PANDA CLOUDINTERNETPROTECTION

*Simply... **Evolution***

ADVANCED PERSISTENT THREATS

PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD EMAIL PROTECTION

PANDA CLOUD INTERNET PROTECTION

PANDA SECURITY

INDEX

1. Definition

There is no universally accepted definition for Advanced Persistent Threats (APT), but in general, such attacks have the following characteristics:

- **Timeline:** Attacks take place over a prolonged period of time. They often last for months or even years and are generally preceded by a significant reconnaissance phase prior to actual infiltration of systems.

- **Attackers:** Attackers are highly skilled, well organized and well funded. Organized crime syndicates or foreign governments often support their efforts and access to resources is not a problem.

- **Targets:** End users are targeted, often through web-based attacks. Social engineering generally plays a substantial role and is aided by thorough reconnaissance. This is often combined with a variety of technical exploits, which combine both known and unknown attack vectors.

2. Phases

Phases of the attack will depend on the specific situation but the following general phases are typically encountered:

- **Reconnaissance:** The goal of this phase is securing information about targets that will aid the technical and social engineering aspects of the initial attacks and any further compromises. This can include both personal and professional information. It may be gained through passive monitoring of public or semi-public sources such as social networks. It could also involve active reconnaissance via compromising other targets or through physical intelligence.

- **Initial attack:** The purpose of the initial attack is to gain and secure a foothold within the target organization. This will generally involve installing a backdoor in the compromised machine and additional attack tools such as keyloggers and utilities. This enables data gathering as well as further attacks.

- **Data gathering:** The ultimate purpose of an APT is generally to gather confidential data for the purpose of financial or political gain or to further additional attacks. As data is retrieved it is generally transported offsite to a third party server controlled by the attacker. Data gathering will continue until the overall goal has been achieved or continue indefinitely in order to continually obtain updated information until the compromise is identified and eliminated.

- **Further attacks:** From the site of the initial attack, additional trusted nodes may be compromised. These may be machines on the same local network, satellite offices or trusted partner networks.

3. How Panda Cloud Internet Protection (PCIP) can protect against APTs

There is no silver bullet when it comes to protecting against APTs. Enterprises must adopt a defense-in-depth approach in order to ensure that multiple layers of protection defend against multi-faceted attacks. PCIP provides several preventive and detective controls against threats including APT.

4. Preventive Controls

In a recent APT case, Operation Aurora, a previously unknown exploit was used against a known vulnerable browser. PCIP enables customers to customize policies to prevent vulnerable browser versions or vulnerable browser plug-ins from accessing the web. Once the exploit became known, PCIP was able to immediately push signatures to the cloud to block the use of the exploit (which was subsequently included in Metasploit, a popular exploit framework). In order to detect and block web-based threats, PCIP provides:

- **Anti-virus/Anti-spyware:** In-line, high speed scanning to prevent infection via known malware variant.
- **Full content inspection:** Complete, bi-directional, SSL capable inspection of all web content to identify malicious active content:
  - Browser exploits.
  - Vulnerable ActiveX controls.
  - Malicious JavaScript.
  - Cross-site scripting (XSS).

In APT, espionage or stealing of secrets is a common motivating factor. There are several Government APT cases including Titan Rain that illustrate this fact. PCIP provides Data Leakage Protection (DLP), which will both block and alert on specific customer content from leaving their network.

Additionally, PCIP provides several policy based controls that may limit the web-based threat footprint. For example, a customer may block web communication to certain countries, IP blocks, URLs and content categorization that may be related to a particular adversary or threat.

5. Detective controls

Log Consolidation – PCIP provides customers with a complete view of their entire enterprise web logs regardless of traffic source, to include customer laptops and mobile devices connecting to the web outside of the enterprise network. PCIP provides an analytic interface to their customers to query, trend, and view logs of interest, which is critical for detecting an ongoing incident.

- Suspicious Communication: APT may include malware that beacons back to a command and control server to receive additional instructions, or uploads stolen documents and keystrokes to a particular drop server. These sorts of traffic patterns can and have been identified within PCIP logs to detect previously undetected infections. PCIP researchers are constantly on guard for threats against their customer base.

- Forensics Analysis: PCIP logging and analytic tools provides the customer with a historical view of all web transactions. If an incident is detected, it is possible for a customer to conduct log analysis to detect what actions the infected host made and detect other potential infections or threats.

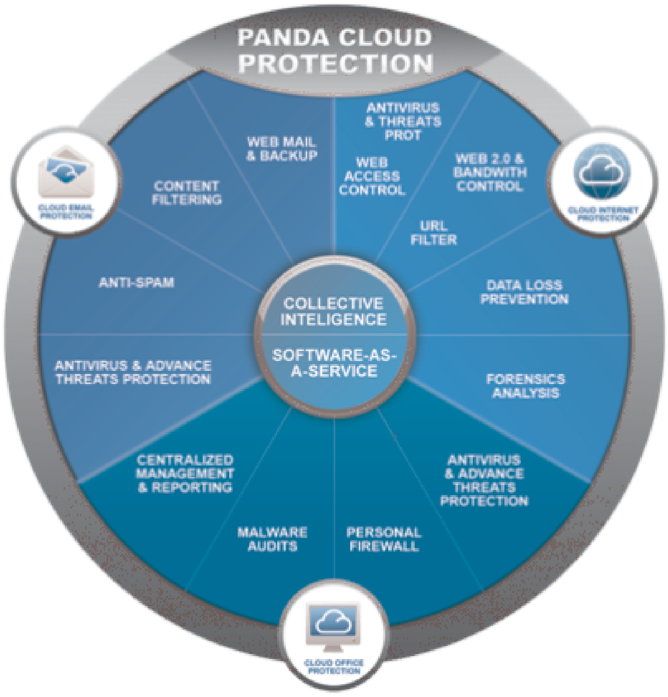
6. Panda Cloud Protection suite

Panda Cloud Internet Protection is part of the Panda Cloud Protection suite which is a complete SaaS security solution that protects all the main threat entry points: endpoint, email and Web traffic, against malware, spam, phishing, cross-site scripting and other advanced Web 2.0 attacks, through a light, secure and simple solution.

As the security suite is based in the cloud it offers maximum protection, while optimizing costs and productivity. Deployment takes just minutes, and day-to-day management is handled easily using Panda’s unique and intuitive Cloud Management Console.

The Panda Cloud Protection suite harnesses the power of Collective Intelligence. Panda's cloud-based Collective Intelligence leverages 21 terabytes of knowledge and experience drawn directly from millions of users to deliver comprehensive, instantaneous, non-intrusive real-world protection against known and unknown malware to all users.

Panda Cloud Protection leverages the power of the cloud to not only provide up-to-the-minute protection against known and unknown threats but also to streamline the delivery of that protection through the anytime, anywhere power of the Cloud Management Console.



PANDA SECURITY

EUROPE
Ronda de Poniente, 17
28760 Tres Cantos. Madrid. SPAIN

Phone: +34 91 806 37 00

USA
230 N. Maryland, Suite 303
P.O. Box 10578. Glendale, CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com