White Paper **WP910003EN**

COOPER POWER
SERIES

Security best practices checklist reminder

Hacking and other malicious cyber-activity continue to be of increasing concern in the U.S. and around the world. Threats to cyber-physical systems continue to pose significant risks with probes and attacks on utility networks being part of the larger concern of threats to critical national infrastructure. Eaton as a supplier of networked products and utility systems and solutions pays special attention to monitoring and understanding the evolving threat environment particularly as it relates to utility systems.

This information note is intended to reiterate to our customers the serious threats being faced and to remind them of the checklist of basic cybersecurity best practices that when instituted have been demonstrated to provide effective, proactive countermeasures to the range of on-going cybersecurity threats. References are also provided to recommended resources that customers can consult for more detailed guidance in reviewing and updating their current security posture. Eaton's Customer Service teams may also be consulted for further information on responding to threat concerns.

Recent cybersecurity threat events

One of the largest cyber-attacks to hit the web, the recent "WannaCry" ransomware [R1] that began on May 12 infected host computers by encrypting all of their data and then demanding a ransom from users to release access. The malware attack began in Europe and affected hundreds of thousands of machines worldwide across a range of industries. The attack was able to take advantage of vulnerabilities that had been publicly identified and that could have been prevented by subsequently released Windows® operating system update patches (Microsoft® Security Bulletin MS17-010 patched the vulnerability in March).

RANSOMWARE

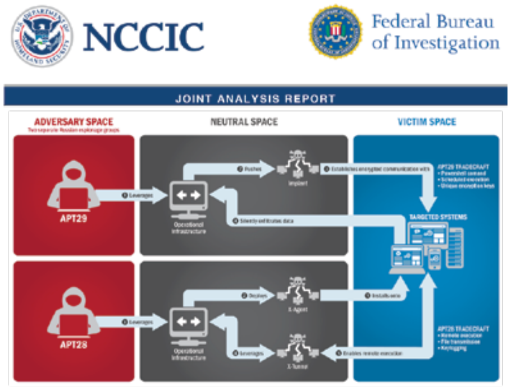
What It Is and What To Do About It

WHAT IS RANSOMWARE?
Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The

HOW DO I RESPOND TO RANSOMWARE?
Implement your security incident response and business continuity plan. It may take time for

The attack drives home the importance of continued network vigilance and the need to institute basic cybersecurity best practices such as regular and timely application and operating system patching. The event also highlights the need for organizations to implement and maintain security incident response and business continuity plans that can be invoked when these incidents strike. As further detailed in this note, this is just part of a set of basic best practices that Eaton recommends be undertaken by utility customers.

Related to another high-profile cyber event, in December 2016, the Department of Homeland Security (DHS) in conjunction with the Federal Bureau of Investigation (FBI) released a Joint Analysis Report that focused specific attention on the threats posed from observed malicious cyber activity. The report [R3] highlighted an ongoing campaign of cyber-enabled operations directed at both the U.S. government and private entities.



Source—Joint Analysis Report: U.S. Department of Homeland Security, Federal Bureau of Investigation (2016). *GRIZZLY STEPPE—Russian Malicious Cyber Activity* (Publication No. JAR-16-20296A). [R2]

The report also identified certain software code signatures associated with surveillance and network probing activity of particular Russian state actors. Press reports further noted the discovery of signature malicious software code on a Vermont electric utility company laptop [R4]. These incidents serve to emphasize the need for particular vigilance on the part of utility IT organizations.

Eaton encourages utility customers to follow the specific advice given by the DHS, which recommends that network administrators review the IP addresses, file hashes, and provided code signature, and add the IP addresses to their firewall watchlist to determine whether malicious activity has been observed within their organizations [R3] (see note below on firewalls). Reports of detected code can be confidentially submitted to the Department of Homeland Security via https://www.us-cert.gov/forms/report.

EATON
Powering Business Worldwide

General best practice reminders

In reviewing the recent cyber-threat assessments, Eaton's smart grid product team in conjunction with the Eaton Cybersecurity Center of Excellence (CCoE) believes that the recent alerts provide an opportunity to reiterate to our customers the importance of continuing to review, implement and maintain recommended cybersecurity best practices. As is well understood, maintaining system security requires an ongoing commitment to observing best practices that include reviewing and, where necessary, updating both technical measures and policy prescriptions. As highlighted in the DHS-FBI Joint Analysis Report [R3] as well as in the technical guidance statement on the recent ransomware attack, a commitment to good cybersecurity best practices and organizational preparedness is critical to protecting networks and systems; attention to fundamentals is important. The report and guidance also provides a set of questions that should be asked and answered within the utility IT network and smart grid organizations to help prevent and mitigate potential cyber attacks. These organization questions are described below with additional annotations from the Eaton Products group and the Eaton Cybersecurity Center of Excellence teams. These questions are meant to reinforce measures recommended to all of our utility customers as also highlighted in previously published security white papers [R5].

DHS essential best practice strategy recommendations

The Department of Homeland Security further provides "Top Seven (7)" recommended mitigation strategies, which network administrators are strongly encouraged to implement. As indicated by the DHS, these recommendations may prevent as much as 85 percent of targeted cyber attacks. As noted, these strategies are also very much common sense ones, yet DHS continues to see intrusions where organizations fail to apply even these basic measures. As a reiteration of the importance of cybersecurity awareness and the value of supporting best practices, the list of Top Seven (7) DHS strategy recommendations are provided below.

Table 1. Cybersecurity best practices—organization questions [R3]

Best practices	Organization questions	Eaton recommendations and support for utility distribution automation systems
Backups	Do you back up all critical information? Are the backups stored offline? Have you tested your ability to revert to backups during an incident?	Eaton recommends a backup policy of a full backup performed weekly with incremental backups for the other days. Archiving should be done for 2 full backups and 1 set of incremental backups. (Contact Eaton Customer Service for more information.)
Risk analysis	Have you conducted a cybersecurity risk analysis of the organization?	Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Eaton's own development cycle process. Eaton can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments. This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 [R14] and NERC-CIP.
Staff training	Have you trained staff on cybersecurity best practices?	Because many of our Substation Automation customers operate systems fall under the requirements of NERC CIP [R7], Eaton has established a program called "*Helping Utilities Meet NERC CIP*." Eaton can provide support to utilities wishing to implement or upgrade their staff training even where NERC CIP compliance is not a requirement. Security training and security policy process measures that address human behavior and activity are essential to limiting system access attacks. As has been often seen, systems are often compromised not by sophisticated attack vectors, but through lower-tech means such as phishing and related social engineering type attacks.
Vulnerability scanning and patching	Have you implemented regular scans of your network and systems and appropriate patching of known system vulnerabilities?	Eaton implements a comprehensive patch and update process for its Yukon™ application server in conjunction with OS updates. Utilities are encouraged to maintain a consistent process to promptly implement patching and updates once notified.
Application whitelisting	Do you allow only approved programs to run on your networks?	Eaton publishes minimum system requirements (OS, DB, Browser and Java) with each Yukon release. All unneeded applications are removed from customer-delivered servers. Customers are recommended to periodically review needed applications on servers. Eaton recommends the disabling of all unused ports in firewalls and enforces the updating of default passwords at installation.
Business continuity	Are you able to sustain business operations without access to certain systems? For how long? Have you tested this?	Wide-scale security events such as those related to the recent ransomware attacks should be used as opportunities for organizations to review and, where possible, exercise their established continuity plans.
Penetration testing	Have you attempted to hack into your own systems to test the security of your systems and your ability to defend against attacks?	A number of utilities have previously undertaken their own penetrating testing related to deployed Eaton smart grid systems. References can be provided to utilities that wish to hire an outside firm to conduct updated penetration testing.

Table 2. DHS Top Seven cybersecurity mitigation strategies [R3]

Strategy measure	Value impact
Application patching	Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
Application whitelisting	Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
Restricted administrative privileges	Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
Network segmentation and segregation into security zones	Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches.
Input validation	Do you allow only approved programs to run on your networks?
File reputation	Tune Anti-Virus file reputation systems to the most aggressive setting possible; some products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
Understanding firewalls	When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

Implementing DHS best practice strategy recommendations on head-end systems

Application patching

Central to cybersecurity best practices is the timely and consistent maintenance of application and operating system update patches. This has been clearly demonstrated by the recent ransomware attack in which only un-updated systems remained vulnerable. Eaton implements a comprehensive patch and update process for its Yukon application server in conjunction with OS updates. Utilities are accordingly strongly encouraged to maintain a consistent process to promptly implement patching and updates once notified. Information on the Eaton patch update process can be found at: http://www.cooperindustries.com/content/public/en/power_systems/resources/securitysupport.html.

Application whitelisting

An application whitelist defines the list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline [R11]. Application whitelists determine which applications can be installed and executed on a particular host system. For Advanced Metering Infrastructure (AMI), Demand Response (DR), and Distribution Automation (DA) services operating in conjunction with the Eaton smart grid head-end systems, Eaton recommends that no non-Yukon-related applications be maintained on servers hosting the Yukon services. Eaton further specifies the set of browsers and their associated versions that are approved for customer service. Where customers choose to implement additional application on Yukon servers, it is recommended that software technology, including those built into host operating systems, be used for automatically maintaining application whitelists. See NIST SP 800-167 for further guidance [R11].

Restricted administrative privileges

Yukon supports role-based access control through which multiple levels of administrative control can be applied (see Yukon User Manual or contact Eaton Customer Service). Eaton recommends that the available facilities be used to ensure that users of the system are restricted to only the level of access necessary to complete their service functions. This will allow for greater security control by limiting the actions that can be taken if individual personnel account credentials are compromised. Together with available Yukon audit logs, the use of appropriately established access control can be periodically reviewed to detect potentially unusual access activity. Further background on the applicable definitions and the assessment of systems for providing access control can be found in the NIST Interagency Report (NISTIR 7316) [R12].

Network segmentation and segregation into security zones

Network segmentation provides greater isolation for more critical information systems and is a key element of a defense-in-depth network protection strategy. At a minimum, Eaton recommends that a utility Industrial Control Systems network be segmented into a three-tiered architecture (as recommended by NIST SP800-82 [R6]) for better security control—and as highlighted in Eaton's security white paper on utility distribution network security [R5].

Input validation

It is recommended that customers only allow approved application programs to run on their Head-End system server network. Approved applications such as those developed to run Yukon web services are designed to perform sufficient validation of user input in order to prevent attackers from submitting input data or other requests that can be interpreted as commands that can run on the server. Yukon web applications perform necessary input validation so that the application's security mechanisms cannot be bypassed when a malicious user tampers with data sent to the application, including HTTP requests, headers, query strings, cookies, form fields, and hidden fields (see NIST SP800-44 [R10]).

File reputation

In addition to anti-virus tuning protections, security measures associated with file reputation also require that systems should be capable of authenticating the source and verifying the validity of all software or firmware that is downloaded for execution. Eaton provides a secure enterprise infrastructure for the transfer of head-end applications to customer networks. The Eaton smart grid RF network also implements public key (RSA-2048) signing and verification of all firmware that is downloaded to RF devices [R9]. Customers are similarly encouraged to ensure that all applications introduced within their head-end systems are assessed for their allowed operating permissions.

Understanding firewalls

Firewall devices and programs allow for controlling the flow of traffic between, into and out of customer networks and facilitate the maintenance of differing security postures. Firewalls provide a frontline external protection to a customer's network, but that protection will be limited to the extent of security configurations and the access provisions permitted at the firewall. Eaton provides a list of ports needed for Yukon and network application protocols and recommends that utility IT staff close all ports not in use by our systems within access firewalls. Any application ports accessible through the firewall should be specifically set only in accordance with an approved and supported application. Additional guidance and policies on firewall configuration can be found is NIST SP 800-41 [R13].

Continued enhancement of your organization’s cybersecurity posture

Eaton encourages utility customers to continue to work to make cybersecurity review and best practices an integral part of their operational processes. A highly recommended resource for guidance on refining overall understanding and approaches to infrastructure system security is the recently updated NIST “*Framework for Improving Critical Infrastructure Cybersecurity*” [R8].

To continue to enhance your organization’s Cybersecurity Posture, the federal government, through the DHS, also offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Eaton’s Customer Service and CCoE team also stands ready to help direct customers to available local and federal cybersecurity resources.

Eaton team contributors

- Roger K. Alexander—Chief Systems Architect
- David Sutton—Yukon Product Architect
- Shailendra Fuloria—Eaton CCoE Security Architect
- Megan Freeman—Marketing Manager

References

[R1] “US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Update on Reported Ransomware Infections including WannaCry Alerts.” https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported

[R2] “Ransomware, what it is and what to do about it.” https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

[R3] “GRIZZLY STEPPE – Russian Malicious Cyber Activity”, Joint Analysis Report, Reference Number: JAR-16-20296, December 29, 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[R4] https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.9db5b8a2c079

[R5] “Cybersecurity considerations for electrical distribution systems”, Eaton CCoE, November 2016. http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=WP152002EN

[R6] National Institute of Technology (NIST) “Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82”, Revision 2, May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R7] “North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP)”, Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[R8] National Institute of Technology (NIST) “Framework for Improving Critical Infrastructure Cybersecurity”, V1.1, January 2017. https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

[R9] “Eaton Smart Grid Radio Frequency (RF) Network Security Overview”, May 2017. http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=WP100003EN

[R10] National Institute of Technology (NIST) “Guidelines on Securing Public Web Servers, NIST Special Publication 800-44”, V2, January, 2007. http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

[R11] National Institute of Technology (NIST) “Guidelines on Application Whitelisting, NIST Special Publication 800-167”, October, 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

[R12] National Institute of Technology (NIST) Interagency Report 7316 “Assessment of Access Control Systems”, September, 2006. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[R13] National Institute of Technology (NIST) Interagency “Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41”, October 2009. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R14] International Electrotechnical Commission, IEC 62443, “Industrial communication networks—Network and system security”

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Electrical Automation Solutions Division
3033 Campus Drive
Suite 350N
Minneapolis, MN 55441
United States
Eaton.com/cooperpowerseries

Printed in USA
Publication No. WP910003EN / Z19565
June 2017

Powering Business Worldwide