21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2018 Grid of the Future Symposium

Substation Cybersecurity: an Asset Management Viewpoint

G. RAJAPPAN
Doble Engineering Company
USA

SUMMARY

Asset management and field personnel are at the forefront of the defense against cyber threats. They design or perform asset maintenance activities that ensure the reliability of the grid. Since they regularly work with critical assets, the technology and processes they use need to be secured and compliant with regulatory requirements. The best security and compliance approach, so as not to impede work, is to start with the work processes and tailor Information Technology (IT) security controls to them. To do this, IT, Operations Technology (OT), and Compliance departments have to work closely together in order to develop a clear, common understanding of the work processes and compliance requirements. This paper will describe key security and compliance considerations in asset management and user-friendly approaches to achieving them. The IT needs of asset management have long been neglected and, as this paper discusses, the activities around security and compliance also has the potential to improve productivity in the field.

KEYWORDS

Cybersecurity, NERC CIP, Transient Cyber Asset (TCA), Security patch management, Field force automation, Malware, Operations Technology (OT).

grajappan@doble.com

INTRODUCTION

On 15 March 2018, the United States Computer Emergency Readiness Team (US-CERT), a division of the US Department of Homeland Security (DHS), issued Alert TA18-074A on Russian Government cyber activity targeting the US energy sector [1]. This extraordinary direct attribution to the Russian Government reflects the perilous times we live in. In response to such advanced cyber threats, FERC and NERC have spearheaded stringent cyber security requirements in the form of Critical Infrastructure Protection (CIP) standards. These standards have improved the security of critical Bulk Electric System (BES) facilities such as control centers and high-voltage substations.

While the industry has made great strides in securing BES facilities, critical vulnerabilities exist outside them. For instance, lax security controls in the corporate IT network can provide an entry-point and foothold for attackers. In fact, the aforementioned hackers first gained access through corporate IT systems such as file servers and email servers. Electronic equipment such as test sets and laptops used by the field personnel are another significant source of vulnerability. Federal Energy Regulatory Commission (FERC) noted this in Order 791 and expressed concern over how such electronic devices could bring malicious software (malware) into critical facilities such as substations [2]. In response to the FERC directive, NERC developed CIP-010-2 R4 requirements to secure Transient Cyber Assets (TCAs).

Field personnel are important bulwark against these two vectors of attack. The attackers, once they gain a foothold in the corporate IT network, attempt to laterally move to OT networks and then exploit any vulnerabilities in the OT network. Testing the substation for vulnerabilities and patching the vulnerabilities, which are tasks performed by the field force, are critical in preventing this from happening. Judicious management of the TCAs are also essential to ensure that they aren't exploited to gain entry to the substation. This important role of the field crew is generally overlooked, partly because the IT departments that control technology don't understand fieldwork, and therefore there is little investment in better equipping them. In this paper, we will attempt to bridge the knowledge gap by taking a fieldwork centric viewpoint of the threats against critical facilities, substations in particular, and the best approaches to mitigating the threats.

THREATS TO SUBSTATION

There are three main sources of vulnerability in substations:

1. Malicious software (malware).
2. Cyber asset/system vulnerabilities and misconfigurations.
3. Data protection weaknesses.

In recent years, there have been several malware tailored to attack Industrial Control Systems (ICS). STUXNET, the first known ICS malware, exploited some Siemens zero-day vulnerabilities. Dragonfly/HAVEX was first used against some European ICS vendors, and a variant of this seems to have been utilized in the recent Russian Government attacks against the US energy sector [3]. BlackEnergy was used in the first Ukraine grid attack in December 2015. CrashOverride was used in the second Ukraine grid attack in December 2016. CrashOverride represents a new generation of ICS malware. As shown in Figure 1, it has modular design with modules for various substation automation protocols such as IEC 61850 and OPC, as well as the capability to issue commands to substation devices, such as an open command to an Intelligent Electronic Device (IED) controlling a circuit breaker. It has the versatility to attack substations with different automation protocols and design.

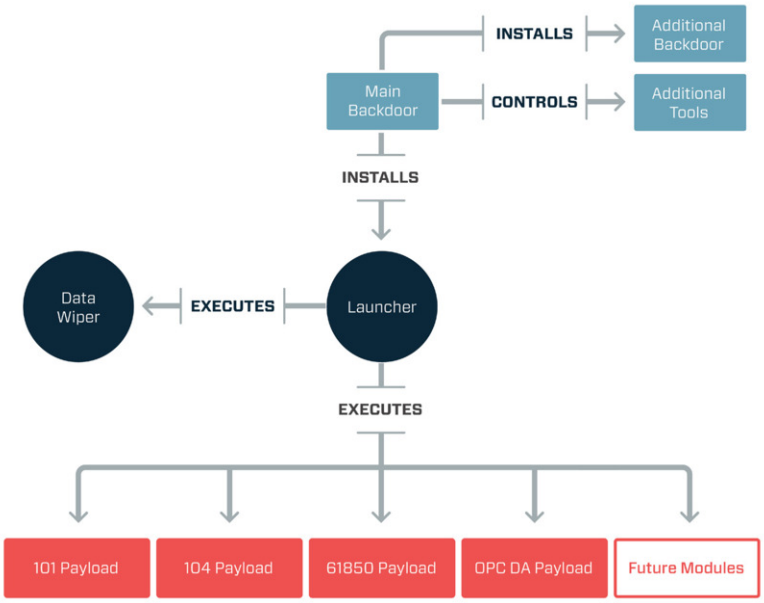
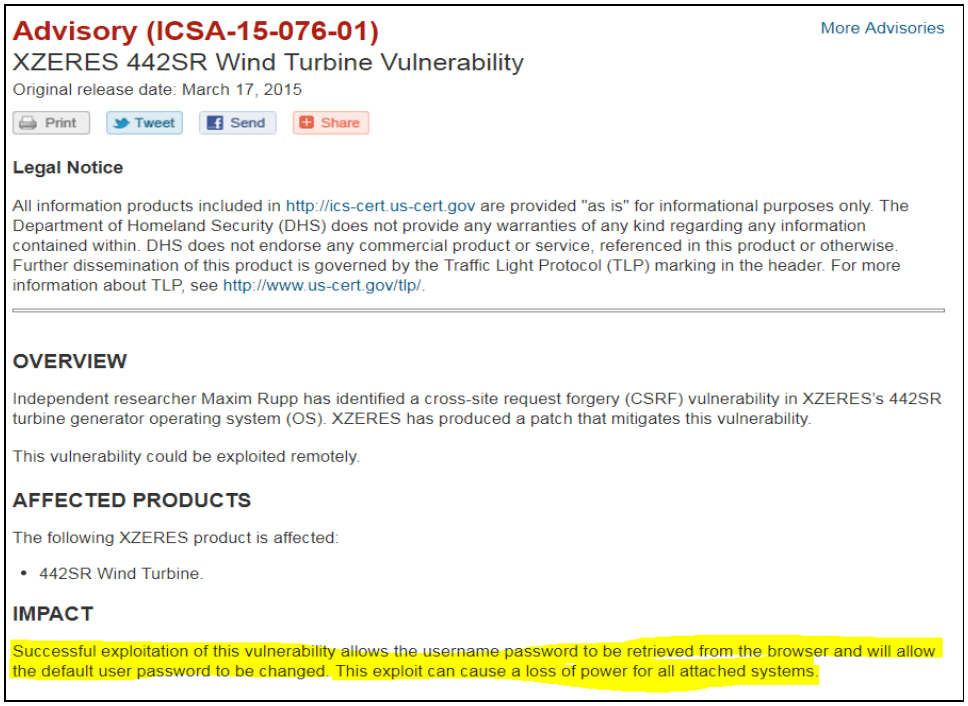


Figure 1 CrashOverride Malware (source: Dragos).



Advisory (ICSA-15-076-01) More Advisories

XZERES 442SR Wind Turbine Vulnerability

Original release date: March 17, 2015

Print Tweet Send Share

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.

Figure 2 Example of a cyber asset vulnerability.

Another common weakness is that the substation devices or TCA may be inherently vulnerable, for instance due to a firmware or software flaw. Figure 2 shows a device vulnerability whose exploitation may ultimately result in the loss of power. The vulnerability illustrated in this figure makes it easy to learn the username and password of a wind turbine operating system. When such a vulnerability occurs together with a misconfiguration, such as in Figure 3, exploitation becomes even easier. For instance, if this turbine were connected using a cellular modem for management purposes and if that cellular modem were misconfigured, the scenario depicted in Figure 3 occurs. In this scenario, the

device is searchable on the Internet using Shodan, which is a search engine for discovering industrial equipment connected to the Internet. Upon discovery, the device login can be reached from anywhere on the Internet, allowing for easy exploit.

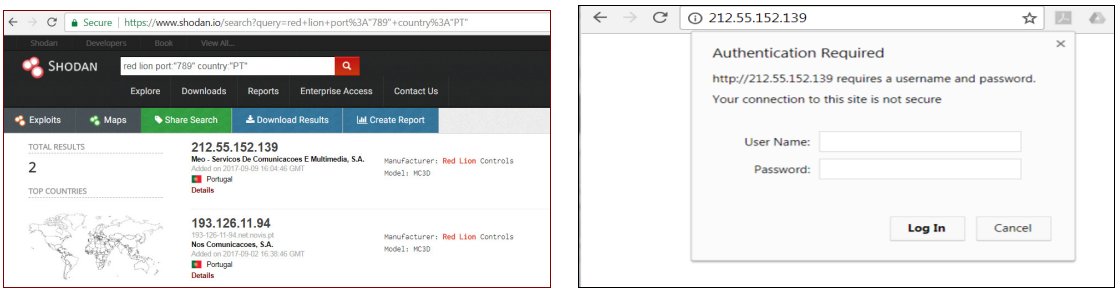


Figure 3 Example of an exploitable misconfiguration.

Advanced attackers harvest unprotected or insufficiently protected data in order to select targets. As described in the recent DHS alert on Russian Government hacking [1], "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." Some real examples of the attackers harvesting information are:

- Sensitive data on flash drives that were 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.

In the following sections, we will describe approaches/investments that could mitigate these vulnerabilities and threats. In particular:

- A well thought out TCA program ensures that the electronic devices used by the field crew aren't exploited to attack the substation.
- Timely security patch management ensures that any threats that do get on the TCA or in the substation do not have vulnerable targets to exploit.
- Consistent data management ensures that sensitive information that an attacker could use to determine what to target is protected.

These measures, when designed thoughtfully, can help improve productivity of the field crew as well.

TRANSIENT CYBER ASSETS

Many utilities worked around the clock to get in compliance with the CIP V5/6 requirements that went into effect on July 1, 2016. But one particularly impactful requirement didn't go into effect along with the others: the Transient Cyber Asset (TCA) requirement that applies to laptops and USB drives used by field personnel. This requirement went into effect on April 1, 2017, after a 9-month buffer for the utilities to get in compliance. So now that it is more than a year since TCA requirements went into effect, are utilities compliant? Our personal experience is that the initial attempts by many in using IT hardening techniques are impacting work. Two common examples are:

- Due to the age of some of the BES Cyber Assets (BCAs), the software applications used to test them are very old as well and, in many cases, no longer supported by the vendor. IT hardening typically disallows such software applications.
- Unforeseen circumstances come up while in the field, such as the need to connect to serial ports through a locked down USB port, which cannot be easily solved in the remote facilities where the testing occurs without providing administrative rights to the tester.

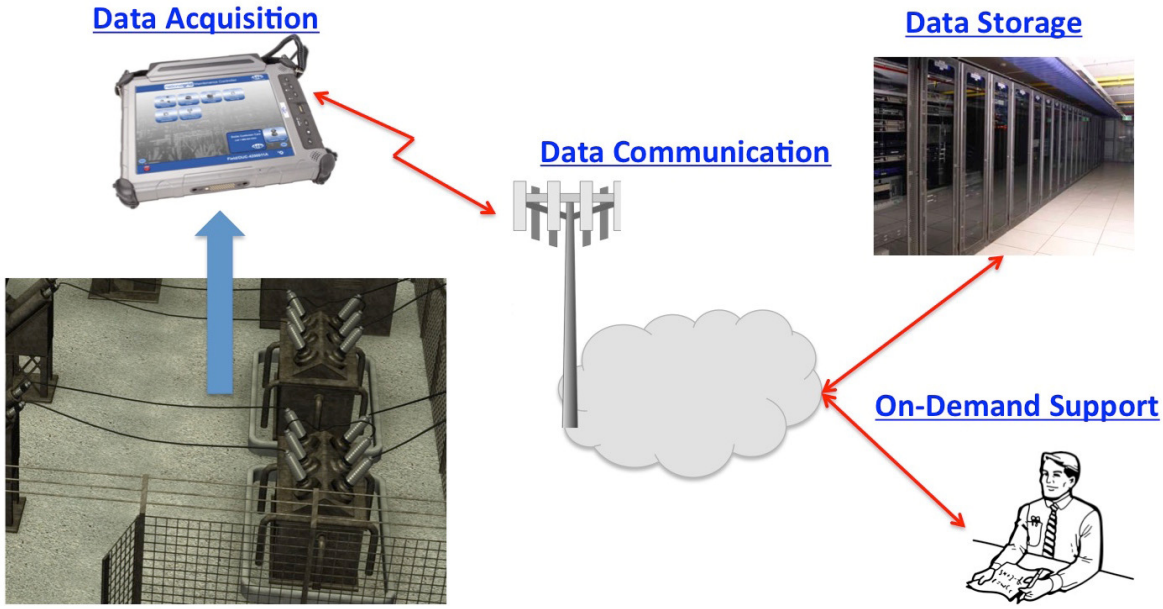


Figure 4 The elements of a TCA program.

So what is the right approach? Start with the work processes that need to be protected and tailor IT security controls to them. The following are some of the elements of the test and maintenance work process:

- The correct test plans and configurations are needed for the task at hand.
- The test results need to be provided to the appropriate storage systems.
- The facilities may be remote without easy access to technical support for issues that arise.
- Various ports such as Ethernet, USB, and Serial are needed to connect to the BCA and the test instrument.
- Some of the BCA are old and can only be tested using old, unsupported software.

In order the facilitate these features, the following elements are needed in a TCA program (also illustrated in Figure 4):

- Transparent communication that automatically syncs the test plans and results on the device with the relevant servers and does it securely.
- Communication management that disables external communication while connected to BCA.
- Secure remote support that meets the NERC CIP requirements.
- Port management that enables the ports appropriate for the testing task at hand, while keeping the unnecessary ones disabled.
- Secure environment for executing old, unsupported software that are needed to test the aged BCA.

This work process-centric approach to security provides NERC CIP compliance while improving work efficiency. Exclusive use of TCAs for fieldwork tasks and curtailing capability such as email and web browsing helps ensure that the TCAs don't get infected with malware.

SECURITY PATCH MANAGEMENT

Security patch management is an immensely important undertaking. As depicted in Figure 5, unpatched systems have been exploited several orders of magnitude more than the security threats that get better media coverage, namely phishing, targeted attacks, and zero day vulnerabilities. This underappreciated field finally entered public consciousness in 2017. Several critical vulnerabilities were disclosed, such as the Windows SMB Remote Execution Vulnerability disclosed in March 2017 [5]. Malware such as the WannaCry ransomware that exploited these vulnerabilities wormed through unpatched computers across the world and sowed chaos [6]. Some of the exploits were based on an allegedly leaked NSA exploit kit [7]. The WannaCry ransomware and the NSA exploit kit were just two among the numerous cybersecurity stories that got wall-to-wall media coverage in 2017. The pace of such disclosures hasn't slowed down in 2018, in particular with the Meltdown and Spectre exploits that target critical vulnerabilities in most modern processors [8].

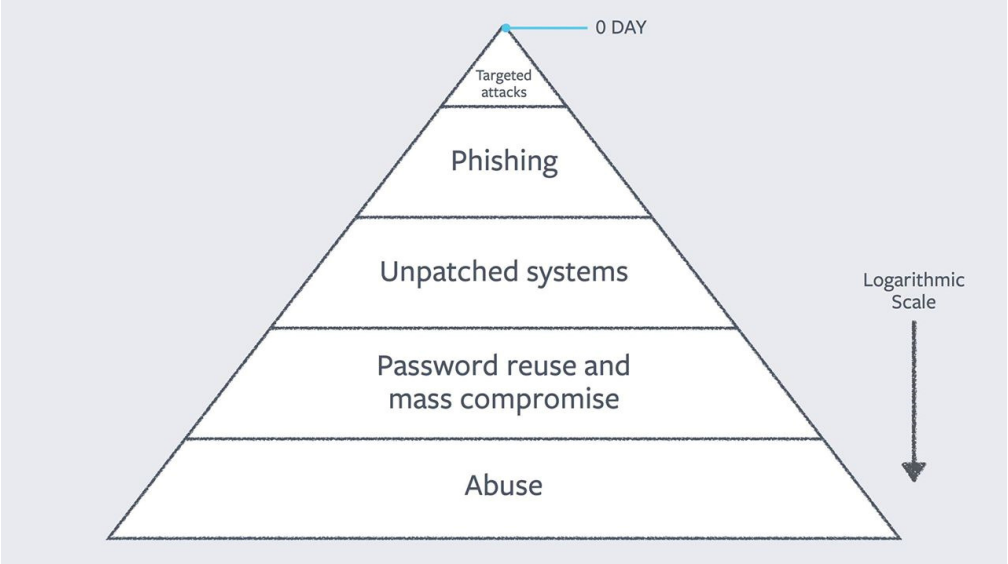


Figure 5 The risk posed by unpatched systems [4].

Due to this bumper-crop of vulnerabilities and exploits, system admins have had their hands full. The patch discovery and application task is especially complicated for utility substation and field devices. There are a number of challenges with security patch management for such devices:

- **Remote and Unreachable:** The field devices are often at remote locations and don't have network connectivity. In the case of TCAs, the device users may turn the device off when they are not in use, further reducing update opportunities.
- **Specialized Build Images:** Due to the specialized nature of the substation and field devices, the device images are quite different from the corporate images, complicating the testing of patches.
- **Unique Software:** Many of the software on these devices are not used elsewhere in the corporate environment, and may be old and not easily patchable. Not only are the IT personnel unfamiliar with the software applications, but the discovery and application of patches may not conform to the standard corporate means.

An effective security patch management program for the field devices would consist of the following elements:

- **Monitoring to Ensure Patching of Unreachable Devices:** Real-time 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.
- **Sophisticated Asset Management:** Asset management system that has 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; and 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.

The purpose of field device security patch management, ultimately, is to ensure the safety of the grid. With this in mind, security patch management should be looked at as part of a larger vulnerability management program. The most common ways that unpatched vulnerabilities are exploited is by targeting unpatched services to gain access or escalate privileges after initially gaining access through social engineering. It follows that the most effective way to protect critical grid systems is to not use the field devices as general purpose corporate computers. By using TCAs that are dedicated for fieldwork, the attack surface is drastically reduced by taking away exploitable services and social engineering vectors such as email and web browsing. This is an essential and complementary aspect of a holistic field force vulnerability management program.

Security patch management has NERC CIP implications as well, with security patching requirements in CIP-007-6 for Bulk Electric System Cyber Assets and CIP-010-2 for Transient Cyber Assets. For NERC CIP audit purposes, careful collection and retention of evidence is necessary. A well-designed security patch management program can greatly enhance system security and provide NERC CIP compliance without impinging on work performance.

SECURING THE DATA

At the core of cyber security is information security, i.e., protecting sensitive information. Why is this important in the electric grid context? Sophisticated attacks such as the Ukraine attack have a long information-gathering phase: the attackers perform reconnaissance and try to understand the system in order to identify and target the highest impact systems. In recognition of this, the NERC CIP-011-2 standard has requirements pertaining to information protection, which directs electric utilities to identify Bulk Electric System (BES) Cyber System information and protect them during storage, transit, and use.

Utilities have become highly competent in protecting the data in their control centers and corporate domains. This has been achieved by the development of strong data governance and control practices and the deployment of innovative Data Loss Prevention (DLP) technologies. But a weak link remains: the data in the field. The laptops and tablets used for field activities such as testing and maintenance of assets have been under close scrutiny of late, due to the NERC CIP TCA requirements. But the TCA requirement is focused on preventing malware propagation.

An overlooked and equally important concern is the security of the information on and accessible by these transient devices. For instance, transient cyber devices that are used to work with protective relays can contain relay settings, network connectivity information, and login credentials. Sophisticated attackers often develop custom malware or repackage existing malware so that the malware signature isn't known to anti-virus programs. If such a malware infects a field device, it can potentially obtain and transmit sensitive data about the BES Cyber Assets (BCAs). This information is extremely useful to the attacker in the development and execution of an attack against the BCAs.

The security measures that would satisfy these requirements in a corporate setting are mature and well understood. While some of these same measures are helpful, such as encrypting the data, most aren't readily applicable to field devices. So how do we protect information on the field devices?

- Implement 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. This 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.

- Put in place a 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.

CONCLUSION

Cyber security is a discipline that is here to stay and grow 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. It is important for asset management professionals to recognize this and become more aware of security threats and countermeasures. This knowledge will enable them to combat the cyber threats. It will also help them take active part in determining the technology and compliance approaches to fieldwork. Such decisions are currently made by the IT and Compliance groups with insufficient input from Asset Management, and the measures often end up impacting work. In order to help rectify this, we are working with utilities to educate Asset Management professionals and develop OT-centric solutions that enhance security and productivity while meeting regulatory requirements such as NERC CIP.

BIBLIOGRAPHY

[1] United States Computer Emergency Readiness Team (US-CERT), Alert TA18-074A, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," 15 March 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A

[2] Federal Energy Regulatory Commission (FERC) Order 791, Version 5 Critical Infrastructure Protection Reliability Standards, 22 November 2013, https://www.ferc.gov/whats-new/comm-meet/2013/112113/E-2.pdf

[3] DRAGOS Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," July 2018, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[4] Alex Stamos, "Preparing for the future of security requires focusing on defense and diversity," Black Hat USA Conference, July 2017, https://www.facebook.com/notes/facebook-security/preparing-for-the-future-of-security-requires-focusing-on-defense-and-diversity/10154629522900766/

[5] National Vulnerability Database, CVE-2017-0143, Windows SMB Remote Code Execution Vulnerability, https://nvd.nist.gov/vuln/detail/cve-2017-0143

[6] Symantec Corporation, WannaCry Ransomware, https://www.symantec.com/outbreak/?id=wannacry

[7] Rapid7, The Shadow Brokers Leaked Exploits Explained, https://blog.rapid7.com/2017/04/18/the-shadow-brokers-leaked-exploits-faq/

[7] Meltdown and Spectre: Vulnerabilities in Modern Computers Leak Passwords and Sensitive Data, https://meltdownattack.com/