University of Louisville

Advanced Persistent Threats

Joseph Eckl

CIS 481

Dr. Andrew Wright

1 July 2018

**Executive Summary**

Advanced persistent threats are a category of security threat that is especially dangerous to information security at a high level. With knowledge of what makes an advanced persistent threat dangerous, how an advanced persistent threat is performed, steps that can be taken against an advanced persistent threat, and lessons learned from previous advanced persistent threats, their potential danger can be reduced.

Advanced persistent threat attacks are performed by skilled actors with driving motives on specific targets. These attacks are designed to steal information and are continuously monitored to maintain hidden from the target. An advanced persistent threat may be carried on several types of targets, including governments, companies, or any other organizations that safeguard valuable data.

An individual advanced persistent threat attack is carried out in three stages. The first stage of the lifecycle is targeting. The actor selects a target and researches its defenses and vulnerabilities. The second phase is entry. The actor uses an entry method to gain access, explore the target’s network, and establish a hidden connection back to the actor’s own servers. In the final exit phase, the actor makes sure their activity is hidden and exfiltrates the data from the target, completing the attack.

There are several ways to guard against advanced persistent threat attacks. The first step is risk assessment. An organization should realize the importance of the data they work with and take appropriate steps. These steps include training employees to recognize methods of entry that may target them, patching systems regularly, and using IDPS and firewalls. Furthermore, organizations can learn from previous attack cases.

1. **An Introduction to Advanced Persistent Threats**

An advanced persistent threat is a type of information security threat unlike most others. These threats target the most secure locations with the desire to gather information over a long period of time and slip out undetected. They are difficult to detect, even more difficult to stop, and are one of the most dangerous threats to secure information and operations of the world’s governments and large corporations.

The most common types of computer security threats are quickly executed and leave behind obvious evidence. Malware, viruses, and worms’ primary purpose is to cause harm to an organization’s systems. The main goal of an advanced persistent threat is usually not to cause damage like other types of threats, but to gather information discreetly and slip away, unnoticed until it’s too late. Therefore, unlike other types of attacks, an advanced persistent threat takes a very long time to run its course, leaves behind little evidence, and is very difficult to detect when done professionally. Where other types of threats come in with the intent to do damage immediately, an advanced persistent threat takes its time to ensure it is not detected, creates a disguising infrastructure, establishes an escape route before starting to steal data while leaving as little evidence as possible.

In addition, the target of an advanced persistent threat is usually a large organization with high levels of security. These types of targets often safeguard the most sensitive and valuable information. The amount of time, manpower, and computer skill needed to accomplish the task of breaching a secure facility and remaining undetected requires teams of professionals entirely dedicated to performing the advanced persistent threat, which are usually backed by governments or secretive organizations. Perpetrators of these sponsored attacks are well protected by their level of skill at remaining hidden and even further by the major powers that support them. Underground organizations use advanced persistent threats to gather personal identification, banking, and other sensitive information from businesses. Governments can use advanced persistent threats to conduct cyber warfare; gathering military and defense information or directly interfering with foreign government operations.

To analogize, other types of attacks can be likened to a burglar breaking into your home. They operate independently or in small groups. The goal of the burglar is to get in, break or steal something, and hopefully get back out. They often leave some type of obvious evidence behind that can potentially be used to track them down and be caught. If you are there and paying attention when the burglary starts, you might be able to stop it. Differently, an advanced persistent threat is similar to a spy infiltrating a government facility. They are most likely an agent of a government or organization. They want to slip in undetected, stay as long as necessary to steal information or quietly interfere, then escape with as little trace as possible. Even if evidence is found after the fact, it is likely too late to do anything, as they might be protected by an international power. More common attacks pose a more widespread problem, but advanced threats carry much more serious consequences.

1. **Formal Definition and Characteristics of an Advanced Persistent Threat**

Advanced persistent threats have several components and characteristics that more formally separate them from other types of information security dangers.

The first is in the term itself. The term advanced persistent threat was first used by the United States Air Force to discuss classified information security threats. “Advanced” implies the ability of the attacker to use sophisticated malware techniques to create and exploit vulnerabilities. “Persistent” means that there is a dedicated command and control team continuously monitoring the progress of the attack with a defined objective in mind. “Threat” means that the subject of the attack was chosen deliberately. These three concepts are the most basic factors that distinguish an advanced persistent threat from other types of malware attacks. Other types of attacks can be executed by novice hackers, execute on a one time only basis, or be spread at random, thus making them neither advanced nor persistent nor designated threats.

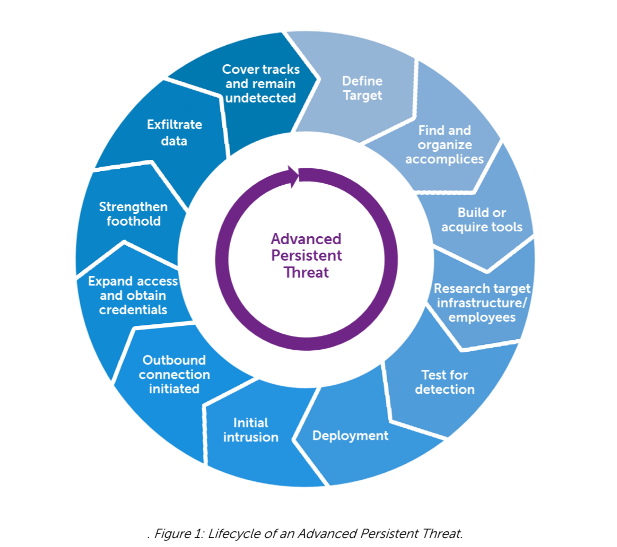
To expand upon this basic definition, there are several characteristics that distinguish advanced persistent threats. The seriousness of these characteristics is what distinguishes an advanced persistent threat.

An actor is the entity behind an attack. The actors in an advanced persistent threat may be nation-states, organized crime, corporate spies, or terrorists. The actors take persistent action against a predetermined target as part of a larger effort supported by an entity with motive. A motive is the reasoning behind performing an attack. An actor may be motivated by many factors, including gaining a financial or competitive advantage, gathering intelligence, damaging the reputation of an organization, or gaining indirect access to another target. The target is the information that is to be retrieved or action to be taken by the attack. Potential targets could be intellectual property, personal information, financial information, network information, classified information, access to credentials, or access to control systems. The more valuable or desirable the information is, the more likely it is that that information will be targeted by an advanced persistent threat.

1. **Use of Advanced Persistent Threats**

The most valuable of information is target by the most persistent actors with various motives. Different types of actors will attack different types of targets. Governments seek classified information from opposing countries. Agencies of governments will directly attack other governments by targeting an attack at the equivalent agency. They may indirectly attack by targeting companies that have connections and contracts with the government. Companies target rival companies in order to steal their intellectual property, customer information, or financial information. Companies attack with one of these objectives in mind, but which one depends on the nature of the target. A software company would be targeted for intellectual property, but a financial institution would be targeted for their customers’ personal financial information. Political groups will target companies or organizations with political connections or smaller branches of governments that have policies that disagree with the group’s political agenda. The purpose behind their attacks is to send a message or threat by compromising the target’s security or stealing private information on the target or its leaders and making it public, sometimes with the threat of blackmail. There are many types of actors and organizations they target.

1. **Advanced Persistent Threat Lifecycle**



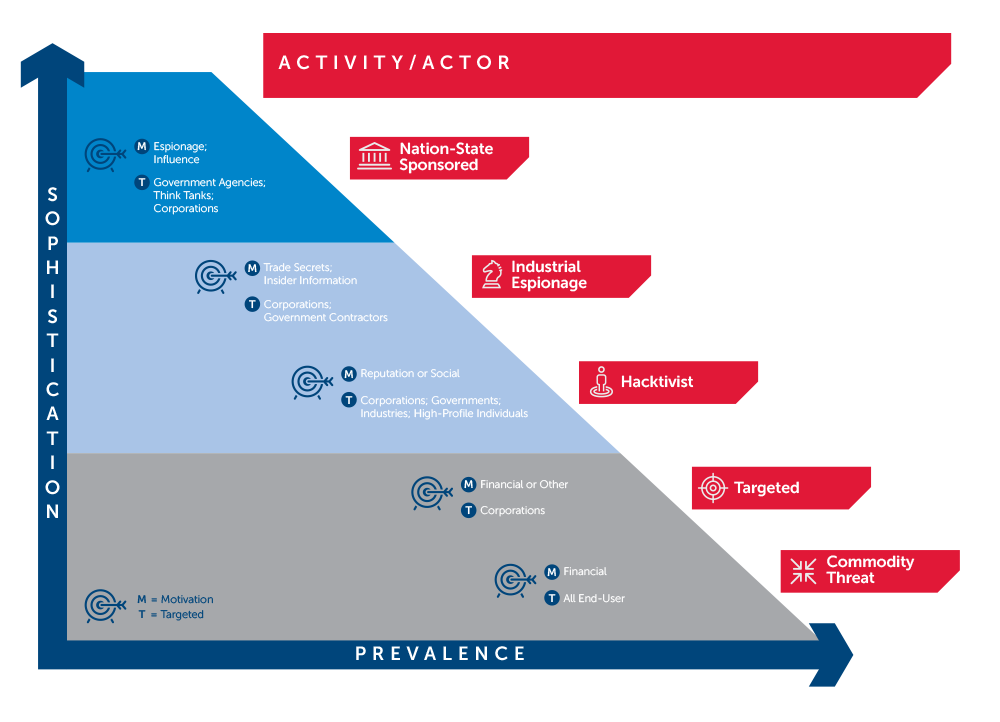
Targeting is just the first step of the first phase of the lifecycle of the advanced persistent threat. The first phase of the cycle is targeting. In this cycle, the target is selected and investigated. The selection of the target depends entirely on the nature of the actor and their motivation as previously noted. The next step is recruitment. The group behind the advanced persistent threat needs to gather together people that have the experience and skill needed to carry out the attack. If the actor is a government, it is likely that there is a government section, department, or branch devoted to activity of this type. If the actor is a large enough company, they may have a task force intended for this kind of work. If the actor is a smaller company or other group, they may need to recruit independent hackers with aligning motives. Next, the group needs to develop tools to use in the attack. This goes in combination with the next step, researching the target and its defenses. The actor will need to learn two important things about the target. The first is the standard setup of a computer in the target’s network. This is for the actor to determine the means of entry. The actor will use this information to determine what method to use to deliver their malicious code with and what vulnerabilities the code will exploit. The second piece of information the actor will need to know is the target’s defensive capabilities. The actor will need to know what kind of monitoring and security the target uses so that the actor can remain hidden during the attack. Once the actor has decided on tools and a means of attack, they may test the target’s defenses before moving on to the next phase.

The next phase in the advanced persistent threat lifecycle is the entry phase. During this phase, the actor will use knowledge obtained from researching the target in the first phase in combination with the tools developed and chosen based on that research. In the deployment step, the actor sets up anything required for the chosen entry method to work most effectively. In the second step, the chosen entry method is carried out. The most common entry method for an advanced persistent threat are spear phishing and baiting. Spear phishing is a targeted form of phishing in which the target, or specific employees of the target, will receive email with attachments or links that contain malicious code. Once clicked on, these attachments and links will activate code written or used by the actor to exploit a vulnerability in the software used by the target. Baiting is a form of social engineering that involves physical media. Instead of the code being contained within email attachments or linked webpages, the code is contained on physical media such as USB drives or CDs that are then left laying purposefully around the target’s location. The goal of baiting is for an employee of the target to find the media and insert it into their computer out of curiosity. Once the media makes it into a computer, the code does its work. The job of this code is to exploit vulnerabilities in the target’s software. Usually these are zero-day vulnerabilities. Zero-day vulnerabilities are new vulnerabilities that are found by the actor and have not been discovered or patched by the target. These vulnerabilities offer a window of opportunity to deliver everything else needed to carry out the attack. In the final step of the entry phase, the actor will initiate an outbound connection. After gaining access, the actor will map out the network and choose the best place to eventually use to take the data from the target. With this taken care of, the actor can get down to the main objective of the attack; stealing the target’s data.

Once inside, the actor must be on high alert. Any of the actor’s traffic or activity noticed by the target could render the attack unsuccessful quickly. Inside the target’s network, the actor can employ method to expand access with remaining hidden and obtain elevated credentials. If the target has a high level of security, the actor could use a rootkit. A rootkit is a type of program that can disguise activity of the actor and normal activity of the target, making it much less likely that the actor will be noticed. The actor can then use the system they already have compromised to work their way across the network, in a process called pivoting. Eventually, the actor will find a way through the network to obtain a higher credential level needed to access the data. However, the actor will do so cautiously. First the elevated credentials can be used to hide the actor’s activity from any lower credential levels. Then the actor may access and exfiltrate the data. The actor can use encryption to secure the confidentiality of the data and send it out to the actor’s servers through the proper port. Encrypted traffic is harder for the target to monitor, and choosing a port associated with encrypted data will make the exfiltration even less suspicious. Finally, the actor will erase as much evidence as possible before concluding the attack.

1. **Risk Assessment and Mitigation**

Any organization that believes that they may potentially be the target of an advanced persistent threat attack should go though risk assessment and enact an appropriate level of security directed specifically at the possibility of an advanced persistent threat.



Following this diagram, it can be summarized that the more important an organization’s data is, the more sophisticated threats it faces. If an organization’s data is less important but still somewhat valuable, the sophistication of a potential advanced persistent threat decreases, but prevalence increases. This means that the organizations safeguarding the most valuable data should expect a major threat and have the best security practices possible. For other organizations, a small robust system can stop the less sophisticated, more common attacks they face.

The first step to developing an effective defense against advanced persistent threats is employee training. The weakest point in any information security system is the people. The majority of advanced persistent threat attacks start with spear phishing or social engineering targeted at the employee of an organization. Training employees to recognize and avoid phishing emails and baited physical media makes the actor’s much more difficult. Making employees smarter and less likely to fall for these intrusion strategies is an extremely important way to deter advanced persistent threats. Technologically, an intrusion detection and prevention system can help to spot and stop an advanced persistent threat. Dual implementation of both a network-based IDPS and a host-based IDPS is most effective. This combination will monitor both network-wide activity and encrypted traffic. The network-based IDPS will monitor traffic across network systems to detect pivoting. Host-based IDPS installed on vital systems will detect any abnormal encrypted traffic that may signal that data is being exfiltrated. Other steps that can be taken to secure against advanced persistent threats are strict patch maintenance, firewalls, and 64-bit system architecture usage. Strict patch maintenance will not protect against zero-day vulnerabilities that the publishing software company does not know about yet, but it will close existing vulnerabilities and patch new vulnerabilities as fast as possible. Firewalls can restrict an individual system’s access to certain domains, making attachments and links associated with spear phishing more difficult to access. Finally, use of 64-bit architecture should be standard, and won’t help much against advanced persistent threats currently being developed, but it will protect against any group trying to get by using older exploits.

1. **Advanced Persistent Threat Cases**

Additionally, much can be learned from previous examples of successful advanced persistent threat attacks. Lessons learned from these impactful attacks form current policy against advanced persistent threats today.

* 1. **Operation Aurora**

Operation Aurora was an advanced persistent threat attack that occurred in 2009. It targeted several large Fortune 100 companies involved in information, security, and defense. It exfiltrated its data from the companies’ software configuration management servers. After investigation, it was found that the actors behind the attack were likely programmers from two universities in China with close ties to a Chinese competitor of Google. The operation began with a spear phishing attack against the companies’ employees. Links contained in the phishing emails brought the user to a website hosting JavaScript designed to trigger a memory vulnerability within Internet Explorer. The actors established a connection through TCP port 443, usually associated with encrypted traffic. This made exfiltration traffic particularly difficult to identify. After initially gaining access, the actors pivoted across systems before reaching the software configuration management system, which had been deemed low priority and left unprotected. The actors then extracted the data, encrypted it, and exfiltrated it to their own servers that used innocent sounding domain names.

* 1. **Stuxnet**

Stuxnet was an advanced persistent threat that occurred in 2009. It targeted the Iranian Nuclear Program and was designed to sabotage the control systems of a nuclear power plant and cause physical damage. To test the Stuxnet attack, the actors would have needed a test environment that closely emulated the targeted nuclear reactor. Therefore, it is widely believed that this attack was conducted by the United States and Israeli governments. Because the programmable logic controllers being targeted are not connected to the Internet, is it believed that the initial intrusion was achieved through baiting with infected USB drives. Stuxnet was encrypted and made use of several zero-day Windows vulnerabilities to make its way into the system. It used a rootkit to conceal itself before beginning to copy itself across the network. The code selected locations to copy itself to based on security software version. Once the industrial control systems and logic controllers had been access, the code executed and caused the reactor to malfunction. It then sent back basic information on the status of the system.

1. **Conclusion**

Advanced persistent threats constitute a great danger to nations and companies that work with and protect our most vital information. Through learning about the purpose, lifecycle, risk, potential solutions, and previous advanced persistent threats, we can gain a better understanding of how to best prepare appropriately against any potential advanced persistent threats in the future.

**Sources**

Beth E. Binde, Russ McRee, Terrence J. O’Connor. *Assessing Outbound Traffic to Uncover*

*Advanced Persistent Threat*. SANS Technology Institute. 2011.

SecureWorks. *Advanced Persistent Threats: Learn the ABCs of APTs*. Dell. 2016

GReAT. *APT Trends Report Q3 2017*. Kaspersky. 2017.

GReAT. *APT Trends Report Q1 2018*. Kaspersky. 2018.

Nikos Virvilis, Dimitris Gritzalis. *The Big Four – What we did wrong in Advanced Persistent*

*Threat detection?*. Department of Informatics, Athens University of Economics and

Business. 2013.

Frankie Li, Anthony Dai. *Evidence of Advanced Persistent Threat: A Case Study of Malware for*

*Political Espionage*. Valkyrie-X Security Research Group. 2011.

Greeg Conklin, John Klein, Mary Landesman, Shiva Persuad, Tom Schoellhammer, Chad

Skipper, Henry Stem. *Cisco 3Q10 Global Threat Report*. Cisco. 2010.