International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 11, Number 2 (2018), pp. 261-272

http://www.irphouse.com

Protect Governments, and organizations Infrastructure against Cyber Terrorism (Mitigation and Stop of Server Message Block (SMB) Remote Code Execution Attack)

Nachaat AbdElatif Mohamed[1]

School of Computer Sciences. Universiti Sains Malaysia, Penang, Malaysia

Aman Jantan[2], Oludare Isaac Abiodun[3]

School of Computer Sciences. Universiti Sains Malaysia, Penang, Malaysia.

Abstract

Windows machines utilize a Server Message Block (SMB) for a wide variety of purposes such as a document, printer sharing, and access to remote Windows administrations. However, a challenging issue is that a network system can be easily controlled and compromised remotely using some tools like Armitage in Kali Linux, and using Eternal blue which developed by National security agency (NSA). Organized criminal gangs and Cyber Terrorism can use Remote Desktop Protocol (RDP) over SMB to manage a complete infrastructure in governments and organizations or encrypt the data as it happened by Run somewhere. Current researches on controlling the SMB remote code execution attack do not sufficiently address these issues. This Paper used MITRE (CAR) Model, (ATT&CK) Matrix, as a countermeasure to these attacks on windows. Also, we propose a new policy we made (we recommend Microsoft to do that with All Windows OS). Also, we use it with any security Appliance available in the market. To prevent WMIC, RDP, and enable public profile firewall state to stop this cyberterrorism attack.

Index Terms: ATT&CK; adversary; hacking; attack; Cyber Terrorism.

I. INTRODUCTION

Imagine there is one Pc controlling SKADA system inside Nuclear power plant, what will happen if cybercriminal attackers take advantage of this machine, or another PC inside Enterprise Network has access to Servers, clouds. It is a massive disaster, if

APTs, retch that PC, they will compromise servers, clouds, and they can take every single piece of data in that network. The Server Message Block Protocol (SMB) is a client-server communication protocol employed in sharing access to files, printers, serial ports and different assets on a system. The SMB protocol transmits multiple messages between a client and a server to establish a connection. It permits the client of an application to access documents on a remote server, and also different assets to other resources, such as printers, mail slots et cetera. Hence, a client application can carry out a number of operations such as open, read, edit etc on the remote server.It can also communicate with any server program that is set up to receive an SMB client request. A client makes his request using commands and the server responds to the client request. This action gives full permission to the system and obviously makes it very attractive for attackers, mainly because of its remote access capability [1]. This can be explained with the recent WannaCry ransomware. The ransomware effectively set off the weakness by a series of execution. A scrambled payload containing the stager for the malware is stacked on the remote machine. The payload conveyed to the remote machine dispatches a service "mssecsvc" from inside the lsass procedure. This service checks the network for machines that are available and have open SMB ports. The service at that point utilizes the previously mentioned vulnerability to access a remote machine and convey the malware payload. These actions are executed rapidly and the attack infiltrates all machines in few minutes. [2]. Other attacks like the MITRE ATT&CK are based on threat model to generate different relevant defensive sensors and build a test to emulate adversary behavior and tactics, [3]. Ccomprehensive tools such as Metasploit, Armitage burp suite, Cobal strike, Setoolkit, Wifififisher, and more are effective at compromising/penetrating network systems, Applications, and WIFI in minutes and causing severe harm [4]. Attackers can use SMB to gain access to the machine and control the whole infrastructure, and Datacenter (underground economy). There are several reports and cases where these attacks were employed and great damage was recorded [6]. Even though various researchers tried to detect and trace the attack but the methods they applied takes a long time and also it is very complicated. SMB vulnerabilities have a significant impact because it uses a substantial percentage of infrastructure for banking, finance, aviation, medical, [7]. There is little consensus about how to make decisions automatically about countermeasures attacks, [8]. In this paper, we simulate this attacks by using security tools to know which tactics attackers are using to exploit network systems and also we propose strategies to mitigate the attacks and protect the systems. We are trying to use a new concept to detect most of the attacks, we are focusing at the Victim behavior, and differentiate between the victim, infrastructure, and APTs ore Cyber terrorism attackers, [30]. Most of the concept try to catch the attack after passing the victim and starts tampering with the network, also, in our paper we provide a method for how to handle attacks that are launched without sending any single file.

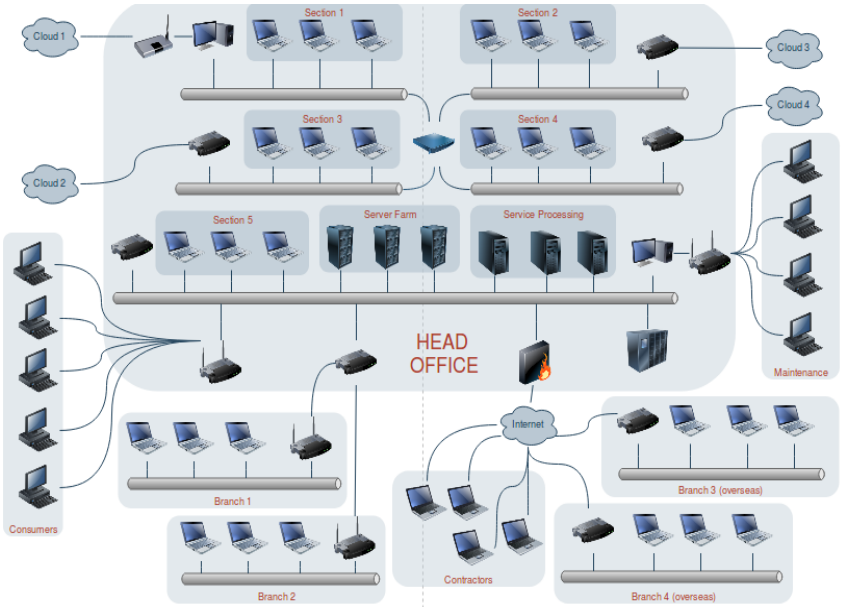

Fig 0 Enterprise Network

II. STATE-OF-THE-ART

We provide a summary of existing literature that is closely related to this research. Korznikov [14] affirms that some attackers do not need hacking tools to make hijacking Attack through SMB/RPC. According to him, everything is done with built-in commands.

Counter Threat Unit Research Team [15] calls into question why some vulnerabilities are not discovered and resolved before putting the software out for use. They suggest that network administrators should review proxy log settings, use advanced endpoint threat detection, implement timely vulnerability patching, and review network access control. Symantec Security Response [16] propose that clients can be protected with Intelligence Services, Web Filter-enabled or with products such as Web Security Service (WSS), Proxy SG, Advanced Secure Gateway (ASG), Security Analytics, Content Analysis, Malware Analysis, SSL Visibility, and Packet Shaper.

In their research, Beechey et al [17] regrettably reach the conclusion that traditional defenses such as WAF, Firewall, Anti Malware and Anti-Virus are not effective for protecting governments and organization infrastructures. They pointed out that many attacks are leveraged through open ports, and also client's visit to the suspicious website.

Tomonaga et al [18] maintain that to mitigate these kinds of attack involves making a restriction on CMD commands mainly used by attackers. A general user has no need for such commands and should be restricted by default from accessing such commands. NSA Information Assurance Directorate [19] must be clear on using AppLocker for application whitelisting as this cannot stop or detect all kinds of malicious code/threat. Corio et al [20], an IT professional suggested the reduction of

total cost of ownership (TCO), by two key strategies, no one is getting all users out of administrator group, second, rationing applications that user run. Alperovitch et al [22] reported that Chinese APTs can Attack systems through Sticky Kayas and osk.exe to open CMD, they can use Windows Management Instrumentation Command-line (WMIC) which is developed by Microsoft, but with the next-generation security architecture you have to ask your vendor how they detect such adversary tricks and malware free intrusion.

Other studies advises the network administrator to create a piece of pseudo-malware after collecting information such as, "replace sticky keys with cmd.exe for persistence and access via RDP", and other information, with the pseudo-malware, a response code to clean the malware can be used to study the behavior of malware, and mitigate this attacks [26].

In the next section, we present how SMB remote execution attack is executed through only one feature we also show in the solution section how our proposed method responds and deter such attacks.

III. HOW A HACKER CAN GAIN ACCESS

We built successful Attack using SMB remote code execution. We show how an attacker employs only one open feature to get a full permission from the victim's system. This attack is carried out using Eternal Blue payload which is developed by U.S. National Security Agency (NSA), and it is available in Kali Linux 2017.2 and 2017.3. It can be located inside Armitage tool in Kali Linux any versions as we mentioned. Figure 1 shows the process to achieve the attack. If the public profile setting is off, it gives a possibility to APT to use SMB remote code execution attack to gain access to the machine. The attacker's mission is to make his infiltration not to be detected. It is very important for the victim not to know his infrastructure, his resources are been controlled remotely. He Enables the support_388945a0 account and add it to the local admin group, Drop the command line Chinese language version of WinRAR on the target, Generates a particularly timed beacon that communicates over HTTP, Turns on RDP if it's not already enabled", [26].

Figure 1 public profile setting is off.

The attacker opens a new terminal then write Armitage. From the Armitage tool, he adds the victim's IP to control it, and he can manage the other network devices through this target as you will see in the next figure. The attacker inserts the target IP in the search area of SMB Version.

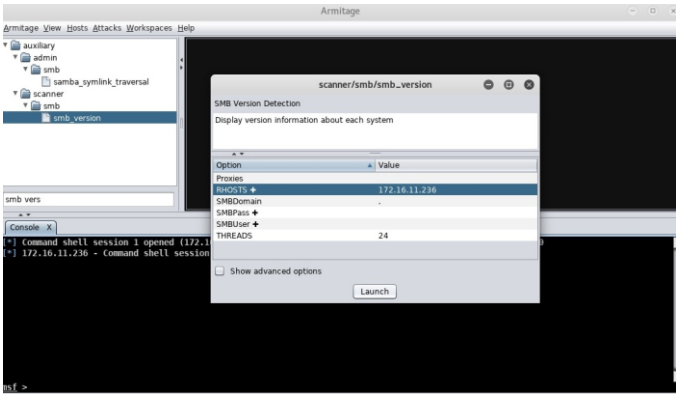

Figure 2. Armitage Screen tries to Add target.

The attacker right clicks on the target and choose a scan option to know the open ports of the victim using Armitage with eternal Blue malware. He can detect OS, open ports, services, and gain access to the victim computer, not only that, and he can control the whole infrastructure. Note: APTs can use a variety of TTP, including: "open-source reconnaissance, spear-phishing emails, watering-hole domains, host-based exploitation, an industrial control system (ICS), and ongoing credential gathering, [28].

The attacker detects the open ports which will assist him to gain access, he will drag and drop ms17_010_eternalblue and hit launch, then he starts to penetrate the victim's machine. We can realize the target is unmistakably attacked, it means the attacker can control the victim's machine and log in to other devices connected to the infrastructure easily, plant the Trojans and malicious file, and monitor servers for a long time.

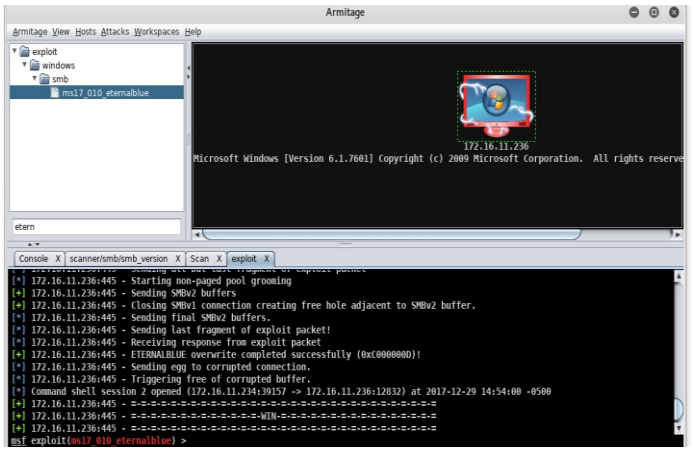

Figure 3. the victim attacked.

The attacker can choose any one of these lines of commands to get shell sessions at target machine, interaction or interpreter.

Our proposed method makes this attack to be futile. The mission will be almost impossible for attackers to execute these commands, which does not need to send amalgam file. For example, if the subject is an interactive shell, the attack may be successful. This is a serious challenge but the good news is our method can solve this critical issue and protect the governments against cyber attack/terrorism. On the other hand, other tools used to attack such as Utilman.exe is a very useful and dangerous tool utilized in built-in window application. It is designed to allow the user to configure Accessibility option, the bad news here, hackers can use this tool to bypass the windows login and make huge damage in government network, [23]. Hacker can also query user from CMD console to get all user details on the victim, connect with any user on that system, if possible, and hijack the administrator's credentials. He can easily dump out the server memory and get user passwords. Obviously, attackers are not interested in playing with your system, but they are interested in what they can do with the techniques learned in compromising your infrastructure [24].

In figure 5, we can see that the session is working with correctly and the victim's system and infrastructure are compromised completely. The attacker can use Remote Administration Trojan (RAT), a malicious malware code to control the entire infrastructure. RAT allows executing of command via CMD, upload/download files to and from victim's system. RAT acts as a client to a remote server [29].

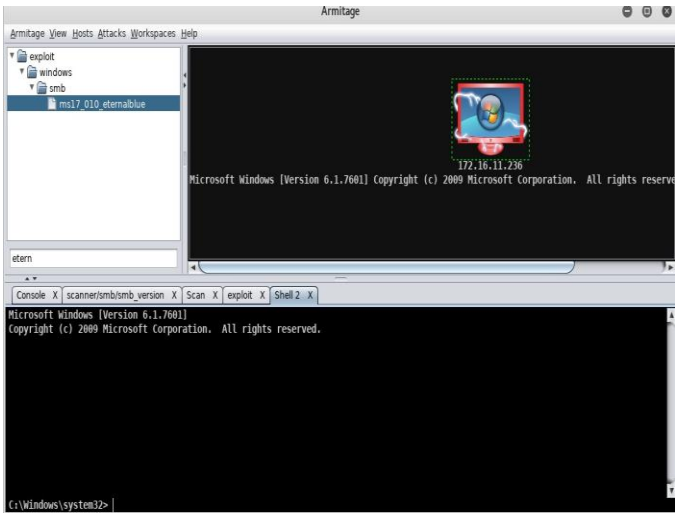

Figure 4. interaction shell is working now.

IV. SOLUTION

To mitigate the attack described in the previous section, we demonstrate how to respond to such attack **using our** policy/method to stop this attack, the method is described in Fig. 5, with a supporting step by step. Most organizations simply buy security solution and put it on the network as it is. Such security solution can protect

the network but not from all attacks, for example, the SMB, and zero day attacks. The success of SMB attack is leverage on the victim not detecting any malicious file. The intuition lies in the attack using open features without sending any malicious file to the victim specifically SMB.

In this section, we will present how this kind of attacks can be stopped through only one feature, turn on the public profile firewall. Note: the other features must be embraced in our policy, (prevent WMIC, RDP, enable public profile firewall state in windows firewall), and finally if still any strange behavior, differentiate between victim, infrastructure, and APTs from network connection, by applying our method, will help to alleviate attacks which hijacking systems. Hackers can use OpSec Safe Techniques for retrieving hashes and credentials from Windows workstations, like Enumeration of user/s running, MS cached credentials, Hash spraying, Dumping of Domain controller hashes using NTDSUtil, Dumping of Domain controller hashes using the drsuapi method, Ability to decrypt password hashes, Enable/Disable RDP on a remote machine, and enable/Disable UAC on a remote machine, [24].

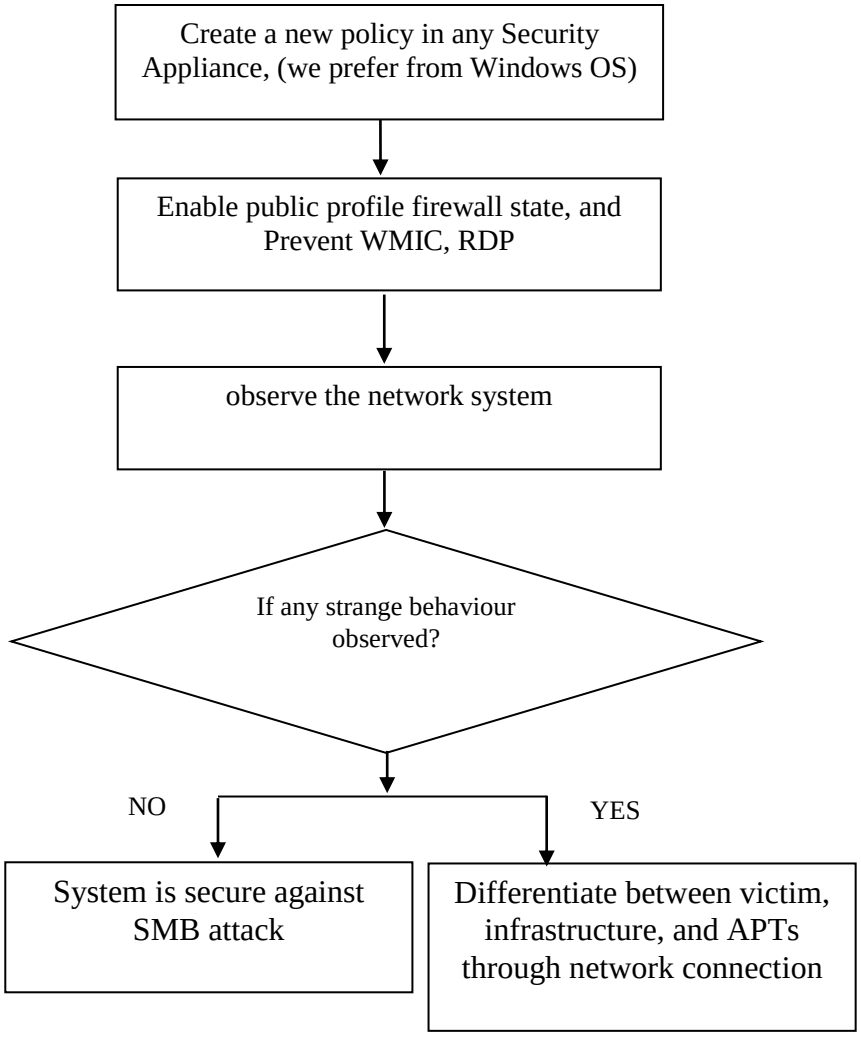

Figure 5. A flowchart of the proposed method.

V. EVALUATION USING SMB ATTACK ANALYSIS

In this section, we demonstrate how an attacker tries to compromise a network system and we employ the approach proposed in this paper as a response to the attack. We used the Figure 6 through 9 to prove that our proposed method counter the SMB attack and therefore should be employed in real-life systems to mitigate the SMB attack on network systems.

Figure 6. public profile is on now (firewall state).

An attacker tries to use SMB Version to detect the machine and Operating System (OS), but the Armitage responds, scanned 1 of 1 hosts. Although, physically Armitage will not present any computer on the screen or any OS. This is because of the public profile firewall state is set to be on. If the firewall state is set to be off and RDP is enabled, the attacker can retrieve Local Hashes using weak local credentials by using this command, ./redsnarf.py -H ip=172.16.11.236 -uC security. In addition, he can retrieve hashes across a network range using domain administrator credentials using the next command, ./redsnarf.py -H range=172.16.11.236/24 -u administrator -p Password01 -d yourdomain.com, [25].

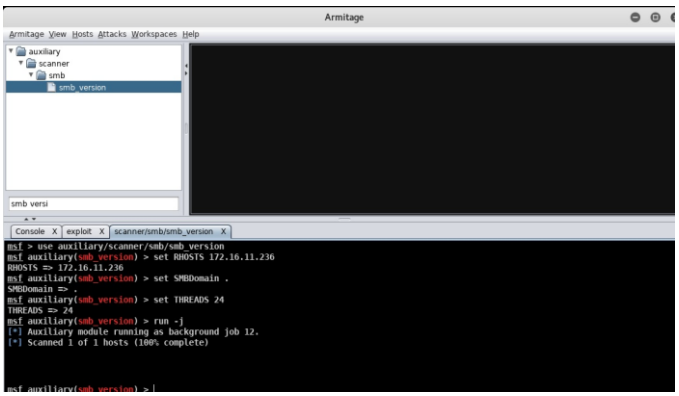

Figure 7. cannot detect the target.

If the above method fails, the attacker will try to detect the machine by another way through open hosts menu then >> Nmap >> Scan then quick scan (OS discover), as

you see the command shell session Closed, Armitage will present dummy machine without any OS as you will see in the next figure 8.

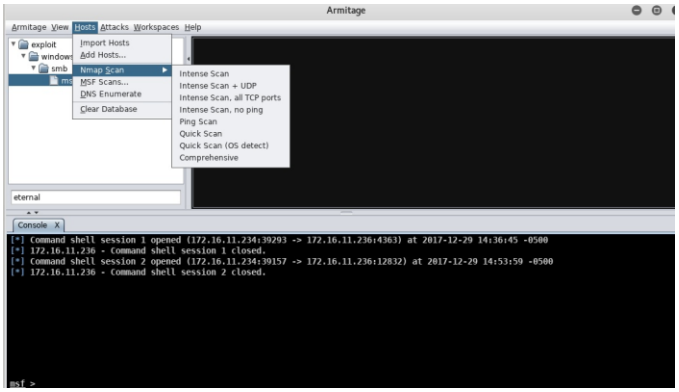

Figure 8. hacker try to detect in another way.

Tha attacker may use the MS17_010_Eternalblue to attack the machine but he cannot create any sessions from the victim's system because of the public profile firewall state is turned on. Therefore, the request from APT Machine is declined.

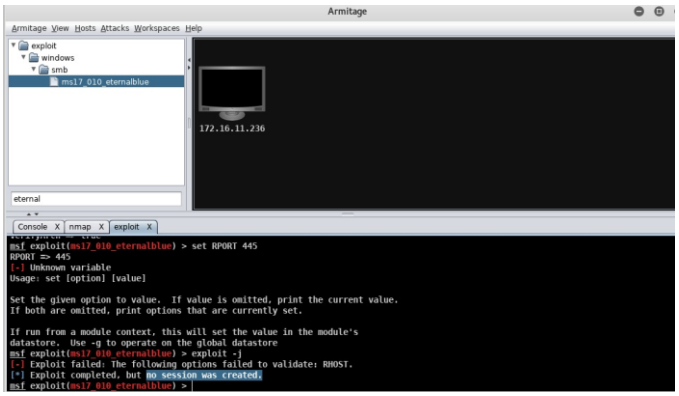

Figure 9. no sessions.

VI. FUTURE WORK

Our concept was, try to catch any strange behavior in the first moment on the victim before transferred to the infrastructure network, We recommend that Microsoft Corporation develop built-in application integrating all Microsoft Windows applications, controlled by windows, and administrator, to implement our approach and give a direct message prompt to the user to easily detect when an attacker is about to infiltrate the system. Message prompt such as 'check your computer,' 'strange

behavior detected' and so on will be adequate to alert the user who can easily prevent such attacks. In conclusion, we request that researchers should look at this area of research thoroughly as there are many attacks that need to be investigated and mitigated to deter hacking which tops one of the cyber-problems that needs immediate attention. Areas such as ATT&CK,CAR, CyDef et cetera.

VII. OS, AND TOOLS

- Kali Linux 2017.3
- Microsoft Windows7
- Armitage
- MS17_010_Eternalblue

VIII. CONCLUSION

In this paper, we have explored both in detail and with pictorial representation and description how an attacker can use MS17_010_Eternalblue from Armitage inside Kali Linux 2017.3 to get an advantage through a Server Message Block (SMB) remote code attack in windows7. We demonstrate how to stop this kind of Attack by inventing a policy, to prevent WMIC, remote access RDP, and enable public profile firewall state. Finally, we propose a strategy to differentiate between victim, infrastructure, and an attacker if there is still any strange behavior observed in the network system.

ACKNOWLEDGMENT

This research was partially supported by the Fundamental Research Grant Scheme (FRGS) for ''Content-Based Analysis Framework for Better Email Forensic and Cyber Investigation'' [203/PKOMP/6711426], Security and Forensic Research Group (SFRG) Lab, School of Computer Sciences, Universiti Sains Malaysia.

REFERENCE

[1] Holm, Hannes, et al. "Success rate of remote code execution attacks: expert assessments and observations." Journal of universal computer science (Online) 18.6 (2012): 732-749.

[2] Ali Islam, Nicole Oppenheim, Winny Thomas (2017, May 26). SMB Exploited: WannaCry Use of "EternalBlue". Retrieved December 11, 2017.

[3] Strom, Blake E., et al. "Finding Cyber Threats with ATT&CK™-Based Analytics." (2017).

[4] Stiawan, Doris, et al. "Penetration Testing and Mitigation of Vulnerabilities

Windows Server." IJ Network Security 18.3 (2016): 501-513.

[5] Ullah, Ikram. Detecting Lateral Movement Attacks through SMB using BRO. MS thesis. University of Twente, 2016.

[6] Greco, Alessandro, et al. "Advanced Widespread Behavioral Probes against Lateral Movements." (2016).

[7] Bodeau, Deborah, and Richard Graubart. "Cyber Prep 2.0." (2017)

[8] Bodeau, Deborah, and Richard Graubart. "Cyber Resiliency Design Principles." (2017)

[9] Kimura, Margot, Troy DeVries, and Susanna Gordon. The Cyber Defense (CyDef) Model for Assessing Countermeasure Capabilities. No. SAND2017-6078. Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2017.

[10] Bodeau, Deborah, and Richard Graubart. "Structured Cyber Resiliency Analysis Methodology (SCRAM)." (2016).

[11] Akkas, Abdurrahman, Christos Nestoras Chachamis, and Livio Fetahu. "Malware Analysis of WanaCry Ransomware." (2017).

[12] Vijayalakshmi, Yellepeddi, et al. "Study on Emerging Trends in Malware Variants.".

[13] Kharraz, Amin. "Techniques and Solutions for Addressing Ransomware Attacks." (2017).

[14] Korznikov, A. (2017, March 17). Passwordless RDP Session Hijacking Feature All Windows versions. Retrieved December 11, 2017.

[15] Counter Threat Unit Research Team. (2017, October 12). BRONZE BUTLER Targets Japanese Enterprises. Retrieved January 4, 2018.

[16] Symantec Security Response. (2017, November 7). Sowbug: Cyber espionage group targets South American and Southeast Asian governments. Retrieved November 16, 2017.

[17] Beechey, J. (2010, December). Application Whitelisting: Panacea or Propaganda?. Retrieved November 18, 2014.

[18] Tomonaga, S. (2016, January 26). Windows Command Abused by Attackers. Retrieved February 2, 2016.

[19] NSA Information Assurance Directorate. (2014, August). Application Whitelisting Using Microsoft AppLocker. Retrieved March 31, 2016.

[20] Corio, C., & Sayana, D. P. (2008, June). Application Lockdown with Software Restriction Policies. Retrieved November 18, 2014.

[21] Microsoft. (2012, June 27). Using Software Restriction Policies and AppLocker Policies. Retrieved April 7, 2016.

[22] Alperovitch, D. (2014, October 31). Malware-Free Intrusions. Retrieved November 4, 2014.

[23] Korznikov, A. (2017, March 17). Passwordless RDP Session Hijacking Feature All Windows versions. Retrieved December 11, 2017.

[24] Beaumont, K. (2017, March 19). RDP hijacking—how to hijack RDS and RemoteApp sessions transparently to move through an organization. Retrieved December 11, 2017.

[25] NCC Group PLC. (2016, November 1). Kali Redsnarf. Retrieved December 11, 2017.

[26] valsmith. (2012, September 21). More on APTSim. Retrieved September 28, 2017.

[27] Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.

[28] US-CERT. (2017, October 20). Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved November 2, 2017.

[29] Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Remote Administration Tools & Content Staging Malware Report. Retrieved March 16, 2016.

[30] Mohamed, Nachaat AbdElatif, Aman Jantan, and Oludare Isaac Abiodun. "An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network." Proceedings of the International MultiConference of Engineers and Computer Scientists. Vol. 1. 2018.