Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 4, April-2016

A SURVEY REPORT ON ADVANCED PERSISTENT THREAT

Vrundalu Poriya[1], Ravi K Sheth[2],

[1,2] Raksha Shakti University, Ahemedabad
India
[1]12.vrundaliporiyaa@gmail.com, [2]rks.it@rsu.ac.in

Abstract. The Advanced Persistent Threat (APT) has become the countersign for today's cyber espionage. It is continuously involves a piece of malware programs that can conceal detection, remain in target systems for the long periods of time and reach out across the Internet to exfiltration data or allow an attacker to exert further control of the system. Using APTs attacks economic losses are increasing very widely about billion to hundreds of billions of dollars per year. There are different defensive tools, procedures and other controls commonly put in place to handle produce security threats are often inadequate against targeted APT-style attacks because the actors behind the intrusion are focused on a specific target and are able to customize and alter their Tactics, Techniques and Procedures (TTP) to predict and evade security controls and standard incident response practices. In this paper we have focus on process of working about APTs and related case studies about the attack and according to that give related solution against same.

Keywords: APT, Malware, TTP, SIEM, C&C

1 Introduction

Advanced - an attacker has the skill to avoid detection and the capability to hike information and maintain access as well secured networks and confidential information involved within them. It is generally adaptive and well-resourced thing.

Persistent - The persistent nature of the threat makes it difficult to prevent access to your computer network and once the threat actor has successfully gained access to your network, it is very difficult to remove.

Threat - The attacker has not only the intent but also the capability to gain access to sensitive information stored electronically.

Targeted attacks are also known as "advanced persistent threats (APTs)". However, instead of focusing on the attack methods and effects to improve network defences. On another hand, some believe that the threat actors behind these campaigns have mythical capabilities both in terms of operational security and the exploits and malware tools they use. In fact, they do not always use zero-day exploits and often use older exploits and simple malware.

In current scenario we are seeing targeted cyber-attacks on organizations grow increasingly more sophisticated, more serious, and more extensive. According to the "black hat" community evolved from adolescent hackers bent on mayhem to organized crime networks, fuelling highly profitable identity theft schemes with massive loads of personal data harvested from corporate and government networks. Recently, changes in IT infrastructure and usage mode is including mobility, cloud computing, and virtualization have dissolved traditional enterprise security perimeters, so it creates a "target-rich" environment for the hackers But perhaps the most significant new element in the threat landscape is the emergence of highly targeted, long-term, international espionage and sabotage campaigns by covert state actors. These long-term, state-sponsored campaigns are sometimes known as Advanced Persistent Threats (APTs). The term has become a buzzword used and misused by the media, and by some technology vendors. While APTs do represent a real danger in today's world, it is important to understand how they figure within a larger context. Only by separating reality from hype and seeing how APTs relate to the broader field of targeted attack methods and techniques will organizations be able to safeguard their information and operations in the coming decade.

2 Phenomenon of APT

An APT is a type of targeted attack. APTs can and often do use many of these same techniques, including drive-by download, SQL injection, malware, spyware, phishing, and spam, etc.. An APT is always a targeted attack, but vice versa is not always right. APTs are different from other targeted attacks in the following ways:

A. Customized attacks

APTs often use highly personalized tools and intrusion techniques, developed specifically for the warfare. These tools include zero-day vulnerability exploits, viruses, worms, and rootkits. In addition, APTs often launch multiple threats or "kill chains" concurrently to breach their targets and ensure current access to targeted systems, sometimes including a "propitiatory" threat to conspiracy the target into thinking the attack has been successfully repelled.

B. Low and slow —

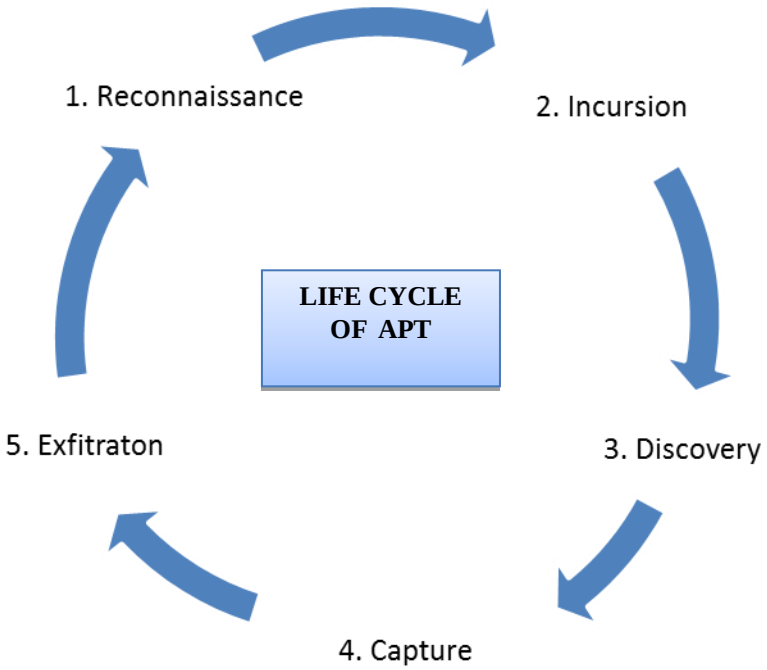
APT attacks transpire over long periods of time during which the hackers move slowly and quietly to avoid detection. In contrast to the "smash and seize" tactics of many targeted attacks placed into orbit by more ordinary cybercriminals, the aim of the APT is to stay undetected by moving "low and slow" with stable monitoring and interaction until the hackers achieve their decided objectives.

• Higher desires—unlike the fast-money schemes typical of more common targeted attacks, APTs are designed to satisfy the requirements of international espionage and/or sabotage, usually involving covert state actors. The objective of an APT may include military, political, or economic intelligence gathering, confidential data or trade secret threat, disruption of operations, or even destruction of equipment. The groups behind APTs are well funded and staffed; they may operate with the support of military or state intelligence.

C. Specific targets —

While nearly any large organization seizing intellectual property or confidential information of customer is vulnerable to proposed attacks, APTs are aimed at a much smaller range of targets. The main targets of APT's are government agencies and facilities, defense contractors, and manufacturers of products that are highly competitive on global markets. APT also attack on vendor and partners organizations for revenge purpose with primary target.

LIFE CYCLE OF ADVANCED PERSISTENT THREAT



Phase 1: Reconnaissance:
APT attacks often exploit large numbers of researchers who may spend months studying their targets and making themselves familiar with target systems, processes, and people, including partners and vendors n also gain more and more information. Information gathering may be used both online and using conventional surveillance tricks.

•Spear Phishing
•Information gathering

Phase 2: Incursion:
In targeted attacks, attackers typically split into the organization's network by these following methods like social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods. These methods are also used in APTs, often in concert. The main difference between targeted attacks and normal attacks is that while common targeted attacks use short-term, "smash and grab" methods, APT incursions are designed to establish a beach head from which to launch covert operations over an extended period of time.

- •Social engineering
- •Manual operations
- •Zero day vulnerabilities

Phase 3: Discovery:
Once inside, the attacker maps out the organization's network and automatically scans for confidential and sensitive data or, in the some APTs, operational instructions and functionality. In Discovery stage it may include unprotected data and networks as well as software and hardware vulnerabilities, exposed credentials, and pathways to additional resources or access points. Again where most targeted attacks are opportunistic, APT attacks are more efficient and go to remarkable lengths to avoid detection.

- •Multiple vectors
- •Run silent, run deep
- •Research and analysis

Phase 4: Capture:
In this phase, disclosed data stored on unprotected systems which is immediately accessed by an attacker. More in this phase, rootkits may be stealthily installed on targeted systems and network access points to capture data and instructions as they flow through the organization.

- •Long term occupancy
- •Control

Phase 5: Exfiltration:
Once the intruders have seized control of target systems, they may proceed with the theft of intellectual property or other confidential data and sensitive information.

- •Data transmission
- •Ongoing analysis

3 Related work

A. Why APT happen..??

1. Host Behavior Baselines that look for scans on the network or invalid TCP flag patterns cannot detect an Advanced Persistent Threat. Comparing how a host usually talks on the network to how it is using the network now can certainly find threats but, this will never help network to detect of on-going targeted attacks.
2. Packet Signature systems that watch for bit patterns. This effort is unlikely going to help find an APT. APTs often use secure connections on port 443 and encrypt their sneaky efforts.

B. Effective fight against APT

1. IP Host Prominence can often help to find APTs because it compares all connections with hosts on the internet to a position database. Warning flags will be raise from poor reputed hosts whose connection will be poor. These databases are updated frequently and the Command and Control (C&C) server will be a part of APT on the list.
2. Setup a Honeypot and watch all connections and operations from the internet. Then, watch who and with what the honeypot tries to communicate with on the corporate network. An ideal solution for this is Net Flow Monitoring. By Net Flow Report we came to know about with whom who the honeypot server is trying to communicate, how often and with what port (e.g. TCP port 443). If any internal hosts are communicating in a similar way with the same internet host the honeypot is, you could have a problem that is worth investigating and it's a sign of an malicious activity.

4 CASE STUDY

"OPERATION POTAO EXPRESS - Analysis of a cyber-espionage toolkit"

Potao is an example of targeted espionage (APT) malware detected mostly in Ukraine and a number of other CIS countries, including Russia, Georgia and Belarus. Among the victims that we were able to identify, the most notable high-value targets include Ukrainian government and military entities and one of the major Ukrainian news agencies. The malware was also used to spy on members of MMM, a financial pyramid scheme popular in Russia and Ukraine.
One of the most interesting discoveries during our Potao investigation and research was the connection to a Russian version of the now discontinued popular open-source encryption software, TrueCrypt. The website truecryptrussia.ru has been serving a Russian language localized version of the TrueCrypt application that also contains a backdoor, in some specific cases. The trojanized version of the application is only served to selected victims which is another indicator of targeting by the malware operators and also one the reasons why the backdoor has gone unnoticed for such a long time. In addition to serving trojanized TrueCrypt, the domain also acted as a C&C server for the backdoor. The connection to Potao lies in the fact that Win32/Potao has been downloaded in a few cases by Win32/FakeTC (ESET detection name of the trojanized encryption software). The Potao malware is a universal modular cyber-espionage toolkit. The attacks where it was employed were of the targeted (APT) type but there were also several cases where we detected the Trojan in mass spreading campaigns.

Attack timeline

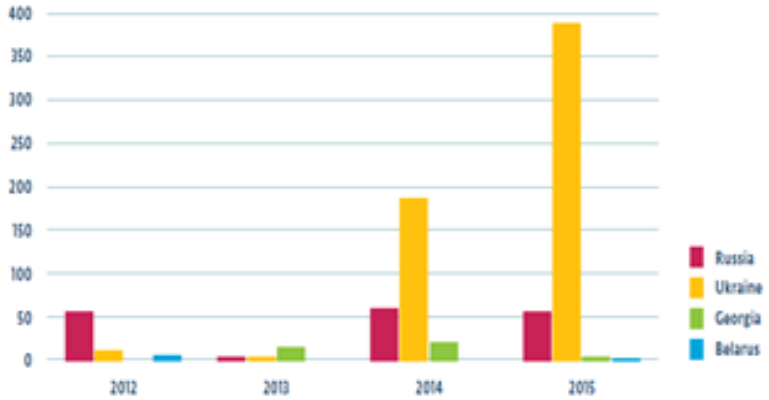


Figure 1: Detection statistics for WIN32/Potao according to ESET live grid

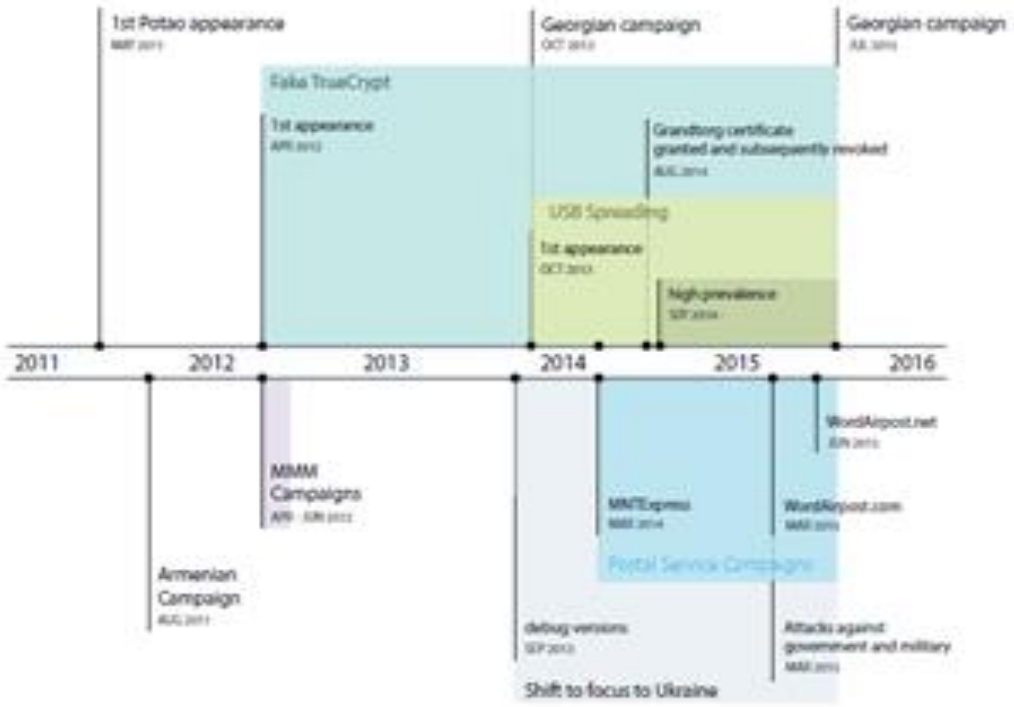


Figure 2: Timeline of selected POTAO campaigns

The main reason for the increase in Potao detections in 2014 and 2015 were infections through USB drives. The timeline in Figure 2 lists a selection of Potao attack campaigns and other important events, according to dates when they were first detected by ESET, or by the compilation timestamps in the binaries.

5 Prevention Technique

A. Network Traffic Analysis:

This technique considers inspecting DNS flow traffic in analysis; in other words, conducting in-depth network traffic monitoring and analysis with Net Flow Traffic Analyzer software and some other software which will analyze network traffic.

B. Network Forensics:

This technique considers using a Network Forensic Analysis Tool (NFAT) to detect and analyze security incidents solutions that mount efficient and effective post-incident response investigations.

C. Payload Analysis:

This technique suspects can provide detailed reports about malware behavior from sandbox analysis, either as a solution on-premises or cloud-based.

D. Endpoint Behavior Analysis:

This technique sees Endpoint Security and Control that provide intelligence and correlation for behavior analysis to block malware and fend off zero-day attacks, if not as a strategy for ATA defense.

E. Endpoint Forensics:

This technique serves as an endpoint security tool that helps detect hidden malware and other signs of compromise or irregular activities on endpoints across the enterprise. It can be used to identify attacker behavior, investigate and respond to cyber-attacks on the endpoint before critical data loss occurs.

APT examples

The APTs on this list differ in size and importance. The following top ten consists of the most sophisticated, most widespread or otherwise interesting examples.

a) Wicked Rose:

The original APT had done in 2006 and the main target was US military was suspicious to be equalized from China

b) Ghost net:

The oldest APT happens in 2009. In detection process of this attack attacker infected 1295 hosts in 103 different countries.

c) Stuxnet:

Surprised APT attack till now for security researchers by knowing previously unknown security issues. This proves that the hackers are able to execute their own security research.

d) Operation Aurora:

This attack takes place in end of 2009 and detect in 2010. The aim was to steal or compromise the source code of several US tech companies. One of the victims was Google and also announced by Google first.

e) Duqu:

This APT was done in 2010 and it was one of the most advanced attacks in that duration.

f) Uroburos / Turla / Snake:

It was detected in 2011 and it has the very sophisticated property that infect nodes which are communicate with each other and making it also possible for attacker that they can compromise nodes even there are not connected to internet.

g) Windigo:

Recent APT from 2015 which uses multiple ways to attack on networks. Moreover it can able to increase several UNIX and LINUX server and computers that are normally much less vulnerable. The reason is that Windigo is able to intercepts SSL sessions and capture credentials. These credentials will help attacker to log in to the servers as well computers.

Some smaller but interesting APTs in the list are the following:

h) The Monju incident:

Detected in 2014. This was infected in a single node in Japanese power plant which was having an infected media player. The incident could be a unplanned event, or the first step in nuclear attack. As the culprits have not been caught, we do not know for sure.

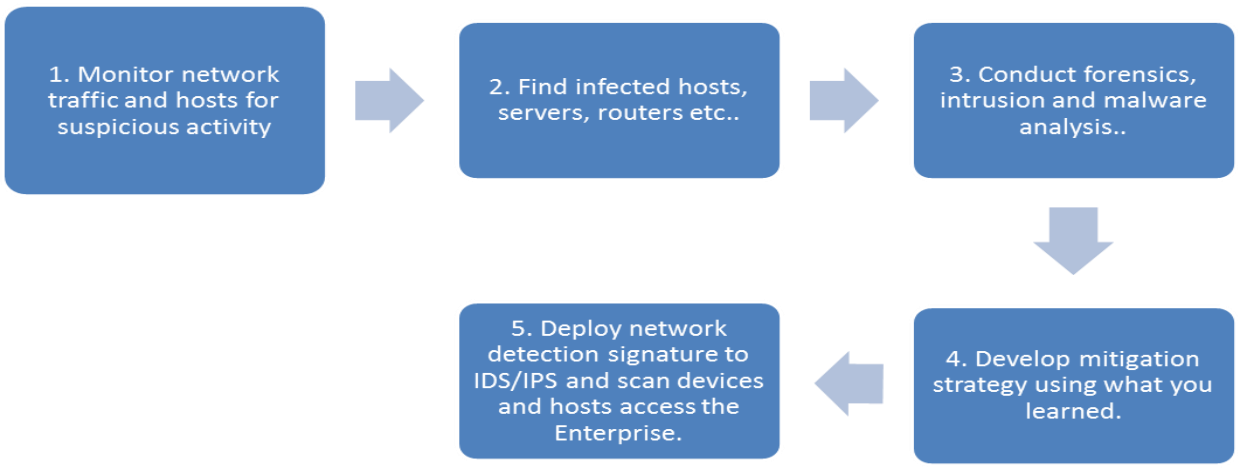
i) The Dark Hotel:

Threat from 2014 was aimed individually at CEOs of organizations, and was able to infect these CEOs and follow them through the Wi-Fi networks of hotel chains

j) Anunak:

From 2014 was aimed specifically at banks. This was one of the most targeted attacks, aimed at only striking a few times but getting millions of dollars in each incident.

Anti-APT life cycle



6 Conclusion

After all analysis we finally conclude that APT attacks are successfully bypassing high level security defences, and the majority of IT professionals now believe their organization has been targeted and compromised. So we have to use more and more prevention techniques so that APT will be detected in primary stage and confidential data will not be compromised. Moreover we have to monitor our network and also communication operations continuously. So that we can make our organization more secure. And also use more malware analysis tool. We can propose one anti APT tool for organizations or for a particular node for preventing it from APT attack.

References

[1] 1. A decade review of Advanced Persistent threat Available via : http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf
[2] Understanding Advanced persistent threats Available via :https://www.linkedin.com/pulse/understanding-advanced-persistent-threats-george-moraetes
[3] Cyber-attacks on government websites: India goes on offensive against cyber rogues available via: http://articles.economictimes.indiatimes.com/2011-12-03/news/30471838_1_cyber-attacks-hackers-symantec-india
[4] https://alwaysonsecurity.wordpress.com/
[5] Malicious code trends available on :http://securityresponse.symantec.com/en/uk/threatreport/topic.jsp?id=malicious_code_trends&aid=industrial_espionage
[6] Anatomy of a Data Breach Why Breaches Happen and What to Do About It Available on:http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf
[7] How to Detect Advanced Persistent Threats – 2 Primary Technologies available on :https://www.plixer.com/blog/network-behavior-analysis-2/how-to-detect-advanced-persistent-threats-2-primary-technologies/
[8] Current Trends in the APT World available via: http://resources.infosecinstitute.com/current-trends-apt-world/
[9] An overview of advanced persistent threats available on :http://ictinstitute.nl/advanced-persistent-threats/
[10] Operation Potao Express: Analysis of a cyber-espionage toolkit available on :http://www.welivesecurity.com/2015/07/30/operation-potao-express/
[11] OPERATION POTAO EXPRESS Analysis of a cyber-espionage toolkit available on :http://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdfhttp://www.threattracksecurity.com/press-release/threattrack-security-introduces-automated-apt-remediation.aspx