Advanced persistent threat (APT)

What is an APT?

An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.

The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast, and include:

- Intellectual property theft (e.g., trade secrets or patents)
- Compromised sensitive information (e.g., employee and user private data)
- The sabotaging of critical organizational infrastructures (e.g., database deletion)
- Total site takeovers

Executing an APT assault requires more resources than a standard web application attack. The perpetrators are usually teams of experienced cybercriminals having substantial financial backing. Some APT attacks are government-funded and used as cyber warfare weapons.

APT attacks differ from traditional web application threats, in that:

- They’re significantly more complex.
- They’re not hit and run attacks—once a network is infiltrated, the perpetrator remains in order to attain as much information as possible.
- They’re manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets.

- They often aim to infiltrate an entire network, as opposed to one specific part.

  More common attacks, such as remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), are frequently used by perpetrators to establish a foothold in a targeted network. Next, Trojans and backdoor shells are often used to expand that foothold and create a persistent presence within the targeted perimeter.

  Advanced persistent threat (APT) progression

  A successful APT attack can be broken down into three stages: 1) network infiltration, 2) the expansion of the attacker's presence and 3) the extraction of amassed data—all without being detected.

  Stage 1 – Infiltration

  Enterprises are typically infiltrated through the compromising of one of three attack surfaces: web assets, network resources or authorized human users.

  This is achieved either through malicious uploads (e.g., RFI, SQL injection) or social engineering attacks (e.g., spear phishing)—threats faced by large organizations on a regular basis.

  Additionally, infiltrators may simultaneously execute a DDoS attack against their target. This serves both as a smoke screen to distract network personnel and as a means of weakening a security perimeter, making it easier to breach.

  Once initial access has been achieved, attackers quickly install a backdoor shell—malware that grants network access and allows for remote, stealth operations. Backdoors can also come in the form of Trojans masked as legitimate pieces of software.

  Stage 2 – Expansion

After the foothold is established, attackers move to broaden their presence within the network.

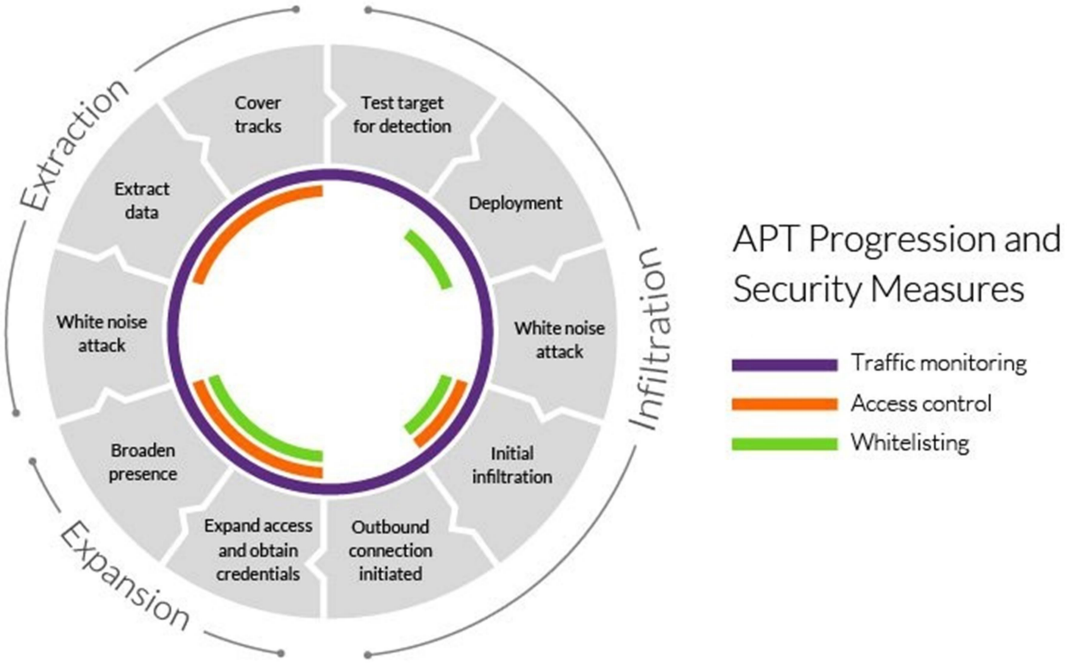
This involves moving up an organization's hierarchy, compromising staff members with access to the most sensitive data. In doing so, they're able to gather critical business information, including product line information, employee data and financial records.

Depending on the ultimate attack goal, the accumulated data can be sold to a competing enterprise, altered to sabotage a company's product line or used to take down an entire organization. If sabotage is the motive, this phase is used to subtly gain control of multiple critical functions and manipulate them in a specific sequence to cause maximum damage. For example, attackers could delete entire databases within a company and then disrupt network communications in order to prolong the recovery process.

Stage 3 – Extraction

While an APT event is underway, stolen information is typically stored in a secure location inside the network being assaulted. Once enough data has been collected, the thieves need to extract it without being detected.

Typically, white noise tactics are used to distract your security team so the information can be moved out. This might take the form of a DDoS attack, again tying up network personnel and/or weakening site defenses to facilitate extraction.



APT security measures

Proper APT detection and protection requires a multi-faceted approach on the part of network administrators, security providers and individual users.

Traffic monitoring

Monitoring ingress and egress traffic are considered the best practice for preventing the installation of backdoors and blocking stolen data extraction. Inspecting traffic inside your network perimeter can also help alert security personnel to any unusual behavior that may point to malicious activity.

A web application firewall (WAF) deployed on the edge of your network filters traffic to your web application servers, thereby protecting one of your most vulnerable attack surfaces. Among other functions, a WAF can help weed out application layer

attacks, such as RFI and SQL injection attacks, commonly used during the APT infiltration phase.

Internal traffic monitoring services, such as a network firewalls, are the other side of this equation. They can provide a granular view showing how users are interacting within your network, while helping to identify internal traffic abnormalities, (e.g., irregular logins or unusually large data transfers). The latter could signal an APT attack is taking place. You can also monitor access to file shares or system honeypots.

Finally, incoming traffic monitoring services could be useful for detecting and removing backdoor shells. These can be identified by intercepting remote requests from the operators.

Application and domain whitelisting

Whitelisting is a way of controlling domains that can be accessed from your network, as well as applications that can be installed by your users. This is another useful method of reducing the success rate of APT attacks by minimizing available attack surfaces.

This security measure is far from foolproof, however, as even the most trusted domains can be compromised. It's also known that malicious files commonly arrive under the guise of legitimate software. In addition, older software product versions are prone to being compromised and exploited.

For effective whitelisting, strict update policies should be enforced to ensure your users are always running the latest version of any application appearing on the list.

Access control

For perpetrators, your employees typically represent the largest and most vulnerable soft-spot in your security perimeter. More often than not, this is why your network users are viewed by intruders as an easy gateway to infiltrate your defenses, while expanding their hold within your security perimeter.

Here, likely targets fall into one of the following three categories:

- Careless users who ignore network security policies and unknowingly grant access to potential threats.
- Malicious insiders who intentionally abuse their user credentials to grant perpetrator access.
- Compromised users whose network access privileges are compromised and used by attackers.

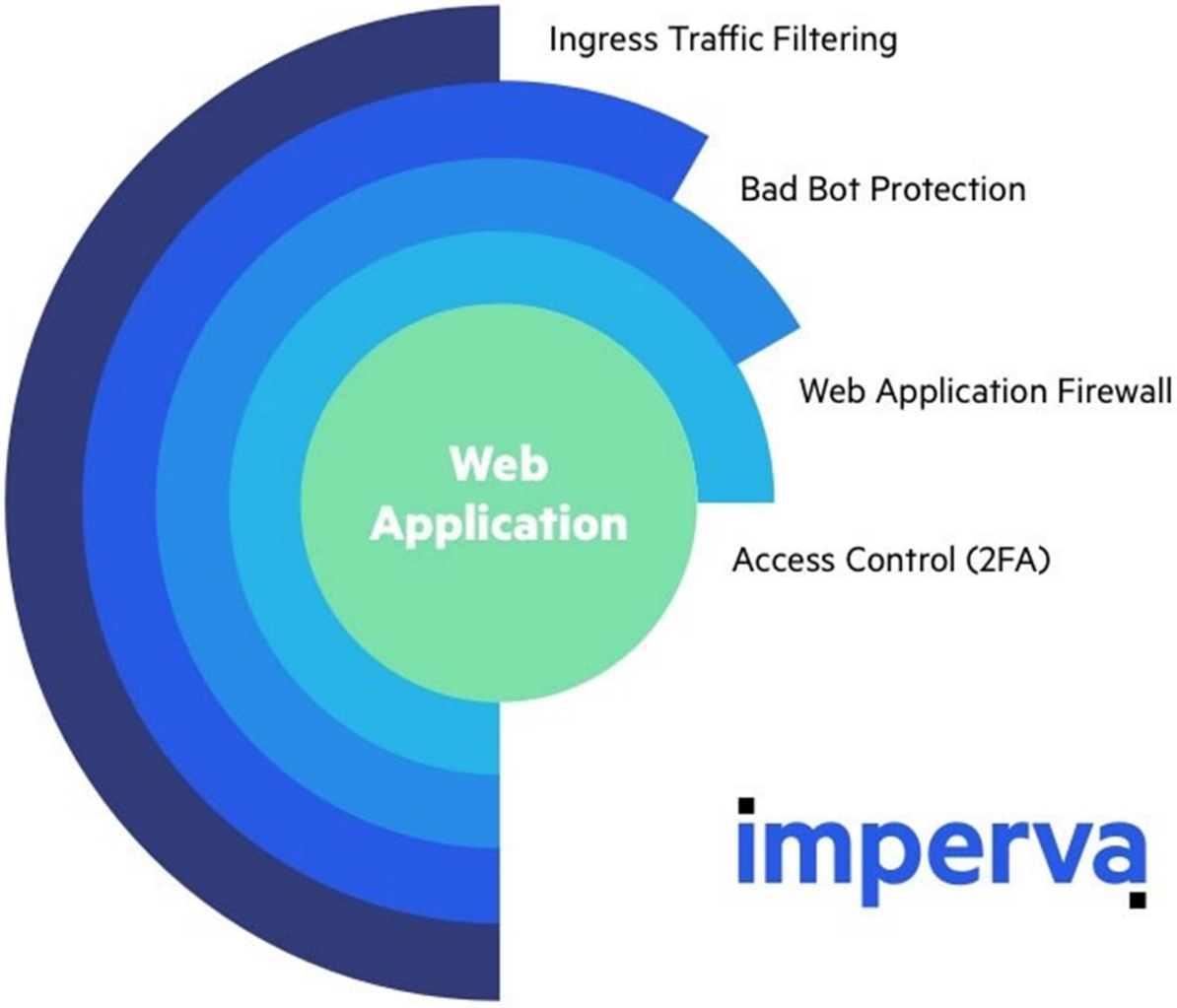
Developing effective controls requires a comprehensive review of everyone in your organization—especially the information to which they have access. For example, classifying data on a need-to-know basis helps block an intruder's ability to hijack login credentials from a low-level staff member, using it to access sensitive materials.

Key network access points should be secured with two-factor authentication (2FA). It requires users to use a second form of verification when accessing sensitive areas (typically a passcode sent to the user's mobile device). This prevents unauthorized actors disguised as legitimate users from moving around your network.

Additional measures

In addition to those above, these are best practice measures to take when securing your network:

- Patching network software and OS vulnerabilities as quickly as possible.
- Encryption of remote connections to prevent intruders from piggy-backing them to infiltrate your site.
- Filtering incoming emails to prevent spam and phishing attacks targeting your network.
- Immediate logging of security events to help improve whitelists and other security policies.



APT security measures

An effective APT protection strategy requires a combination of security measures to protect every part of your perimeter. Imperva is able to play a key role in protecting your web servers and web application with the following solutions:

- Web Application Firewall – Our PCI DSS compliant service is an enterprise-grade security solution that monitors incoming web traffic and blocks all hacking attempts on the edge of your network. The WAF is offered as a cloud-based managed service and is maintained by a team of experts. The solution comes

complete with a custom rules engine that can be used for access control and enforcement of case-specific security policies.

- Backdoor protection – A WAF feature that takes a novel approach to backdoor detection. Instead of looking for suspect files, which are often carefully disguised, While inspecting traffic to a web server, this service intercepts attempts to interact with the shell to reveal its location.
- Two-factor authentication – A flexible access control solution that allows you to deploy a 2FA gateway on any URL address, with the click of a button. The service also allows easy management of access privileges and can be integrated with any web environment.
- DDoS protection – An award winning service that mitigates all application and network layer attacks, including the white noise attacks used to distract security personnel and weaken your network perimeter.

  All Imperva cloud security services include a SIEM integration option. With it you can seamlessly integrate Imperva cloud WAF with your existing security and event management solutions. Doing so will provide centralized access to valuable, granular real-time information about traffic on the edge of your network perimeter.

Reference –

https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

https://en.wikipedia.org/wiki/Advanced_persistent_threat