National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

ROYAL CANADIAN NAVY CYBER INCIDENT RESPONSE TEAM

LCdr J.T.D.S. Turner

JCSP 42

Service Paper

PCEMI 42

Étude militaire

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

ROYAL CANADIAN NAVY CYBER INCIDENT RESPONSE TEAM

LCdr J.T.D.S. Turner

Word Count: 2434

Compte de mots: 2434

ROYAL CANADIAN NAVY CYBER INCIDENT RESPONSE TEAM

AIM

1. The Royal Canadian Navy (RCN) has entered a new age with its modernized frigates, their highly computerized and networked systems and their improved connectivity. As with any technological improvement, there are two edges to the sword: improved performance or functionality and increased or new vulnerabilities. In today's age where cyber-attacks are very prevalent the RCN must be prepared to respond to serious cyber incidents and quickly restore essential combat capability. This paper will examine the current capability gap for an RCN Cyber Incident Response Team and provide recommended courses of action (COA).

INTRODUCTION

2. The Halifax Class Modernization (HCM) project introduced a significant amount of commercial-off-the-shelf (COTS) technology into the Halifax Class frigate's combat suite. In addition, the Halifax Class Integrated Platform Management System (IPMS) replaced the legacy Integrated Machinery Control System (IMCS) and it is also heavily based on COTS technology. Many of the new combat systems and IPMS that were installed as part of HCM utilize COTS Operating Systems (OS) as well as COTS networking infrastructure. As a result, these systems will exhibit the same software flaws and vulnerabilities as many computerized systems in all industries. Although, these vulnerabilities and flaws can be managed and repaired not all of them can be eliminated and the systems will always have some residual weaknesses.[1]

[1] Margaret H. Hamilton, "Zero-Defect Software: The Elusive Goal: It is Theoretically Possible but Difficult to Achieve; Logic and Interface Errors are most Common, but Errors in User Intent may also Occur," *Spectrum, IEEE* 23, no. 3 (1986), 53.; Michael Dubakov, "Zero Defects? are You Kidding Me?" *TargetProcess (Blog),* March 2009, accessed February 6, 2016. https://www.targetprocess.com/blog/2009/03/zero-defects-are-you-kidding-me/.; Mike Richman, "The Quest for Zero Defects: Are we Closer to the Goal of Zero Defects Now than we were 25 Years Ago?" *Quality Digest Magazine,* April, 2005, accessed February 6, 2016. http://www.qualitydigest.com/april05/05_article.shtml.

3. In 2010 the world was introduced to a revolutionary computer virus, the Stuxnet worm.[2] This malicious software (malware) was revolutionary for several reasons including the fact that it was highly likely a state sponsored attack; that it caused physical damage to machinery and that it had the ability to jump air gaps.[3] This virus provided a real demonstration of what was possible and moved malware from a problem of the internet and users who made poor choices to a concern for even the most secure networked systems regardless of being disconnected from the Internet. This attack not only targeted Microsoft Windows based computers but Programmable Logic Controller (PLC) programming software, and PLCs used on industrial machinery. This attack showed that embedded systems, like diesel engine controllers or radars, could be susceptible to attack along with their Supervisory Control and Data Acquisition (SCADA) systems, like IPMS or the HCM Combat Management System (CMS).

DISCUSSION

Organizational Challenges

4. Currently, the RCN relies on each formation's (Pacific and Atlantic) N6 and Base Information Services (BIS) organizations to respond to Information Technology (IT) related incidents or failures. Combat Systems or machinery control system (i.e. IPMS) failures are dealt with by the Fleet Maintenance Facilities (FMF). The N6 organizations primarily address

---

[2] Viruses and worms are types of malware that spread themselves to other computers. It is important to note, that most malware has other functionality (i.e. fits in to many types or categories of malware) included beyond just spreading or self-replicating. Michael Sikorski and Andrew Honig, *Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software* (San Francisco, CA: no starch press, 2012), 4.; Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the most Menacing Malware in History." *Wired*, sec. Security, July 11, 2011, accessed February 6, 2016. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

[3] The term *jumping air gaps*, means that the virus was able to infect closed networks (i.e. not connected to the Internet) and standalone computers thus figuratively jumping through the air to infect another computer or system. Stuxnet was able to jump air-gaps through human involved processes but another description is provided in the following: Dylan Love, "Hackers can Infect Your Computer Even if it's Not Connected to the Internet," *Business Insider*, March 5, 2014, accessed February 6, 2016. http://www.businessinsider.com/what-is-air-gap-malware-2014-3.; Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32. Stuxnet Dossier," *White Paper, Symantec Corp., Security Response* (2011), 3.

information system (IS) security policy and compliance related issues as well as being in the IT incident response chain. The BIS organization provides technical IT service delivery and repair. Both of these organizations are focused on traditional IT or IS.[4] Although some of the hardware, software and network infrastructure may be familiar, there are distinct differences in how SCADA systems must be managed and operated (e.g. focused on reliability as well as having more significant consequences due failure). The FMFs perform up to and including third line maintenance functions for Combat Systems and IPMS depending on existing in-service support (ISS) contracts but do not deal with IS security issues or IS security policy compliance. Despite the fact that modern Combat Systems and IPMS are very similar to traditional IT/IS in construction, components and software there is not a capability in the FMFs to deal with IS security. This leaves a gap between the organizations that traditionally deal with IS security issues and IT problems and the FMFs who have focused on maintaining Combat Systems and IPMS.

Incident Response Challenges

5. The current incident response capabilities are again focused on traditional IT/IS and ultimately lead back to the Canadian Forces Network Operations Centre (CFNOC). CFNOC is charged with defending and monitoring the Department of National Defence's (DND) networks but again this traditionally has meant networks like CSNI.[5] Although, they do possess unique capabilities to respond to cyber incidents, capabilities are tooled and skilled to deal with the

[4] Traditional IT or IS are computer networks, such as the Defence Wide Area Network (DWAN) or the Consolidated Secret Network Infrastructure (CSNI), mainly used for administrative and corporate communication purposes. Although, CSNI is used to some extent for command and control, it is not used for this purpose in a real-time or tactical context. Combat Systems and IPMS are considered non-traditional IT/IS. Although much of these systems uses the same components and software as traditional IT/IS, ultimately the end-points of the networks/systems are effectors (weapons or sensors) or machinery (engines, pumps, generators, etc). Eventually, this separation may no longer be required but at this point it is considered important and reflective of the organizational view of the problem space.

[5] Chief of Defence Staff. CANFORGEN 090/02, *Canadian Forces Network Operations Centre* (Ottawa: DND, 2002).

hardware, network infrastructure and software that makes up the DND's core networks. In some cases, those capabilities are limited by the tools used and by the capacity (i.e. number of trained personnel) to use those tools. Given the broad scope of their task, responding to incidents in unfamiliar networked systems (i.e. Combat Systems) may be too challenging. Combat Systems and IPMS are highly specialized systems and there would be no economy in attempting to train CFNOC incident responders to an adequate level of expertise to become even limited subject matter experts. As a result, the incident response and handling chain is primarily administrative and for tracking purposes, although in some specific cases existing expertise could be useful or cross over to non-traditional IS/IT problems.

Required Capabilities

6. While there are many types of IS security incidents that might occur, a malware infection affecting the confidentiality, integrity or availability (CIA) of the system is of key concern. The infection will possibly be discovered by anti-virus software, if installed in the system, or due to abnormal system behaviour which could include repeated system failure. The challenge of initially detecting malware on non-traditional IT/IS, is a problem unto itself and considered out of the scope of this paper. This problem will need to be addressed through system design, operation and first line maintenance procedures. The scope of this discussion is on response to an infection or incident where an infection is suspected.

7. The worst case of the two initial detection scenarios is where the anti-virus software does not detect a problem and the incident is related to abnormal system behaviour. This is more challenging as the malware must be localized in the system before further action can be taken. As this is the worst case, it will be the scenario from which the required capability is outlined.

Localize the Threat

8. The process for responding to a malware infection can be likened to the *detect to engage* sequence.[6] As already stated the *detect* phase is out of the scope of this discussion. The next phase is *localize* and in the case of a malware infection, this will be the action of finding the source of the infection through a variety of methods. At this point digital forensics would be required to determine what may have changed in the system as well as determining the abnormal from the normal.[7] CFNOC currently has a forensic capability but it is focused on a few automated software tools.[8] Digital Forensics software tools are an important component to a forensics capability but like many capabilities the forensic analyst is the most important component. In order to be an effective analyst, one would need to have a deep understanding of the system being examined. To educate or train the existing analysts in a just-in-time fashion is not likely feasible nor would it be a timely option. In the long run forensic analysts with the some level of Combat System or IPMS understanding, at least at a systems level, and the proper software tools are required. These analysts would then be enabled to perform digital forensics on the affected system and find the malware.

Understand the Threat

9. Once the malware is located, it is essential to understand it and this can be aligned to the *classify/identify* phase as well as the *threat evaluation* component of the *engage* phase. During this phase it is important to determine some key pieces of information such as has it been seen before, how it was delivered, how it maintains persistence, what is its payload (i.e. what does it

[6] The *detect to engage* sequence is *detect, localize* (or *resolve*), *classify/identify, track,* and *engage (threat evaluation and weapon assignment).*

[7] Moira J. West Brown et al., *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd ed. (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003), 26-27, accessed February 6, 2016. http://www.sei.cmu.edu/reports/03hb002.pdf.

[8] The assessment of CFNOC capabilities is based on the author's involvement in several IS incidents where forensics was required.

try to do to the system), and does it try to communicate externally.[9] Additionally, a very important question to answer is: was this a targeted attack? Answering the first question would be the first step in understanding if it was a targeted attack. If the answer to the first question is yes, then this scenario becomes somewhat simpler. If the malware has been seen before it was likely detected by anti-virus software and detailed analysis has likely already been conducted. In this case, clean-up procedures are likely already developed as well as a sound understanding of the payload or types of payloads commonly seen. Again, this capability must examine the worst case (i.e. not detected by anti-virus software). The malware may still be known or previously seen but not detected as it was a polymorphic version.[10] At this point the analysts must quickly determine if the infection was one of two types: accidental or targeted. If the infection is accidental a clean-up would still be required and it would still be an issue but the risk of the virus specifically attacking the specialized functionality of the system is unlikely. Since the risk and challenges go up significantly in the case it is a targeted attack this determination must be founded on strong evidence with an assessment of confidence. In order to gather this evidence and assess the confidence of the determination, the team would require malware analysts. These analysts would need to perform reverse engineering of the malware to uncover its purpose, methods of spread, persistence and communications as well as being able to compare accurately to known malware. Currently, this capability does not exist in an operational sense.[11] These analysts would require some system specific knowledge to determine what was elements of the malware were relevant but could operate with less that of a system expert.

---

[9] Ibid.

[10] Polymorphic viruses alter their form to evade detection by signature based anti-virus software. Chet Hosmer, "Polymorphic & Metamorphic Malware" (Presentation, Black Hat 2008, Las Vegas, NV, August 7, 2008, accessed February 6, 2016. https://www.blackhat.com/presentations/bh-usa-08/Hosmer/BH_US_08_Hosmer_Polymorphic_Malware.pdf.

[11] CFNOC does not have an advertised malware analysis or software reverse engineering capability and relies on automated analysis tools (known as sandboxes) or external agencies to perform these activities.

Eliminate the Threat and Restore the System

10. A commonly held belief is that in the worst case scenario the system could be restored by formatting all of its hard drives and reinstalling all the necessary software. If this were always true, the capabilities discussed in the previous paragraphs would not be necessary. Unfortunately, a number of examples have been recently provided of firmware based viruses that would persist after this restoration effort. Two notable examples of firmware based viruses are Thunderstrike 2 and BadUSB. The former, and more recent, is a proof-of-concept attack that allows the spread of a virus from Apple computer accessories, storing itself in Read-Only Memory making it invisible to anti-virus software and persistent through hard disk formatting and OS reinstall.[12] The latter example is also a proof-of-concept attack where a Universal Serial Bus (USB) device's (i.e. USB memory stick) firmware, not the memory, is infected allowing it to again hide from scanning and persist through formatting of the memory.[13] These two proof-of-concept attacks demonstrate that brute force recovery will not always function effectively to eliminate the threat once it has established itself in the system. Without a forensics or malware analysis capability at an expert level, attacks like this would be missed and the significant effort of restoring the system would be wasted as it would become re-infected immediately. With knowledge of these types of threats, it would be challenging for a ship's Captain to be confident in the system's integrity and performance after an infection unless it was addressed appropriately. Based on these potential threats and the requirement to address the threat persistently, development of an effective restoration plan would require cyber security experts supported by digital forensic analysis as well as reverse engineering of the malware.

---

[12] Kim Zetter, "Researchers Create First Firmware Worm that Attacks Macs," *Wired*, sec. Security, August 3, 2015, accessed February 6, 2016. http://www.wired.com/2015/08/researchers-create-first-firmware-worm-attacks-macs/.

[13] Andy Greenberg, "The Unpatchable Malware that Infects USBs is Now on the Loose," *Wired*, sec. Security, November 2, 2014, accessed February 6, 2016. http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/.

11. Additionally, the forensic results and malware analysis would provide important feedback in developing defensive measures for the system so a similar attack would not be successful in the future.[14] The actions to develop these defensive measures are out of scope for this discussion and should be addressed separately.

Potential Team Composition

12. The previous discussion supports the requirement for digital forensics, malware analysis and system expertise in order to respond to potential cyber incidents. Potential options for maintaining this expertise are as follows:

a. *Status quo.* The RCN deploys Technical Assistance Visits (TAV) composed of system experts when required. As part of TAV where a cyber-incident is suspected, the RCN could request support from CFNOC or other external agencies to support the forensics functions and malware analysis functions. This ad-hoc team would loosely fit the RCN's current model in responding to un-forecasted issues.

b. *FMF-BIS-N6 Team*. The RCN could combine key resources from these three organizations in each formation focused on responding to the worst-case scenario described above. This team could function as a secondary duty for the individuals tasked. This would allow them to perform their primary duties most of the time and forming the team on an as required basis. This team would require further education and training of specialist in digital forensics and malware analysis. In this case the FMF personnel would focus on developing some skills in cyber-

[14] West Brown et al., *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 31-32.

security related fields and the BIS and N6 personnel would develop broad Combat Systems and IPMS knowledge.

c. *DND-Industry Team*. This team would be formed around a core of DND cyber security professionals with digital forensics and malware analysis expertise. This core would be educated and train on Combat Systems and IPMS to the extent that is deemed economical. As part of future ISS contracts industry would provide system experts that, as part of the contract, would integrate into this team regularly for training and exercise purposes as well as deploy with the team as necessary. In this concept the DND personnel would maintain their primary focus on cyber-security skills with system knowledge being secondary while getting system expertise support from the appropriate contractors.

CONCLUSION

13. It is clear that the days of security through the obscurity of military specific hardware and software are gone. Also gone is the concept that disconnecting a system from the Internet will make it totally secure. There is a possibility that there are threat-actors capable of launching attacks against the RCN's modernized systems and causing physical damage or critical system failure.[15] It is no longer a question of if a system will be infected by a virus, it is when it will happen and the RCN must be prepared to quickly respond, restore the affected capability and have confidence the system will continue to operate after that recovery. Regardless of the actions taken to address this capability gap, action must be taken for the RCN to be prepared for this dangerous eventuality.

[15] Traditionally the military has been concerned with the loss of sensitive data but the availability and integrity of the systems are important. This represents a paradigm shift in the understanding of what IS security aims to protect.

RECOMMENDATION

14. It is recommended that the RCN develop a *DND-Industry* cyber-incident response team (CIRT). It is essential that the RCN possess expertise in responding to threats from malware to its critical systems. This core knowledge and skillset must be an organic resource that can respond and surge on demand. Industry is best suited to provide the subject matter expertise for the systems they have delivered and it is an economical method to maintain specialists. The RCN resources, which could reside in Director General Maritime Equipment Program Management (DGMEPM), FMF, BIS, or elsewhere, would provide the general cyber-security expertise while industry would provide the system specialists.

BIBLIOGRAPHY

Chief of Defence Staff. CANFORGEN 090/02. *Canadian Forces Network Operations Centre*. Ottawa: DND, 2002.

Dubakov, Michael. "Zero Defects? are You Kidding Me?" *TargetProcess (Blog)* (March 2009), accessed February 6, 2016. https://www.targetprocess.com/blog/2009/03/zero-defects-are-you-kidding-me/.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. Stuxnet Dossier." *White Paper, Symantec Corp., Security Response* (2011).

Greenberg, Andy. "The Unpatchable Malware that Infects USBs is Now on the Loose." *Wired*, November 2, 2014, sec. Security, accessed February 6, 2016. http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/.

Hamilton, Margaret H. "Zero-Defect Software: The Elusive Goal: It is Theoretically Possible but Difficult to Achieve; Logic and Interface Errors are most Common, but Errors in User Intent may also Occur." *Spectrum, IEEE* 23, no. 3 (1986): 47-53.

Hosmer, Chet. "Polymorphic & Metamorphic Malware." Presentation, Black Hat 2008, Las Vegas, NV, August 7, 2008, accessed February 6, 2016. https://www.blackhat.com/presentations/bh-usa-08/Hosmer/BH_US_08_Hosmer_Polymorphic_Malware.pdf.

Love, Dylan. "Hackers can Infect Your Computer Even if it's Not Connected to the Internet." *Business Insider* (March 5, 2014), accessed February 6, 2016. http://www.businessinsider.com/what-is-air-gap-malware-2014-3.

Richman, Mike. "The Quest for Zero Defects: Are we Closer to the Goal of Zero Defects Now than we were 25 Years Ago?" *Quality Digest Magazine* (April, 2005), accessed February 6, 2016. http://www.qualitydigest.com/april05/05_article.shtml.

Sikorski, Michael and Andrew Honig. *Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software*. San Francisco, CA: no starch press, 2012.

West Brown, Moira J., Don Stikvoort, Klaus Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. 2nd ed. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003, accessed February 6, 2016. http://www.sei.cmu.edu/reports/03hb002.pdf.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the most Menacing Malware in History." *Wired*, July 11, 2011, sec. Security, accessed February 6, 2016. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

———. "Researchers Create First Firmware Worm that Attacks Macs." *Wired,* August 3, 2015, sec. Security, accessed February 6, 2016. http://www.wired.com/2015/08/researchers-create-first-firmware-worm-attacks-macs/.