WHAT IS AN "ADVANCED PERSISTENT THREAT"? APTS EXPLAINED

We live in an increasingly digital world and keeping organizations secure in this environment has become more demanding than ever before.

Persistent threats have hidden and continuous computer hacking processes that target a specific entity. These threats are covert, focus on accomplishing a specific task and can happen continuously over time. They are considered persistent because an external system continuously monitors and extracts data from the target.

In the case of an advanced persistent threat (APT), persistent threats can also involve planting remote administration or exploit software in the target's network that allows access to the victim's network and acquires administrator privileges on the victim's computer. Ultimately, hackers can steal data from the victim's network.

Enterprises can address challenges created by advanced persistent threats through effective and timely remediation as they strive to uphold security, liability and accountability for consumers.

What is APT?

An APT is a calculated network attack on any organization. These threats occur when a hacker, or group of hackers, establishes a foothold inside of an enterprise network. APTs go undetected for prolonged periods of time, allowing for sensitive data to be mined.

APTs are unique in that they have certain goals and objectives. Hackers implementing an APT are trying to achieve one or more of the following:

- Theft of intellectual property
- Obtaining sensitive information on people
- Sabotaging the infrastructure of an enterprise
- Orchestrating a site takeover to push a message or agenda

Think of APTs as complex, manual processes that often result in costly damage to an enterprise business. Recall how the public reacted when Home Depot and Target suffered devastating breaches in 2014, exceeding half a billion dollars in expenses to date.

APTs have a lifecycle which will be defined in more depth below but usually occur in the form of fairly common attacks. These include the following:

- SQL injection
- Remote file inclusion (RFI); and
- Cross-site scripting (XSS)

Once a foothold is established using one of the above methods, additional attacks are discharged to make the infrastructure increasingly vulnerable.

Lifecycle and Characteristics of an APT

While no two APTs are the same, in general, advanced persistent threats operate in a fairly predictable way. The lifecycle of an APT happens in four stages, as listed below:

Stage 1: Targeting/Reconnaissance

Initially, an enterprise is targeted by hackers who seek to accomplish a singular agenda. Infiltrating occurs through identified weaknesses in the network, web assets or other resources that hackers can gain access to.

Stage 2: Entry

Hackers gain access using SQL injections, RFIs or implementing phishing scams that enable entry via user access points. These are the kinds of threats enterprises face every day. Additional attacks may be used to create a smoke screen that allows hackers time to gain access undetected.

Once inside a network, hackers will often create a backdoor by uploading malware that allows repeatable entry.

Stage 3: Discovery

Entry into the system is the first milestone for a hacker launching a calculated APT attack. The next involves taking steps to avoid detection.

To do this, hackers will map out the organization's infrastructure and launch additional attacks to the system, geared at gaining access to user accounts higher in the hierarchy. The higher in the hierarchy a malicious cyber attacker can get the better the access to sensitive information.

Stage 4: Capture

An infrastructure left vulnerable from multiple cyber attacks is easier to move around in, undetected. Under these conditions, hackers begin capturing data over an extended period of time.

Stage 5: Data Exfiltration

Once identified, infiltrators can deploy malware extraction tools to steal desired data. Usually this means creating "white noise attacks" to cover cyber attackers who want to mask their intentions. They also mask their entry point, leaving it open for further attacks.

Characteristics

APTs have identifiable characteristics which include the following:

- **Objective driven:** APTs have a specific goal, these are intentional cyber attacks targeting specific vulnerabilities for the purpose of stealing important information.
- **Attackers are resourceful:** In an APT situation, hackers are resourceful; they understand important things about infrastructure, coding and malware.
- **Attacks are timely:** Most attacks occur over a prolonged period.

Experts also include several other predictable characteristics of APTs, which include:

- Risk tolerance
- Skills and methods
- Total access points
- Actions taken
- Number of hackers involved in the attack; and
- Where did they get their knowledge from

As our knowledge of APTs expands, enterprise businesses can take steps to better prepare themselves for any attacks in the future.

Advanced Persistent Threats: What to Look For

If an enterprise business has been hit with an APT, it can be hours, days or longer before they discover the problem. But time is of the essence when it comes to protecting your organization.

Monitoring your infrastructure for these signs can help you stay ahead of hackers who try to establish a foothold in your network:

Increase in Late-Night Logging

Are employees suddenly logging in late at night? This could be a warning sign that your system has been exposed to cyber attackers gaining access to your employee's log in's at night when no one is around to stop them.

If enterprise business leaders see this kind of activity, it should be a red flag to further investigate for vulnerabilities.

Trojans are Prolific in The Network

When hackers access a computer in a network, they often install a trojan which gives them total control over that machine, even after passwords have been updated for security.

If enterprise organizations have a network full of trojans, they should consider the possibility the network is under attack from an APT.

Unexpected Data Bundles

One way cyber attackers move data is by putting large amounts of data into bundles before shipping it out of the system.

Identifying unexpected bundles of gigabytes of data is a good indicator to check your enterprise infrastructure.

Understand How Information is Supposed to Flow

One way to spot an APT is to look for unexpected flows of data. These could be computer to computer, server to server, in or out of network. In order to identify whether an information flow is unauthorized or unexpected, you have to know what's reasonably expected within your current infrastructure.

Be Conscientious of Suspicious Emails

An early tell-tale sign of advanced persistent threat is suspicious emails popping up among an elite group of key players within the organization. Managers, directors, project leaders, C-suite executives -- are likely groups to be targeted.

If an email goes out with questionable links or downloadable files and it only hits certain employee inboxes, it should be a big red flag.

How to Protect Enterprise Assets

To stay on top of today's complexities, threats and opportunities, large enterprises are developing SecOps strategies that focus on three core areas:

1. **People** — Security and Operations professionals share accountability for making business systems more secure and reliable
2. **Processes** — Guide and integrate the activities of key stakeholders in Security and Operations
3. **Technology** — Heighten security by replacing error-prone manual processes with automated tools.

Overall, the approach should also include the following steps:

- Monitoring and detection
- Incident response plan
- Disaster recovery plan
- Security and vigilance training for employees

Another way IT organizations can help enterprises prepare for APTs is by examining the various

ways that hackers infiltrate a system.

Final Thoughts

Advanced persistent threats are complicated, calculated, long-game attacks that can have devastating effects on an enterprise business. According to an impact study by Ponemon Institute, data breaches do more harm to a company than just to its reputation. This is evidenced in the statistics below.

- Breaches resulting in legal action -- 34%
- Decrease in productivity – 50%
- Customer loss of loyalty – 41%
- Bad press – 30%
- Customer attrition – 28%
- Decrease in share price after breach – 25%

Unfortunately, an APT is not something can be easily predicted. But there are some warning signs that IT and other employees can watch for to decide if they need to take action. These include the following key points:

- Paying attention to time and frequency of employee logs
- Uncovering trojan horses in your network
- Finding strange, unexpected bundles of data
- Finding information with a counterintuitive flow; and
- And always being conscientious of suspicious emails to stakeholders

Enterprise organizations don't have to be at the mercy of attackers. They can implement strategies that include monitoring and response planning to create a big picture of what to do if a breach occurs. In turn, this creates a need to balance Security and Operations. This will help digital organizations move faster while maintaining availability and keeping their customers happy.

BMC offers expert IT service management for enterprise businesses that includes threat detection. TrueSight Vulnerability Management offers fast-tracked security fixes and transparency via easy-to-read dashboards that will give your organization peace of mind.

By implementing TrueSight, you can expect to benefit from the following:

- Powerful dashboard capabilities
- Workflows, streamlined for your organization
- Awareness of blind spots within your infrastructure
- Data import and export capabilities

For more information on TrueSight, contact the team at BMC today.