact Info: Abbie Trimble, abbie@ energysec.org
http://cipcompliance-lasvegas.eventbrite.com/

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the "ICS-CERT Monthly Monitor" approximately 12 times per year. Generally, each issue includes information collected in the previous 28 to 31 days.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT web page at: http://www.us-cert.gov/control_systems/ics-cert/.

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at: ics-cert@hq.dhs.gov

What is ICS-CERT?

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to:

- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The "ICS-CERT Monthly Monitor" offers a means of promoting preparedness, information sharing, and collaboration with the 18 critical infrastructure/key resource (CIKR) sectors. ICS-CERT accomplishes this on a day-to-day basis through sector briefings, meetings, conferences, and information product releases.

This publication highlights recent activities and information products affecting industrial control systems (ICS), and provides a look ahead at upcoming ICS-related events.

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. This coordinated disclosure process ideally allows time for a vendor to develop and release patches and for users to test and deploy patches prior to public disclosure of the vulnerability. While this process is not always followed for a variety of reasons, ICS-CERT continues to strive for this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@hq.dhs.gov or toll free at 1-877-776-7585.

Notable Coordinated Disclosure Researchers in March 2012.

ICS-CERT appreciates having worked through the coordinated disclosure process with the following researchers:

- Celil Unuver from SignalSec Corp, ICSA-12-081-01 Invensys Wonderware System Platform Buffer Overflows, March 30, 2012.
- Luigi Auriemma, ICSA-12-088-01-Rockwell Automation FactoryTalk RNADiagReceiver DoS Vulnerabilities, March 28, 2012.
- Billy Rios and Terry McCorkle , ICSA-12-083-01 Invensys Integraxor ActiveX Directory Traversal, March 23, 2012.
- Luigi Auriemma through ZDI, ICSA-12-079-01-Microsoft Remote Desktop Protocol memory Corruption Vulnerability, March 19, 2012.
- Luigi Auriemma through ZDI, ICSA-12-032-01-GE Intelligent Platforms Proficy Historian Data Archiver Memory Corruption Vulnerability, March 13, 2012.
- Luigi Auriemma through ZDI, ICSA-12-032-03-GE Intelligent Platforms Proficy Real-Time Information Portal Directory Traversal, March 13, 2012.
- Luigi Auriemma through ZDI, ICSA-12-032-02-Multiple Memory Corruption Vulnerabilities in Proficy Plant Applications, March 13, 2012.

Researchers Currently Working with ICS-CERT in 2012

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Luigi Auriemma
Joel Langill
Rubén Santamarta
Dillon Beresford
Eireann Leverett
Secunia
Yun Ting Lo (ICST)
Justin W. Clarke
Kuang-Chun Hung (ICST)
Terry McCorkle
Shawn Merdinger
Celil Unuver
Knud Erik Højgaard (nSense)
Billy Rios
Greg MacManus (iSIGHT Partners)
Alexandr Polyakov
Carlos Mario Penagos Hollmann
Alexey Sintsov
Adam Hahn
Manimaran Govindarasu
Jürgen Bilberger
Reid Wightman