A SURVEY PAPER ON APT (ADVANCED PERSISTENT THREAT) IN CLOUD SECURITY

Shashikanth Kandukuri[1]
Assistant Professor
CSE Department, VITS
Karimnagar,Telangana
shashi1215@gmail.com

Boddukuri Divya[2]
Assistant Professor
CSE Department, VITS
Karimnagar,Telangana
divyaboddukuri@gmail.com

Challa Rajesh[3]
Assistant Professor
CSE Department, VITS
Karimnagar,Telangana
challarajesh97@gmail.com

Jangalapelli Shiva[4]
Assistant Professor
CSE Department, VITS
Karimnagar,Telangana
shiva0539@gmail.com

ABSTRACT

An Advanced Persistent Threat (APT) is a prolonged, aimed attack on a specific target with the intention to compromise their system and gain information from or about that target.The target can be a person, an organization or a business. When these threats were dubbed their targets were governments and military organizations. The word threat doesn't mean to imply that there is only one kind of malware involved, because an APT usually consists of several different attacks.APTs are cyber attacks executed by sophisticated and well-resourced adversaries targeting specific information in high-profile companies and governments, usually in a long term campaign involving different steps. To a significant extent, the academic community has neglected the specificity of these threats and as such an objective approach to the APT issue is lacking. In this paper, we present the results of a comprehensive study on APT, characterizing its distinguishing characteristics and attack model, and analyzing techniques commonly seen in APT attacks. We also enumerate some non-conventional countermeasures that can help to mitigate APTs, hereby highlighting the directions for future research.

Keywords: Threat, Cyber Attacks, APT, Malware

1. INTRODUCTION:

An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets either private organizations, states or both for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

APT usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attacks. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible

period. Knowing the attacker artifacts, such as file names, can help a professional make a network-wide search to gather all affected systems.Individuals, such as an individual hacker, are not usually referred to as an APT, as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target of Advanced Persistent Threats.

2. ANALYSIS OF ADVANCED PERSISTENT THREATS:

If you know how they exert you, you can learn how to stop them

From cyber criminals who seek personal financial information and intellectual property to state-sponsored cyber attacks designed to steal data and compromise infrastructure, today's advanced persistent threats (APTs) can sidestep cyber security efforts and cause serious damage to your organization. A skilled and determined cyber criminal can use multiple vectors and entry points to navigate around defenses, breach your network in minutes and evade detection for months. APTs present a challenge for organizational cyber security efforts.

Figure 2.1 Analysis of APT

2.1: The six steps of an APT attack

To improve your cyber security and successfully prevent, detect, and resolve advanced persistent threats, you need to understand how APTs work:

1. The cyber criminal, or threat actor, gains entry through an email, network, file, or application vulnerability and inserts malware into an organization's network. The network is considered compromised, but not breached.
2. The advanced malware probes for additional network access and vulnerabilities or communicates with command-and-control (CnC) servers to receive additional instructions and/or malicious code.
3. The malware typically establishes additional points of compromise to ensure that the cyber attack can continue if one point is closed.
4. Once a threat actor determines that they have established reliable network access, they gather target data, such as account names and passwords. Even though passwords are often encrypted, encryption can be cracked. Once that happens, the threat actor can identify and access data.
5. The malware collects data on a staging server, then exfiltrates the data off the network and under the full control of the threat actor. At this point, the network is considered breached.
6. Evidence of the APT attack is removed, but the network remains compromised. The cyber criminal can return at any time to continue the data breach.

Traditional cyber security measures such as defense-in-depth, firewalls and antivirus cannot protect against an APT attack, and leave organizations vulnerable to data breaches. The Adaptive Defense approach from FireEye is the best strategy to intercept possible APTs at any point in your network, analyze them with the latest available information on threat actors and methodology, and support your security professionals with extensive knowledge of industry and threat groups they may encounter

2.2: Life Cycle of APT:

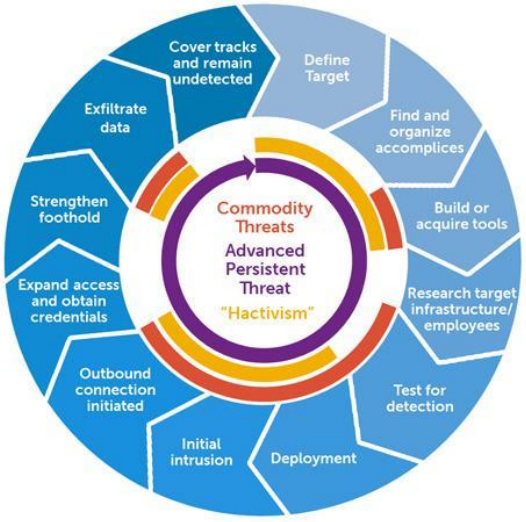

Figure 2.2 Life Cycle of Advanced Persistent Threat

Actors behind advanced persistent threats create a growing and changing risk to organizations' financial assets, intellectual property, and reputation by following a continuous process or kill chain:

1. Target specific organizations for a singular objective
2. Attempt to gain a foothold in the environment(common tactics include spear phishing emails)
3. Use the compromised systems as access into the target network
4. Deploy additional tools that help fulfill the attack objective
5. Cover tracks to maintain access for future initiatives

The global landscape of APTs from all sources is sometimes referred to in the singular as "the" APT, as are references to the actor behind a specific incident or series of incidents.

2.3: Notable Example of Advanced Persistent Attack:

Deep Panda (2015)

A recently discovered APT attack affecting the US Government's Office of Personnel Management has been attributed to what's being described as on-going cyberwar between China and the U.S. The latest rounds of attacks have been referred to using a variety of different codenames, with Deep Panda being among the most common attribution. The attack on OPM in May 2015 was understood to have compromised over 4million USpersonnel records with fear that information pertaining to secret service staff may also have been stolen.

3. SYMPTOMS OF APTS:

Hackers who employ APTs (advanced persistent threats) are a different breed. A real and constant threat to the world's companies and networks, APT hackers tend to be well organized, working together as part of a professional team. Their goal, typically, is to steal valuable intellectual property, such as confidential project

descriptions, contracts, and patent information.

Generally, APT hackers employ familiar methods, using phishing emails or other tricks to fool users into downloading malware. But the ultimate objective tends to be very ambitious. If you discover a break-in where the only apparent intent was to steal money from your company, then it probably wasn't an APT hack. Those who deal in APTs are trying to be your company.

Because APT hackers use different techniques from ordinary hackers, they leave behind different signs. Over the past decade, I've discovered the following five signs are most likely to indicate that your company has been compromised by an APT. Each could be part of legitimate actions within the business, but their unexpected nature or the volume of activity may bear witness to an APT exploit.

3.1 Symptom-1: APTs rapidly escalate from compromising a single computer to taking over the whole environment. They do this by reading an authentication database, stealing credentials, and reusing them. They learn which user (or service) accounts have elevated privileges and permissions, then go through those accounts to compromise assets within the environment. Often, a high volume of elevated log-ons occur at night because the attackers live on the other side of the world. If you suddenly notice a high volume of elevated log-ons while the legitimate work crew is at home, start to worry.

3.2 Symptom-2: Finding widespread backdoor Trojans

APT hackers often install backdoor Trojan programs on compromised computers within the exploited environment. They do this to ensure they can always get back in, even if the captured log-on credentials get changed when the victim gets a clue. Another related trait: Once discovered, APT hackers don't go away like normal attackers. Why should they? They own computers in your environment, and you aren't likely to see them in a court of law.

These days, Trojans deployed through social engineering provide the avenue through which most companies are exploited. They are fairly common in every environment and they proliferate in APT attacks.

3.3 Symptom- 3: Unexpected information flows

If I could pick the single best way to detect APT activities, this would be it: Look for large, unexpected flows of data from internal origination points to other internal computers or to external computers. It could be server to server, server to client, or network to network.

3.4 Symptom-4: Discovering unexpected data bundles

APTs often aggregate stolen data to internal collection data appearing in places where that data should not be, especially if compressed in archive points before moving it outside. Look for large (we're talking gigabytes, not megabytes) chunks of formats not normally used by your company.

3.5 Symptom 5: Detecting pass-the-hash hacking tools

Although APTs don't always use pass-the-hash attack tools, they frequently pop up. Strangely, after using them, hackers often forget to delete them. If you find pass-the-hash attack tools hanging around, it's OK to panic a little or at least consider them as evidence that should be investigated further.

4. Advanced Persistent Threat (APT) Protection; best Approaches

Within the anatomy of an attack – from insertion and incubation to execution and exfiltration — an advanced persistent threat tends to take much longer to infect target systems than other threats. It's estimated that it could have taken Stuxnet around eight months to infiltrate Iran's uranium enrichment facility.

4.1 Identifying weaknesses

Organizations need to gain insight into which information assets are most likely to be targeted, as well as which need most protection if an environment is targeted by an advanced persistent threat. Within an environment, a particular application and its associated data might be operation critical. Asset awareness, thus, is the first step to defending against an advanced persistent threat.

To illustrate this point, take a company's quarterly financial data. This data is critical in the period between the end of a quarter and before the quarterly results announcement. Beyond this time frame, this data diminishes in value.

Advanced persistent threats are usually targeted against organizations having strategic value. Given the resources involved in launching a persistent attack, apart from the requisite expertise, APTs are usually backed by state agents and may be used for espionage or cyber-warfare.

The impact of an advanced persistent threat on entities such as governments, or strategic installations such as power grids, research centers, oil platforms or arsenals, could be disastrous in terms of disruption of services and theft of classified information. An instance would be that of a private operator in power generation getting targeted by an advanced persistent threat. This could potentially bring entire grids and everything connected to them to a standstill.

4.2 Handling Advanced Persistent Threats

Any threat must be identified before it can be tackled. Organizations need to be aware not only of threats at large, but also threats specifically targeted at them.

4.2.1. Broad polices and governance mechanisms:

The first line of defense against an advanced persistent threat is the information security policy. Policies define access controls and the security posture of an enterprise. A robust information security of Governance framework is another important aspect. Factors such as planning for remediation and eradication are an intrinsic part of defending against loss from an advanced persistent threat.

4.2.2Correlation and threat management:

Correlation mechanisms should be available in real time for threats to be identified as soon as a compromise is initiated. This is essential to leveraging any existing global information to protect against the advanced persistent threat entering your environment.

Identifying the sources of your advanced persistent threat is an important factor. For example, if evidence suggests that assets in country X keep getting targeted by attacks originating from country Y, it makes sense to be extra cautious and screen all connections to and from that geographic location.

5. Conclusion:

Most major security vendors have global intelligence networks providing reputation databases and live feeds for emerging threats. However, unless there is a proper governance and correlation mechanism in place, a security feed would merely generate false positives. These two aspects in conjunction provide an effective means to leverage threat intelligence and provide actionable data against an advanced persistent threat, while reducing the incidence of false positives.

REFERENCES

[1].https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

[2].https://en.wikipedia.org/wiki/Advanced_persistent_threat#History_and_targets

[3].https://www.csoonline.com/article/2615666/security/security-5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html

[4].http://www.computerweekly.com/tip/Advanced-persistent-threat-APT-defense-best-practices

[5]. Dr. Sam Musa. "Advanced Persistent Threat - APT". "Anatomy of an Advanced Persistent Threat (APT)". Dell SecureWorks. Retrieved 2012-05-21.

[6]."Are you being targeted by an Advanced Persistent Threat?". Command Five Pty Ltd. Retrieved 2011-03-31.

[7]."Search for malicious files". Malicious File Hunter. Retrieved 2014-10-10.

[8].Eric M. Hutchins; Michael J. Clopperty; Rohan M.Amin.McGraw-Hill Osborne Media. ISBN 978-0071772495.

[9]. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (PDF). Lockheed Martin Corporation Abstract. Retrieved March 13, 2013.

[10]."Assessing Outbound Traffic to Uncover Advanced Persistent Threat" (PDF). SANS Technology Institute. Retrieved 2013-04-14.

[11]."Introducing Forrester's Cyber Threat Intelligence Research". Forrester Research. Retrieved 2014-04-14.

[12]."Advanced Persistent Threats: Learn the ABCs of APTs - Part A". SecureWorks. SecureWorks. Retrieved 23 January 2017.

[13].Olavsrud, Thor. "Targeted Attacks Increased, Became More Diverse in 2011". PCWorld.

[14].Sean Bodmer; Dr. Max Kilger; Gregory Carpenter; Jade Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation.

[15]."Outmaneuvering Advanced and Evasive Malware Threats". Secureworks. Secureworks Insights. Retrieved 24 February 2016.

[16]. "APT1: Exposing One of China's Cyber Espionage Units". Mandiant. 2013.