NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

Modular Malware Targeting Electric Industry Assets in Ukraine

Initial Distribution: June 13, 2017

The E-ISAC is issuing a Level 1 NERC Alert to inform NERC registered entities of capabilities found in malware that targeted electric industry assets in Ukraine.

Why am I receiving this? >>
About NERC Alerts >>

Status:	No Reporting is Required – For Information Only
	**PUBLIC:** No Restrictions More on handling >>
Instructions:	NERC advisories are designed to improve reliability by sharing critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure for use as your organization deems appropriate. **No response is necessary.** A NERC advisory is not the same as a Reliability Standard, and your organization will not be subject to penalties for a failure to implement any recommendations or practices provided in this advisory. Additionally, issuance of this advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the advisory if such failure constitutes a violation of a Reliability Standard.
Distribution:	**Initial Distribution:** Balancing Authority, Distribution Provider, Distribution Provider – UFLS, Frequency Response Sharing Group, Generator Owner, Generator Operator, Planning Authority, Reliability Coordinator, Resource Planner, Regulation Reserve Sharing Group, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, Transmission Service Provider Who else will get this alert? >> What are my responsibilities? >>
Primary Interest Groups:	Cyber Security – Control Systems, Cyber Security – Corporate IT, Generation Engineering, Generation Operations, System Operations – Transmission Engineering, System Operators, System Operators – System Protection, Transmission Planning

Advisory:

Cybersecurity firms Dragos Inc.[1] and ESET[2] reported on malware that specifically targets electric industry assets and has been associated with the cyber-attack that caused an electric outage in Kiev, Ukraine in December 2016. The following is a collaborative effort between the E-ISAC and Dragos Inc. to provide recommended actions in light of the information in their reports.

The malware is a framework comprised of modules that can be added or removed depending on the desired capabilities and the specific devices and equipment found in a victim's environment.

The malware can cause loss of visibility, loss of control, manipulation of control, interruption of communications, and deletion of local and networked critical configuration files.

By leveraging preloaded configuration file(s) with the utility's asset deployment information, the malware can identify open platform communication (OPC) server items and devices that control circuit breakers. These configuration files may also allow the malware to run independently. The malware can also establish communications to cross the Information Technology/Operational Technology (IT/OT) boundary. This was done through customization of the malware to use internal proxy hosts, showing significant understanding of the target environment.

The malware can cause a loss of visibility and control by setting all OPC items to an "out of limits" value, or by killing the Communication Service process, establishing communication with slave devices and behaving as the master process. As the master process, it can set specific values, enumerate Information Object Addresses (IOAs) or set Remote Terminal Unit (RTU) IOAs to open or toggle between open and close. The malware can perform these actions over Transmission Control Protocol (TCP)/Internet Protocol (IP) and serial communications.

After the malware performs its desired effect, it deletes key operating system files and settings of the compromised host and wipes Industrial Control System (ICS) configuration files on local and mapped networked drives.

The malware can reportedly perform a denial of service attack on a specific series of digital protective relays by leveraging a patched vulnerability that will cause an unpatched relay to become unresponsive. Requiring a manual reset of the relay.

[1] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[2] https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-dangerous-malware-designed-to-disrupt-industrial-control-systems/

Importantly, the malware causes the aforementioned effects by leveraging the common functionalities and the inherent system-to-system trust typically found in grid operations. It does not leverage vulnerabilities or zero-day exploits for its core desired effects. The malware was coded with advanced knowledge of grid operations and, when used in the cyber-attack in Kiev, was delivered to specifically impact the target location's human machine interfaces (HMIs), remote terminal units (RTU), and circuit breakers.

The malware requires detailed information of the victim's environment to cause desired effects. This information may have been obtained prior to the attack on the Ukrainian utility and loaded into the configuration file(s). Alternatively, the malware may be used to obtain the information.

The malware's framework design allows for the swapping in and out of modules that can tailor its capabilities for different grid ICS environments. While the Ukrainian victim's deployment in that scenario used communication protocols not typically found in the United States (IEC 60870-5-101, and IEC 60870-5-104), the modules that leveraged those communication protocols could be replaced with modules to impact protocols that are relevant and in high use throughout North America. Therefore, the malware's attack capabilities may not be limited to a technology or specific vendor.

Direct external communication was not necessary for the malware to function. The Ukraine utility's ICS environment required the malware to communicate externally using a local proxy. The proxy communicated externally by beaconing on 3128/tcp. Once a connection was established, it initiates a backdoor by sending POST requests that include the compromised Windows system's global unique identifier (GUID) in the body of the packets. The GUID is used to authenticate the compromised system. Communication to an external command and control (C2) server is accomplished through the proxy and across TOR exit nodes.

The malware sample examined by ESET was reported to have a denial of service module that leveraged the patched vulnerability CVE-2015-5374. This vulnerability targets SIPROTECT digital protective relays. Although this vulnerability is vendor specific, the malware does not need this module's functionality to perform its core objective. Additionally, there is no evidence that SIPROTECT relays were targeted in the Ukraine attack.

Due to the malware's capability to act autonomously through time bombs, passive defenses such as air gapping will not prevent the malware from being activated once in the network. In the attack on the Ukrainian utility, the time bomb was used to execute ICS file wiping hours after the breakers were set to open or toggle between open and close.

Currently, the E-ISAC is not aware of how the malware was introduced into the Ukrainian victim's network.

Recommended Actions:

The E-ISAC encourages members to limit privileged access and remove unnecessary privileged accounts from the ICS environment. Authentication should include two factor authentication. Also, members should develop an understanding of the communication protocols used in their ICS environment and create a baseline of how these protocols are typically used. This base knowledge should be used to monitor network traffic for deviations in Master/Slave communication and abnormal telemetry and IOA settings.

The modular nature of the malware makes it is unlikely that file hashes and other signature-based detection methods will effectively detect the malware on a host. Application whitelisting on HMIs may prevent some malware from executing. Behavior-base detection methods, such as YARA rules, may provide a higher confidence of detection.

Proper patch management processes will also help mitigate the effectiveness of some add-on functionalities of the malware, such as the denial-of-service module. Software updates should be validated with digital hashes from the vendor. Additionally, a redundant backup and recovery strategy can mitigate the effects of the malware's data wiping functionality.

Background:

The malware at the center of this notification is a development and improvement on previous cyber-attack trade craft used to attack Ukraine's electric infrastructure. Prior to the December 18, 2016 cyber-attack that leveraged this malware, Ukraine's electric infrastructure was the victim of another cyber-attack that affected approximately 225,000 customers for several hours.

On December 23, 2015, three of Ukraine's 23 *Oblenergos* were attacked. The coordinated attacks focused on breaker controls at three electricity distribution sites. The breakers were opened through remote access to the operations environment.

The 2016 attack on Ukraine's grid automated a lot of the actions necessary to cause the desired effect. The actors behind these cyber –attacks appear to continue developing and improving their ability to impact Ukraine's power grid.

Generally, the E-ISAC continues to request:

- Member feedback on the quality of indicator provided by the E-ISAC.
- Additional details, including activity logs or forensic artifacts, such as binaries or network captures to derive stronger context or indicators that can be shared with members and partners.
- High-confidence indicators or signatures for both untargeted and targeted threats to the electricity sector.

With this information, the E-ISAC can provide updates allowing members to be more effective in detecting and scoping of this activity and other threats. We encourage members that have information regarding successful detections of threats, or updates involving suspected activity later determined benign, to share them on the E-ISAC portal (https://www.eisac.com).

Contact:

Electricity ISAC
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600 – North Tower
Atlanta, GA 30326
alerts@eisac.com

Alert ID: A-2017-06-13-01

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560 | www.nerc.com