SECURANCE CONSULTING

the advantage of insight

Thieves in the Network: Advanced Persistent Threats

www.securanceconsulting.com

ADVANCED PERSISTENT THREATS

Advanced persistent threats (APT) are the natural evolution of cyber attacks in a technological landscape bursting with juicy data to steal. As the name implies, these types of attacks are methodical, prolonged, and present a significant threat to an organization's confidential information.

APT threaten the security of information, such as:

- Intellectual property (IP)
- Classified data
- Personally identifiable information (PII)
- Critical system credentials

They also lead to detrimental consequences, including database deletion, website takeover, and access to sensitive or incriminating communications. Multi-faceted, targeted, and quiet, APT present a challenge to every industry, not just government agencies and major financial institutions. Any retail company or small community bank that stores payment information could be a victim of an APT attack— because it's less about the size of the organization than the size of the information payout.

APT attackers gain access to a network via one of three attack surfaces:

1. Networks **2.** Web-Based Systems **3.** Human Users[3]

This white paper will detail how APT compromise and breach victims' systems, provide an example of a highly successful APT attack, and explain the best precautionary measures enterprises can take to help avoid APT attacks altogether.

Life Cycle of a Threat

APT are designed with a specific target in mind but still largely adhere to a common set of attack stages to accomplish their goals.

1. Choosing a Victim

In this stage, the attacker selects a target and decides what his overall goal will be for the attack, whether to steal application source code, payment information, trade secrets, or any other information he shouldn't rightly have.

2. Reconnaissance

Next, the attacker will gather information about the target in order to facilitate a successful APT attack. Recon tactics might include network scanning and mapping or social engineering techniques, employee profiling, public domain searches, or information garnered from a simple phone directory. Any information they find is another potential avenue into a system.

3. Delivery

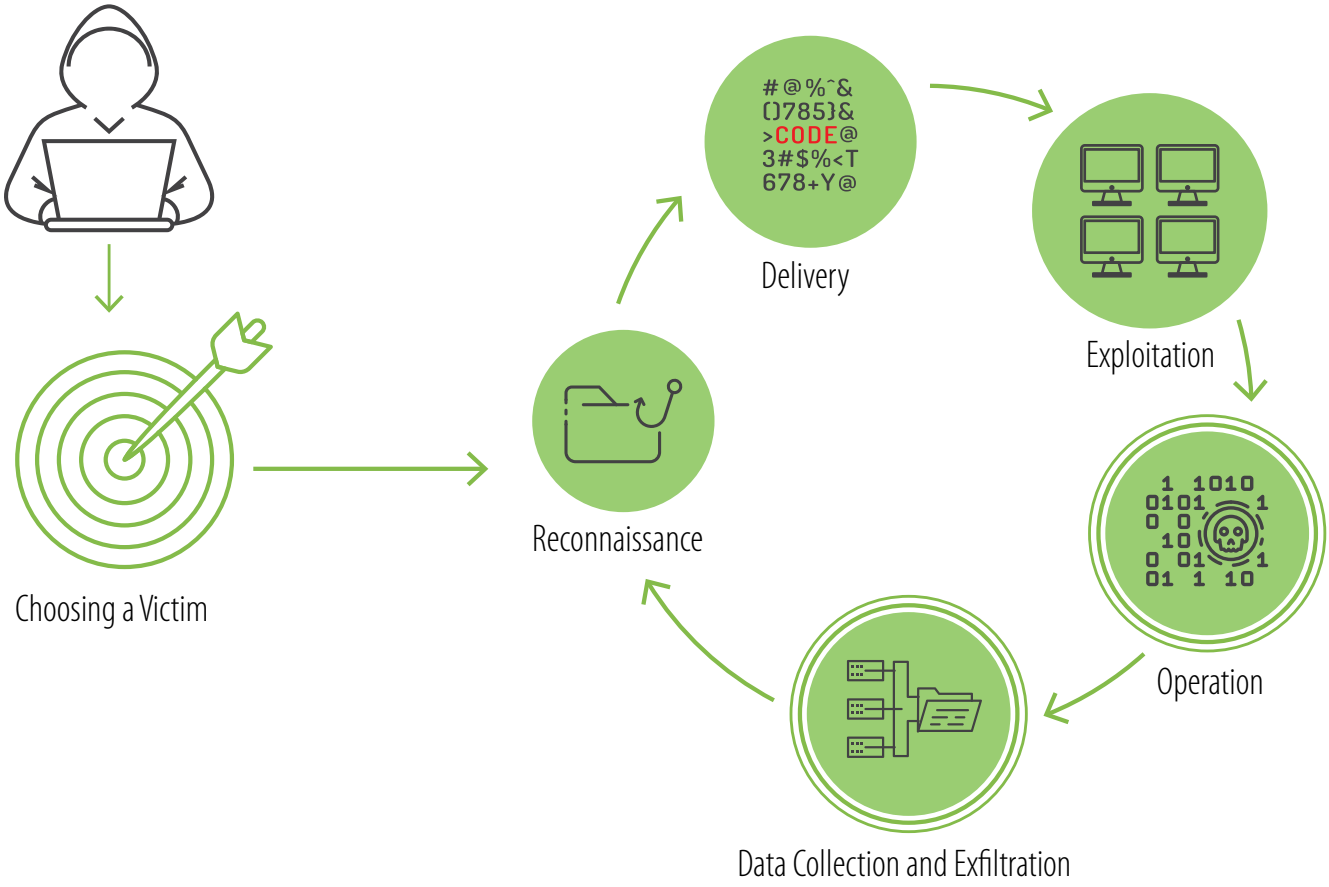
With the information obtained from the reconnaissance phase, the attacker will then attempt to penetrate the target network. They will develop malicious code to exploit the vulnerabilities they identified, attach it to seemingly innocent file types (e.g., PDF, PPT, DOC) or create a link leading to the malware, and deliver it via email or USB to their chosen victim(s) within the target organization. If the user opens the malicious file or clicks the link, the attacker proceeds to the next step.

> To stay below the radar, attackers choose tactics, such as less aggressive network recon and slower data exfiltration, that minimize the ability of the victim to detect, track, or reconstruct the attack.[4]

4. Exploitation

The malicious link or file delivered to the target installs a backdoor shell (a Trojan or other malware in disguise) for the attacker to establish an outbound connection to his command center. At this point, malware has now compromised the victim's workstation (though the system is not yet considered breached) and searches for vulnerabilities to execute its payload. It establishes both a foothold in the network and a connection with the attacker's command center to relay information about the infected computer and accept additional malicious code.

Life Cycle of a Threat



5. Operation

Once a foothold has been established, the attacker makes himself at home. His goal is to sit inside the network long-term, move laterally to gain new strategic footholds, and slowly attempt to gain not only access to more devices within the network, but administrator privileges, as well. The more points of compromise the attacker creates, the easier it will be to continue the attack when other points are closed.

> APT attackers use sophisticated malware techniques, such as encryption, obfuscation, and code rewriting to hide their activity from their targets.[3]

6. Data Collection and Exfiltration

Having compromised the network and gained administrator privileges, the attacker will gather all the sensitive data he has found on a staging server and transmit it via encrypted channels to multiple external servers, which is meant to obscure the true final destination of the data. To distract security teams from noticing or interfering with the outbound data transfer, attackers commonly conduct a white noise attack, such as a distributed denial of service (DDoS) attack. It is at this point that the network is formally considered breached.[5]

If an attacker completes the APT attack without being detected, he will continue to sit inside the network and wait for new attack opportunities. In effect, one organization could experience relentless, silent attacks by one attacker indefinitely, which is why it is critical to stay informed of best practice detection methods.

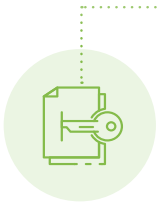
Attack Branching Example

Branch 1 – Phishing

An attacker sends an attachment with malware or a malicious hyperlink for the victim to click to install a keylogger on the victim's system, which records the victim's user credentials for future exploitation.

Branch 2 – Intranet Service Exploit

Credentials gained through phishing allow an attacker to log into a web portal on the enterprise network. This exposes the database server, which is vulnerable to SQL injection, and the web server, which is vulnerable to PHP and HTTP exploits.



Branch 3 – SQL Injection

Using SQL injection, an attacker can either run a command to extract a SAM (password hash) file from a host for offline password cracking or install network scanning tools to perform recon on the database server's network. Either of these can be leveraged to gain remote privileged access to a payment server or other sensitive server and enable the attacker to continue lateral movement throughout the network.[4]

HOW TO DETECT A THREAT

APT are sophisticated and notoriously difficult to detect, but if an organization takes a conscious approach to avoiding them, it is possible to successfully stave off an attack. The following are common warning signs that an organization is experiencing an APT attack.

1. Spear-Phishing Emails. If employees are receiving suspicious emails with file attachments or embedded links, they are likely being specifically targeted to create an entry point in the network. Spear-phishing is different from regular phishing in that the latter are distributed indiscriminately, while the former use information related to the target to appear more trustworthy and trick targets to click malicious links or download files. Any emails with unknown file attachments sent to executives should be considered red flags.

2. Irregular Logins. Tracking and monitoring login activity can alert you to an APT attack. Logins occurring after working hours or exhibiting strange patterns should be investigated, particularly if the credentials being used belong to high-ranking executives, who likely have high-level access to the organization's systems. Cyber criminals will attempt to penetrate your network when they suspect fewer staff are in the office to catch them, which is why logins at irregular hours should be investigated. They could also be snooping from another country, which could account for the time difference.

3. Trojans. This might be common sense, but if an organization identifies a Trojan virus, it should consider the implication that a hacker has infiltrated the network and left a backdoor that he can exploit even if credentials are modified in the future.

4. Shifty Data. When a hacker is in the network, he is looking for something specific and likely moving data between servers or to external computers. Keep an eye out for large batches of information moving around the network and unusual internal and external connections.

5. Data Ready for Export. To make exfiltration easier and more expedient, hackers will clump data into large files, oftentimes where it doesn't belong. Stay vigilant for this telltale sign that data is about to be exfiltrated, paying particular attention to the file types. More often than not, organizations will be able to identify suspicious instances of compressed data by their foreign file extensions.[6]

> Users fall victim to APT attacks by opening seemingly harmless emails or web links. Drive-by download attacks can even compromise an endpoint without requiring the user to make a single click.[2]

A STUDY IN STEALTH: APT41

To provide context as to the scale, impact, and pernicious nature of APT, we present the example of APT41.

APT41 is a dual espionage and cyber crime operation based out of China that has seemingly chosen its targets to align with China's five-year economic development plan (which more than suggests that APT41 is a state-sponsored attacker). Its purpose is to steal IP and other valuable information generated by significant occurrences, such as mergers, acquisitions, and political events, in line with China's national policy priorities. The country is prioritizing higher value products and services, including pharmaceuticals, semiconductors, and other high-tech industries, to stimulate its economy. Verticals targeted by APT41 to achieve this goal include:

- Healthcare
- Telecommunications
- Software Technology
- Travel
- Media and Entertainment
- Education
- Pharmaceuticals
- Video games
- Retail
- Cryptocurrency

Much like a smaller scale APT attacker, APT41 takes advantage of timely news stories to entice users to click on malicious links and file attachments (i.e., spear-phishing) and uses keyloggers to steal credentials. Additional tactics include "moving laterally from trusted third parties, leveraging stolen credentials, using the CHINACHOP web shell, and accessing victim organizations using remote desktop sharing software, such as TeamViewer."[7]

Once APT41 deploys malware into a victim's system, its goal is to identify and exfiltrate information that will aid China in securing a significant market advantage against competitors.

> Digital certificates are sold on the black market for anywhere from $399 USD to upwards of $1,699 USD.[7]

APT41 hides its malware by quietly releasing rootkits on Linux systems and master boot record bootkits, such as ROCKBOOT, on Windows systems. Bootkits are an effective way for attackers to install malware, because the code used resides outside of the operating system (OS); are initialized prior to installation on the OS; and operate in kernel mode. These factors make it very difficult for OS applications and security tools to detect bootkits. Luckily, bootkit use is rare, unless the target is particularly high-value. Ordinarily, attackers will rely on dynamic link library (DLL) search order hijacking or modifying Windows registry keys to conduct an APT attack.[7]

One of the many concerning aspects of APT41 is that it regularly compromises systems with valid, unrevoked digital certificates, decreasing the likelihood of detection. These valid digital certificates allow malicious files to circumvent automated scanning or blocking solutions and bypass Windows group policies, which restrict unauthorized code from running.[7] Even if these certificates are found to have been abused, certificate authorities often move slowly to deactivate them, which gives attackers even more time to use them as they please.

APT41 has also been observed to block antivirus updates from downloading to victims' systems by tampering with the DNS management console, enabling them to freely install ransomware as a service (RaaS), such as Encryptor RaaS, through group policy. As if the loss of sensitive information weren't enough, ransomware presents a whole new, expensive challenge for any afflicted organization.

Despite the sophistication of attackers like APT41, there are precautionary measures organizations can take to prevent and reveal APT before they become a costly problem.

> Even when detected, malicious files signed by a digital certificate from a trusted partner or associated business are less likely to draw suspicion. According to an advertisement in an underground marketplace, the success rate of installing a payload increases by as much as 50 percent when signing files with valid digital certificates.[7]

APT ADVICE

Traditional cybersecurity measures, such as defense in depth, firewalls, and antivirus software cannot protect against an APT attack. The best method of defense is to stay informed and build a strong culture of security awareness throughout the organization. Best practices include:

1. Education. You can't fight a threat you don't understand. Effective user awareness is invaluable against APT, because every user is empowered with the knowledge to recognize and avoid attackers' attempts at weaseling their way into the network via social engineering. Organizations should establish a formal user security awareness program, complete with interactive training, test phishing campaigns, regular reminders, and incentives, to underscore the importance of stopping an APT attack before it starts.

> "A 2018 Ponemon Institute study revealed that U.S. companies took an average of 197 days to detect an APT intrusion."[9]

2. Security Patches. This should be part of any IT department's routine, but many organizations do not update their systems and apply patches in a timely manner, leaving weaknesses in the system for malicious actors to exploit. Set up automatic updates when possible and continuously keep abreast of new patches for identified security weaknesses.

3. Secure Sensitive and Critical Information. Adding more safety measures for sensitive information will help ensure only the right people can access certain data. For example, administrator rights should not be widely provided. Users with admin access can accidentally make changes to the system that create vulnerabilities attackers are more than ready to exploit. Also, the more users with high-level access, the more potential targets and entry points an attacker has to work with when attempting to compromise an organization.

4. Enlist the Help of Cybersecurity Experts. Small or large, any organization can become an APT target. As cyber threats become more sophisticated, independent cybersecurity experts can help organizations identify vulnerabilities and exposures within the IT environment and provide customized remediation recommendations to thwart APT. Third-party experts can also perform simulated APT testing, which will allow organizations to understand their risk of compromise and breach, the consequences of experiencing an attack, and the steps necessary to proactively prevent APT from crippling operations, reputation, privacy, and finances.[6]

It is important to remember that no IT infrastructure is ever 100-percent secure. There are, however, steps all organizations can take to significantly reduce the risk of experiencing a cyber crime.

When strengthening defenses against APT, remember these four logical categories:

1. Administrative – employee training and physical security
2. Networking – network hardware, segmentation, and segregation
3. System administration – restricting administrator privileges and utilizing built-in operating system defense features
4. Specialized security solutions – whitelisting, patching, hardening, filtering, logging, anti-spam, firewall, and anti-malware capabilities[10]

Organizations with the resources to do so can also consider investing in an endpoint detection and response (EDR) solution. Just like a home alarm alerts a homeowner that a door or window has been opened, an EDR solution provides expert monitoring services to ensure the organization receives early warnings against malicious intrusions, phishing, malware, ransomware, and other endpoint threats. There are also managed security service providers (MSSP) that go beyond surveillance by offering threat analysis, incident response recommendations, and intelligence updates to apprise organizations of breaking threats.

Thirdly, because attackers move laterally within a network to bypass security controls, server security is a large concern. Servers are objects of malware and targeted attacks, because they often store a wealth of sensitive data. Monitored server protection services can provide heightened visibility for organizations concerned with this aspect of security.

With security solutions, the name of the game is visibility, a critical advantage against attackers who rely on stealth.

Four basic strategies for preventing APT attacks:

1. Use application whitelisting to help prevent malicious software and unapproved programs from running

2. Patch applications, such as Java, PDF readers, Flash, web browsers, and Microsoft Office

3. Patch operating system vulnerabilities

4. Restrict administrator privileges within operating systems and applications based on user duties[10]

> IT security teams must address the root cause of APT attacks—user behavior— by performing IT risk assessments, implementing comprehensive policies and procedures, establishing a formal user security awareness program, and regularly monitoring and evaluating the IT environment.[5]

CONCLUSION

APT are a serious and evolving cybersecurity threat. Imagine a robber hiding in the guestroom, while you go about your day, unaware. Keepsakes and jewelry go missing. That million-dollar idea that's been in the works for years: gone. And when you look for even a footprint of the culprit, the floors are freshly waxed. This is the vulnerable position in which modern hackers put organizations. However, employing proactive measures, such as building a formal user security awareness program, practicing regular system patching, securing sensitive data, and working with a professional cybersecurity company, will greatly increase organizations' odds of not only finding a hacker in the network, but stopping them from entering in the first place.

To aid in the fight against these sophisticated threats, Securance offers APT simulation testing, which models an authentic, long-term APT attack and tests an organization's ability to prevent, detect, and respond to APT. Over a minimum of 120 days, our experts attempt to compromise the network and steal sensitive data, exactly like a real hacker. The simulation reveals IT security weaknesses, strengths, and risks associated with experiencing an APT attack and helps organizations avoid becoming victims. Read more about **APT simulation testing here**.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.absolute.com/media/1935/2019-endpoint-security-trends-report.pdf
2. https://www.secureworks.com/blog/endpoint-security-guide-management-protection-detection
3. https://www.cynet.com/cyber-attacks/advanced-persistent-threat-apt-attacks/
4. http://reports-archive.adm.cs.cmu.edu/anon/isr2017/CMU-ISR-17-100.pdf
5. https://www.researchgate.net/profile/Attlee_Gamundani/publication/301689293_How_Advanced_Persistent_Threats_Exploit_Humans/links/57223ec208ae586b21d3e6c6/How-Advanced-Persistent-Threats-Exploit-Humans.pdf
6. https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat
7. https://content.fireeye.com/apt-41/rpt-apt41/
8. https://www.csoonline.com/article/3534003/chinese-hacker-group-apt41-uses-recent-exploits-to-target-companies-worldwide.html
9. https://www.ciosummits.com/Online_Assets_Proofpoint_Gartner_Best_Practices.pdf
10. https://encyclopedia.kaspersky.com/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts/

Thieves in the Network: Advanced Persistent Threats

SECURANCE CONSULTING

the advantage of insight

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com