ARL-CR-0759 • FEB 2015

US Army Research Laboratory

Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems Version 1.0

Daniel T Sullivan
Raytheon Company
22260 Pacific Blvd
Dulles, VA

under contract W911QX-14-F-0020

Approved for public release; distribution unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-CR-0759 ● FEB 2015

US Army Research Laboratory

Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems Version 1.0

Daniel T Sullivan
Raytheon Company
22260 Pacific Blvd
Dulles, VA

under contract W911QX-14-F-0020

Approved for public release; distribution unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
February 2015	Final	07/2014–11/2014

4. TITLE AND SUBTITLE
Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems Version 1.0

5a. CONTRACT NUMBER
W911QX-14-F-0020

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Daniel T Sullivan

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Raytheon Company
22260 Pacific Blvd
Dulles, VA 20166

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-CR-0759

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Army Research Laboratory
ATTN: RDRL-CIN-S
2800 Powder Mill Road
Adelphi, MD 20783-1138

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Critical infrastructure is vulnerable to cyber threats and the consequences of attacking an industrial control system (ICS) may result in loss of life. ICSs are different in several ways from information technology (IT) systems. As a result, the processes to protect IT cannot be applied to ICS infrastructure. This report presents common threat vectors to ICSs and lessons learned from recent malware to provide recommendations to protect critical infrastructure from cyber attacks.

15. SUBJECT TERMS
ICS, SCADA, Malware, Computer Security, Network Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	26	Daniel T Sullivan
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER (Include area code) 301-394-0248

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Tables iv

1. Introduction 1

2. ICS Cyber Vulnerabilities 1

3. ICS Cyber Threats 1

4. Survey of Recent Malware 2

4.1 Malware Characteristics 3

4.2 Lessons Learned From Malware 7

5. Comparison of ICS and IT Systems 7

6. ICS Cyber Risk Mitigation 9

6.1 Recommendations when Acquiring New Components 9

6.1.1 Encryption 10

6.1.2 Software Quality 10

6.1.3 Access Controls 10

6.1.4 Unused Software 10

6.1.5 Intrusion Detection 10

6.1.6 Patches 10

6.2 Recommendations to Secure Existing Systems 11

7. Conclusions 13

8. References 15

List of Symbols, Abbreviations, and Acronyms 18

Distribution List 19

List of Tables

Table 1 Most common weaknesses in installed ICS systems 1
Table 2 Causes of ICS system incidents 2
Table 3 Sources of malware in ICS systems 2
Table 4 Characteristics of recent malware 4
Table 5 Comparison of IT and ICS characteristics 8

1. Introduction

"The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." — Executive Order 13636 Improving Critical Infrastructure Cybersecurity

Protection of critical infrastructure components is vitally important to industrial control systems (ICSs). Undetected cyber attacks are a threat to human life and may incur significant material losses and detrimentally impact the reputation of entire industries. This technical report reviews recent malware threats and provides recommendations for computer network defense (CND) to maintain the availability, integrity, and confidentiality of the ICS infrastructure.

2. ICS Cyber Vulnerabilities

The US Department of Homeland Security (DHS) catalogues ICS vulnerabilities and identified the most common ones. These metrics are derived from security assessments of new ICS products as well as assessments of ICS installations conducted from 2004 to 2010. Included in the metrics are vulnerabilities learned from the DHS Control System Security Program (CSSP) site assessments, ICS Cyber Emergency Response Team (ICS-CERT) activities, and asset owner evaluations using the Cyber Security Evaluation Tool (CSET). The top 3 cyber vulnerabilities are presented in Table 1.[1]

Table 1 Most common weaknesses in installed ICS systems

Rank	DHS CSSP Site Assessment	ICS-CERT Incident Response	CSET Gap Areas
1	Credentials Management	Network design weaknesses	Lack of formal documentation
2	Weak Firewall Rules	Weak firewall rules	Audit and accountability (Lack of security audits, assessments, poor logging practices)
3	Network Design Weaknesses	Audit and accountability (poor logging practices)	Permissions, privileges, and access controls

3. ICS Cyber Threats

Malware attacks comprise the main cause of ICS incidents as presented in Table 2.[2] Software errors and failure of supervisory control and data acquisition (SCADA) components are the 2nd and 3rd reasons, respectively, of ICS incidents.

Table 2 Causes of ICS system incidents

Cause of Incident	Percentage
Malware attacks	35%
Software error	23%
SCADA component failure	19%
Other	12%
Operator error	11%

As shown in Table 3, corporate networks are the most common threat vector for malware to enter process control networks.[2]

Table 3 Sources of malware in ICS systems

Source of Malware	Percentage
Corporate network	35%
Remote access	26%
Outside contractors	10%
Internet connections	9%
Human-machine interface (HMI)	8%
Wi-Fi	5%
Mobile devices	4%
Universal serial bus (USB)	3%

Malware does not have to deploy a malicious payload to impact ICS processes. If malware causes 100% central processing unit (CPU) load on a server or controller, this may harm process automation safety or operations since ICS processes require deterministic communications. In considering an approach to mitigate risks due to cyber threats, a review of recent malware will be helpful to understand their characteristics and identify countermeasures.

4. Survey of Recent Malware

Analysis of recent malware attacks illuminates how malware persists and spreads through a network. The characteristics of Stuxnet, Duqu, Flame, Shamoon, and 2 remote access Trojans (RATs) developed by the Energetic Bear group are presented and lessons learned derived.

4.1 Malware Characteristics

Table 4 presents the characteristics of recent malware in how the malware was introduced to the victim site, how it spread, and the damage caused. The "Dropper Method" column explains how the malware was introduced into the victim's environment. The "Malware Spreading Method" column describes the lateral movement of the malware through the target organization. The "Persistence Method" column presents how the malware is restarted after the infected system is rebooted. The "Command and Control" column reveals how the malware communicates with the attackers.

Table 4 Characteristics of recent malware

Malware Name	Dropper Method	Malware Spreading Method	Persistence Method	Command and Control	Damage Caused
Stuxnet	Stuxnet gained initial entry to a facility network via an infected USB drive or Siemens project file. Stuxnet exploited 4 zero-day vulnerabilities:[4,5] • Win32K.sys Local Privilege Escalation (CVE-2010-2743) • LNK Shortcut Vulnerability (CVE-2010-2568) • RPC Print Spooler Service Impersonation (CVE-2010-2729) • Task Scheduler Vulnerability (CVE-2010-3338)	Spread through a facility control network via infected USB memory sticks, infected Siemens project files, connection to the Siemens WinCC database server, and to other computers on a local area network using shared network drives and print spooler services.[3]	Stuxnet installer created files masquerading as drivers using two stolen certificates.[4] Malware files are copied to the Windows System 32 and system driver setup folder. A service is created to inject Stuxnet into trusted Windows services at system boot. A 2nd service is installed, which operates a root kit to hide Stuxnet files on removable media.[5]	Sent encrypted data using Hypertext Transfer Protocol (HTTP) on port 80 to command and control (C&C) servers reporting data about the infected machine and if Siemens Simatic WinCC Step 7 software is installed. Infected PCs downloaded modules from the C&C servers.[4] Stuxnet established a peer-to-peer network among infected hosts so all will receive the new version of Stuxnet when one infected host is updated.[5]	Stuxnet installed a rootkit in the WinCC HMI and re-programmed the Programmable Logic Controller (PLC) to damage the nuclear fuel refining centrifuges by speeding and slowing their motors at set intervals.[3]
Duqu	A Microsoft Word document contained the Duqu installer. When the document was opened, the installer exploited a true-type font (TTF) zero-day vulnerability (CVE-2011-3402) to run programs as the kernel. The installer created a driver file, configuration file, main dynamic link library (DLL), and a boot service to start the driver.[6]	Duqu did not self-replicate. Forensic evidence indicates that attackers downloaded a keylogger and network survey modules. The keylogger captured credentials. The attacker copied Duqu to a target computer using file shares and authenticated with the credentials intercepted by the keylogger. Using the credentials, the attacker created a scheduled task to install Duqu on the targe.[6]	The Duqu launcher was disguised as a system driver file and was signed with a stolen certificate. At system initialization, the launcher then injected Duqu into the services.exe process. Duqu unpacked and injected itself into other trusted processes.[6]	Infected computers encrypted stolen data and sent the data to C&C servers using HTTP (port 80) and Hypertext Transfer Protocol Secure (HTTPS) (port 443). Some data were embedded into graphics files to obfuscate network activity. Infected victim computers which connect to the Internet acted as a proxy for compromised computers within a secure zone. The computers in a secure zone sent their data to the proxy using a file-sharing protocol. The proxy forwarded the data to the C&C servers.[6]	Cyber espionage. Captures keystrokes, focused on data mining and reconnaissance.[6]

Table 4 Characteristics of recent malware (continued)

Malware Name	Dropper Method	Malware Spreading Method	Persistence Method	Command and Control	Damage Caused
Flame	Possible ways of initial infection are spear phishing and downloads from a web site.[7]	The infected computer created a man-in-the-middle attack by advertising itself as a proxy using Web Proxy Autodiscovery Protocol (WPAD). Uninfected computers connected to this rogue proxy and downloaded malware masquerading as Windows updates. The malware was signed with a forged Microsoft code-signing certificate. Malware could also spread via USB memory sticks with Autorun enabled and exploiting print spooler vulnerability which permitted remote code execution (zero day vulnerability CVE-2010-2729).[7,8]	Flame installed itself as a custom authentication package in the Windows registry and was automatically started at system boot. Flame installed many modules in Windows Program Files, System32, and temp directories.[7]	Recorded data were encrypted and sent to C&C servers using HTTPS on ports 443 and 8080.[9] Flame also downloaded modules from C&C servers. The C&C layer consisted of multiple domains.[10]	Cyber espionage, Flame recorded keystrokes, network traffic, and screenshots. Flame also recorded Skype conversations and used Bluetooth to download contact info from cell phones, which was then sent to C&C servers.[8,10]
Shamoon (W32.Dist Track)	Initial infection vector is unknown.[11] The malicious executables were encrypted in the resources section of the dropper. The dropper installed Shamoon in the Windows system folder, replaced a driver file with a digitally signed wiper, and created a service. Shamoon could infect 32- and 64-bit Windows operating systems.[12]	Enumerated IP addresses of local computer and then spreads via Admin$ shares. After Shamoon copied itself to the remote computer, it executed a task to run Shamoon on the newly infected host.[13]	Shamoon created a Windows service which automatically launched Shamoon when Windows starts.	Shamoon sent data about the host IP address, domain, and number of files overwritten to the C&C server using HTTP GET request.[12]	Shamoon overwrote files with an image and then overwrote the master boot record, preventing the PC from booting. The overwritten data was lost.

Table 4 Characteristics of recent malware (continued)

Malware Name	Dropper Method	Malware Spreading Method	Persistence Method	Command and Control	Damage Caused
Backdoor.Oldrea (also known as Havex) and Trojan.Karagany. Both are RATs.	The group known as "Dragonfly" and "Energetic Bear" used 3 attack vectors: 1. Spear phishing email with infected portable document format (PDF) attachment 2. "Water hole" web sites re-directed users to download the Lightsout exploit 3. The installer of downloadable ICS software was modified to install Havex.[14]	Neither Trojan self-replicated to other hosts.	Backdoor.Oldrea installed a DLL in the Windows System folder and created an Autorun registry entry to start the DLL when the user logs in. The DLL injected the malware into the Windows Explorer process. Trojan.Karagany is an executable and created a link in the Startup folder.[15]	Both RATs used HTTP POST messages on port 80 to send stolen data to C&C server. All data are encrypted. The C&C servers sent commands and executables to the RATs.[15]	Cyber espionage against US and European energy companies and energy controls manufacturers. The RATs looked for ICS configuration files, Outlook email addresses, and Havex sniffed OLE Process Control (OPC) protocol for details on ICS equipment.[15]

4.2 Lessons Learned From Malware

The behaviors of the malware described in Table 4 provide many lessons to be considered when designing defenses to protect ICS networks:

- Certificates cannot be relied to guarantee the provenance of driver files and patches. Flame distributed itself disguised as Microsoft patches using a forged code-signing certificate. Stuxnet used 2 stolen code-signing certificates to masquerade as driver files.
- Each malware sample connected to a C&C server. In addition, Stuxnet and Duqu established peer-to-peer connections between infected hosts in secure enclaves with an infected host acting as proxy to a C&C server. Most of the malware could receive updated modules from the attackers and could execute commands as directed by them. While some malware could function without additional modules from C&C servers, the outgoing, persistent connections to transfer data are an indicator of compromise (IOC).
- Data sent from the malware to the C&C servers were sent outgoing in encrypted payloads. Outgoing Internet connections are not normally blocked by enterprise firewalls.
- Some malware exploited zero-day vulnerabilities as well as attempted to exploit vulnerabilities for which Microsoft already had patches available. The duration between discovery of the zero-day vulnerabilities and the release of patches was several months. Even after a patch is released, additional time is needed to test the patches prior to deployment.

5. Comparison of ICS and IT Systems

Strategies for mitigating cyber risks on ICS components must take into account unique characteristics of their components and emphasis on availability and safety. Table 5 presents important distinctions between ICS and IT systems.[16]

Table 5 Comparison of IT and ICS characteristics

Category	Information Technology System	Industrial Control System
Performance	• Non-real time • Response must be consistent • High throughput • High latency and jitter may be acceptable	• Real time • Response is time-critical • Modest throughput is acceptable • High delay and/or jitter is not acceptable
Availability	• Rebooting is acceptable • Availability deficiencies can often be tolerated, depending on the system's operational requirements	• Rebooting may not be acceptable because of process availability requirements • Availability requirements may necessitate redundant systems • Outages must be planned and scheduled days/weeks in advance • High availability requires exhaustive pre-deployment testing
Risk Tolerance	• Data confidentiality and integrity is paramount • Fault tolerance is less important—momentary downtime is not a major risk • Major risk impact is delay of business operations	• Human safety is paramount, followed by protection of process • Fault tolerance is essential, even momentary downtime may not be acceptable • Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
Unintended Consequences	• Security solutions are designed around typical IT systems	• Security tools must be tested (e.g., offline on a comparable ICS) to ensure that they do not compromise normal ICS operation
Communications	• Standard communications protocols • Primarily wired networks with some localized wireless • Typical IT networking practices	• Many proprietary and standard communications protocols • Several types of communications media used including dedicated wire and wireless (radio and satellite) • Networks are complex
Managed Support	• Allow for diversified support styles	• Service support is usually via a single vendor
Component Lifetime	• Lifetime on the order of 3 to 5 years	• Lifetime on the order of 15–20 years
Access to Components	• Components are usually local and easy to access	• Components can be isolated, remote, and require extensive physical effort to gain access to them

Many process control networks were designed with the paradigm of being air-gapped from corporate networks. However, Mr Sean McGurk, Director of the DHS National Cybersecurity & Communications Integration Center, testified before Congress that when DHS conducts onsite assessments, they see on average 11 direct connections (and as many as 250) between the enterprise corporate network and the process control network.[17]

Since process control network components can be in service for up to 20 years, the attack surfaces that we are aware of today were unknown when these components were designed. Process components built 15 to 20 years ago may not have the resources (e.g., memory or processor speed) to accept new firmware or other patches to mitigate vulnerabilities. Also, protocols designed 20 years ago were not designed for confidentiality or integrity. As a result, ICS components relying on these older protocols are susceptible to replay attacks. Modbus is a common ICS protocol developed in 1979 and does not have security elements, even in the version for Transmission Control Protocol/Internet Protocol (TCP/IP) transport.[18]

New patches require extensive testing. Deploying a patch may need to wait several months until the process component can be taken offline and patched. As a result, the processes and solutions to mitigate cyber threats in an IT environment may not be appropriate for process networks.

6. ICS Cyber Risk Mitigation

Because the enterprise and process control networks are no longer protected by an air gap and these 2 networks can be inadvertently directly connected, we recommend protecting process control networks with defense in depth to slow the spread of malware and using both signature and behavior sensors to detect IOCs caused by malware.

6.1 Recommendations when Acquiring New Components

When purchasing new ICS components, include requirements for compliance with information assurance (IA) controls. The Energy Sector Control Systems Working Group (ESCWG) has recommendations for request for proposal (RFP) language to specify required IA controls and post-sale processes with vendors.[19] A summary of the IA controls and processes to be specified in RFPs follows.

6.1.1 Encryption

Some vendors use their proprietary encryption and these algorithms have not withstood public crypto analysis. Require that vendors implement approved algorithms, which are listed in the Federal Information Processing Standard (FIPS) 140-2. Only specify secure protocols to be used to ensure data integrity and prevent replay attacks.

6.1.2 Software Quality

Request the vendor provide documentation of secure software coding practices such as using static analysis tools. Some commercial software store passwords in plain text or use hard-coded passwords. Stuxnet exploited a hard-coded password that had been posted on Internet websites.

6.1.3 Access Controls

Specify the software use customer-defined, role-based access controls. Each role should have the minimum privileges necessary for the task. Two-factor authentication should be specified for remote access and elevated privileges.

6.1.4 Unused Software

Most ICS software is delivered on Windows or Linux distributions. In the RFP, specify that all unused software, drivers, ports, and protocols be removed or disabled. This reduces the attack surface available to malware and reduces the need to install patches for services that are unused. Verifying that unused software is removed or disabled should be part of the site acceptance test (SAT).

6.1.5 Intrusion Detection

A host-based security system is needed to detect malware and root kits as well as enforce security policies. Request the vendor include a host-based malware detection product or recommend one. If the vendor is unable to recommend this type of product, request the vendor recommend an application whitelisting tool.

In order to implement anomaly detection, request information on normal communications ports, protocols, and network traffic patterns.

6.1.6 Patches

Vendors typically do not publically disclose software vulnerabilities until a patch is ready, and the time between the initial report of a zero-day vulnerability and the released patch could be several months. Request the vendor provide information about all software vulnerabilities, including those not publically disclosed, and the

vendor's recommendations for mitigations to be implemented until a patch can be released. Specify that the vendor will provide a patch within a set time period to mitigate critical vulnerabilities.

In addition to fixing critical vulnerabilities, request the vendor to provide a process on how customers can verify the integrity of patches and other software delivered. The Energetic Bear group modified the installation programs of 3 ICS vendors, which caused RATs to be installed in customer networks.

6.2 Recommendations to Secure Existing Systems

The overall strategy to thwart malware is to prevent malware from spreading and detect its presence, which enables defenders to contain the malware. Based upon threats posed by malware and behavior of recent APTs, the following recommendations are provided to organizations to protect their critical infrastructure:

1. Conduct a threat risk assessment to identify the most common attack vectors, their severity of impact, and probability of occurring. Based on the risk assessment, establish defense in depth in the process control network with security zones in accordance with International Society for Automation/International Electrotechnical Commission-62443 (ISA/IEC-62443) standard.[20] A security zone is a group of assets that share common security requirements and restricting data flows to only those endpoints that exchange information will slow the spread of malware.

2. Since 35% of malware enters via corporate networks, recommend all email attachments and downloaded files to be screened for malicious content. Most malware is encrypted and will have higher entropy than innocuous content.

3. With the ICS vendor's approval, use application whitelisting to only allow trusted applications and DLLs to operate. This will prevent malware from running and injecting code into trusted applications and operating system services. This recommendation is expected to be effective in ICS networks since changes are implemented less often than in IT networks.

4. Document expected incoming and outgoing network connections. Control access for outgoing connections by whitelisting external IP addresses or domain names. This prevents malware from beaconing to its C&C servers, receiving updates, and exfiltrating data. Firewalls are routinely configured to block incoming connections while malware within a target network initiates outgoing beacons.

5. Establish a baseline trend of all outgoing network connections as well as monitor the duration and the amount of data sent out from these outgoing connections. Investigate outgoing connections that have the longest connection times and most data sent out as possible malware beacons and data exfiltration activity. Capture packets from these connections and assess if the data sent out are encrypted or obfuscated as 1 IOC.

6. Install ICS-aware firewalls with deep packet inspection (DPI) to protect controllers such as PLCs and remote terminal units (RTUs). An ICS firewall with DPI is preferred over a corporate IT firewall, because the DPI feature will inspect the commands sent to controllers and verify the command is permitted. An example of a command that is suspicious is a remote user conducting a firmware upgrade. Not all IT commercial firewalls can parse commands from ICS protocols.

7. Implement port security to prevent unauthorized devices connecting to the process control network.

8. Restrict process control network user privileges to only those required for the person's job, preferably with role-based access control

9. The process and corporate networks should have their own separate infrastructure services. Examples of this are separate Active Directory (AD) servers, separate patch repositories, separate dynamic host configuration protocol (DHCP) servers, and separate domain name system (DNS) servers. The AD servers on the process and corporate networks should not have a trust relationship. This separation of infrastructure services is necessary to prevent malware on the corporate network penetrating the process control network.

10. The process control network data historian should share data with the corporate network only through a one-way data diode. This reduces the risk of a structured query language (SQL) injection attack from the corporate network.

11. Configure the intrusion detection system (IDS) to alert if a firewall rule is permitting blocked traffic through. If the IDS alerts on traffic that should be blocked, the firewall administrator can take corrective action on the firewall configuration.

12. Harden ICS equipment by disabling all unnecessary services and network daemons. Some equipment is delivered with Telnet and file transfer protocol (FTP) services installed, which have well-known vulnerabilities. Recommend unnecessary services be disabled during SAT to reduce the

attack surface. During SAT, the equipment should be thoroughly tested with these unneeded services disabled. Once the equipment is installed, disabling the services will be difficult while maintaining high availability. An example of an open vulnerability is very small aperture terminal (VSAT) stations installed with a Telnet server running with weak passwords and accessible to anyone on the Internet.[21]

13. Periodically verify the firmware in controllers is the correct version. One attack is to reverse engineer firmware and insert malicious code into firmware and then deploy this version into controllers.

14. Install honey pots within the process control network. If logs show activity within the honey pot, then further investigation should be initiated to determine which boundary protection has been penetrated.

15. Disable web and email access for administrative accounts. This prevents administrators downloading email attachments with malicious code and prevents the possibility of installing malware via Trojan downloads and browser exploits.

16. Use two-factor authentication for privileged root level access and remote access. This eliminates obtaining access using weak passwords or factory set accounts.

17. Prevent malware from surviving reboots by restricting permissions to write files to the Windows system folders and restricting the creation of registry entries.

7. Conclusions

ICSs were once thought to be completely isolated and therefore unreachable to malware. However, ICSs are, in many cases, no longer "air gapped" and may be inadvertently connected to a corporate network, therefore making them vulnerable to malware originating on the Internet. Besides threats originating from external networks, removeable media can also allow malware to enter a process network. To protect critical infrastructure, it is recommended that asset owners conduct a security risk analysis of existing plant networks as well as plans for new plant automation. They should identify cyber risks and implement defense in depth to protect critical assets. Defense in depth should be implemented with layers of technical security controls (e.g., ICS-aware firewalls) to control network traffic and prevent the spread of malware. Intrusion detection technologies should be deployed between each defensive layer to warn of the presence of a cyber attack. Critical assets should be protected by the most number of defensive layers.

This process of implementing defense in depth can be phased in to protect existing process networks, since availability is of the greatest importance to asset owners. For new plant automation, it is recommended that customers specify IA controls in RFPs with which new products must comply when acquiring new plant assets.

8. References

1. Common Cybersecurity Vulnerabilities in Industrial Control Systems. Department of Homeland Security; May 2011 [accessed 2014 Nov]. https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.

2. Cyberthreats to ICS Systems: You Don't Have To Be a Target To Become a Victim. Kaspersky Lab; 2014 [accessed 2014 Nov]. http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf.

3. Byres E, Ginter A, Langill J. How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems Version 1.0. Tofino Security 2011 Feb 22 [accessed 2014 Nov]. https://www.tofinosecurity.com/how-stuxnet-spreads.

4. Mittal P. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired Magazine. 2011 Jul 11 [accessed 2014 Nov]. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

5. Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier Version 1.4. Symantec Corporation. 2011 Feb [accessed 2014 Nov]. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

6. W32.Duqu: The precursor to the next Stuxnet Version 1.4 Symantec Corporation. 2011 Nov 23 [accessed 2014 Nov]. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.

7. Gostev A. Flame: Bunny, Frog, Munch, and BeetleJuice. Kapersky Lab ZAO. 2012 May 30 [accessed 2014 Nov]. http://securelist.com/blog/incidents/32855/flame-bunny-frog-munch-and-beetlejuice-2/.

8. Udi (n.d.) A. How did the 'Flame' family of malware spread? Boston University. [accessed 2014 Nov]. http://www.cs.bu.edu/~goldbe/teaching/HW55813/flame.pdf.

9. Global Research & Analysis Team. Full Analysis of Flame's Command & Control servers. Kapersky Lab ZAO; 2012 Sep 17 [accessed 2014 Nov]. https://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers.

10. Gostev A. The Flame: Questions and Answers. Kapersky Lab ZAO; 2012 May 28 [accessed 2014 Nov]. http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.

11. Technical Lessons Learned from the Shamoon Malware Attacks. US Department of Energy; 2012 Oct [accessed 2014 Nov]. http://www.nwppa.org/cwt/external/wcpages/wcmedia/documents/_newsletters/cip%20awareness%20bulletin-shamoon%20technical%20lessons%20learned.pdf.

12. The Shamoon Attacks. Symantec Corporation; 2014 Jan 23 [accessed 2014 Nov].http://www.symantec.com/connect/blogs/shamoon-attacks.

13. Tarakanov D. Shamoon the Wiper in details. Kapersky Lab; 2014 Aug 21 [accessed 2014 Nov]. http://www.securelist.com/en/blog?print_mode=1&weblogid=208193795.

14. Dragonfly: Cyberespoinage Attacks Against Energy Suppliers Version 1.21. Symantec Corporation; 2014 Jul 7 [accessed 2014 Nov]. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.

15. Hentunen D. Havex Hunts For ICS/SCADA Systems. F-Secure. 2014 Jun 23 [accessed 2014 Nov]. http://www.f-secure.com/weblog/archives/00002718.html.

16. National Institutes of Standards and Technology (NIST) Special Publication 800-82 Revision 1 Guide to Industrial Control System (ICS) Security. NIST; 2013 May [accessed 2014 Nov]. http://dx.doi.org/10.6028/NIST.SP.800-82r1.

17. The Subcommittee on National Security, Homeland Defense, and Foreign Relations CyberSecurity: Assessing the Immediate Threat To The United States. US Congress; 2011 May 25 [accessed 2014 Nov]. http://oversight.house.gov/wp-content/uploads/2012/04/5-25-11-Subcommittee-on-National-Security-Homeland-Defense-and-Foreign-Operations-Hearing-Transcript.pdf.

18. Modbus. Digital Bond Incorporated; [accessed 2014 Nov]. http://www.digitalbond.com/scadapedia/protocols/modbus-2/.

19. Cybersecurity Procurement Language for Energy Delivery Systems. Energy Sector Control Systems Working Group (ESCSWG); 2014 Apr [accessed 2014 Nov]. http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

20. ISA-62443-1-1 (99.01.01) Security for Industrial Automation and Control Systems Terminology, Concepts, and Models Draft 2, Edit 4. [accessed 2014 Nov] http://isa99.isa.org/Documents/Drafts/ISA-62443-1-1-WD.pdf.

21. Bansal S. Small satellite terminals (VSAT) are vulnerable to Cyber attack. The Hacker News; 2014 Jan 9 [accessed 2014 Nov]. http://thehackernews.com/2014/01/small-satellite-terminals-vsat-are.html.

List of Symbols, Abbreviations, and Acronyms

AD	Active Directory
C&C	command and control
CERT	Cyber Emergency Response Team
CND	computer network defense
CPU	central processing unit
CSET	Cyber Security Evaluation Tool
CSSP	Control System Security Program
CVE	common vulnerabilities and exposures
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLL	dynamic link library
DNS	domain name system
DPI	deep packet inspection
ESCSWG	Energy Sector Control Systems Working Group
FIPS	Federal Information Processing Standard
FTP	file transfer protocol
HMI	human-machine interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	information assurance
ICS	industrial control system
ICS-CERT	ICS - Cyber Emergency Response Team
IDS	intrusion detection system
IOC	indicator of compromise
IP	Internet Protocol

ISA/IEC	International Society for Automation/International Electrotechnical Commission
IT	information technology
OPC	OLE for Process Control
PDF	portable document format
PLC	Programmable Logic Controller
RAT	remote access Trojan
RFP	request for proposal
RPC	remote procedure call
RTU	remote terminal unit
SAT	site acceptance test
SCADA	supervisory control and data acquisition
SQL	structured query language
TCP	Transmission Control Protocol
TTF	true type font
USB	universal serial bus
VSAT	very small aperture terminal
WPAD	Web Proxy Autodiscovery Protocol

1 (PDF only)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DIRECTOR US ARMY RESEARCH LAB RDRL CIO LL IMAL HRA MAIL & RECORDS MGMT
1 (PDF)	DIRECTOR US ARMY RESEARCH LAB RDRL CIN S D SULLIVAN