ICS-CERT MONTHLY MONITOR

June/July 2012

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INCIDENT RESPONSE ACTIVITY

SITUATIONAL AWARENESS

CSSP NEWS

NCCIC NEWS

RECENT PRODUCT RELEASES

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

UPCOMING EVENTS

COORDINATED VULNERABILITY DISCLOSURE

Contact Information

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

Email: 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

GAS PIPELINE CYBER INTRUSION CAMPAIGN—UPDATE

ICS-CERT continues to gather information on the recent Oil and Natural Gas (ONG) pipeline intrusion campaign. This campaign, as first outlined in the April issue of the Monthly Monitor, refers to an active series of cyber intrusions targeting natural gas pipeline sector companies.

Recent reports and analysis conducted by ICS-CERT indicate that information pertaining to the ICS/SCADA environment, including data that could facilitate remote unauthorized operations, has been exfiltrated as part of this campaign. Despite this, ICS-CERT has not received any reports of unauthorized access into the ICS environment; however, this may be due to limited monitoring and intrusion detection capabilities in the targeted companies control networks. The intent of the attackers remains unknown.

ICS-CERT recently issued an update to the original advisory (ICSA-12-136-01BP) with new information, indicators, and updated malware characterization. This advisory is available to asset owners/operators who have portal accounts in the Control Systems Center on the US-CERT secure portal (https://portal.us-cert.gov). Asset owners/operators can request a portal account by sending an email to: ics-cert@hq.dhs.gov.

INTRUSION CAMPAIGN—ONSITE SUPPORT

ICS-CERT has provided extensive remote and onsite support and technical guidance to a number of companies targeted by the intrusion campaign. In this Monitor, we highlight two of the onsite incident response deployments that were conducted in May and June.

May

In May, ICS-CERT provided onsite assistance to an energy company targeted in the ONG pipeline campaign. Prior to the onsite visit, the asset owner provided ICS-CERT with firewall logs, samples of the spear phishing emails, and hard drive images from the targeted systems for offsite analysis. Although the initial analysis of asset owner artifacts indicated that the attempted compromise was not successful, the asset owner requested an onsite visit by ICS-CERT.

In addition to providing ICS-CERT with artifacts, the company decided to temporarily disconnect its control systems from all other networks, including the business network. The asset owner had initially assessed the control system disconnection as infeasible; however, closer inspection of actual user needs confirmed that real-time access was not required and manual daily data transfers would serve company needs. Ultimately, the company has decided to keep their control systems network disconnected indefinitely.

While onsite ICS-CERT provided guidance and recommendations for improving the company's overall cybersecurity posture as well as a threat briefing for company executives. ICS-CERT also conducted a CSET evaluation to help the company assess their security posture.

June

In June, ICS-CERT provided onsite assistance to a manufacturing company that detected intrusion activity related to the ONG pipeline campaign.

ICS-CERT onsite analysis included a search for host-based and network-based indicators to identify additional hosts for further analysis. ICS-CERT hashed files from approximately 1700 machines and compared them to hashes of known malicious files and examined proxy logs to identify any suspicious network activity. ICS-CERT discovered some indicators of compromise in the network logs and identified the hosts that made the requests.

At the end of the onsite visit, the company provided ICS-CERT with a complete database dump of logging data and forensic images from an additional five machines for further analysis. Since the onsite visit, the company has reported receiving additional spear-phishing emails and has coordinated them with ICS-CERT for follow on analysis. Incident response activities for this company are ongoing.

Common Onsite Activities

In both onsite cases, ICS-CERT performed the following activities at the customers' facilities:

- Reviewed the corporate and ICS network/communications architecture and provided guidance on reducing risk footprint.
- Discussed the company's connection points between the corporate and ICS networks and strategies to reconfigure systems in a more defensible manner.
- Delivered a high-level threat briefing to technical staff and senior management with a focus on how spear-phishing campaigns are conducted, and how policies, people, and procedures impact incident response.

Conclusion

Combating sophisticated attacks is challenging for any organization. For that reason, ICS-CERT works with the community to develop more strategic and layered approaches to detecting and mitigating these threats.

ICS-CERT continues to recommend defense-in-depth practices and to educate users about social engineering and spear-phishing attacks. In addition, ICS-CERT recently released an update to its Targeted Cyber Intrusion Mitigation Strategies (ICS-TIP-12-146-01A) in response to this specific campaign. Readers are also encouraged to review the ICS-CERT Incident Handling Brochure for tips on preparing for and responding to an incident.

ICS-CERT INCIDENT SUMMARY REPORT

The ICS-CERT Incident Summary Report was released on June 28, 2012 summarizing incident response activities, trends, and analysis from 2009 through 2011. Since its inception in 2009, ICS-CERT has made a consistent effort to develop trusted relationships with public and private sector partners and to help asset owners and operators establish policies and controls that prevent incidents. The report depicts a sharp increase in reported incidents, partly due to increased communication with partners and increasing awareness of the threats targeting ICS owners and operators.

Full visibility into the number and types of incidents impacting critical infrastructure and key resources (CIKR) is difficult; this report reflects only a limited view of actual incidents occurring, as observed by ICS-CERT. The majority of CIKR is privately owned and cyber incident reporting to ICS-CERT is voluntary.

As a result, ICS-CERT relies on relationships with CIKR owners and other private and governmental partners to promote cyber

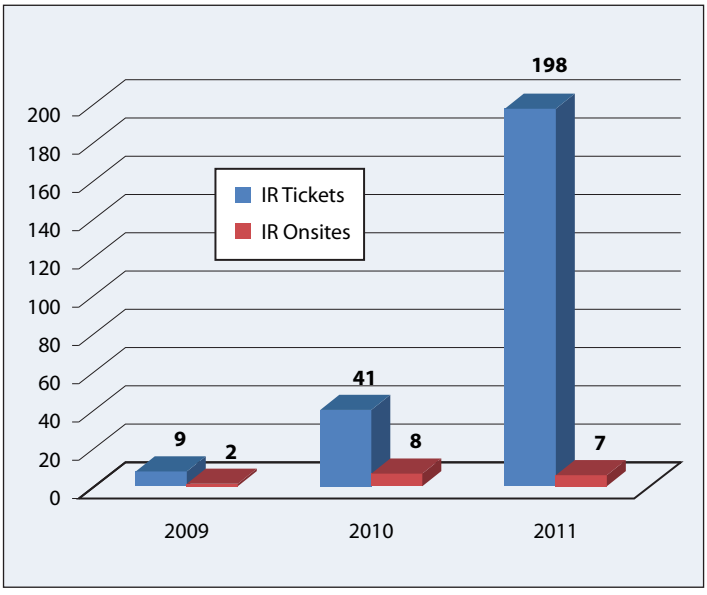


Figure 1. ICS-CERT incident response trends data.

incident reporting and information sharing. Those relationships have strengthened significantly through a variety of outreach activities and situational awareness products; incident reporting has increased accordingly.

ICS-CERT receives incident reports in a variety of ways:

1. An asset owner self-reports a cyber incident directly to ICS-CERT.
2. ICS-CERT is notified by a trusted third party i.e., law enforcement, the IC, a sector-specific agency, or the researcher community.
3. ICS-CERT locates information of concern in open source channels and reports it back to the asset owner for awareness and validation.

While much progress has been made in the ICS community to identify, report, and respond to cyber activity involving CIKR assets, much remains to be done. ICS-CERT encourages that asset owners and operators report cyber incidents for tracking, correlation, and support.

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.

A DAY IN THE LIFE OF AN ICS-CERT INCIDENT HANDLER

We wrote above about the Incident Summary Report and the ways in which ICS-CERT receives notification of an incident. In this segment, we will take a look into a day in the life of an ICS-CERT incident handler.

ICS-CERT operations exist in two geographically dispersed centers; at the Cybersecurity Operations Center (CSOC) in Idaho Falls, ID, and at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, VA.

When ICS-CERT receives notification of an incident, the watch officer creates a ticket for response tracking and assigns an incident handler to the case. The incident handler then becomes the company's primary contact within ICS-CERT to provide consistent communications for the duration of the response effort.

The incident handler works with the victim entity to gather all available information about the incident and develop a mitigation plan to assist with recovery efforts. Sometimes this plan includes the analysis of digital artifacts (drive and memory images, logs, malware, etc.). The incident handler helps to facilitate transfer of artifacts to the Advanced Analytical Laboratory (AAL) for analysis. The ICS-CERT AAL team analyzes the data to validate the incident and to identify any additional indicators that the victim can use for detection and defensive purposes. The AAL produces indicator reports and digital media analysis reports from the analyzed data, and provides those reports directly to the affected entity (all data is protected under the DHS Protected Critical Infrastructure Information (PCII) program).

ICS-CERT strives to provide expert guidance to assist organizations in addressing cybersecurity incidents and strengthen their overall cybersecurity posture. This guidance can, at the request of the organization and when the situation merits, include the deployment of an onsite incident response team. An onsite response team generally includes ICS-CERT cyber analysts, control system subject matter experts, and an onsite team lead. In cases where law enforcement is involved, the team coordinates closely with the appropriate agencies (i.e., local, state, federal) before, during, and following the onsite effort. When deployed, an incident response team mobilizes at the site to assist the victim entity with analysis and to provide mitigation strategies to help identify and eradicate the threat from networks.

After the onsite concludes, the incident handler coordinates ongoing assistance and analysis activities as needed to facilitate additional analysis reports and assistance to the organization. The watch officer closes the ticket for an incident only after ICS-CERT has completed analysis, prepared and delivered written reports, discussed the results with the affected entity, and determined that the asset owner needs no additional support.

No two incidents are completely alike; incident handlers must closely coordinate with the affected entity to determine the level of attention and resources necessary to effectively resolve the situation.

For more information on incident response or services offered by ICS-CERT, contact ICS-CERT toll-free at 1-877-776-7585, or visit us on our Web page: http://www.us-cert.gov/control_systems/ics-cert/.

Follow ICS-CERT on Twitter: http://twitter.com/icscert

WIDESPREAD WEAK KEYS IN NETWORK DEVICES

Recently, ICS-CERT coordinated with researchers from the University of Michigan (UM) and the University of California at San Diego (UCSD) concerning vulnerabilities in SSH and SSL encryption certificates. The researchers, Nadia Heninger (UCSD), and Zakir Durumeric, Eric Wustrow, and J. Alex Halderman (all UM), recently published a paper titled "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices." The project was supported by the National Science Foundation (NSF), Air Force Research Laboratory, and a NSF Graduate Research Fellowship.

The researchers scanned the Internet for devices performing a SSH and SSL handshake and logging the certificate exchanges. They found a large number of discoverable devices that had either reused encryption keys or certificates, or that lacked adequate entropy to generate sufficiently random keys. Their study took into account both RSA and DSA keys. The researchers plan to present their findings at the 21st USENIX Security Symposium in August 2012.

Their study clustered and investigated vulnerable hosts, finding that the vast majority appeared to be headless or embedded devices. This vulnerability could be applicable to industrial control systems that use entropy at startup to generate their encryption keys. When there is insufficient entropy at the startup of a device, the keys can be factored or discovered whereby an attacker can use a Man-in-the-Middle attack to send messages or execute remote code on the affected device. In addition, some devices use duplicate keys and certificates that could be collected by the attacker and exploited by calculating other keys generated within the entropy pool.

ICS-CERT is currently coordinating with multiple vendors that could be affected by this vulnerability. ICS-CERT has previously released an advisory on the Innominate mGuard products that generated their RSA keys with inadequate entropy.

Mitigations for vendors include the following:

- Avoid using default keys or certificates.
- Ensure entropy sources are effective.
- Test cryptographic randomness of the complete device.

Mitigations for asset owners include the following:

- Replace default certificates and keys (where possible) with certificates and keys generated with sufficient entropy.
- Check for known weak keys.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

Vendors who believe their products might be affected by this vulnerability are encouraged to contact ICS-CERT for more information or assistance at: ICS-CERT@dhs.gov, or 1-877-776-7585.

DOE RELEASES RISK MANAGEMENT PROCESS GUIDELINE

The Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability, in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC), today released guidance to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks. The Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline, which provides a flexible approach to managing cybersecurity risks across all levels of the organization, was developed by a public-private sector team that was led by the Office of Electricity Delivery and Energy Reliability and included representatives from across the industry.

We Want to Hear from You

A key aspect of our mission is providing relevent and timely cybersecurity information products and services to industrial control system (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 can 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.

CSSP NEWS

ICSJWG 2012 FALL MEETING

Come to Denver this October! The ICSJWG 2012 Fall Meeting will be held at the Grand Hyatt Denver on October 15 – 18, 2012. The ICSJWG Fall Meeting is open to all members interested in learning about cybersecurity issues facing the Nation's critical infrastructure control systems. This is an excellent resource for government professionals (federal, state, local, tribal, and international); control system vendors and systems integrators; research, development, and academic professionals; and owners and operators (management, engineering, production, and IT). Meeting attendees will be able to discuss the latest initiatives impacting industrial control systems security and will have the opportunity to interact with colleagues and peers who are addressing the risks of threats and vulnerabilities to their systems.

There is no cost to attend the meeting sessions or any associated meetings and training. Travel, accommodations, meals, beverages, and other incidental expenses are the responsibility of the meeting participants and will NOT be covered by ICSJWG or the Control Systems Security Program (CSSP). To submit an abstract, or register for the meeting, please visit the ICSJWG site at: http://www.uscert.gov/control_systems/icsjwg/2012/fall/index.html

CATCH UP WITH CSSP

One of the main goals of the CSSP is to coordinate activities that reduce the risk of cyber attacks against crtical infrastructre control systems. So far this fiscal year, CSSP has provided briefs and presentations to over 9,600 attendees at 164 different conferences and meetings covering 15 critical infrastructure and key resources (CIKR) sectors for outreach and awareness purposes. Recent events include:

- Association of American Railroads (AAR) Annual Information Security Committee Meeting;
- 24th Annual Forum of Incident Response and Security Teams (FIRST) Conference;
- Lone Star Information Security Forum;
- Automation Summit 2012;
- International Society of Automation (ISA) Power Industry Division (POWID) Annual Symposium; and
- American Water Works Association (AWWA) Annual Conference and Exposition.

For onsite assessments, CSSP has completed 63 assessments across 11 of the CIKR sectors using the Cyber Security Evaluation Tool (CSET), a product that has been distributed to over 5,100 individuals in FY-12. CSSP has given 43 training sessions (Introductory, Intermediate, and Advanced), educating nearly 2,000 cybersecurity professionals who work in the industrial control systems community.

For more information on CSSP, downloading CSET, available trainings, and reviewing other services & products, please visit our Web site at http://www.us-cert.gov/control_systems/

NCCIC NEWS

DIRECTOR, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER—LARRY ZELVIN

Larry Zelvin has joined DHS, taking the helm as the Director of the National Cybersecurity and Communications Integration Center (NCCIC) in June 2012.

Mr. Zelvin's last assignment was at the White House National Security Staff (NSS) where he was the acting senior crisis manager during major events such as the 2010 Haitian earthquake, the 2010 BP Deepwater Horizon oil spill, and the 2011 Japanese earthquake, tsunami, and nuclear incident. He was also instrumental in the creation of a new inter-agency Cyber Response Group to meet the Cyberspace Policy Review requirement for a White House chaired cyber incident response policy group.

Mr. Zelvin is a retired U.S. Navy Captain and Naval Aviator with 26 years of active service, including command of a U.S. Navy squadron. He also served as a politico-military planner in the Joint Chief of Staff's Homeland Security Division, Strategic Plans and Policy Directorate (J-5) during the 9/11 attacks.

NCCIC MISSION

Many of our nation's essential services rely on cyber and communications networks, and threats on these networks are growing in number and sophistication. Due to the vast interconnectedness of cyber and communications technologies – from critical infrastructure, to private businesses, to the public sector, to consumers, it is critically important to share information at a national level, and to fully coordinate response activities.

On a 24x7, steady-state basis, the NCCIC fuses and coordinates information from:

- DHS operational elements, including:
  - U.S. Computer Emergency Readiness Team (US-CERT)
  - Industrial Control Systems Cyber Emergency Response Team, (ICS-CERT)
  - National Coordinating Center for Telecommunications (NCC)
  - DHS Office of Intelligence & Analysis
- Federal partners, such as the Department of Defense, Department of Justice, Federal Bureau of Investigation, U.S. Secret Service, and the National Security Agency
- State and local representation; and
- Private sector and non-government partners.

During a cyber or communications incident, the NCCIC serves as the national response center, able to bring the full capabilities of the federal government to bear, in a coordinated manner, with state, local, and private sector partners.

By integrating information from all partners—public and private, state and federal, in both the cyber and communications arenas—the NCCIC creates and shares a common knowledge, coordinates response activities, and protects our nation's critical networks.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

ICS-CERT compiles this section from multiple resources including current events as disclosed on Web sites, 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.

US industrial control system attack reports skyrocket

2012-06-29

US critical infrastructure providers are failing to implement adequate information security measures, according to the US Industrial Control System Cyber Emergency Response Team (ICS-CERT).

The security team, set up in 2009 under the Department of Homeland Security, received 198 security incident reports in 2011, a massive increase in from the 41 it received in 2010.

Despite the surge in incident reports, ICS-CERT's investigations uncovered just seven instances in 2011 where an organization suffered an intrusion, which was actually down from the eight it confirmed in 2010.

http://www.cso.com.au/article/429122/

http://abcnews.go.com/blogs/headlines/2012/06/when-stuxnet-hit-the-homeland-government-response-to-the-rescue/

http://fcw.com/articles/2012/07/02/ics-cert-report-cyber-attacks-skyrocket.aspx

DHS to give agencies free computer threat-detection packages
2012-06-26

The Homeland Security Department in 2013 expects to present each agency with what amounts to security-in-a-box for computers. The free, three-piece package will include near real-time threat sensors, a control panel for prioritizing fixes and consulting services to make all the pieces work together, DHS officials said.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

Under the department's proposal, $202 million in DHS funding would subsidize what Homeland Security calls "continuous monitoring as a service" at all federal offices. Officials made the announcement at a briefing for federal employees and contractors on Monday.

http://www.nextgov.com/cybersecurity/2012/06/dhs-give-agencies-free-computer-threat-detection-packages/56459/

Researchers Crack RSA SecurID Tokens, Extract Keys
2012-06-25

Researchers from Project-Team Prosecco have published a paper describing an attack method that can compromise cryptographic keys used in some of the leading authentication and access control products available on the market today.

http://www.infosecisland.com/blogview/21726-Researchers-Crack-RSA-SecurID-Tokens-Extract-Keys.html

Cyber Security Debate Pits Corporate Interests Against National Security
2012-06-25

National security is running headfirst into corporate and privacy interests. It is centering on two competing versions of cyber security legislation, which would either give government more power to regulate private, but vital, networks or which would make any new rules voluntary.

The networks in question are integral to the U.S. economy and are owned by private utilities and telecom operators. But if they are destroyed and cause massive upheaval, then the country's welfare is at stake. Business groups say that it is already in their interest to buck up whereas both the Obama and Bush administrations say that more is necessary and that national security is the foremost concern.

http://www.forbes.com/sites/kensilverstein/2012/06/25/cyber-security-debate-pits-corporate-interests-against-national-security/

Iran says detected "massive cyber attack:" state TV
2012-06-21

Iran has detected a planned "massive cyber attack" against its nuclear facilities, state television said on Thursday, after talks with major powers this week failed to resolve a row over Tehran's disputed nuclear activities.

Iran's Intelligence Minister Heydar Moslehi said the country's arch enemies, the United States and Israel, along with Britain, had planned the attack.

"Based on obtained information, America and the Zionist regime (Israel) along with the MI6 planned an operation to launch a massive cyber attack against Iran's facilities following the meeting between Iran and the P5+1 in Moscow," Iran's English-language Press TV quoted him as saying.

http://www.reuters.com/article/2012/06/21/us-iran-cyber-nuclear-idUSBRE85K1EA20120621

Hacked companies fight back with controversial steps: Some victims of hackers are retaliating with a full-on cyber assault
2012-06-19

Frustrated by their inability to stop sophisticated hacking attacks or use the law to punish their assailants, an increasing number of U.S. companies are taking retaliatory action.

Known in the cyber security industry as "active defense" or "strike-back" technology, the reprisals range from modest steps to distract and delay a hacker to more controversial measures. Security experts say they even know of some cases where companies have taken action that could violate laws in the United States or other countries, such as hiring contractors to hack the assailant's own systems.

In the past, companies that have been attacked have mostly focused on repairing the damage to their computer networks and shoring them up to prevent future breaches.

But as prevention is increasingly difficult in an era when malicious software is widely available on the Internet for anyone wanting to cause mischief, security experts say companies are growing more aggressive in going after cyber criminals.

http://today.msnbc.msn.com/id/47849023/ns/technology_and_science-security/#.T-Ho1vVEKuM

Downloading of software updates for lifesaving medical devices proves very dangerous
2012-06-19

When it comes to security, one of the scariest things out there sounds like science fiction and pertains to hacking implantable medical devices. Pacemakers and insulin pumps do help save lives, but they are vulnerable to lethal attacks; there are continued warnings that exploiting these medical devices will eventually cost someone their life. Here's a slightly different take on the scenario; you've heard of drive-by-downloads that can infect a machine with malware without the user agreeing to the automatic download, but how about serving up malware in software updates for medical devices such as ventilators?

http://blogs.computerworld.com/malware-and-vulnerabilities/20554/software-updates-lifesaving-medical-devices-found-tainted-malware

Attacks Targeting US Defense Contractors and Universities Tied to China
2012-06-13

UPDATE: Researchers have identified an ongoing series of attacks, possibly emanating from China, that are targeting a number of high-profile organizations, including SCADA security companies, universities and defense contractors. The attacks are using highly customized malicious files to entice targeted users into opening them and starting the compromise.

The attack campaign is using a series of hacked servers as command-and-control points and researchers say that the tactics and tools used by the attackers indicates that they may be located in China. The first evidence of the campaign was an attack on Digitalbond, a company that provides security services for ICS systems. The attack begins with a spear phishing email sent to employees of the targeted company and containing a PDF attachment. In Digitlbond's case, the file is called "Leveraging_Ethernet_Card_Vulnerabilities_in_Field_Devices.pdf.exe" and when it's opened, the file installs a Trojan downloader called spoolsvr.exe.

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS (Continued)

In addition to the attack on Digitalbond, researchers have found that the campaign also has hit users at Carnegie Mellon University, Purdue University and the University of Rhode Island. Also, the Chertoff Group, a consultancy headed by former secretary of Homeland Security Michael Chertoff, and NJVC, another defense contractor, have been targeted. Carnegie Mellon and Purdue both have high-profile computer security programs.

Moreover, this attack has strong similarities with other campaigns which were successfully compromising important US targets.

http://threatpost.com/en_us/blogs/attacks-targeting-us-defense-contractors-and-universities-tied-china-061312

http://blogs.csoonline.com/malwarecybercrime/2219/new-spear-phishing-campaign-targets-universities-government-contractors-and-security-companies

http://blog.ioactive.com/2012/06/old-tricks-new-targets.html?m=1

Flame authors order infected computers to remove all traces of the malware
2012-06-07

The creators of the Flame cyber-espionage threat ordered infected computers still under their control to download and execute a component designed to remove all traces of the malware and prevent forensic analysis, security researchers from Symantec said on Wednesday.

Flame has a built-in feature called SUICIDE that can be used to uninstall the malware from infected computers. However, late last week, Flame's creators decided to distribute a different self-removal module to infected computers that connected to servers still under their control, Symantec's security response team said in a blog post.

http://www.cio.com.au/article/427005/flame_authors_order_infected_computers_remove_all_traces_malware/

DOE: Twenty-One Steps to Improve SCADA Security
2012-06-05

Supervisory control and data acquisition (SCADA) networks contain computers and applications that perform key functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste treatment, transportation) to all Americans.

As such, they are part of the nation's critical infrastructure and require protection from a variety of threats that exist in cyber space today. By allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide great efficiency and are widely used.

http://www.infosecisland.com/documentview/21535-DOE-Twenty-One-Steps-to-Improve-SCADA-Security.html

http://www.infosecisland.com/download/index/id/95.html

DHS To Critical Infrastructure Owners: Hold On To Data After Cyber Attack
2012-05-29

The Department of Homeland Security Is Offering Organizations That Use Industrial Control Systems advice or mitigating the effects of cyber attacks. Among the agency's recommendations: hold on to data from infected systems and prevent enemies from moving within your organization.

DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published a technical paper on cyber intrusion mitigation strategies on Friday. The document calls on critical infrastructure owners to take a number of steps to thwart attacks, or limit the damage they cause; among them: improving their ability to collect and retain forensic data, and to detect attempts by attackers to move laterally within their organization.

http://threatpost.com/en_us/blogs/dhs-critical-infrastructure-owners-hold-data-after-cyber-attack-052912

Researchers Discover Hacker-Ready Computer Chips
2012-05-29

A pair of security researchers in the U.K. have released a paper [PDF] documenting what they describe as the "first real world detection of a backdoor" in a microchip—an opening that could allow a malicious actor to monitor or change the information on the chip.

These chips are used in an enormous variety of applications, including communications and networking systems, the financial markets, industrial control systems, and a long list of military systems.

http://blogs.scientificamerican.com/guest-blog/2012/05/29/researchers-discover-hacker-ready-computer-chips/

http://www.guardian.co.uk/technology/2012/may/29/cyber-attack-concerns-boeing-chip

Department of Energy Releases Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline
2012-05-23

The Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability, in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC), today released guidance to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks. The Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline, which provides a flexible approach to managing cybersecurity risks across all levels of the organization, was developed by a public-private sector team that was led by the Office of Electricity Delivery and Energy Reliability and included representatives from across the industry.

http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

UPCOMING EVENTS

July

Chemical Sector Security Summit
July 30–August 01, 2012
Baltimore, Maryland

August

GFIRST
August 19–24, 2012
GFIRST Conference
Atlanta, Georgia

September

American Water Works Association (AWWA) Water Security and Emergency Preparedness Conference & Exposition (WSEPC) 2012
September 9–12, 2012
Hilton St. Louis at the Ballpark
St Louis, Missouri

5th Annual National Dam Security Forum (in conjunction with the Association of State Dam Safety Officials (ASDSO) Dam Safety 2012
September 16–20, 2012
Colorado Convention Center
Denver, Colorado

3rd Annual Cybersecurity Summit
September 27, 2012
Ronald Reagan Building and International Trade Center
Washington, DC

October

Advanced Training (International Partners): Control Systems Cyber Security Advanced Training and Workshop (1 week)
October 8–12, 2012
Control Systems Analysis Center
Idaho Falls, Idaho
Course Description
Registration

ICSJWG 2012 Fall Meeting
October 15–18, 2012
Grand Hyatt Denver
Denver, Colorado
ICSJWG Fall 2012 Meeting Information
Registration

ICSJWG 2012 Fall Meeting—Intermediate Cybersecurity for Industrial Control Systems
October 18, 2012
Denver, Colorado
Course Description
Registration

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/

November

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (5 days)
November 5-9, 2012
Idaho Falls, ID
Course Description
Registration

December

Advanced Training: Control Systems Cybersecurity Advanced Training and Workshop (5 days)
December 3-7, 2012
Idaho Falls, ID
Course Description
Registration

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

RECENT PRODUCT RELEASES

ALERTS

ICS-ALERT-11-343-01A—(UPDATE) Control Systems Internet Accessibility

ICS-ALERT-12-020-07A—(UPDATE) WAGO I/O 750 Multiple Vulnerabilities

ICS-ALERT-12-179-01—Sielco Sistemi Winlog Multiple Vulnerabilities

ICS-ALERT-12-137-01—Pro-face Pro-Server EX Multiple Vulnerabilities

ICS-ALERT -12-136-01—Wonderware SuiteLink Unallocated Unicode String

ADVISORIES

ICSA-12-179-01—Pro-face Pro-Server EX Multiple Vulnerabilities

ICSA-12-131-02—GE Intelligent Platforms Proficy HTML Help Vulnerabilities

ICSA-12-171-01—Wonderware SuiteLink Unallocated Unicode String DoS

ICSA-12-146-01A—RuggedCom Weak Cryptography for Password Vulnerability

ICSA-12-167-01—Innominate mGuard Weak HTTPS and SSH Keys Vulnerability

ICSA-12-158-01—Siemens WinCC Multiple Vulnerabilities

ICSA-12-138-01—Emerson DeltaV Multiple Vulnerabilities

ICSA-12-146-01—RuggedCom Weak Cryptography for Password Vulnerability

ICSA-12-145-01—Measuresoft ScadaPro dll Hijack Corruption

ICSA-12-145-02—xArrow Multiple Vulnerabilities

ICSA-12-137-02—Advantech Studio ISSymbol ActiveX Buffer Overflow

ICSA-12-122-01—WellinTech KingView DLL Hijack Vulnerability

ICSA-12-129-01—WellinTech KingSCADA Insecure Password Encryption

ICSA-12-131-01—Progea Movicon Memory Corruption Vulnerability

OTHER

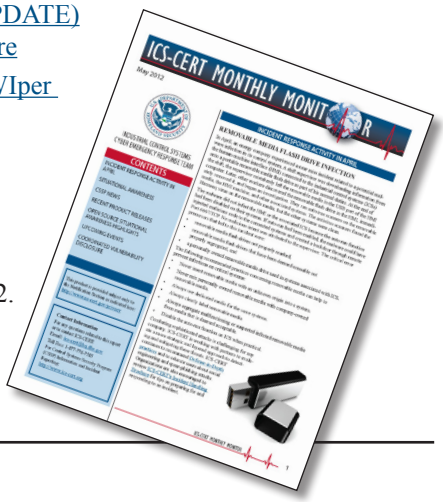
ICS-CERT Incident Summary Report (June 28, 2012)

ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies

JSAR-12-151-01A—(UPDATE) sKyWIper Flame Malware

JSAR-12-151-01—sKyWIper Flame Malware

The ICS-CERT Monthly Monitor May 2012 issue includes highlights of activities from April 2012.



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 May and June 2012

- ICS-CERT appreciates having worked through the coordinated disclosure process with the following researchers:
- Independent researchers Carlos Mario Penagos Hollman and Dillon Beresford, ICSA-12-179-01 Pro-face Pro-Server EX multiple vulnerabilities (June 27, 2012)
- Independent researcher Andrea Micalizzi, ICSA-12-131-02 - GE Intelligent Platforms Proficy HTML Help Vulnerabilities, (June 27, 2012)
- Independent researcher Luigi Auriemma, ICSA-12-171-01 - Wonderware SuiteLink Unallocated Unicode String Vulnerability (June 19, 2012)
- Independent researcher Justin W. Clarke, ICSA-12-146-01A - RuggedCom Weak Cryptography for Password Vulnerability (June 18, 2012).
- An independent research group comprised of Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman, ICSA-12-167-01 - Innominate mGuard Weak HTTPS and SSH Keys Vulnerability (June 15, 2012)
- Kuang-Chun Hung (Morgan) (ICST), ICSA-12-138-01 Emerson DeltaV Multiple Vulnerabilities (May 30, 2012).
- Justin W. Clarke, ICSA-12-146-01 RuggedCom Weak Cryptography for Password Vulnerability, (May 25, 2012).
- Carlos Mario Penagos Hollmann, ICS-CERT Advisory ICSA-12-145-01 - Measuresoft ScadaPRO dll Hijack Corruption (May 24, 2012).
- Luigi Auriemma, ICSA-12-145-02—xArrow Multiple Vulnerabilities, (May 24, 2012).
- Independent researcher Dmitriy Pletnev of Secunia, ICS-CERT Advisory ICSA-12-137-02 - Advantech Studio ISSymbol ActiveX Buffer Overflow, (May 16, 2012).
- Dillon Beresford, ICSA-12-122-01—Progea Movicon Memory Corruption Vulnerability (May 10, 2012).
- Carlos Mario Penagos Hollmann, ICS-CERT Advisory ICSA-12-122-01 Wellingtech KingView DLL Hijack Vulnerability (May 01, 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	Kuang-Chun Hung (ICST)	Alexandr Polyakov	Justin W. Clarke
Joel Langill	Terry McCorkle	Carlos Mario Penagos Hollmann	Dan Tentler
Rubén Santamarta	Shawn Merdinger	Alexey Sintsov	Nadia Heninger
Dillon Beresford	Celil Unuver	Adam Hahn	Zakir Duremeric
Eireann Leverett	Knud Erik Højgaard (nSense)	Manimaran Govindarasu	Eric Wustrow
Secunia	Billy Rios	Jürgen Bilberger	J. Alex Halderman
Yun Ting Lo (ICST)	Greg MacManus (iSIGHT Partners)	Reid Wightman	