June 2017

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

—ICSJWG EXPANDING THE COMMUNITY—

Upcoming Events

- September 12–14: ICSJWG 2017 Fall Meeting
  Pittsburgh, PA

ICS-CERT Resources

[Training Resources](#)
[Incident Reporting](#)
[Assessments](#)
[CSET®](#)
[Alerts](#) & [Advisories](#)
[HSIN](#)
[Latest Monitor](#)

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on members like you for our Newsletter, Meetings, and Webinars. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations.

Upcoming ICSJWG 2017 Fall Meeting

ICS-CERT is excited to announce that they will host the 2017 Fall Industrial Control Systems Joint Working Group (ICSJWG) Meeting on September 12–14, 2017, in Pittsburgh, Pennsylvania, at the Omni William Penn Hotel. This meeting will provide an opportunity for stakeholders to interface with peers, network with industry leaders, and stay abreast of the latest initiatives impacting security for industrial control systems and critical infrastructure. The Fall 2017 meeting will provide a forum for all control systems stakeholders to gather and exchange ideas about critical issues in ICS cybersecurity. The Meeting will include three full days of presentations and discussions and will feature the following:

- Keynote speeches from
  - NCCIC Director John Felker and
  - Joel Brenner of MIT/IPRI-CIS;
- A Hands-on Technical workshop;
- Vendor Expo; and
- “Ask Me Anything” session with ICS-CERT.

Meeting registration and the Call for Abstracts are now open. If you’d like to attend or present at the 2017 Fall Meeting, please visit the ICSJWG web page for the registration link and the Call for Abstracts form. For information about the Omni William Penn Hotel and an ICSJWG room block, please go to https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. We look forward to seeing you in Pittsburgh!

Thank You and Farewell

After over a decade of service with ICS-CERT, Marty Edwards has decided to leave the federal government to face his next challenge in a global non-profit organization. He is now the Managing Director of the Automation Federation, working with automation professionals worldwide. We would like to thank him sincerely for his leadership and contributions to ICS-CERT and the ICSJWG and we look forward to working with him in his new capacity in the community.

Contributed Content Disclaimer: ***The advice and instructions provided in the contributed content are specified as is with no warranties and should be confirmed and tested prior to implementation.***

WannaCry Ransomware and Industrial Control Systems

By: Ernie Hayden MIPM, CISSP CEH GICSP (Gold) PSP BBA USA, Inc.

There’s been substantial discussion in the media and on the interwebs about the ransomware called “WannaCry”. This malicious software (malware), which blocks access to data until a ransom is paid, has been destructive. It’s caused financial consequences as well as extreme inconveniences for critical businesses across the globe, such as the National Healthcare Service in the United Kingdom, which was one of the first and most significant victims of the attack (a total of 300,000 computers in 150 countries had been locked by WannaCry as of the end of May 2017).

With initial receipt of the WannaCry news some in the industrial controls industry did not see it as a threat; however, as you examine the WannaCry targets and realize it is focused on unpatched Windows-based systems, the threat to industrial control systems (ICS) is significant – even though a small number of U.S. critical infrastructure operators were reportedly affected. Full article available here.

Not all Devices are IoT or IIoT

By: Daniel Ehrenreich, SCCE, Consultant and Lecturer on OT Cyber Security

Business opportunities created by Internet of Things (IoT) and the Industrial IoT (IIoT) are among the most debated topics, as these are designed to function in a broad range of consumer and industrial applications. Manufacturers of IoT components believe in this new trend, but many of them still not understand the essence of the IoT concept. In reality, not every controlled device is an IoT nor IIoT.

The IoT/IIoT concept is a communication-based eco-system in which control devices, CCTV cameras and industrial sensors communicate via the Internet with cloud-based computer systems and data sources, and the result of this process is displayed on a computer screen, smartphone or used for optimal activation of a process. Through an IoT/IIoT ecosystem you may boost productivity and achieve unique benefits. Examples of IoT/IIoT include applications such as; remote operation of home appliances, medical devices, check on availability of a product in a store, warnings of unusual conditions and malfunctions and more.

Leading market research firms already estimate that by 2020 there will be over 20 billion devices worldwide, defined as part of IoT/IIoT systems. Although the forecasted number is growing every year, it is not clear whether these figures correctly refer to what can be and what cannot be considered IoT or IIoT. It is strongly recommended that decision factors such as outlined below shall be taken into consideration. Click here to read full article.

Attack in Depth

By: Monta Ekins - Security Architect, FoxGuard Solutions

Let's discuss a type of attack methodology, Attack in Depth, as recently demonstrated by a well-resourced attacker. The technique is neigh non-existent in the I.T. infrastructure space, but is expected to become standard for future attacks against critical infrastructure, (by nation state / APT attackers.)

The purpose of this white paper is to define this style of attack. The recognition, identification, and naming of a thing will make discussions of the technique and ultimately development of prevention measures easier. To continue reading click here.

CIP & Your HMI: A Simplified Solution

By: Gary Overstreet, Vice President FoxGuard Solutions

The North America Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) under the direction of the Federal Energy Regulatory Commission (FERC), has created compliance standards for the Bulk Electric System (BES). Entities operating within the BES must adhere to these standards. These standards are in place to insure that our electrical generation, transmission, and distribution can continue uninterrupted, especially as it would relate to interruptions caused by cyber events. Penalties for not adhering to these standards can be significant. In February of 2016, NERC issued a full notice of penalty regarding an Unidentified Registered Entity, FERC Docket No. NP16-_- 000. The penalty amount was $1.7M. In October of 2016, NERC issued a full notice of penalty regarding an Unidentified Registered Entity, FERC Docket No. NP17-_-000 in the amount of $1.25M. The stakes are very high relative to being NERC CIP compliant. More information available here.

2017 Chemical Sector Security Summit

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP) and the Chemical Sector Coordinating Council invite you to attend the 2017 Chemical Sector Security Summit, **July 19, 2017 through July 21, 2017** at the **JW Marriott, Houston, Texas** located directly across the Houston Galleria**.**

The Chemical Sector Security Summit serves as the annual event that brings together industry owners and operators, key government officials, first responders, and law enforcement to engage in face-to-face discussions and share the latest in security best practices. We look forward to hosting this year's event in Houston—a major hub of the Chemical Sector–which facilitates in-person participation and the growing public-private partnership.

Questions?
For more information, please visit www.dhs.gov/chemical-sector-security-summit or contact the Chemical Summit Team at chemicalsummitreg@dhs.gov.

IIOT and the Cyber Threat: A Perfect Storm of Risk

By: Chris Grove, CISSP, NSA-IAM

The IT/OT convergence that is propelling the Fourth Industrial Revolution has opened up a can of worms in terms of risks to both IT and industrial control systems. Meanwhile, these risks are being compounded by the divide between these two worlds.

At the product level, industrial equipment providers are introducing a myriad of new advances to their automation technology. Especially with respect to networking, which is producing more intelligent controllers (PLCs, RTUs, etc.), devices, and objects (e.g., industrial sensors) that can share vast amounts of data. The data generated by these networked devices is being used for machine-learning and operational analysis in order to make real-time adjustments to industrial control processes. Additional information available here.

A Flight Recorder for Forensics

By: Lior Frenkel, CEO and Co-Founder Waterfall Security Solutions LTD

Cyber attacks only become more sophisticated over time, and current trends in targeted attacks, particularly targeted ransomware, are disturbing. When remediating such attacks, reliable forensics are indispensable; how else can we be assured that we have discovered all compromised equipment, and discerned the original attack path?

For more than a decade, targeted remote attacks have breached countless networks, even heavily-defended ones. A targeted attack is one where our attacker has a specific target in mind - us. The common wisdom of "we need only to be better defended than our neighbor" does not hold for targeted attacks. Such attacks often start with "spear phishing" - well-researched, forged emails that trick us into revealing remote login credentials, or into somehow activating malware. Once our enemy has a foothold on our networks, they seed remote-control malware, create new accounts for themselves, and work deeper into the most-sensitive of our networks until they have reached their goal. Their goal may be sabotage, it may be espionage, or in recent months it may simply be extortion. Further reading available here.