



Substation Cybersecurity: an Asset Management Viewpoint

Gowri Rajappan

30 October 2018



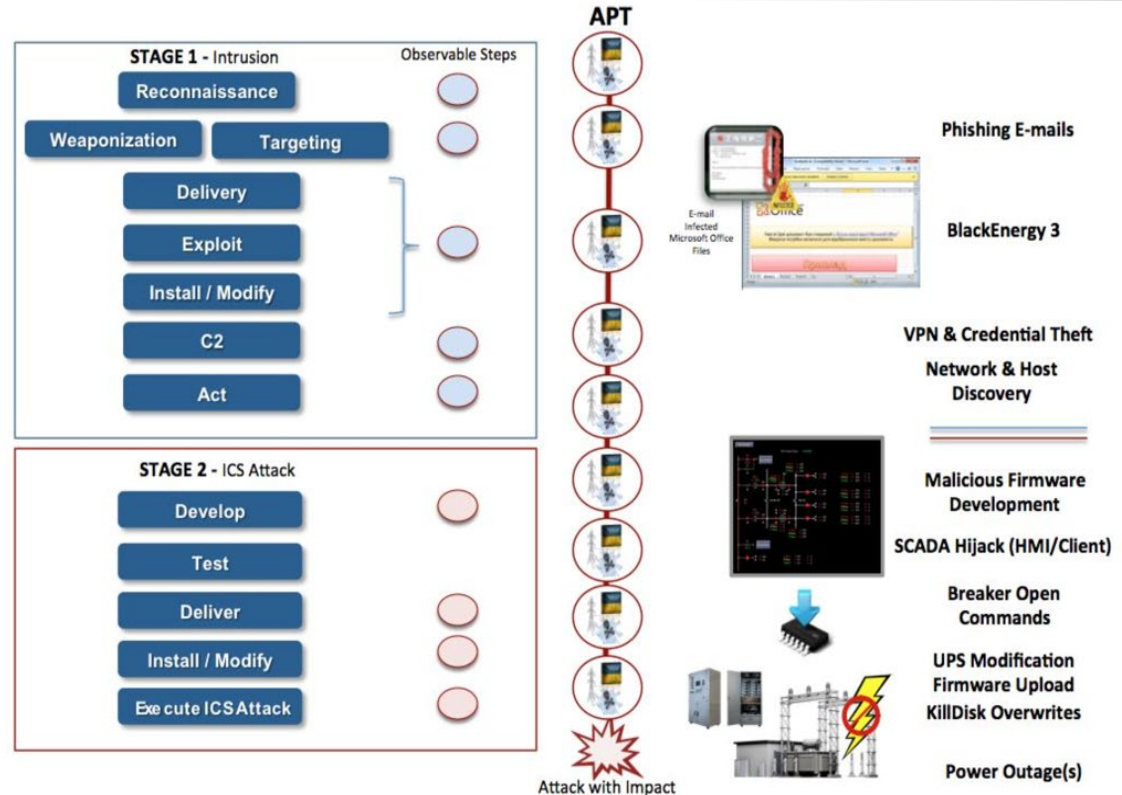
- Main Vulnerabilities / Threats
 - Malware
 - Device / System Issues
 - Data Protection Issues

- Countermeasures
 - TCA Program
 - Patch Management Program
 - Data Management Program

- STUXNET
 - Siemens WinCC Insecure SQL Server Authentication (ICSA-12-205-01)
 - Siemens SIMATIC STEP 7 DLL Hijacking Vulnerability (ICSA-12-205-02)
- Dragonfly/HAVEX
- BLACKENERGY 2
 - GE CIMPLICITY Path Traversal Vulnerabilities (ICSA-14-023-01)
 - Siemens WinCC Remote Execution Vulnerabilities (ICSA-14-329-02D)
 - Advantech WebAccess (ICSA-14-281-01B)
- CRASHOVERRIDE
- TRITON

Ukraine Grid Cyberattacks

- In December 2015, attackers compromised SCADA and opened circuit breakers in at least 30 substations.
 - Interruption of service to over two hundred thousand customers.
 - Switched to manual mode of operation to restore power.
- In December 17th, 2016 against a transmission substation in Kiev, Ukraine – appears to be a proof of concept to test automated exploitation of transmission substation.
- Started with phishing emails that infected corporate machines.
- Another potential vector is to infect asset testing & maintenance machines.

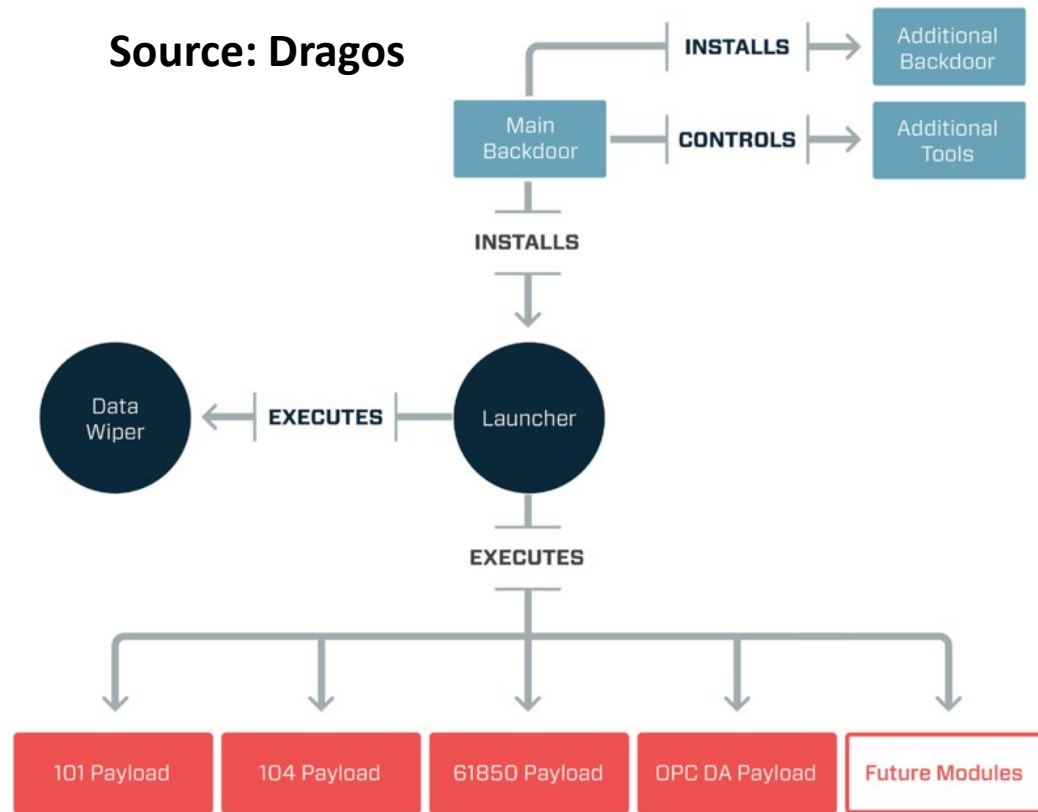


CRASHOVERRIDE



- Advanced modular framework consisting of a backdoor, a loader, supporting modules, and payloads.
- Backdoor provides remote access to the system and has the ability to work through the local proxy.
- Currently identified payloads are IEC 61850, OPC DA, and IEC-60870-5-101/104.

Source: Dragos



CRASHOVERRIDE IEC 61850 Module



Source: ESET

- Tries to connect to Port 102 of IEDs whose IP addresses it either read from a config file or discovered from the network.
- If target responds to ConnectionRequest packet, it sends an InitiateRequest.
- If successful, getNameList is sent.
- Appears to look for Switch Controller (CSWI) Logical Node
- May issue MMS Read request for Model and stVal.
- May issue an MMS Write request that will change its state.

Device Vulnerabilities



Advisory (ICSA-16-147-02)

Sixnet BT Series Hard-coded Credentials Vulnerability

Original release date: May 26, 2016



Advisory (ICSA-15-076-01)

XZERES 442SR Wind Turbine Vulnerability

Original release date: March 17, 2015



Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

OVERVIEW

Independent researcher Maxim Rupp has identified a cross-site request forgery (CSRF) vulnerability in XZERES's 442SR turbine generator operating system (OS). XZERES has produced a patch that mitigates this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following XZERES product is affected:

- 442SR Wind Turbine.

IMPACT

Successful exploitation of this vulnerability allows the username password to be retrieved from the browser and will allow the default user password to be changed. This exploit can cause a loss of power for all attached systems.

[More Advisories](#)

Advisory (ICSA-17-143-01)

Moxa OnCell

Original release date: May 23, 2017



[More Advisories](#)

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

CVSS v3 9.8

ATTENTION: Remotely exploitable/low skill level to exploit.

Vendor: Moxa

Equipment: OnCell

Vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Plaintext Storage of a Password, and Cross-Site Request Forgery

Device Vulnerabilities



Secure | <https://www.shodan.io/search?query=red+lion+port%3A789+country%3A%22PT%22>

Shodan Developers Book View All...

SHODAN red lion port:"789" country:"PT" 🔍

Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
2

TOP COUNTRIES

Portugal 2

TOP ORGANIZATIONS

Nos Comunicacoes, S... 1
Meo - Servicos De Co... 1

TOP PRODUCTS

Red Lion Controls 2

212.55.152.139
Meo - Servicos De Comunicacoes E Multimedia, S.A. Manufacturer: Red Lion Controls
Added on 2017-09-09 16:04:46 GMT Model: MC3D
Portugal
Details

212.55.152.139

Authentication Required

http://212.55.152.139 requires a username and password.
Your connection to this site is not secure

User Name:

Password:

Log In Cancel


red lion Connect. Monitor. Control.

PID CONTROLLERS

PAX2C
PXU
T48/P48
TSC/PSC
Modular Controller
Modular Controller Modules
DLC
Product Selector

Home » Products » Industrial Automation » Controllers & Data Acquisition » PID Controllers » Modular Controller

Modular Controller



Overview:
Red Lion's CSMSTR Modular Controller allows for a custom controller to be configured for unique applications. CSMSTR allows up to 16 slave modules to be connected and powered by a single master controller.

DHS Alert TA18-074A : “The threat actors appear to have deliberately chosen the organizations they targeted, rather than pursuing them as targets of opportunity. Staging targets held preexisting relationships with many of the intended targets.”

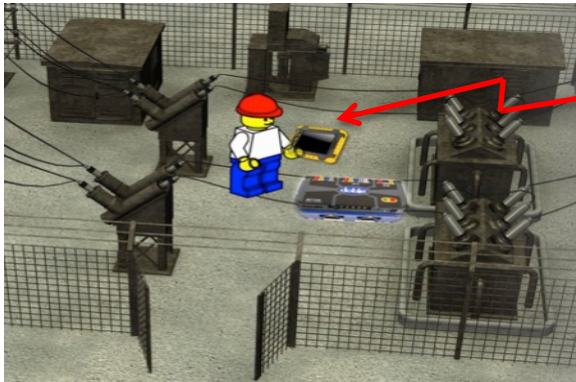
- Sensitive data on flash drives lost or stolen.
- Photos posted on a publicly accessible Human Resources webpage, when enhanced, displayed control systems equipment models and status information in the background.
- Compromise of trade publication websites and altering them to include malicious content for harvesting corporate credentials of the website visitors. This is known as a watering hole attack, since these websites cater to specific industries, and therefore are “watering holes” that attract people in that industry.

Field Force Enablement

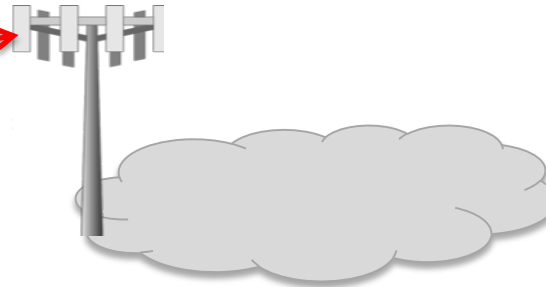
Separate device for substation / control environments

- Keep corporate computers used for email and general web-browsing out of the substation.
- Software under whitelist controls so as to prevent malware.
- Eliminate USB drives, a leading malware propagation mechanism.

Data Acquisition



Data Communication



Data Storage



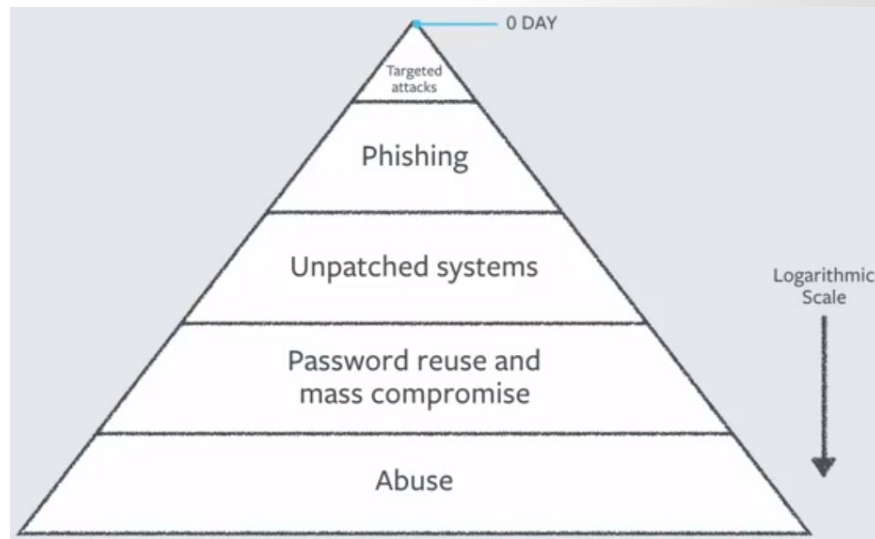
On-Demand Support



Patch Management



- Important measure for operational integrity.
- Planned replacement of vulnerable older assets with discontinued support.
- Difficult problem:
 - Knowing device portfolio.
 - Tracking vulnerabilities for those devices – hundreds of vendors, change in ownership, abandoned products.
 - Identifying locations of the devices.
 - Scheduling work at these locations within a timeline appropriate for the severity of the vulnerability.



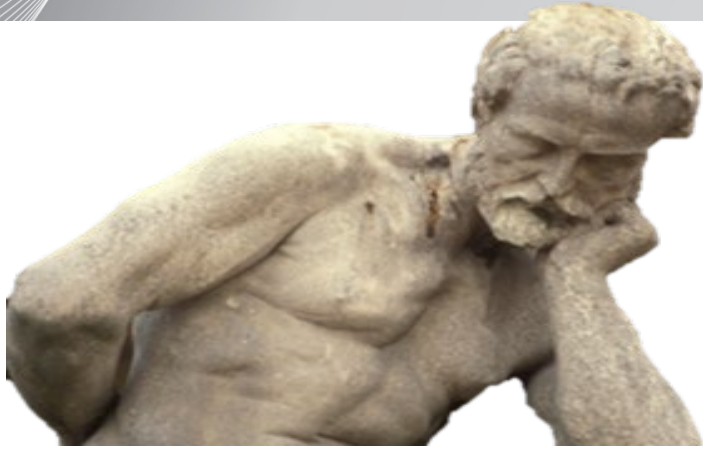
**Source: Alex Stamos (Facebook CSO),
keynote @ Black Hat USA 2017**

- **Monitoring to Ensure Patching of Unreachable Devices:** Monitoring capability is needed for awareness of the patching status of all the devices, so that appropriate intervention can be undertaken for devices that aren't patched in a timely manner.
- **Asset Management:** Accurate and up-to-date information on the various field devices, images, software applications, and versions in use, so that they can be updated in a manner consistent with their use.
- **Comprehensive Vulnerability Monitoring and Patching:**
 - A vulnerability monitoring program that continuously monitors, identifies and evaluates for new vulnerabilities and corresponding patches or workarounds
 - Multiple patch deployment means in order to ensure that even the most difficult applications can be patched
 - When all else fails, it may take the entire application to be replaced with the new version.

- Strong encryption scheme, such as full-disk encryption with pre-boot authorization, in order to ensure that information from the device cannot be extracted even if the attacker has physical access to the device.
- Restrict communication capability so that they can only communicate with the private databases and servers needed to manage the data and the devices.
 - Prevents any information from these devices from being sent to an attacker.
 - A key implication of this is that the field devices cannot be used as general-purpose computers.
- Regularly purge sensitive information from the field devices so that the intelligence obtained from it is minimal and incomplete.
- Field device management program that is able to track all the field devices and help identify unusual activity such as not reporting in for an extended period of time.

- Cybersecurity grows in importance with each newly discovered cyberattack
- Asset management professionals, due to their close contact with critical assets, are at the forefront of the defense
 - Need to become more aware of security threats and countermeasures
 - Help combat the cyber threats
 - Take active part in determining the technology and compliance approaches to fieldwork
- When security / compliance solutions are field operations-centric, productivity also improves

Questions?



Gowri Rajappan, PhD
Doble Engineering
grajappan@doble.com

