plixer International

“Fighting Advanced Persistent Threats”

Defense in Depth Through Network Flow Analytics

Scrutinizer™

NetFlow & sFlow Analyzer

Whitepaper

Introduction: What is an Advanced Persistent Threat?

Since 2006[1] Advanced Persistent Threats (APTs) as coined by the United States Air Force, have been lurking on the Internet and targeting specific companies all under the radar of most traditional behavior anomaly detection systems. Victims of APTs have included such companies as Google, Adobe, Marathon Oil, ExxonMobil, ConocoPhillips, Sony, Lockheed Martin and RSA.

What does APT really mean? Breaking down the acronym we find:

- **Advanced**- the adversary is conversant with computer intrusion tools and techniques and is capable of developing custom exploits.
- **Persistent**- the adversary intends to accomplish a mission. They receive directives and work towards specific goals.
- **Threat**- the adversary is organized, funded and motivated.

An APT is often not the typical brute force scan of the network or a specific host. It is a low and slow form of computer espionage generally used to target a specific government or business agencies. Frequently, the perpetrators are well paid and in some cases, wear familiar uniforms! Unfortunately, classic prevent/detect techniques such as next-gen firewalls, anti-virus and intrusion detection systems that rely on traditional signature based detection do not effectively counter the APT infiltration.

"I divide the entire set of Fortune Global 2,000 firms into two categories: those that know they've been compromised and those that don't yet know."
-Dmitri Alperovitch, former VP of Threat Research at McAfee.

Initially, the goal of the APT is to gain a foothold within its intended environment. In some cases, the initial access is done with a phishing campaign. Once that is achieved, the APT sets up camp and awaits its orders using secure connections such as TCP port 443. The use of encrypted communication mechanisms is a serious issue for signature-based threat detection technologies.

The threat of APTs is on the rise and must be adequately addressed at all levels within an organization. A strategy of "layered defensive tactics can prevent security breaches"[2] from many forms of APTs.

1 http://www.informationweek.com/news/security/cybercrime/232600562
2 http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf

The Advanced Persistent Threat Attack Process

Security experts recognize that compared with traditional attackers, APTs are highly motivated to get inside the targeted organization. The individuals have sophisticated hacking skills, are well compensated, and are very patient.

Often times the experts behind APTs only need a single successful attack vector, or entry point into the organization. In an effort to find holes in the victim's defenses, they pursue the objective repeatedly for extended period of time. As the defending company resists the efforts of the APT, the criminals adapt their efforts and reinvent their approach until they finally succeed in establishing a beachhead.

Once a foothold within the organization has been established, the attacker will focus on exfiltration of information, undermining or impeding critical aspects of a mission, program or organization; or positioning itself to carry out these objectives sometime in the future.[3] Once they are inside an organization, they don't need to hack through again; instead they set up camp with a long-term presence that allows them to move about the company freely, laterally and undetected.

Initiating an APT on the part of the attacker often involves seven stages as outlined by Mandiant:[4]

1. Reconnaissance: Attackers research and identify individuals they will target in the attacks, using public search or other methods. Sites such as Facebook and Linkedin are often resources. They use these sites to obtain their email addresses or instant messaging handles.

2. Intrusion into the network: It all typically starts with spear-phishing emails, where the attacker targets specific users within the target company with spoofed emails that include malicious links or malicious PDF or Microsoft Office document attachments. These files infect the employee's machine and give the attacker a foot in the door. Among the most common file names for these malware are: svchost.exe, iexplore.exe, iprinp.dll, and winzf32.dll -- all of which don't raise any red flags and could easily be overlooked. Most of these attackers evade anomaly detection by using outbound HTTP connections, as well as process injection.

3. Establishing a backdoor: The attackers try to get domain administrative credentials and extract them from the network. Since these credentials are typically encrypted, they then decrypt them using pass-the-hash or other tools and gain elevated user privileges. From here, they move "laterally" within the victim's network, installing backdoors here and there. They typically install malware via process injection, registry modification, or scheduled services.

3 http://techauthor.posterous.com/apt-advanced-persistent-attack-defined

4 http://www.darkreading.com/database-security/167901020/security/attacks-breaches/222600139/index.html?pgno=2

4. Obtaining user credentials: Attackers get most of their access using valid user credentials, and access an average of 40 systems on the victim's network using the stolen credentials, according to Mandiant. The most common type: domain-administrator credentials.

5. Installing multiple utilities: Utility programs are installed on the victim's network to conduct system administration, including installing backdoors, grabbing passwords, getting email, and listing running processes. According to Mandiant, utilities are typically found on systems without backdoors.

6. Privilege escalation, lateral movement, and data exfiltration: Now the attackers start grabbing emails, attachments, and files from servers via the attacker's C&C infrastructure. They typically funnel the stolen data to staging servers, where they encrypt and compress it, and then delete the compressed files from the staging server.

7. Maintaining persistence: If the attackers discover they are detected or remediated, they use other methods to ensure they don't lose their presence in the victim's network, including revamping their malware.

How to Detect an Advanced Persistent Attack

Forensic NetFlow and IPFIX analysis tools are ideal security layers with which to detect and investigate APTs. Network flows provide a complete account of all network activity both at the perimeter of the network as well as the network core. Advanced flow analysis solutions trigger alarms by monitoring for suspect behavioral patterns within the network flows. Identifying suspicious traffic patterns involves automated correlation of different types of contextual information then, deciphering the intent and danger associated within the hidden messages. The Flow Analysis system measures traffic flow within the organization in an effort to detect anomalous conditions that indicate data exfiltration or network enumeration. Given the use of pattern recognition and behavior analysis of flows, encryption of the attack traffic has little effect on the detection process.

One of the best ways to detect if internal hosts are communicating with other external APT launch points, is to compare NetFlow data to a host reputation list. By sending NetFlow from the Internet facing routers to a NetFlow collector that can compare all flows to the host reputation database, internal machines talking with known compromised Internet hosts, can be identified.

"We've learned that NetFlow can tell us who is talking to who across our network, but how can we tell if either who is a bad actor? By checking the reputation of the IP addresses at both ends of the conversation."

- Mike Schiffman, Cisco

Companies that have implemented an IP Host Reputation strategy include:

• Barracuda	• McAfee	• SonicWALL
• Cisco Systems	• Palo Alto Networks	• Watchguard
• Juniper	• Plixer International	

Lists of suspicious hosts can be imported from these vendors and merged with network flows using a device Flow Collector such as Plixer's Scrutinizer technology. Internal hosts communicating with known compromised Internet hosts should be monitored closely – as well as the Internet traffic these suspects exhibit. An internal host communicating with compromised Internet hosts identified via host reputation lists, could be participating in an APT.

Another way to identify if a company is being targeted by an APT is to setup a Honey Pot or "Dark Net"- an Internet available host setup for the sole purpose of attracting Internet hosts trying to push malware onto the company. Honey Pots are generally setup without patches and usually contain hoax data designed to lure an intruder's interest. Applications such as honeyd can be used to simulate network hosts providing realistic banners, ping responses, and even false login prompts. Internet hosts that can access the Honey Pot are flagged as highly suspicious. Any subsequent activity from the suspect hosts, especially with legitimate Internet facing servers, should be closely supervised for characteristics of an APT.

With Scrutinizer Flow Analytics, a single console can be provided to allow security analysts to identify hosts involved with significant volumes of unique alarms. Once this is obtained, the pertinent username, time of day, and applications allow those involved with the investigation to engage in a deeper reconnaissance effort whereby the analyst can counter the attack with the steps necessary in a timely, efficient, and cost-effective manner. However, APTs require methodical and patient investigations before attempting mitigation.

Before the APT can be removed, it must be monitored to determine:

- Areas where the malware has spread
- What other hosts communicate with the same Internet command and control hosts

Remember, APTs favor lateral movement across the organization as they search for back doors. Once in, they never leave. Despite the desire to rid the company of the intrusion, careful, methodical reconnaissance must be deployed.

Since the average APT infects up to 40 hosts, a careful, methodical discovery process will eventually provide the actionable intelligence needed to remove all traces of the APT. And, since the scripts

involved with the APT are intelligent, they will quickly remove themselves and delete all traces of their

presence if they suspect they have been detected. Carefully limiting access to the infected machines, monitoring, and recording all communications of the malware, can help achieve reasonable quarantine.

To follow with legal recourse, recording the data is needed. A single Scrutinizer NetFlow Analyzer can collect over 100K flows per second and scale to millions of flows per second in a distributed environment. With the ability to save raw flows for several years and recover all details in seconds, a full audit trail of the APT and its history can be produced including: information related to connections to the C&C hosts, the act of scanning the internal or external network for new hosts to infect, and the exfiltration of the stolen intellectual property. Network flows are instrumental in rooting out the APT, ensuring all hosts impacted by the compromise are identified and removed.

How to shut down an Advanced Persistent Attack

If a company confirms it is being infiltrated by an APT they should not panic and clean the infection. Time should be spent to investigate the extent to which the APT has moved laterally within the internal network.

- Study the infection and locate all the machines within the organization that are infected. Allowing the attackers to continue on without detection allows the victim to gather necessary intelligence for cleaning all impacted hosts on the network and alerting the authorities.
- Once the machines infected with APT malware are pinpointed, the traffic and the hosts they communicate with on the Internet can now be monitored until all suspected machines are identified. If and when the security team is satisfied with the identification process, machines involved with the APT are taken offline, cleansed and reinstalled.

Another effective way to shut down APT, is to uncover and block the Command and Control (C&C) conduit between the compromised systems and the attackers, which Gunter Ollmann advises, vice president of research for Damballa.[5] "Then they have to go to their backup systems and re-infect the host. The Achilles' heel is their C&C. They require interactive access to the systems to control them and to target and extricate information ... by detecting and denying that, you've muted the attack," Ollmann noted.

Summary: Protection from APTs is Ceaseless

Safeguarding a company's data from APT invasion is an ongoing, daily task. Paranoia is a good defense against the possible insurgence. Many experts combating APTs suggest that organizations always be

5 http://www.darkreading.com/database-security/167901020/security/attacks-breaches/222600139/index.html

on the alert, that is assuming an APT is always present or already underway, and to operate defensively rather than passively. Adding a layer of security with Scrutinizer Flow Analytics is one of the best ways to detect internal malware that has circumvented the traditional firewalls of threat detection measures. Many APTs have no trouble sneaking right past even the best security appliances, however, they have a habit of exhibiting the same suspicious behaviors: large transfers of data to hosts that have poor reputations. Scrutinizer with Flow Analytics constantly compares all flows to a regularly updated host reputation database. Positive matches can trigger alarms.

To deploy an APT detection measure, companies should develop an Incident Response Guide and routinely test the procedure for mitigating this type of advanced intrusion. This will help provide clear guidelines and protocols on:

- What should happen with an APT is detected.
- Which individuals within the company should be mobilized.
- What information will be needed.
- What services could be disrupted by the breach and subsequent cleanup.
- What outside resources/individuals can the company tap into for additional assistance
- A thorough disaster recovery plan.

Security administrators should also be aware of state and federal regulations and laws that require the disclosure of information upon detecting such threats. Depending on the agency, organizations such as the Health Insurance Portability and Accountability Act (HIPPAA) have specific guidelines that must also be followed.

“After working with over 40 customers to develop case studies, I learned that for many companies the Scrutinizer is first and foremost a threat detection and mitigation tool,” said Michael Patterson,CEO, Plixer International. “As the first NetFlow and IPFIX security and analysis company, we have been performing host reputation look ups for most of our customers since 2009.”

Education is a major deterrent to APT invasions. Regular employee trainings must be conducted to share up-to-date knowledge on how social networking sites and email can be used to assist in the spread of APTs and other forms of malware.