INTRODUCTION:

Sophisticated cyber-espionage operations aimed at pilfering trade secrets and other sensitive data from corporate networks currently present the biggest threat to businesses. Advanced threat actors ranging from nation-state adversaries to organized cyber-crime gangs are using zero-day exploits, customized malware toolkits and clever social engineering tricks to break into corporate networks, avoid detection, and steal valuable information over an extended period of time.

In this paper, we will cut through some of the hype surrounding Advanced Persistent Threats (APTs), explain the intricacies of these attacks and present recommendations to help you improve your security posture through prevention, detection and mitigation.

WHAT IS AN APT?

The term APT, which stands for Advanced Persistent Threat, is a computer network attack that allows an adversary (usually a highly skilled and well-funded hacking group) to gain access to a network and stay there undetected over an extended period.

These threat actors use a cocktail of spear-phishing attacks, zero-day exploits, SQL-injection techniques, customized malware, drive-by downloads and clever social engineering to hack into computer systems. Once a machine is compromised, APT groups use sophisticated network tools to burrow deep into a corporate network and maintain persistence over a period of time before finding valuable data to hijack and transmit to command-and-control servers around the world.

Examples of successful APT attacks litter the news landscape with victims ranging from Lockheed Martin, SONY, Google, Adobe and RSA to highly classified government and diplomatic institutions around the world. However, it’s important for businesses of every size to understand that the tools and capabilities used by well-funded APT groups are being used by cyber-criminal gangs and the majority of these network breaches are never publicly reported.

The 4 Stages of an APT:

A typical APT includes the following 4 components:

● **Reconnaissance:** Scoping out a specific target and preparing an attack.

● **Intrusion and infection:** Distributing malware via spear-phishing or drive-by downloads

● **Lateral movement:** Tunneling through the infected network with password crackers and privilege escalation exploits.

● **Data exfiltration:** Harvesting ‘interesting’ and valuable data for upload to command-and-control servers controlled by attack group.

Lets look deeper at each of these components.

STAGE ONE: RECONNAISSANCE

The preparation phase is multi-faceted and involves the collection of information on specific targets. It starts with the trawling of social networks like LinkedIn, Facebook and Twitter to collect e-mail addresses, phone numbers, business contacts that will be used later to ensure the ‘infection’ phase of the attack is as efficient as possible.

For example, a planned attack against the Human Resources director of a business will include the gathering of data on all job openings and the types of candidates that are being considered. This information is then used by the attacker to create the initial spear-phishing e-mail rigged with exploits.

In the 2011 targeted attack against security vendor RSA, the attacker focused on two small groups of employees and sent two different phishing e-mails over a two-day period. The email subject line read “2011 Recruitment Plan”. The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached Excel file that was a spreadsheet titled “2011 Recruitment plan.xls”. The spreadsheet contained a zero-day exploit that installed a back-door through an Adobe Flash vulnerability (CVE-2011-0609). It was clear that the attack group had conducted reconnaissance to determine the type of document that had to be used to ensure the file was opened.

The preparation for the RSA breach also provided information on how to bypass authentication systems and gain remote access to the networks of the initial target.

During the reconnaissance phase, APT actors also collect information on the operation systems used, the types of anti-malware software running on the target machine and data on unpatched third-party desktop software in the environment. They also gather intelligence on security controls and procedures to build bypass and evasion tools.

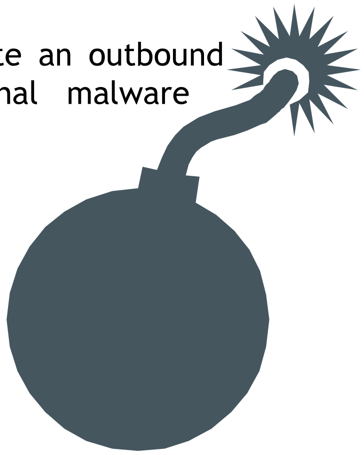
STAGE TWO: INTRUSION AND INFECTION

Using information gleaned during preparation/reconnaissance phase, the attackers create and deploy custom malware to the target. Spear-phishing is a common technique used to trick the target into downloading first-stage malware but attackers have also used drive-by downloads, watering holes, man-in-the-middle attacks and even "spray-and-pray" phishing techniques to gather victims.

Spear-phishing, as described in the RSA attack above, are specially created e-mails that include a link to a malicious website or an e-mail attachment that is booby-trapped with exploits for known or unknown (zero-day) software vulnerabilities. Spear-phishing emails are popular among APT actors who typically modify legitimate documents from a targeted organization and spoof the sender of the e-mail to look like it was sent by a work colleague.

If a user visits clicks on a link and visits a malicious website, a drive-by download occurs and the initial intrusion is successful. In cases where malicious attachments are used, a Word .doc or an Adobe PDF file can be rigged with exploits to ensure an infection.

Once the initial infection occurs, the attackers initiate an outbound connection and sets up the machine for additional malware downloads.



STAGE THREE: LATERAL MOVEMENT

The attackers now have control of the machine that was initially infected but the core of an APT attack is the ability to move laterally within a network and establish a beachhead. This is done by downloading additional malware to the infected machine in the form of rootkits, network backdoors, password-cracking utilities, Remote Access Trojans (RATs) and privilege escalation exploits.

The goal is to expand the access to the compromised network and maintain stealthy persistence for a long period of time. On average, according to data from the Ponemon Institute, it took about 225 days to detect APTs launched by an organization. In some cases, attack groups can remain undetected for years.

Using these specialized attack tools, the attackers gain access to additional machines and hijack authentication data that allows them to burrow deeper into the network. In most cases, the attacker is looking for a domain administrator account that allows the elevation of privilege into the most sensitive parts of the network.

STAGE FOUR: DATA EXFILTRATION

Now that the initial infection is completed and lateral movement and persistence is achieved, the attackers get down to the business of stealing and transmitting the stolen data. In most cases, the attackers hijack everything from the network that might be of interest.

Stolen data typically includes Microsoft documents (Word, Excel, and PowerPoint), e-mail databases and user accounts found on the network. One approach is to use custom tools to harvest data based on file extensions with .doc, .xls, .ppt and .pdf among the most popular. Some advanced threat actors know exactly what they are looking for and know exactly where the high-value data is stored, making collection and exfiltration easier and less noisy.

This data is then encrypted and transmitted to command-and-control servers for later retrieval by the attack groups.

DEFENDING THE FORT:

Alex Stamos
CISO, Yahoo!

Now that it has been established that skilled APT actors have an arsenal of tools to compromise a corporate network, it is crucial that you make the right investments in security technologies and incident response plans to mitigate the threat and reduce your exposure to risk.

In an April 1, 2015 article in SC Magazine entitled "The Failure of the Security Industry," Yahoo! CISO Alex Stamos stated "*For the most part, the security vendors I meet believe that IT departments want to run another agent on their Windows laptops, that production engineers are willing to put a cheap Lintel [Linux on Intel] 1U security device in their critical path, and that every company's security team is staffed like a Top-5 bank. These assumptions are not true. Companies across the world are waking up to the fact that their security posture is insufficient to fend off the threats that breached Sony, Anthem and JPMC . . .*"

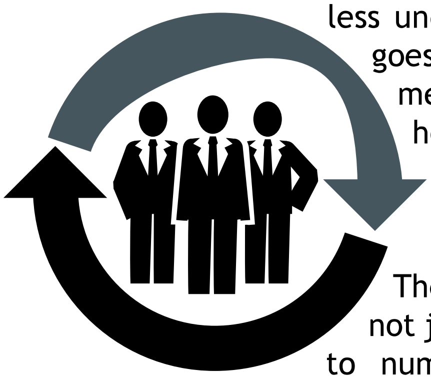
It's clear that multiple point products by a multitude of vendors in the security market today are hit-and-miss at effectively stopping threats, particularly in small and medium sized business that don't have the resources, training and expertise that larger Enterprise companies have.

Companies across the world are waking up to the fact that their security posture is insufficient to fend off the threats...

LISTENING TO YOUR LAYERED SECURITY

This isn’t a bash on deploying layered security in your environment.

Point products are of course useful, but real cyber-threat discovery can be found in the ability to compare and correlate what the products are seeing and doing collectively by interpreting device log data. Unfortunately, effectively forming a conversation from device logs involves aggregating and sifting through colossal volumes of data - making it an unmanageable job to track (much less understand) what is really happening. This is why Stamos goes on to say “The explosion of security needs means the median security engineer in 2015 is less experienced than her counterpart in 2005. Security companies need to recognize that most of their addressable market cannot properly consume their products . . .”



The bottom line is: security has become incredibly complex - not just in the number of moving parts, but the ability to listen to numerous devices spewing mountains of data is nearly impossible for today’s security practitioners. The hard truth is that a vast majority of the high profile breaches could have been prevented if device logs were more closely monitored and/or acted upon. (Verizon 2012).

A SOLUTION USING SIEM TECHNOLOGY

Many organizations are turning to SIEM (Security Information and Event Management) technology platforms to tune into these machine conversations to identify security incidents. SIEM (pronounced SIM) vendors often boast of a great number of correlation rules “out of the box” – immediately ready to root out threats.

The reality is SIEM correlation rulesets must be honed and fine-tuned over a long period to ensure maximum detection and minimal false positives. Once up and running, SIEM products do a great job of aggregating this machine log data, but in addition to being expensive they still rely on in-house security expertise to know what to do if an incident occurs. And who is watching at 3:00 AM, or on the weekend, when many hacking attacks occur?

Network administrators and CISOs should also monitor APT activities closely and implement network scans using available IOC (Indicators of Compromise) data to weed out known cyber-espionage campaigns. This data can also be used to implement early-warning systems and incident response initiatives to thwart future attacks.

A SOLID STRATEGY

A proper detection, remediation and mitigation plan should include the following:

24/7 Cyber-threat Detection: This can be used to identify potential security breaches through intelligent correlation of various log and performance streams. Vast amounts of machine data can be converted into potential security alerts.

Security Alert Assessments: In addition to threat detection, businesses should consider tools to analyze and prioritize security alerts to actionable incidents. This helps to reduce false alarms and ensure resources are properly assigned to deal with threats.

24/7 Incident Response: Create and implement round-the-clock incident response capabilities. Network administrators should have access to specialized security professionals for complex breaches. An on-call incident response team can provide support and guidance on how to best mitigate and remediate issues as they occur.

THEN, REALITY HITS...

Businesses can be challenged when they come to the realization they need 24/7 monitoring of log, performance and configuration data. Obviously the best and most effective method of sifting through millions of log files and data is to implement a SIEM platform. But again, the cost is very high, configuration is complex and rulesets take significant time to fine-tune. Perhaps the biggest challenges though are building the infrastructure and staffing it with security experts around the clock.

IT departments often have a hard time keeping their headcount staffed during an 8 hour day, let alone 24/7! Dealing with turnover and keeping workers engaged can be problems, too. These issues make the task of staffing a SOC (Security Operations Center) with experienced workers 24/7/365 an enormous challenge.

Keep in mind IT security monitoring is potentially 99% sitting and waiting for an incident and 1% remediation. How do you keep a highly skilled (and often, highly paid) worker happy when most of their job isn't doing what they're trained to do?

For this reason, many businesses are turning to Managed Service Providers to manage their security strategy and perform these advanced services. This market is expected to grow at 45% over the next 5 years.