Security Notification – CrashOverride/Industroyer Malware

15-June-2017

Overview

Schneider has become aware of reports made public from ESET and Dragos that details an Industrial Control System (ICS) targeted attack platform dubbed CrashOverride/Industroyer. This malware platform was thought to have been used in the 2016 cyberattack against Ukraine's critical infrastructure. Schneider Electric wants its customers to be aware of this threat and the indicators that highlight presence of the malware.

Details

The modules of this platform are designed to disrupt the working processes of an ICS used primarily in electrical substations leveraging the following protocols: IEC870-5-101, IEC870-5-104, IEC61850, and OPC DA.

Reported malware capabilities include:

- Issues valid commands directly to RTUs over ICS protocols which can potentially sequence toggle circuit breakers in a rapid open-close-open-close pattern. This could result in physical damage.
- Prevents legitimate communications with field equipment by denying service to local serial COM ports on Windows devices
- Scans and maps ICS environment using OPC, making it easier to provide reconnaissance to execute payload
- Includes a wiper module which could result in an unusable windows system

Mitigation

Schneider Electric recommends customers follow the instructions outlined in the released US CERT alert:

https://www.us-cert.gov/ncas/alerts/TA17-163A

For customers requiring additional support, Schneider Electric Industrial Cybersecurity Services team are available to help with assessments and deployment support:

http://www.schneider-electric.com/b2b/en/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

For More Information

- Dragos- CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
- ESET- WIN32/INDUSTROYER A new threat for industrial control systems: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric: Schneider Electric is the global specialist in energy management and automation. With revenues of €27 billion in FY2015, our 160,000 employees serve customers in over 100 countries, helping them to manage their energy and processes in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies will reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2017.06.16 17:12:04 -04'00'