

SOPHOS

Security made simple.



Advanced Persistent Threats: Detection, Protection and Prevention

By **Barbara Hudson**, Senior Product Marketing Manager

The many ways in which industry experts have defined advanced persistent threats (APT) have not exactly led to a better understanding. This paper is designed to give you an overview of the common characteristics of APTs, how they typically work, and what kind of protection is available to help reduce the risk of an attack. Network security is all about ensuring you close the holes an attacker can get through. But you also need measures in place to detect the signs of an attack in progress to stop it from unfolding. In this paper we'll explain how a multi-faceted approach to protect against APTs including layers of defense can reduce the risk of attacks.

The threat landscape is changing, or is it?

Many papers on the topic of APTs begin with ominous references to the changing threat landscape and stories of how highly sophisticated cyber attacks are becoming more prevalent. That can be misleading. The majority of attacks today still use many techniques that have been around for years—social engineering, phishing emails, backdoor exploits and drive-by downloads, to name the biggest ones. Such attacks are neither advanced nor particularly sophisticated when broken down into their individual components and often rely on the weakest link in any organization—the user. However, the way in which hackers use combinations of techniques and the persistent behavior of the attackers is something that does set APTs apart from other attempts to compromise security.

Advanced Persistent Threats

The term APT has become widely used and misused over the past few years. You will also hear the term advanced targeted attack (ATA), which generally refers to the same thing. APT and ATA have been used to describe everything from attacks on high-profile enterprises or nation states, to diverse cybercrime campaigns, hacking techniques, or even individual pieces of malware. For many companies, it's become difficult to see beyond the hype and understand what an APT actually is and is not—and what they can do to prevent or at least detect them.

Some common traits of APTs are:

1. Targeted

Attacks are mostly targeted against a particular organization, group or industry. Before the attack, it may require extensive research on the part of the attackers to collect intelligence about their target. Such groups of attackers are usually very well funded and organized.

2. Goal-oriented

The attackers generally know what they want to achieve or access before they get in. With sufficient intelligence, the attackers will have a number of options to actually penetrate a network and get to the information or systems they want.

3. Persistent

Having successfully found a way into a network, the first infected client may not necessarily be of great interest but is more a means to an end. Once inside, such attackers are likely to slowly move further into the network and target systems which have access to more valuable data, e.g., IT administrators or senior executives who have the credentials to access higher value systems.

4. Patient

Whereas many cyber attacks are designed to wreak havoc by blocking access to systems, and extracting data, APTs are very likely to initially do nothing. The idea is for the attack to go unnoticed, and the best way to do that is to avoid attracting attention in the first place. This non-activity can continue over days, weeks, months or even years.



68%
**OF IT MANAGERS
DON'T KNOW
WHAT AN APT IS**

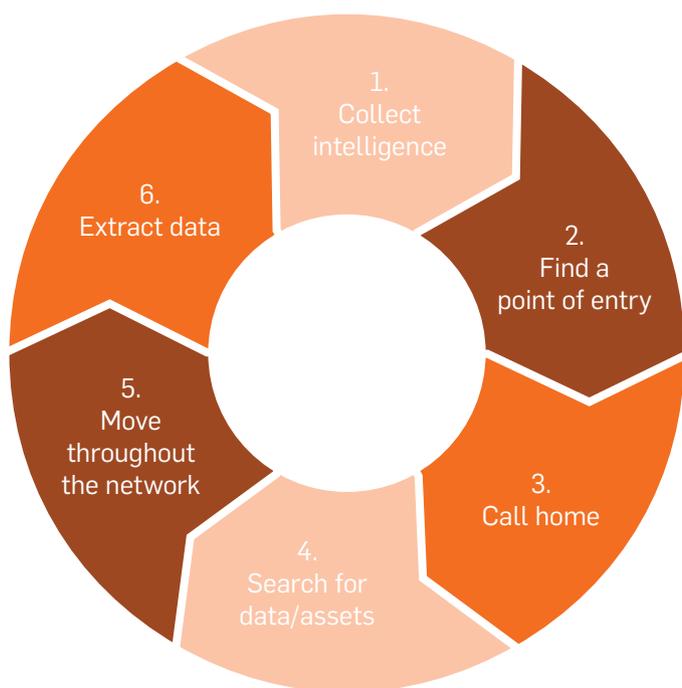
**Source: Ponemon
Institute, The Risk of
an Uncertain Security
Strategy, Nov 2013**

5. Call home

No attack is complete without some kind of communication to the outside world. At some point, they will call home. They may do so once the first system has been infected, or after the data they've targeted is located and collated, or when the systems infected have sufficient access to that data. Communication with the command and control (C&C) host is generally a repeated process to receive further instructions or to begin extracting data in bite-sized chunks.

The typical APT lifecycle

The common lifecycle of an APT is easiest to explain based on examples of techniques which have successfully been used in the past. The example below is not an actual APT, but does draw on real examples. The sequence of some of the phases is interchangeable—for example, lateral movement could start before locating data; and other phases often occur throughout the whole lifecycle, e.g., communication with the C&C host.



1. Collect intelligence

A group of attackers has decided to target a company in the pharmaceuticals industry. Their aim is to get data related to a new drug currently being developed which would give the target company a distinct competitive advantage. They study the Internet, including social media sites, and visit trade fairs to put together a profile of the company and find out about some key employees.

→ **Top sources of intelligence—the Internet and social media:** Although employees may not post confidential business information, posts about business trips and company events can provide the opening that attackers are looking for.

2. Find a point of entry

Based upon the data gathered in step 1, the attackers are aware that the company intends to hold a sales kick-off meeting in Las Vegas in the spring. With this knowledge, they know that a large number of employees from all levels will be in the same place at the same time. They visit the event location at the time of the event and leave a number of USB keys in the meeting room and areas they know the company employees will be present. They hope that either curiosity will get the better of someone and that they will plug in the USB key to find out what is on it, or just plug it in, in the hope that it leads them to the owner. However, tempting as it may seem, a USB key left lying around could contain just about anything.

→ **Real life example:** A similar tactic was used for Stuxnet, an APT that targeted the Iranian nuclear program in 2010. USB keys were left in a parking lot the attacker knew to be used by the employees at the nuclear plant.

3. Call home

Assuming that one of the employees did plug in the USB key, the malware it contains will want to inform the attackers that it has successfully got in. To that aim, it is designed to call home to a command and control (C&C) server and report where it is or receive new instructions. In many cases, this first call home is also designed to update the malware to something more suitable for the next steps of the attack.

In a typical APT lifecycle, the communication with the C&C host is a repeated process throughout the complete lifecycle. This allows malware to adapt as more knowledge is gained.

→ **Don't trust outgoing traffic:** The call home is the point where many security solutions can come undone—if you're not checking your incoming and your outgoing traffic, there could be communication taking place which is not in your interest.

4. Search for data/assets

After infecting the first client, the malware gets a first glimpse of the network from the inside. No amount of research can provide such an insight, unless there is insider knowledge. Depending on the credentials of the user, they may have access to systems of interest to the attackers, or they may just be the first stepping stone. In this case, if the infected client belongs to an administrative employee with no access to systems containing data about the drug, the next step would be to identify which systems are of interest and who has access to them to define the next steps.

→ **Watch out for malicious port scanning:** Port scanning is a typical technique which is used to detect what systems a computer has access to that could contain interesting data. Antivirus, application control and intrusion prevention systems can detect a number of malicious port scanning applications.

5. Move throughout the network

The ideal target for any such attack is the IT department, as they generally have access to a broader range of systems than a typical employee. Once the attackers have identified who the IT employees are and how easy it will be to reach their machines, one of two things will generally happen:

- a) The attackers will infect other clients as stepping stones to get to their target.
- b) The attackers will introduce a further attack to access those systems more quickly, e.g., social engineering, or a web vulnerability specifically targeting the IT staff.

→ **Patch, patch, patch:** Previously known vulnerabilities can provide enough of an opening for attackers to infect a network. Therefore, it is imperative that all systems are kept up to date with security patches at all times.

6. Extract data

Once our attackers have reached the systems of interest and found the data they are looking for, actually extracting the data is the next hurdle. This is the point of the attack where the malware will make frequent communication with the C&C host, as it will likely extract the data in small, encrypted pieces to avoid detection.

→ **Watch out for unusual behavior:** Apart from identifying outgoing traffic, you need security systems in place that show unusual patterns of behavior. Having full real-time reporting capabilities—including historical data—readily accessible can help to identify peaks in traffic to particular hosts or particular data types, such as encrypted files.

Two big myths about APTs

1. APTs only target large enterprises and nation states

Whatever size organization you work in, as an IT manager or chief security officer, you're tasked with protecting valuable data from unauthorized access. Your business and probably your job depend on it.

- If your data is valuable to you, then it could be of value to another company, e.g., competitors.
- If you deal with personally identifiable data of any kind you are required by law in most countries to protect it from unauthorized access.
- Large enterprises and government organizations often use a diverse supply chain made up of smaller companies. If you're one of those suppliers, you could be liable if the data you handle is breached, even if it is not your own.
- Previous APTs have shown that an attack can spread to other organizations that were not the original target.



ONLY 36%
OF SMALL FIRMS
APPLY SECURITY
PATCHES

Source: Naked Security

2. Traditional defenses are no good

Since the fight against APTs has been recognized as an attractive business sector, you will hear many vendors saying that only their solution can protect you, and that traditional security solutions such as antivirus systems are obsolete.

- No single solution can protect you from an APT.
- The best practice is always to have many layers of protection to improve your defenses against a number of different threats.
- Web exploits, phishing emails and remote access Trojans are all common tools used in APTs. Traditional security systems are an essential part of your toolbox to detect the initial stages of an attack and prevent it from moving to the next stage.

Technologies you need for advanced threat protection

There is no silver bullet to defend against an APT attack, no matter what vendors of specialist systems would like to have us think. Intelligent security practices including an end-to-end strategy are still the most effective protection against advanced and common cyber attacks.



The layers of protection you need include:

Firewall

The first layer of network defense is traditionally a packet filter-based firewall and is a convenient way to close the most common holes (or ports).

Intrusion prevention systems (IPS)

Network-based IPSes take a deeper look at network traffic and add an additional layer of protection at the perimeter. Host intrusion prevention systems, or HIPS, are typically part of an antivirus solution. Through constant monitoring, IPSes can detect a wide range of vulnerabilities. It is always worth checking the number of signatures a vendor uses, and how flexible the settings are to prevent checking signatures for operating systems you don't use or those which are obsolete and could slow down your performance.



HOW COMMAND & CONTROL WORKS
[Watch the video](#)

Botnet/command and control detection

As already mentioned above, APTs keep up communication with their host to receive new instructions and updates. By scanning for malicious hosts, outgoing traffic can be blocked and therefore, the communication with the C&C host prevented. Vendors who offer C&C detection will need either their own or an OEM partner to provide a professional lab infrastructure to ensure that data remains up to date. Solutions generally combine the use of traffic analysis mechanisms based upon DNS look-ups, IP tables and an application control engine.

What about sandboxing?

Sandboxing is a much-discussed topic in protecting against APTs. A sandbox is either a physical or virtual secure environment used to run and test unverified code or programs. The sandbox is isolated from any production environment where it could do harm and therefore allows testing and analysis, even for malicious code. There are different types of sandboxing with very different requirements when it comes to administration and performance.

- **Selective sandboxing**

Selective sandboxing is used to identify unknown files when they are selected for analysis. If the file is found to be malicious, a new definition is created and distributed to prevent future infections. Such analysis generally relies on an existing lab infrastructure, similar to SophosLabs. Within the Sophos UTM system, clients can opt out of sending files to the labs. However, sharing anonymized data to improve threat protection can benefit the security community as a whole. Selective sandboxing as part of an existing next-generation firewall solution can greatly improve the level of protection if its implementation is simple and it is fully integrated with other security solutions. Such sandboxing techniques are offered by many leading vendors in the network security space, who generally use a cloud-based infrastructure designed to have a minimal effect on the system performance.

- **Full sandboxing**

Some systems focus on forensics and analyze all data in a sandbox. The way in which these systems work is very diverse and it would not be accurate or fair to assess them all together. In general, they consist of dedicated appliances hosted on-premise and which do not include other security solutions. When selecting a system that uses full sandboxing there are some general things to consider:

- How much training is required to get the system up and running?
- Is it scalable for your size of business and your requirements?
- Do you have the necessary resources and expertise to effectively implement such a system?
- What other security can the solution offer?
- What effect does the solution have on your overall network performance?

In most cases, a sandboxing solution is not designed to replace a next-generation firewall, so you will still need to implement another network security appliance to provide complete protection.



**LEARN MORE
ABOUT NETWORK
THREATS**

**and watch our short
3 min hacking videos**

Web protection

It's essential to keep up to date with regular patching, but also to make sure that web policies are effective even when employees are not on the corporate network. The number of mobile workers today has led to a new challenge for IT departments, but there are simple methods to ensure that users are protected no matter how they access the network.

Web capabilities vary greatly between solutions. Web filtering and application control can protect users against malicious URLs and exploit code. For protection against the latest threats, advanced web malware protection with powerful emulation capabilities is available.

 Recommended whitepaper: [The 5 Stages of a Web Malware Attack](#)

Email protection

Email is still a favorite vehicle of many attackers to spread their malware. People will always be curious and tempted to click on links or open attachments they shouldn't. Today, phishing emails can contain information which makes them very hard to identify—shoddily created logos and spelling mistakes are definitely a thing of the past.

Even security companies have become victims of such attacks. For example, a security breach a few years ago at RSA started with phishing emails containing malicious attachments. Effective email protection should not only include spam and malware detection but also solutions for email encryption and data loss prevention (DLP). Email encryption has often been hindered by the requirement for a public key infrastructure (PKI) at both the sender and recipient sites. However, there are solutions which enable simple, seamless secure communication without the need for key management solutions and which add policy-based DLP to automatically encrypt or block emails containing sensitive data.

 Recommended whitepaper: [Who's Snooping on Your Email?](#)

Web application firewall

Websites are one of the most common sources of malware and keeping their own website safe is something many companies neglect. Systems running within a de-militarized zone, or DMZ, require effective protection to prevent attacks on your website that could not only infect your own clients but also those of visitors to your website. Also, with many organizations using web-based applications such as SharePoint, Outlook Web Access and Salesforce, users are now accessing systems from outside the perimeters of the corporate network.

SQL injection attacks have been frequently implicated in prominent data breaches over the past years. Adding an additional layer of protection between web servers and the Internet such as reverse-proxy authentication can help to provide additional protection for business critical systems. Also, the use of two-factor authentication with a one-time password can prevent form-based or browser-based logins to web servers from becoming a weak spot in your security.

 Recommended whitepaper: [Closing the Back Door on Network Application Vulnerabilities](#)



PHISHING – TARGETING THE WEAK LINK

[Watch the video](#)

Antivirus

Host and client antivirus systems are still essential components of any security strategy and when kept up to date can effectively prevent a wide range of attacks from developing further. Here it is very important to differentiate between the different types of solutions.

Purely signature-based solutions can only detect known malware, therefore it is essential to have a solution in place which also looks at traffic behavior, accesses real-time data to detect newer threats, and offers the possibility to analyze potentially malicious content.

It is also worth noting that in many UTM or next-generation firewall solutions you will find that vendors use flow or stream-based scanning for their antivirus. Although such solutions have a more minimal effect on performance, they only look at the first few bytes of any package and so cannot detect certain types of malware. Also they can't look into encrypted files and only scan a very limited number of archive file types. So, faster performance comes with a security tradeoff, versus proxy-based antivirus solutions that look at the whole package and can scan encrypted or compressed files.

Wireless and remote connectivity

Whatever other technologies are implemented, security can be compromised by using an insecure wireless network or an insecure connection to corporate data. With today's mobile workers accessing data from different locations and different devices, it's hard enough to keep data secure.

A first step is to ensure that your own wireless network is using secure encryption and that it is set up to enable visitors and guests to have Internet access without compromising your security. Employees working from home or in small satellite offices should not be the weak link in your security. A secure site-to-site VPN solution can ensure that you don't make any security compromises once people leave the central office.



Recommended whitepaper: [5 Tips for Securing Your Wireless Network](#)

Sophos Complete Security

Sophos offers a range of security solutions to protect your network, servers and end user clients. With individual point solutions, cloud-based protection, network security appliances and virtualized options, we can help you to select the protection best suited to your requirements, available resources and budget. Many of our solutions offer integration options to work better together and provide a more unified approach to IT security.

Sophos UTM

At Sophos, we apply a very pragmatic approach to advanced threat protection by providing multiple layers of protection within one simple-to-manage solution. We recognize that many IT departments do not have the resources to effectively manage numerous point solutions. But that shouldn't mean compromising on security. By bringing together a number of technologies in one system, and by making the deployment as easy as flicking a switch, we make security that gets the job done, no matter what size business you have. In addition, we offer a plug-and-play solution to protect branch offices and remote locations.

The Sophos UTM is a modular solution you can add features to when you need them. It includes options for:

- **Network protection** including advanced threat protection, IPS and application control
- **Web protection** with all the features of a secure web gateway in a single unified appliance
- **Web server protection** with reverse-proxy authentication
- **Email protection** including anti-spam, email encryption and DLP
- **Wireless protection** with extensive hotspot support for guest networks
- **Endpoint protection** using dual antivirus scanning integrated into the UTM

Sophos UTM

Get a free trial at sophos.com/try-utm

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA
© Copyright 2014. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2/14.NP.wpna.simple

SOPHOS