Research and Develop the Apt Defense from Attack System Using Sandbox Technique

Son Hai Ly[1], **Tung Thanh Do**[1], **Nhi Yen Thi Tran**[1]*

Van Lang University, Ho Chi Minh City, Vietnam

Correspondence: **Nhi Yen Thi Tran**, Van Lang University, Vietnam

E-mail: nhi.tty[at]vlu.edu.vn

Abstract: ***Advanced Persistent Threat is an insidious, persistent, and with a specific aim attack into a target system. According to statistics in Vietnam and the world, many APT attacks cause significant negative effects. Therefore it is crucial to find a solution to combat these attacks. This thesis will give a comprehensive introduction about APT attacks; their specific features; preventative measures; malware analysis and its technique, static analysis technique; sandboxing technique; automatic analysis and report about malware behaviors without human intervention; and suggest an integrated model solution that detects and prevents APT using sandboxing technique. Through installation trials, the thesis proves that the sandboxing technique can analyze and detect malware behaviors on the system.***

Keywords: APT, Sandbox, Sandboxing

1. Introduction

Nowadays, the cyber environment is getting more complicated. The cyber environment is a virtual one but its effects and repercussions have literal socio-economic impacts. Cyber attacks have been a pressing global issue with many different types of attacks such as APT - Advanced Persistent Threats. APT is usually executed by high tech, advanced criminal groups whose targets are governments and big financial institutions. To execute these attacks, these groups have to spend an enormous amount of time to survey and analyze their target and the exploitation process is fragmented and attacks can take place over several years. Therefore, traditional defense systems and methods virtually cannot detect APT. The repercussions of APT left behind are highly severe for the finance, politics, prestige, and image of corporations and organizations.

After having pointed out the urgency of the aforementioned problem, my research topic is essential and has high practicality. In recent years, there have been many APT attacks around the world and even in Viet Nam. Between 2016 and 2017, many APT attacks have left severe negative impacts and many attacked organizations cannot detect and cope with the attacks.

APT attacks are a series of many small attacks over time therefore there is no specific solution to completely detect APT attacks. To detect and defend against APT, there needs to be a separate and unique monitoring system and this system is built on the following mechanisms:

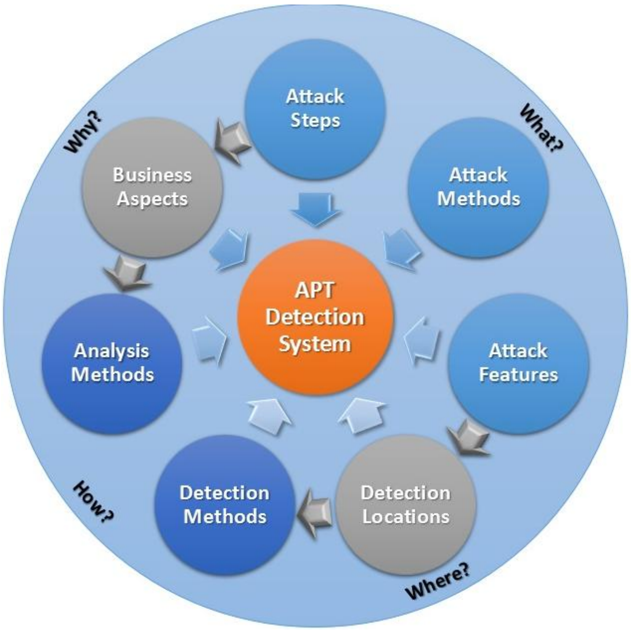


Figure 1: APT attack detection system

- What: What are the steps? Methods? Functions and techniques?
- Where: The areas, sectors?
- How: Detection and monitoring methods? Event analysis methods?
- Why: Impacts on business?

Monitor, analyze, and detect throughout each stage of attacks. At different stages, different tools and techniques can be implemented but with a common aim that is to get the expected results at each stage. Therefore, setting systems that collect information and monitor throughout stages of the attacks is the most effective method.

At each stage, 3 things need to be identified:

- Detection Locations
- Detection Methods
- Analysis Methods

2. Method

2.1 Collect and categorize malwares

Malwares collection

Collecting malwares is the process of finding out which files are contaminated to research, analyze, and eradicate. There are many ways to collect samples such as the Honeypot system, user-submitted samples, internet, and buying from cybersecurity brands.

A common way to collect samples is on contaminated computers. However, in order to ensure safety, a backup of the infected drive is essential. Next, the search for foreign files in the system is conducted. After that, a procedure to analyze processes is enacted to find out the abnormal process and its root, then the sample is compressed and moved to the analysis stage. Example: a sample named Rbot which is usually used in DdoS attacks works by opening a channel in the victim's computer and participating in an IRC chat channel to be commanded by the attacker. Based on abnormal internet bandwidth, some softwares can be used to determine processes and analyze the location of Rbot.

Send the malwares

After collecting the samples, besides conducting one's own research and analysis, it is important to also send these malwares to Antivirus software companies so these companies can update their sample database and release update signatures.

2.2 Analyze basic information

Take note of specific features, categorize malwares, check the properties of files, size and other basic information to initially categorize malwares. This identification process is conducted by sending malwares to sites like virustotal.com, malwr.com or through Antivirus softwares.

Basic identification process can be described like the picture 2.2

Step 1: Analyze the properties of files, hash values, and strings.

Step 2: Analyze the compressed files to see if the files are compressed? If yes then use unzip softwares then return to step 1, if not proceed to step 3.

Step 3: Check the results, upload the hash values to Virustotal to see if they have been analyzed yet? If yes, save as reference for future analysis.

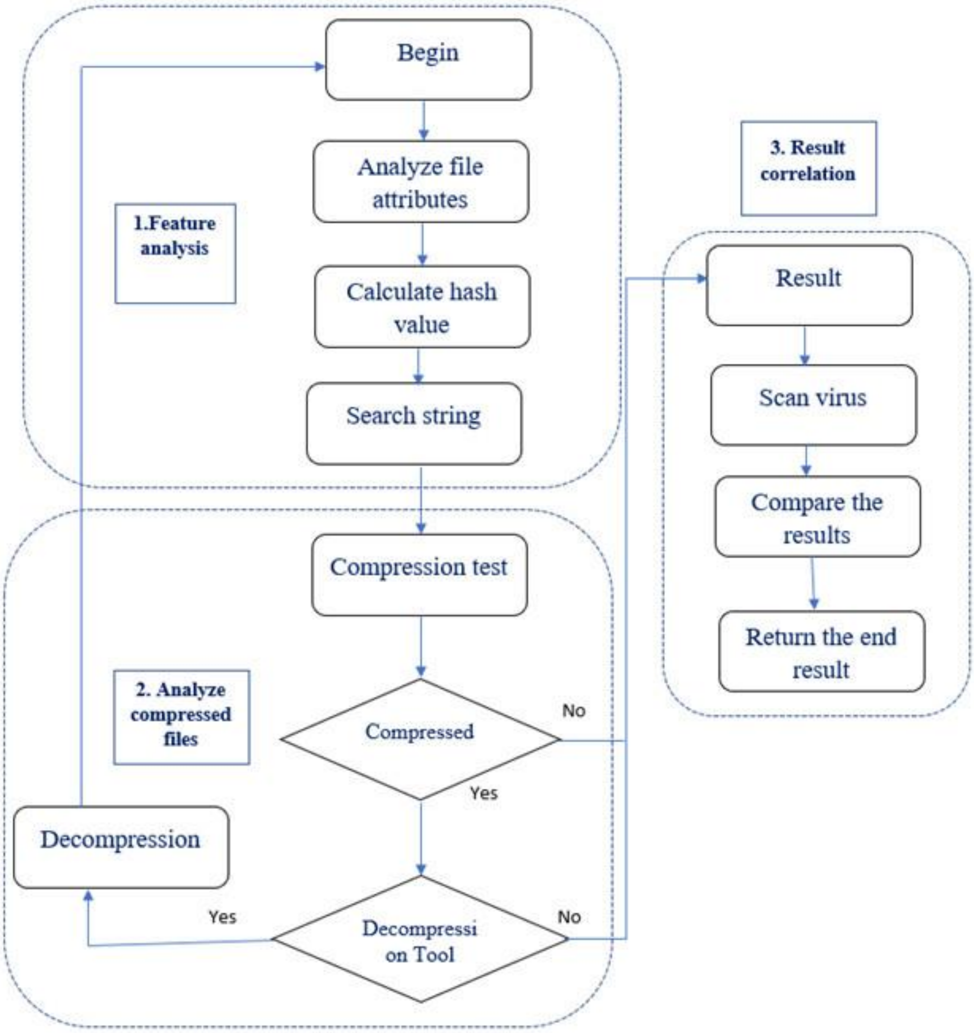


Figure 2: Basic analysis steps

Here are examples of information collected from Virustotal.com after sending malware samples. The information provided is as follows: SHA256 hash value, sample name, there are 4/58 of Antivirus softwares that can identify this malware and this malware sample just got uploaded on Virustotal.

2.3 Analyze the activities

This process uses a dynamic analysis method which builds a virtual analysis environment that is separate from the actual environment. That environment simulates Internet services and appropriate factors for the malwares to function. It allows us to observe suspicious files in action? How do they run? What do they do on the computer and how do they interact with internal services?

Static analysis method is a method which reads the execution codes of the malwares using a Disassembler to reverse translate the codes inside the malwares into a form of assembly. From that it is now possible to know what the malwares are capable of. The commands are executed by CPU so these commands will know exactly what the malwares do. However, in order to execute static analysis, it requires a deep understanding of assembly, commands, and API in the operating system. This method is crucial to detect specific activities of malwares.

2.4 Write report on the activities of malwares

After the process of analyzing the malwares comes the reporting phase that gives a general report on the activities of the malwares. Here is an example of a report.

Table 1: Report after analyzing malware Order.exe

Sample characteristics	Value
Microsoft	Backdoor
File SIZE	1172480 bytes
MD5	8d27a5556ec035ccb65b5a24cd9765bc
SHA1	59445a01810886c241783a6bd57979336922104e

Table 2: Malicious variant names by brands

Company name	Malicious variant names by brands
Bkav	W32.Clod4ea.Trojan.d8ee
MicroWorld-eScan	Gen: Variant.Zusy.199317
CAT-QuickHeal	Backdoor.Fynloski
ALYac	Gen: Variant.Zusy.199317
Malwarebytes	Trojan.Dropper
VIPRE	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.151026.9950.9989
Sysmantec	Trojan.Gen.2
TrendMicro	TROJ_GEN.R02PC0DH116
Avast	Win32:Malware-gen
Kaspersky	HEUR: Trojan.Win32.Generic
BitDefender	Gen: Vaariant.Zusy.199317
McAfee	BehavesLike.Win32.Backdoor.tc

Table 3: Activity level

Activity	Level
Write to the memory area of a process	High
Write to the memory area of the Windows system process	High
Write in the memory area of a process that has been run before	High
Edit Windows firewall configuration	Normal
Run an extra Windows Explorer display	Normal
Collect information about system files and folders	Normal
Collecting information on processes	Low
Add and edit Cookie information on a Web browser	Low

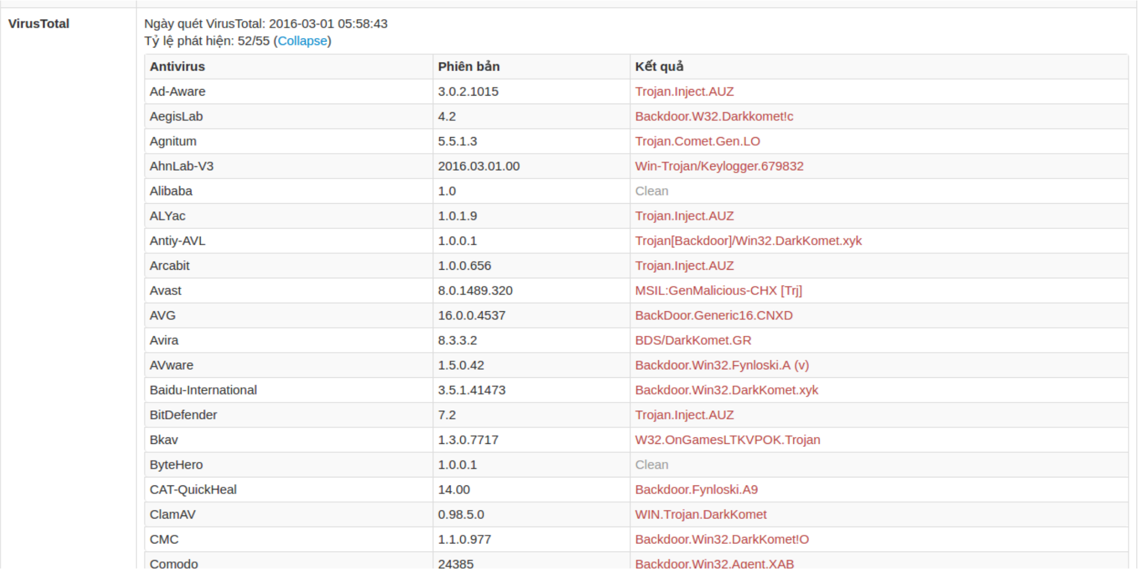
Table 4: Change the process

<table>
<tr><th colspan="4">Change the process</th></tr>
<tr><th>API</th><th>ARGUMENTS</th><th>STATUS</th><th>RETURN</th></tr>
<tr><td><b>NtCreatSection</b></td><td>ObjectAttributes: C:\Global\Cor_Private_IPCBlock_1592
DesiredAccess: 0x000f007
SectionHandle: 0x000000ac
FileHandle: 0x00000000</td><td>success</td><td>0x00000000</td></tr>
<tr><td><b>ZwMapViewOfSection</b></td><td>SectionOffset: 0x0012f8ec
SectionHandle: 0x000000ac
ProcessHandle: 0xffffffff
BaseAddress: 0x00c10000</td><td>success</td><td>0x00000000</td></tr>
<tr><td colspan="4">Change a file</td></tr>
<tr><th>API</th><th>ARGUMENTS</th><th>STATUS</th><th>RETURN</th></tr>
<tr><td><b>NtCreatFile</b></td><td>ShareAccess:1
FileName
C:\DOCUMENT~1\User\LOCALS~1\Temp\order.exe.config
DesiredAccess: 0x80100080
CreatDisposition: 1
FileHandle: 0x00000000</td><td>failed</td><td>0xc0000034</td></tr>
<tr><td><b>NtCreatFile</b></td><td>ShareAccess: 1
FileName
C:\DOCUMENT~1\User\LOCALS~1\Temp\order.exe
DesiredAccess: 0x80100080
CreatDisposition: 1
FileHandle: 0x0000009c</td><td>success</td><td>0x00000000</td></tr>
<tr><td><b>NtQueryInformationFile</b></td><td>FileHandle: 0x0000009c
FileInformation:
\x00\xf0\x11\x00\x00\x00\x00\x00\xe4\x11
\x00\x00\x00\x00\x00\x01\x00\x00\</td><td>success</td><td>0x00000000</td></tr>
</table>

	x00\x00\x00\x00\x00		
Registry Changes			
API	ARGUMENTS	STATUS	RETURN
RegOpenKeyExW	Ordinal: 0 Functionname: RegQueryValueExW FunctionAddress: 0x77dd6ffef ModuleHandle: 0x77dd0000	Success	0x00000000
RegQueryValueExW	Handle: 0x0000009c DataLength: 72 ValueName: InstallRoot Type: 1	Success	0x00000000
RegCloseKey	HandleL: 0x0000009c	success	0x00000000

3. Results

After developing this function during the analyzing malware process, the function will check for the MD5 value on Virus Total and obtain the results from there. The obtained result will show the type of malwares if it exists on the database of Antivirus softwares. This result allows for the fast identification of previous malwares. However for malwares that have not been identified, there will be no returning results.



VirusTotal

Ngày quét VirusTotal: 2016-03-01 05:58:43
Tỷ lệ phát hiện: 52/55 (Collapse)

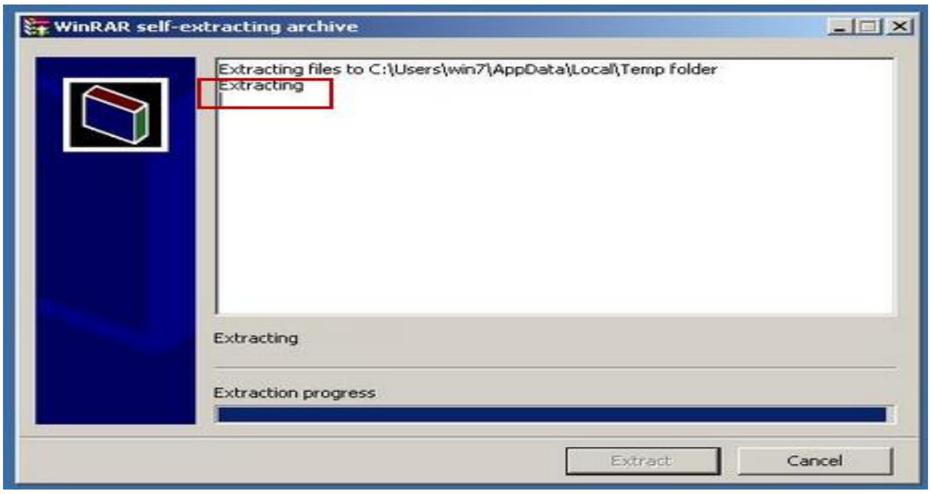
Antivirus	Phiên bản	Kết quả
Ad-Aware	3.0.2.1015	Trojan.Inject.AUZ
AegisLab	4.2	Backdoor.W32.Darkkomet!c
Agnitum	5.5.1.3	Trojan.Comet.Gen.LO
AhnLab-V3	2016.03.01.00	Win-Trojan/Keylogger.679832
Alibaba	1.0	Clean
ALYac	1.0.1.9	Trojan.Inject.AUZ
Antiy-AVL	1.0.0.1	Trojan[Backdoor]/Win32.DarkKomet.xyk
Arcabit	1.0.0.656	Trojan.Inject.AUZ
Avast	8.0.1489.320	MSIL:GenMalicious-CHX [Trj]
AVG	16.0.0.4537	BackDoor.Generic16.CNXD
Avira	8.3.3.2	BDS/DarkKomet.GR
AVware	1.5.0.42	Backdoor.Win32.Fynloski.A (v)
Baidu-International	3.5.1.41473	Backdoor.Win32.DarkKomet.xyk
BitDefender	7.2	Trojan.Inject.AUZ
Bkav	1.3.0.7717	W32.OnGamesLTKVPOK.Trojan
ByteHero	1.0.0.1	Clean
CAT-QuickHeal	14.00	Backdoor.Fynloski.A9
ClamAV	0.98.5.0	WIN.Trojan.DarkKomet
CMC	1.1.0.977	Backdoor.Win32.DarkKomet!O
Comodo	24385	Backdoor.Win32.Agent.XAB

Figure 3: Results obtained from VirusTotal

VirusTotal allows identification from 52 different AntiVirus softwares: Bkav, MicroWorld-eScan, nProtect, CAT-QuickHeal, McAfee, Malwarebytes, K7AntiVirus, K7GW, TheHacker, NANO-Antivirus, F-Prot, Symantec, Norman, TotalDefense, Avast, ClamAV, Kaspersky, BitDefender, Agnitum, SUPERAntiSpyware, Sophos, Comodo, F-Secure, DrWeb, VIPRE, AntiVir, TrendMicro, McAfee-GW-Edition, Emsisoft, Jiangmin, Antiy-AVL, Kingsoft, Microsoft, ViRobot, AhnLab-V3, Gdata, Commtouch, ByteHero, VBA32, Baidu-International, ESET-NOD32, Rising, Ikarus, Fortinet, AVG, Panda.

The development of this function helps analyze more malwares. Supported document types: applet, bin, dll, doc (docx), exe, html, jar, pdf, zip. For each different type of files there will be different configurations which allows for further involvement in the analyzing process. This deep involvement is impossible in automated processes such as analyzing a compressed file that has a password. The system can support the analysis of .zip files through the zip.py library of the directory cuckoo/ analyzer/ windows/ modules/ packages. With this editing and configuring the source of the file zip.py, we can list all the files in the folder and apply the appropriate analysis package.

After changing the system, we test the function by creating a zip file example.zip which has example.part1.exe and example.part2.dll. The example.part1.exe requires example.part2.dll to work and create example.exe as a result. Now upload the example.zip onto the system for further analysis.



WinRAR self-extracting archive

Extracting files to C:\Users\win7\AppData\Local\Temp folder
Extracting

Extracting

Extraction progress

Figure 4: Example.exe is created from 2 original files

Advanced Persistent Threat is an insidious, persistent, and with a specific aim attack into a target system. According to statistics in Vietnam and the world, many APT attacks cause significant negative effects. Therefore it is crucial to find a solution to combat these attacks. After extensive research time, here are the current solutions for the APT threats.

4. Conclusion and Recommendation

In the near future, to solve the detection problem of APT defense, the research approach should focus on building a sandboxing system that connects with the real internet system to increase cyber defense for the unit. I would like to sincerely thank Van Lang University for supporting us throughout the research process.

References

[1] Bennet Yee, D. S. (2009). *Native Client: A Sandbox for Portable, Untrusted x86 Native Code*, Appear in the 2009 IEEE Symposium on Security and Privacy , Google Inc.

[2] Bennet, N. V. (2012). *Detecting APT Activity with Network Traffic Analysis*, Trend Micro.

[3] Ghafir I., P. V. (2014). *Advanced Persistent Threat Attack Detection: An Overview*, Proceedings of International Conference On Advances in Computing, Electronics and Electrical Technology.

[4] Horneman, D. S. (2014). *Investigating Advanced Persistant Threats 1*, Carnegie Mellon University.

[5] Hudson B. (2013). *Advanced Persistent Threats*, Detection, Protection and Prevention.

[6] Jover R.P., G. P. (2013). *How vulnerabilities in wireless networks can enable Advanced Persistent Threats*, International Journal on Information Technology (IREIT).

[7] Light, M. H. (2011). *Malware Analyst's Cookbook and DVD Wiley Publishing*, Inc.

[8] McAfee. (2011). *Combating Advanced Persistent Threats*.

[9] Nikolaos. (2015). Virvilis-Kollitiris. *Detecting Advance Perisistant Threats through Deception Techniques*, Athens University of Economics and Business.

[10] Robert Wahbe, S. L. (1993). *Efficient Software-Based Fault Isolation.*

[11] Schmid, M. (2002). *Protecting data from malicious software*, Proceedings of the 18th Annual Computer Security Applications Conference.

[12] Tankard, C. (2011). *Advanced persistent threats and how to monitor and deter them*, Network security.

[13] W, A. (2016). *How to combat advanced persistent threats*, APT strategies to protect your organization.

[14] Websense. (2013). *Advanced Persistent Threats and other Advanced Attacks*.