A Case Study of the CRASHOVERRIDE Malware, Its Effects and Possible Countermeasures

Samuel Rector
Tidewater Community College

A Case Study of the CRASHOVERRIDE Malware, Its Effects and Possible Countermeasures.

Samuel Rector

Advised by Leigh Armistead President of Peregrine Technical Solutions

COVA CCI Undergraduate Research, Spring 2024

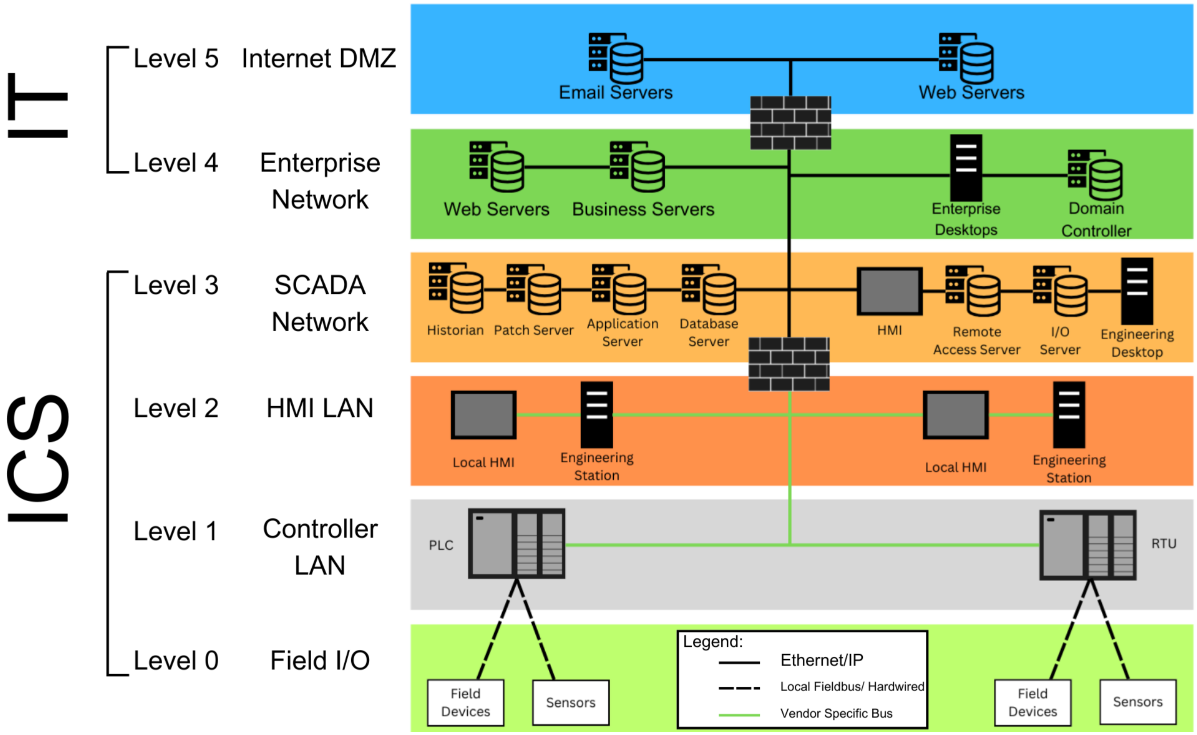
Abstract

CRASHOVERRIDE is a modular malware tailor-made for electric grid Industrial Control System (ICS) equipment and was deployed by a group named ELECTRUM in a Ukrainian substation. The malware would launch a protocol exploit to flip breakers and would then wipe the system of ICS files. Finally, it would execute a Denial Of Service (DOS) attack on protective relays. In effect, months of damage and thousands out of power. However, due to oversights the malware only caused a brief power outage. Though the implications of the malware are cause for researching and implementing countermeasures against others to come. The CISA recommends several defenses implement additional ICS firewalls, enable Application Whitelisting, and start configuration/ patch management programs, etc.

Keywords: industrial control systems, electrical grid, SCADA

1.0 What are ICS networks and why do they matter?

ICS networks are composed of two smaller networks that work in conjunction to record and control physical processes e.g. car manufacturing. On layers three through two is the Supervisory Control And Data Acquisition (SCADA) network, the SCADA network records onto various servers and controls processes at a high level via Human Machine Interfaces (HMIs) and through various other means. Lower down on layers one through zero is the production network where field devices such as sensors and actuators send and receive commands from Programmable Logic Controllers (PLCs) or other field controllers such as Remote Terminal Units (RTUs). Typically, most communication on the SCADA network is mediated through Ethernet/IP and on the production network it can vary depending on the field device and controller e.g. (IEC 104, IEC 61850, Lonworks) [2,5,8]. Outside of the ICS network will be found the enterprise network on layer four which is then connected to the internet, layer five.



1.1 What is CRASHOVERRIDE – what, where, when, why and how.

CRASHOVERIDE, aka INDUSTROYER, is malware tailor-made for the electric grid deployed by ELECTRUM on a single Ukrainian substation on December 17th, 2016. After analysis it appears that the deployment of this malware was a prototype run rather than fully functional malware. What sets this ICS malware apart is that the malware was made to be modular and with the intent to target electric grid ICS equipment . CRASHOVERIDE consists of several modules although the most relevant being the backdoor, this provides access to a compromised machine; the loader module, this allows for the payloads to execute properly; and the payload modules, these perform desired malicious actions (e.g. data wiping) [8]. Once executed this malware would launch protocol exploits that flip breakers rapidly; two hours later data would be wiped on the systems infected. Finally, the malware would execute a DOS exploit on protective relays. In effect more than 225k Ukrainian residents would be out of power for weeks or possibly months [3].

1.2 Initial access to the enterprise network.

Initial access to the enterprise network is mostly unknown. However, there is more credible evidence as to how ELECTRUM was able to access the ICS network. It's likely that credentials and supplementary authentication information were taken from the IT network and repurposed for use to eventually gain access to the ICS network. Evidence shows that the initial access was likely through a Microsoft SQL server dual-homed to the ICS network or that the server had features to access the IT network with two similar servers being accessed around that time[6,4]. Shortly after the server was compromised several quick actions were done to allow for new privileged accounts to be made as well as event logging is disabled [4].

2.0 Attack pre-positioning

After little activity the adversaries came back on 12 December 2016 to profile the ICS network via the three Microsoft SQL servers. On that day ELECTRUM performed network connectivity testing, directory info querying, directory listings for about two hours. Going on to authenticate the capabilities of a series of hosts. Along with rapidly sending out RPC authentication attempts to another set of hosts for the user “Administrator” utilizing the same password. Interestingly the tools leveraged by ELECTRUM were mainly native and relatively unused by other adversaries making them as of 15 December 2016 still completely undetected [8]. After authentication ELECTRUM then decided it was time to push out the CRASHOVERRIDE framework out to specific hosts December 16 2016. The CRASHOVERRIDE framework consists of the launcher module, payload (dependent on ICS protocols), a wiper module, and a configuration file. After additional testing, ELECTRUM then began to push out malicious software to hosts connected to the SQL servers on December 17 2016 with the exception of the launcher module. The launcher module would later be deployed once further reconnaissance showed what payload needed to be loaded in by the loader module as each host uses a different protocol [4].

2.1 CRASHOVERRIDE modules

CRASHOVERRIDE has several important modules to understand its operation. There is a backdoor module that is implemented into the framework but was scantly used and was implemented well after first intrusion is mostly irrelevant. Starting from the top is the launcher module, this module is responsible for executing the payloads and the data wiper. In most cases, when the launcher reaches a certain date it will start two tasks set at the highest priority. One will try to load the payload and the next will stand by for two hours and then attempt to load the data wiper. Next down the line are the payload modules, these are specific to what host is being targeted. First is the payload covering IEC 101 and IEC 104 which is an international protocol used for tracking and commanding electric power networks. IEC 101 is conducted through a serial connection whereas IEC 104 is an extension allowing IEC 101 to run via TCP/IP [1, 4]. Essentially IEC 101 and 104 modifies the state of Information Object Addresses (IOAs) values ultimately to flip breakers on and off continuously. Separate from that is the IEC 61850 payload which is a protocol, partly developed by ABB, that is used for substations globally. This payload produces the same output as the IEC 101 and 104 payloads just through different means. The same goes for the other payloads such as the Open Platform Communications (OPC) payload and the hybrid OPC and IEC 61850 payload. The next module is the wiper module which is the final phase of the attack and is executed two hours after the execution of the payloads. This module consists of three stages: set all system registry values to zero, remove any ICS related files e.g. ABB file types , and end system processes. In effect the system will crash and be bricked making it hard for system recovery. One last addition to the malware was a Denial Of Service (DOS) attack that was attempted on the Siemens SIPROTEC protective relays in the substation. Where the protective relays would need to be rebooted manually to regain functionality. The implication is, once operators manually return power to the grid they'll be restarting it unprotected, potentially causing a major electrical fault [4].

2.2 Fallout of attack on ICS network.

The fallout of the attack was less catastrophic than had been intended. First the DOS attack on the protective relays failed and due to some oversites in the adversary's code the malware was only able to affect less than 225k customers and power loss was brief. For the most part ICS cybersecurity companies were able to decipher the intentions and the functionality of the malware making the data wiper less effective. Though the implications of what possibly could happen are why countermeasures are to be taken [4].

3.0 Countermeasures against future ICS malware.

There are no simple passive measures that can be taken to ensure a secure ICS network though the CISA has provided potential effective defenses against further attacks. One defense is utilizing Application Whitelisting (AWL); this prevents any unauthorized code execution from occurring and it adds another layer for adversaries to hurdle through. As seen in the initial intrusion into the ICS network, adversaries utilized captured credentials. Which is why the CISA recommends that "Asset owners/operators " should integrate "authentication and authorization protocols" [6] or should leverage ICS firewalls for legacy devices if not already implemented. Multi factor authentication should be implemented where possible and if passwords are needed they should be complex and should be rotated every 90 days at a minimum. Aside from the ICS network the CISA recommends that strictly the corporate network and ICS network need separate credentials. If malware still enters the ICS network it's important that those systems are backed up into offline storage and tested. [6, 7]. Another solution, this relates to the DOS attack, the CISA gives is to make a configuration/ patch management program. With such a program, devices will get the necessary patches they need [6].

4.0 The future of ICS cybersecurity

CRASHOVERRIDE marks a significant advance in adversaries' tradecraft from the ICS specific protocol exploits to the DOS attack on protective relays and with a little tweaking the CRASHOVERRIDE could've been highly successful in causing a massive power outage spanning several weeks [4]. With that, defense measures have been recommended from the CISA. In summary ICS networks need to be more segmented, updated, and backed up [7]. ICS cybersecurity tends to be behind IT, so if ICS can meet with IT security then far fewer incidents would happen.

References

[1] Anton Cherepanov, (2017, Jun 12), WIN32/INDUSTROYER A new threat for industrial control systems, ESET, https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf

[2] Brendan Galloway, Gerhard P. Hancke, (2013), Introduction to Industrial Control Networks, IEEE, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6248648

[3] Joe Slowik, (2019, Aug 15),CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack, Dragos, https://www.dragos.com/wp-content/uploads/2021/03/CRASHOVERRIDE.pdf?hsCtaTracking=aa9179e5-48b0-464b-9b78-ffd6242fb635%7C30d0dd95-4a2b-4045-a7cc-c6bfa1be5e2d

[4] Joe Slowik, (2018, Oct 10), Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE, Dragos, https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf?hsCtaTracking=25456437-61c7-415a-ab14-7ec85e60babb%7Cef8df52d-ed60-405b-929a-df2b1b05dbdc

[5] Joseph Bush, et al, (2022, Aug), Installation Utility Monitoring and Control System Technical Guide, USACE, https://erdc library.erdc.dren.mil/jspui/bitstream/11681/45081/1/ERDC-CERL%20SR-22-1.pdf

[6] Michael McFail, Jordan Hanna Daniel, Rebori-Carretero, (2021, Dec), Detection Engineering in Industrial Control Systems., MITRE,

https://www.mitre.org/sites/default/files/2022-04/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf

[7] (2021, Jul 20), CrashOverride Malware, CISA, https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware

[8] (2017, Jun 12), CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations, Dragos, https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf?utm_referrer=https%3A%2F%2Fwww.dragos.com%2Fresources%2Fwhitepaper%2Fcrashoverride-analyzing-the-malware-that-attacks-power-grids%2F