Lifecycle of an Advanced Persistent Threat

Counter Threat Unit research
Table of Contents

Summary ................................................................................................................................. 2

Background: Who, not what ................................................................................................. 3
  Organized ........................................................................................................................... 3
  Efficient ............................................................................................................................. 3
  Tenacious .......................................................................................................................... 3

APT Lifecycle ....................................................................................................................... 5
  Preparation ......................................................................................................................... 6
  Initial intrusion .................................................................................................................. 6

Primary Objective ............................................................................................................... 9
  Expansion .......................................................................................................................... 9
  Persistence ......................................................................................................................... 11
  Search and Exfiltration .................................................................................................... 12
  Cleanup ............................................................................................................................. 14

Conclusion .......................................................................................................................... 15
  About Dell SecureWorks .................................................................................................. 15
Summary

Advanced Persistent Threats (APT) are a serious concern in today’s threat landscape. They represent a threat to an organization’s intellectual property, financial assets and reputation. In some cases, these threats target critical infrastructure and government suppliers, thereby threatening the victim country’s national mission.

The defensive tools, procedures and other controls commonly put in place to handle commodity security threats are often ineffective against targeted APT-style attacks. This is because the actors behind the intrusion are focused on a specific target and are able to customize and adapt their Tactics, Techniques and Procedures (TTP) to predict and circumvent security controls and standard incident response practices. As a result, developing an effective and efficient defense strategy requires good situational awareness and understanding.

This analysis explains common APT lifecycle phases and provides an understanding of why APT defensive strategies require careful thought that goes beyond the implementation of common security hardware and software solutions.
Background: Who, not what

Advanced Persistent Threat (APT) attacks happen when someone or some organization decides you specifically have something they want and they are willing to invest resources and time to get it. You are not a generic target. You have been singled out for a specific reason. Understanding this is fundamental to combating APT. Individual malware can be detected by antivirus solutions and vulnerabilities targeted by mass exploit kits can be patched. The fact that a person or group and all of the cognitive abilities and resources at their disposal are being applied with the singular goal of obtaining your assets changes the game. It means the threat actors can and will adapt to specific situations until the actors achieve their objectives or the cost of the operation outweighs the perceived value of those objectives.

Organized

The organized nature of APT attacks is what makes them advanced and it is this attribute combined with the focus on a specific target that sets them apart from other threat scenarios. Operations start with a plan. The objectives are defined and a series of well-rehearsed and coordinated procedures are put into motion.

“Teamwork makes the dream work.” This statement is true for many things, including APT operations. APT actors appear to organize on several levels. In all but the smallest of targeted intrusions, cells of one or more people specializing in various technologies or techniques collaborate as needed to accomplish their shared objectives.

Efficient

With few exceptions, the tools observed in APT attacks are not particularly advanced. Malware deployed in the initial salvo are often simple downloaders or basic Remote Access Trojans (RATs). These malware are often custom written and contain no novel technologies or techniques. Other tools used in APT attacks are generally derivations of common password dumping and system administration tools.

This is not to imply that the technical capabilities and resources of the actors are limited. On the contrary: the ability to unleash advanced resources as necessary is clearly present with many of the groups behind these operations. The value of the objectives and the situation dictate the required spending and effort. In many cases, very basic technical and social engineering techniques are all that are required to penetrate the target systems. The actors may have 0-day exploits at their disposal, but they will not use them if a basic spear phishing campaign accomplishes their goal. When current effort levels are being repelled by the target or are otherwise failing to accomplish the objectives, the actors’ TTP can and usually do escalate. The principle of using (and revealing) only necessary capabilities is one tactic the actors behind these operations seem to have learned well.

Tenacious

APT actors are tenacious in their pursuit of your resources. Unlike many malware incidents, cleaning infected systems, patching vulnerabilities, closing firewall ports and updating security software do not
make the problem go away. The APT actors approach their operations in a professional manner, much like a business approaches project setbacks. Issues and obstacles rarely result in abandonment of the objective. Instead, they trigger meetings to adjust strategy and to prepare for the next attempt. Many organizations respond to security incidents by cleaning the threat, correcting the vulnerability and getting back to business as usual as quickly as possible. This approach is not effective against a tenacious adversary because the threat is the actor, not the malware — and the actor is still engaged.

Organizations can be plagued by a single APT campaign for months or years, even after they become aware of the efforts against them. The incident response drags on as the actors continue to adapt to defensive measures and look for new weaknesses in the target’s security posture that will allow them to achieve their goals. In most cases, the actors can dedicate as much time as needed to focus on the target, while IT and security staff have competing priorities and experience fatigue as the intrusion efforts drag on.
Adversaries may have multiple campaigns running in parallel, each consisting of one or more operations. These targeted operations can be dissected into a series of phases. Phases such as preparation and gaining the initial entry point are prerequisites. Other parts of the operation may be parallelized and divided amongst available cells for efficiency. Figure 1 diagrams the basic operational phases commonly observed in a single APT intrusion. The next several sections discuss these phases in detail.
Preparation

The “Preparation” phase includes the following aspects of the lifecycle:

- Define Target
- Find and organize accomplices
- Build or acquire tools
- Research target/infrastructure/employees
- Test for detection

APT attack and exploitation operations typically involve a high degree of preparation. Additional assets and data may be needed before plans can be carried out. Highly complex operations may be required before executing the exploitation plan against the primary target(s). For example, the breach of RSA’s systems provided access to materials necessary for the actors to subsequently bypass authentication systems and gain remote access to the networks of what appear to have been their primary targets. In the preparation phase, actors enumerate the components necessary to execute their plan and begin their efforts to collect the components. These components commonly include infrastructure, tools, data, information on the targets’ environment and other required assets. Actors also collect intelligence on security controls and procedures they are likely to encounter to create evasion and response plans.

For example, actors may register new domains or configure domains at dynamic DNS providers, set up malware command and control (C2) servers at hosting sites or on previously compromised systems, allocate web and FTP (File Transfer Protocol) servers to host phishing or exploit sites and data drops, acquire email servers for relaying spam or for data exfiltration, and so on. Even public services like Google code, documents and chat, Twitter, IRC (Internet Relay Chat) and blog sites may be set up ahead of time for use as C2 channels. For attack operations, actors may need to construct or rent botnets. The infrastructure needed to carry out an operation will vary based on the target and the objective, but necessary resources will be identified and prepared ahead of the direct action against the target. Monitoring of preparation activities can sometimes provide insight into upcoming targets and objectives.

As mentioned earlier, APT actors are tenacious and that makes APT a battle of attrition. Attackers can dedicate a month to compromise the email system at the primary target’s business partner and to collect documents and target profile information if it means that spear phishing attempts are more likely to succeed. Some operations last for years and are focused on such high-value objectives that the time spent in the preparation phase represents a small investment in the overall operation.

Initial intrusion

The “Initial Intrusion” phase includes the following aspects of the lifecycle:

- Deployment
- Initial intrusion
- Outbound connection initiated

After the attacker completes preparations, the next step is an attempt to gain a foothold in the target’s environment. An extremely common entry tactic is the use of spear phishing emails containing a web link or attachment.
Email links usually lead to sites where the target’s web browser and related software are subjected to various exploit techniques or where the APT actors attempt to social engineer information from the victim that can be used later. If a successful exploit takes place, it installs an initial malware payload on the victim’s computer.

Figure 2 illustrates an example of a spear phishing email that contains an attachment. Attachments are usually executable malware, a ZIP or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities in the victim’s applications to ultimately execute malware on the victim’s computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system.

These phishing emails can be very convincing and difficult to distinguish from legitimate email messages. Tactics to increase their believability include modifying legitimate documents from or related to the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code and then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations related to the target or public email services. Emails can also be sent through mail relays with modified email headers to make the messages appear to have originated from legitimate sources.

Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this can be accomplished using exploits for known vulnerabilities, 0-days can be developed or purchased for use in intrusions as needed.

Figure 2: APT actor sends spear phishing email to target with malicious content.
Gaining a foothold in the target environment is the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is commonly a simple downloader, basic Remote Access Trojan or a simple shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful and that it is ready to accept commands.

Figure 3: Malware initiates outbound connection from victim to APT actor’s C2 server.
Primary Objective

After the requisite steps of preparation and gaining control of a system in the target environment, the APT actor can use the infected system as a conduit into the target network and as a deployment mechanism for additional tools that will facilitate the fulfillment of their primary objectives. This section explores several potential objectives commonly observed by the Counter Threat Unit (CTU) research team.

Expansion

The “Expansion” phase includes the following aspects of the lifecycle:

- Expand access and obtain credentials
- Strengthen foothold

In some cases, the objective of the exploitation is a single system that can be directly targeted. If the initial intrusion can gain access to the objective, then there may be no need for access expansion. More often however, achieving the actor’s objectives will require access to more than one system or data store. In these cases, one of the first actions performed by APT actors after the initial intrusion is an expansion of access.

The objective of this phase is to gain access to additional systems and authentication material that will allow access to further systems. A common pattern to gain domain level administrative privilege is to:

1. Obtain administrative access to the initial target.
2. Capture cached credentials for a domain administrator account that has logged into the initial target.
3. Utilize the “pass the hash technique” with the captured cached administrative credentials to gain access to other systems.

As shown in Figure 4, once elevated access has been obtained, an initial target in the expansion phase is often the environment’s domain controller (DC) or the Active Directory server serving the DC role. From these systems, APT actors can capture and exfiltrate the account information and password hashes for all user accounts for offline cracking. Passwords of eight characters or less fall in a few hours (sometimes seconds) on modern password cracking systems\(^1\). Longer passwords with predictable patterns or other common weaknesses are also vulnerable. Heterogeneous IT environments often contain security tradeoffs for interoperability purposes that can make password credential capture and password recovery much simpler.

Once the APT actors possess the target’s account credentials, movement through the network can become more difficult to track. After all, when you have the correct username and password you are no longer hacking, you are logging in. When done from the right systems and in the right patterns, it can be very difficult to differentiate between authorized and unauthorized access until the data has been stolen and the forensic analysis occurs. The account credentials, group information, naming standards and other information that is not immediately useful or doesn’t crack quickly may still provide valuable intelligence for future attacks. In many cases, organizations respond by having their users change their passwords. While this action is a good practice, it doesn’t completely mitigate the
data loss. When users use patterns in their passwords and change them in a predictable way, the APT actors may be able to use the data they obtained to gain access even after the account changes have taken place. This is important because if the actors behind the intrusions have not completed their tasks, then it is certain that they will be back in the future to complete their objectives.

Figure 4: Collecting authentication credentials from the target environment.

Not all systems leverage Windows credentials for authentication. Some systems use a separate non-unified authentication system. Examples include database systems and both internal and external web applications. Tools like keyloggers and web form grabbers are useful to capture these credentials. Keyloggers capture and store each keypress scan code for later retrieval by the APT actors. Keyloggers can be used to capture access credentials, passwords to files and many other valuable pieces of data. Commonly deployed Trojans such as Poison Ivy contain keyloggers as a standard feature.

Form grabbers capture data submitted to web forms. Because web application logins are handled via web forms, these credentials are at risk. Web form grabbers work regardless of whether or not the web application is using HTTPS (Secure Hypertext Transfer Protocol). Form grabbers are common in banking Trojans but have also been observed in targeted malware attacks.

When access credentials are not available or are ineffectual, APT actors may employ vulnerability exploitation, social engineering, distribution of infected physical media such as USB sticks or CDs, human bribes, screen capture utilities and other techniques. To the actors behind these intrusions, the TTP are only a means to an end. They will use any means within their power (or their extended support network’s power) to complete their tasks.
APT actors perform expansion efforts to support other phases of the operation. These phases include gaining access to systems that host or can retrieve targeted data during the search and exfiltration phase, systems that make good locations for the installation of persistence mechanisms, and systems with good network locations that can be leveraged to exfiltrate data or serve as proxies in and out of the network.

**Persistence**

The “Persistence” phase spans numerous aspects of the lifecycle.

Overcoming a target’s perimeter defenses and establishing a foothold inside the network can require substantial effort. Between the time APT actors establish a foothold and the time when there is no further use for the assets or existing and future data, APT actors employ various strategies to maintain access.

![Figure 5: Installing additional malware and other persistence mechanisms in target environment.](image)

APT actors know that most organizations run antivirus solutions in their environments. Because of this assumption, they take steps to ensure their tools will not be detected. This usually means producing or customizing malware and rewriting or repackaging commonly-used tools like psexec and password dumpers. These custom tools are then tested against up-to-date antivirus and other security tools to evaluate whether they are detected. Modifications continue until the tools evade all scans. Because the adversary can access most of the same security tools as the targets, this process is effective and makes it less likely the tools will be detected when they are initially deployed.
After an intrusion is detected, the targeted organization can examine impacted systems, recover malware and tools, analyze network traffic and collect other indicators of compromise. Once indicators are collected, it is possible to develop antivirus signatures and subsequently check systems for known bad files, registry entries, memory patterns and other system artifacts. Network activity can be monitored for DNS lookups or traffic to IP addresses known to be involved in the intrusion. These techniques are certainly useful, but they are limited to detecting known indicators and patterns collected from the current or previous incidents.

APT actors are familiar with these response techniques, so they commonly plan a persistence strategy based on diversity. This is accomplished by using a variety of custom malware in the form of additional executables; services and drivers placed on multiple systems throughout the environment, as shown in Figure 5.

Malware agents can be configured to communicate with a variety of C2 hosts to defeat detection via network indicators. APT actors often don’t activate all of their malware at once. Instead, they configure the malware to activate or phone home only after a very long interval of days, weeks, or even months have elapsed. Actors may also include code that monitors the state of other infected systems in the target’s environment. If the primary infected system or systems are determined to be down or no longer infected, the malware will then connect outbound to the command-and-control server, thus creating a new entry point for the actors.

Diversity and delayed activation tactics can make it challenging to locate all infected systems. Leveraging resources such as Netflow for incident response, disk forensics and log analysis can help with the detection problem, but the actors know these responses and in some cases are able to circumvent monitoring or destroy the records of their activity.

Identifying non-traditional locations to install malware, like servers, routers, firewalls, printers, wireless access points and other places not likely to be examined for infection, is yet another way actors maintain persistence.

In some instances, actors may prepare for being completely ejected from an environment by maiming the target’s network and system defenses, crippling the victim’s ability to repel or detect future intrusion attempts. This course of action is a highly premeditated component of preparation.

Search and Exfiltration

The "Search and Exfiltration" phase includes the following aspects of the lifecycle:

- Exfiltrate data

The ultimate target of network exploitation is generally a resource that can be used for future exploit(s) or documents and data that have financial or other perceived worth to the intruder. In many cases, the APT actors have a specific document or type of data in mind before the attack is launched. In other cases they know it is likely that valuable data exists in the target’s network and systems, but they are unsure where the valuable data is stored.

A popular approach to search and exfiltration is to take everything from the network that might be of interest. This includes every document, email and other types of data discoverable on the network. Some frequently examined locations include the infected user’s documents folder, shared drives located on file servers, the user’s local email file and email from the central email server.
Collecting documents based on their file extension is a popular tactic. Commonly targeted extensions include .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX and .PDF. Other extensions may be targeted if the actors are aware of custom applications or unique attributes of interest in the target environment. Taking all common documents is not necessarily an indicator that the actors don’t know what they are looking for.

Taking all available data from a network may be noisy, creating large network flows and other indicators which in turn may alert the target to the actor’s activities. To avoid detection, some actors take a more focused approach: searching documents at the target’s site for keywords and metadata that indicate the document may be of interest to the actors. Several malware samples recovered from targeted intrusions have included keyword search capabilities. Some malware can even be preprogrammed to search for keyword and extension types with no external actor interaction. This capability allows the deployed malware to find and exfiltrate data automatically. This technique is different than the example in Figure 3, as it only requires a drop site and does not employ C2.

In cases where the actors only have access to the user’s account, and therefore their access level, collection may be limited to the infected computer and the victim’s files on several file servers. If the actor is able to elevate privileges (either through pass the hash techniques or by gaining credentials for the administrative level account), the actors are often able to access all files in folders on centrally-managed file servers and for many workstations under the stolen administrative account’s control.

Figure 6: Data is commonly collected and bundled for exfiltration at a central host.
The same is true for email collection. With an individual's user account password, the APT actor can collect the local email stores, such as the PST (personal folder) files used by Microsoft Outlook. When the central email authentication is controlled by the Windows user account, the compromised user account also lets the actor download all email messages, including attachments from the central mail server. If the APT actor gains access to the administrative level account, they may be able to install malware on the central mail servers that can monitor all incoming and outgoing messages. This visibility lets the actors monitor all email within the organization. In many organizations that are deploying unified messaging services, this access also lets the actor read faxes and listen to recorded voicemails that are distributed as audio files attached to email messages.

Other data can also be collected via the installation of network sniffers. Sniffers can collect all or a subset of the network data visible to the infected system.

All of this data is collected and sent to a location where the actors can retrieve it. The data can be sent from each infected host directly to the actor’s drop site. However, it is common to collect the data at a central host, where it is bundled together (as illustrated in Figure 6) and exfiltrated en masse to the actor’s drop site. This is done to avoid detections that might be triggered by many hosts contacting a remote drop site. It also allows the actors to exfiltrate data in chunks, assuring that at least some large set of data can be extracted before security personnel can respond.

To circumvent data loss prevention (DLP) technologies that look for keywords or patterns in documents leaving the network, the stolen data is often placed in an encrypted RAR or other coded archive format.

Data exfiltration can and does occur regardless of proxies, firewall rules or other border control measures. Malware can traverse proxies using system settings and even captured proxy credentials. Firewalls can be automatically tested from inside the network to detect allowed outbound ports. All of these capabilities are present in modern APT malware.

**Cleanup**

The “Cleanup” phase includes the following aspects of the lifecycle:

- Cover tracks and remain undetected

Cleanup efforts during an intrusion are focused on avoiding detection, removing evidence of the intrusion and what was targeted and eliminating evidence of who was behind the event. Sometimes cleanup involves planting or manipulating data in the environment for the purpose of misdirection. The better the APT actors are at covering their tracks, the harder it will be for victims to assess the impact of the intrusion.
Conclusion

APT actors interested in your data are focused on the acquisition and are not tied to any particular TTP. They adapt to failures and continue to hunt for security weaknesses and blind spots in monitoring. When they are able to slip past defenses, they can make rapid lateral movements for persistence and data collection. Once they locate data, they can move it out of the network for offline review. That data is used for future intrusions on you or related targets, to eliminate technical advantages over the actors’ customer or country, to provide advantages in business dealings or for other real-world purposes that can have significant economic and strategic impacts on targeted entities.

Considering security and the mindset of the actors behind the threats when planning network and system architectures can yield better designs that make the task of network instrumentation and system monitoring easier. Good architecture can help with controlling data flows. Segmentation of network resources either by access requirements, services offered or other strategies compatible with organizational needs makes policy development, enforcement and auditing possible. A log retention and monitoring strategy is also important. Planning these considerations ahead of time will make it much harder for APT actors to cover their tracks and will make incident response efforts more effective and efficient.

A well-developed communications plan that helps users understand the threats and how to identify them will help mitigate social engineering attempts. Maintaining the IT environment through vulnerability assessment and efficient patch management is an important step to eliminate opportunities for initial intrusions. Removing local administrative privileges from users’ workstation accounts and limiting access to only what is necessary helps prevent privilege escalation and access expansion efforts.

Modeling the threat through penetration testing and training exercises that emulate APT actor TTP are also a valuable self-assessment and training tools for management and defense staff.

Good situational awareness is critical to forming effective defense strategies. Without a thorough understanding of the threat, defensive strategies and spending will be inefficient at best and ineffective at worst. In the case of APT, security controls must be developed that account for the actors, their ability to adapt and the resolve they have towards obtaining your assets.

About Dell SecureWorks

Should you have any questions about how Dell SecureWorks can help your organization prepare for or respond to advanced, targeted attacks, contact your account manager, email info@secureworks.com or call (877) 905-6661.

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.