What are APTs?

APTs, or Advanced Persistent Threats, are one of the most feared security concerns in large organizations, institutions or governments. APTs include a group of highly skilled attackers, who have a state backing or otherwise almost unrestricted access to a variety of resources. APTs deliver maximum, long-lasting damage and target specific organizations according to their motives. APTs typically use previously unseen malware and exploits (also known as 0-day exploits), with their own tailored software and frameworks to carry out the attacks.

When you think of cyber warfare, you would most likely be thinking of APTs, their nation-state sponsors, and their extreme attacks against other countries, such as cyber espionage.

REAL-WORLD APTs

APT28

APT28, also known as Fancy Bear, Sofacy or Pawn Storm, are Russian-based nation-state hackers specializing in cyber espionage with political motivations and targets militaries, security organizations and governments, especially in the country of Georgia and Eastern Europe. They are infamous for their attack against the Hillary Clinton campaign and attempts to interfere with the US presidential election.

Cobalt Group

The Cobalt Group, also known as Gold Kingswood, is a financially-motivated group that targets ATMs, payment systems and banks. They have targeted banks in Eastern Europe and Russia, using a series of well-orchestrated spear phishing attacks and exploits. Its leader has been arrested in Spain; however, the group has still been continuing its activities.

Cobalt Group has been utilizing a malware called SpicyOmelette, which allows the attackers to gain a strong foothold on the victim system, conduct system reconnaissance and perform privilege escalation. Cobalt Group is one of the very successful APTs, causing over a billion Euros in financial loss across more than 40 countries.

APT32

APT32 is a threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as with foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims. The group is believed to be Vietnam-based.

WHAT MAKES APTs SPECIAL?

APTs are profoundly different from your ordinary threat actors in a variety of ways. First of all, the amount of funding and resources APTs receive, typically from nation-states, is unmeasurably more significant than individuals

or small "hacking groups". APTs typically focus on financial, political or military targets whereas other threat actors have various goals, from resolving their curiosity to hacktivism.

APTs have sophisticated and advanced tools, attack frameworks, malware, exploits (including zero-days) and methodologies to gain and maintain access to networks, which is comparable to simple scripts, public exploits and commodity malware used by typical hackers.

Lastly, as the name suggests, APTs are most interested in acquiring persistent access and control over target systems for espionage, monitoring, surveillance, and other purposes that require uninterrupted access to ensure their goal is achieved. Contrary to this, conventional hackers tend to perform short and typically unsophisticated attacks and stop once they have completed their goal, not focusing on persistence and access.

CASE STUDY: COBALT GROUP

It can be very interesting to explore how APTs leverage malware and scripts to create an 'exploitation chain' to deliver the final payload. In this case study, we will take a look at how Cobalt Group's attacks escalate from a malicious email to a backdoor payload.

Phase 0: In the very first stage, Cobalt Group sends targeted spear phishing emails with malicious PDFs, Word documents or RTF files attached or linked, which will trigger the 'exploit chain' to start. The email can be personalized or broad enough to be sent to a whole mailing list.

Phase 1: Once the user downloads the malicious attached file, such as a PDF file, they may be asked to click on a URL in order to view the file. However, the link actually leads to a Word document which contains a malicious Visual Basic for Applications code. This phase lights the end of the fuse leading to total compromise of the system.

Phase 2: Cobalt Group uses an exploit kit called Threadkit to create malicious documents which can exploit several critical vulnerabilities in Microsoft Office or Internet Explorer and launch batch files which assist with the exploitation process.

Phase 3: In order to bypass AppLocker and execute scripts or remote code, Cobalt Group utilizes legitimate Microsoft applications that are allowed by AppLocker. One method involves using CMSTP (Microsoft Connection Manager Profile Installer) to run a malicious INF file or execute a script using XML tags in scriptlets. Eventually, a DLL dropper is written to disk to launch PowerShell or CMSTP for the next phase.

Phase 4: The launched PowerShell stage downloads the next one, which is obfuscated in layers, with the final layer being shellcode which is loaded into memory. The shellcode decrypts the remaining code to ultimately download, decrypt and launch an encrypted Cobalt Strike beacon payload. Alternatively, a JScript downloader is used to download and run a JScript backdoor payload.

Phase 5: The Cobalt Strike beacon allows a very wide range of backdoor options and a full system compromise. If the JScript backdoor has been installed, it allows encrypted remote command & control and sends system information including antimalware programs and the IP address. At this point, Cobalt Group has successfully penetrated the target system and may proceed to pivot into other systems, maintain persistence or move on to achieve their final goal.

As you can see, APTs use various methods to bypass anti-malware applications, evade analysis and finally deliver the backdoor payload. Notice how a single email containing a malicious document/URL leads to the complete compromise of the victim's system – all the exploits, scripts and programs work like clockwork, with one event leading to another. It is because of their well-orchestrated Tools, Techniques and Procedures that they are able to cause a devasting amount of damage.

Previous Topic
Mark Complete
Next Topic
Back to Lesson