APT:
THE WORLD OF THREAT

Advanced Persistent Threat in less than 15 pages

by :
Oussama Ben Hadj Dahman - Nouha Ben Brahim

APT : The world of Threat

Advanced Persistent Threat in less than 15 pages

April 28, 2024

The concept

"From the moment we first met, it was apparent that a collaboration centered around a unique cybersecurity subject was necessary. Engaging in discussions at various events and conferences, each of us brought our own perspectives and expertise. Nouha, with a background as a red teamer and ethical hacker, and Oussama, as an investigator and blue teamer, represented contrasting yet complementary skill sets. Recognizing the importance of merging these perspectives, we embarked on a journey to explore the world of Advanced Persistent Threats (APTs). Our goal was to unravel the mysteries surrounding the origins and evolution of APTs, elucidating the myriad concepts within cybersecurity threats. Ultimately, we aim to provide comprehensive insights into the mechanisms and steps we believe characterize each APT."

Contents

I - Unveiling the Triad: Risk, Threat, and Vulnerability

In the realm of technology, in an era where artificial intelligence permeates our daily lives and computers and Internet of Things devices serve as the cornerstone of our interconnected world, a new lexicon is emerging with bold prominence in both news media and our daily routines. Television news snippets highlight the frequent and repeated usage of this vocabulary. CNBC, on multiple occasions, discusses a pressing National Security issue titled "Cyber Threat To Infrastructure: National Security On Alert," while delving deeper into potential threats such as "Cyber Threats on US Water Systems." FOX NEWS dedicates entire TV shows to debating the subject, such as "The Cyber Security Threat," and CNN extends the discourse beyond national borders with headlines like "Global Cyber Threat." In this article, co-authored by Oussama Ben Hadj Dahman, a cybersecurity expert and instructor, and Nouha Ben Brahim, CEO of No Breach and Bug Bounty Hunter, we aim to decipher and illuminate the narrative behind Advanced Persistent Threats within the realm of what is commonly referred to as "Cyber Threats," exploring both technical and linguistic dimensions. But first, let's dissect the concept of a threat.

The term "threat" is ubiquitous, not only in the realm of cybersecurity but across various domains including business, experimentation, economy, and politics. From a linguistic standpoint, a threat, according to the British dictionary, signifies "a declaration of the intention to inflict harm, pain, or misery," underscoring its criticality in management contexts. In the realm of cybersecurity, adherence to international standards such as ISO or frameworks like the American NIST's "Risk Management" is imperative for senior management and cybersecurity experts alike. ISO 31000 stipulates that risk exists only in the presence of vulnerability and threat, with likelihood and impact serving as determinants for risk assessment. Hence, an understanding of the interplay between Risk, Vulnerability, and Threat is indispensable; one cannot be discussed without elucidating the others.

ISO 27001 defines vulnerability as "a weakness of an asset or control that could potentially be exploited by one or more threats," with an asset being any valuable location within an organization's systems where sensitive information is stored, processed, or accessed. Vulnerabilities can stem from technical or human factors, which, if exploited by a threat, can lead to unauthorized access using non-engineered methods. A threat, therefore, represents a plausible scenario wherein an identified vulnerability is exploited, prompting crucial questions:

1. Who is likely to exploit the vulnerability?

2. How might they exploit it?

3. From where can an attack be anticipated?

Cybersecurity experts and consultants consider these questions when addressing risk. The "who" corresponds to the "Threat Actor," defined by NIST SP 800-150 as "An individual or a group posing a threat." The "how" is encapsulated by the "Threat Vector," described by CloudFlare as "a way for attackers to enter a network or system," while the "from" elucidates the "threat surface," presented by Fortinet as "the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data."

Upon analyzing these definitions within a unified context, it becomes evident that vulnerabilities, when exploited by threats, transform into risks. Risk, in essence, is contingent on the likelihood of an event occurring and the potential impact thereof on the business or system. Now, let's delve deeper into the nuances of threat actors and their evolutionary trajectories over time.

As we have already defined Threat actors they are considered as "movers and shakers" of the cybercrime underworld. Threat actors can be APTs who are state-sponsored groups, organized cyber-criminal organizations who are financially motivated, or hacktivists with ideological agendas. Recent headlines highlight the activities of Chinese groups exploiting VPN vulnerabilities, Iranian actors targeting Middle Eastern policy experts, Russia-linked groups targeting Eastern European NGOs and the US defense sector ending by the United States and its allies attacking critical infrastructure of their enemies or manipulating different kinds of social media and internet forums for propaganda.

Each of these threat actors is discerned through what cybersecurity professionals term Indicators of Compromise (IOCs). As each actor possesses unique motives, whether achieving penetration or persistence, whether acting individually or as part of a group, they inevitably leave behind traces of their activity. These traces manifest as specific techniques or methods employed during the attack, akin to digital fingerprints. Such evidence not only aids ongoing investigations but also serves as invaluable insight for fortifying future defense systems against similar threats. Understanding these IOCs is pivotal in identifying the type of threat actors encountered, thereby bolstering both reactive measures and proactive defense strategies but still what interest us more during this article is the evolution of one unique kind of actors who has evolved on the way they act, their timing and the high quality evasion techniques they are using to ensure a high level of maturity when it comes to cyber attacks and empowers the results of their damage on politics, security and economics.

II - Key Milestones in APT Evolution

The term "APT," shorthand for "Advanced Persistent Threat," has gained considerable notoriety in the realm of cybersecurity, with widespread attention focused on their actions and the potential ramifications of their exploits. APT groups, backed by substantial financial resources, have continually evolved, investing in research and development to craft unique tools and techniques. These resources extend to secret services, military systems, and even private corporations that may leverage such technologies for sale to high-level political entities or even entire nations.

The narrative of APTs, however, is not a recent one. It traces its roots back to the early days of cyber threats, dating as far back as 1972 when Bob Thomas created the first malware, targeting the ARPANET network, a precursor to the modern internet. This pivotal event laid the groundwork for the emergence of cybersecurity as a profession and a scientific field of study.

In 1986, Markus Hess, a German hacker, is often considered the progenitor of the Advanced Persistent Threat concept. Hess gained access to over 400 American devices, enabling him to clandestinely transmit sensitive information to the Soviet Union. This marked the inception of a highly sophisticated cyber threat landscape that would continue to evolve over the ensuing decades.

The turn of the millennium ushered in an era of unprecedented connectivity, with a computer in nearly every household and the advent of terms such as "Big Data" and "Internet of Things" (IoT). However, this interconnectedness also rendered the world increasingly vulnerable to cyber threats.

In 2005, an insightful article penned by James A. Lewis, a former diplomat at the United States, titled "Computer Espionage, Titan Rain, and China," shed light on the evolving cyber landscape. Lewis highlighted the Pentagon's network being targeted, initially believed to be the work of Chinese hackers but later attributed to bored teenagers in Cupertino, California. However, the Titan Rain attack, a series of persistent intrusions targeting Department of Defense (DOD) facilities, was widely attributed to Chinese actors, though tracing such attacks to a specific source remained challenging.

These highly publicized breaches, including those targeting tech giants like Google, underscored the dominance of APTs in the cybersecurity landscape. Despite the absence of formal nomenclature, it became imperative to confront the reality of these threats openly.

In 2006, the term "Advanced Persistent Threats" was officially coined in a Boeing report, providing a foundational definition that shaped subsequent discourse surrounding APTs.

As the definition of APTs solidified, hackers honed their evasion techniques, operating stealthily to achieve persistence in their attacks. Notable among these was the "Shady RAT" attack, which began in 2006, targeting construction companies in Japan and Korea and then evolved into attacking global critical infrastructure like American water facilities . The attack utilized simple phishing techniques, leveraging droppers in email attachments to install malware that facilitated data exfiltration. This operation, which spanned over four years, highlighted the vulnerability of systems to exploitation, even as late as 2010 when the attack was ultimately discovered.

During the same period, between 2007 and 2010, the "Stuxnet" worm, a joint creation of the NSA and the Israeli 8200 Unit, made headlines for breaching automated industrial SCADA systems. Stuxnet's primary objective was to disrupt Iranian nuclear research, showcasing the unprecedented level of sophistication and strategic intent behind APT activities.

These operations marked pivotal moments in the evolution of cyber warfare, underscoring the need for heightened vigilance and robust defenses against Advanced Persistent Threats.

III - APTs VS Ransomware Syndicates?

Modern ransomware syndicates have evolved into highly organized businesses. APT groups like AtlasCross and Gelsemium demonstrate geographic breadth and innovative tactics, ransomware syndicates showcase a similar level of adaptability and strategic thinking.

Similar to APT groups employing impersonations and clandestine operations, ransomware syndicates have adopted deceptive strategies to maximize their financial gains. Some ransomware operators now distribute ransom notes disguised as legitimate demands for compensation from penetration testers—a tactic reminiscent of the sophisticated impersonation techniques used by APT actors like AtlasCross. This approach not only aims to coerce victims into payment but also reflects a narrative internalized by these criminal enterprises, akin to the calculated methods employed by APT group Gelsemium targeting government entities.

In the broader context of cybercriminal behavior, it's evident that ransomware syndicates, much like APT groups, operate within a structured framework influenced by regional nuances and cultural norms.

In Russian business culture, where organized crime and extortion have historically been prevalent, ransomware operators may perceive their actions as merely following established practices rather than engaging in illicit activities. This normalization of cyber extortion within certain cultural contexts underscores the importance of understanding the motivations and business models driving these criminal enterprises. Just as APT threats vary in complexity and sophistication, ransomware syndicates exhibit a spectrum of capabilities and operational models.

Some groups rely on rudimentary techniques targeting smaller enterprises, akin to novice cybercriminals leveraging cost-effective methods in their initial forays into extortion. Conversely, top-tier ransomware syndicates invest significantly in advanced tools, infrastructure, and personnel, akin to professional freelancers in the ransomware sphere who enlist in major ransomware-as-a-service groups.

As with APT threats, the landscape of ransomware syndicates is dynamic and constantly evolving. The proliferation of new actors and the integration of skilled

professionals from the IT sector into organized cybercrime highlight the adaptability and resilience of these criminal networks. Moreover, just as conflicts within APT groups can arise from the influx of new members and diverging objectives, tensions within ransomware syndicates may emerge as newcomers disrupt established norms and hierarchies. By recognizing the parallels between modern ransomware syndicates and APT groups within the broader cyber threat landscape, organizations can better understand the evolving nature of cyber threats and tailor their defense strategies accordingly.

VI - How do APT attacks work?

Advanced Persistent Threat (APT) attacks involve meticulous planning and execution, unfolding in four distinct stages: incursion, discovery, capture, and exfiltration. In each phase a variety of techniques may be used to achieve the attacker's objectives.

1- Incursion

In targeted attacks, hackers typically infiltrate an organization's network through social engineering, exploiting zero-day vulnerabilities, employing SQL injection techniques, deploying targeted malware, or employing other sophisticated methods. These tactics are also utilized in Advanced Persistent Threats (APTs), often in a coordinated manner. The primary distinction lies in their objectives: while conventional targeted attacks employ short-term, rapid incursions aimed at immediate gains, APTs are characterized by their strategic intent to establish a persistent foothold within the network, enabling clandestine operations over an extended duration. Other characteristics of APT incursions include the following:

Reconnaissance

APT attacks often employ large numbers of researchers who may spend months studying their targets and making themselves familiar with target systems, processes, and people, including partners and vendors. Information may be gathered both online and using conventional surveillance methods. In the case of the Stuxnet attack on organizations believed to be operating Iranian nuclear facilities, the attack team possessed expertise in the design of the programmable logic controllers (PLCs) used for uranium enrichment that were targeted in the attack.

Social engineering

Manipulating individuals to breach security, often by tricking them into clicking on deceptive links or opening malicious attachments. Unlike typical phishing attacks, these methods are refined through extensive research on the target organization. For instance, in one instance, a few HR employees were targeted with a seemingly harmless attachment—a spreadsheet on job listings—that appeared to originate from a reputable website. In another case, users were directed to a picture-hosting site during the Hydraq attack, where they were unwittingly infected through a drive-by download.

Zero-day

Zero-day vulnerabilities refer to security gaps in software that are unknown to the developer, allowing attackers to exploit them before a patch is available. Consequently, the targeted organization has no time to prepare and is caught unprepared. These vulnerabilities are difficult to find and require considerable effort, making them primarily exploited by highly advanced attacker groups. In APT, attackers may initially use one zero-day vulnerability to infiltrate the target, then transition to subsequent vulnerabilities as each point of entry is eventually patched.

Manual operations

Ordinary or widespread attacks typically utilize automation to maximize their impact. "Spray and pray" phishing schemes rely on automated spam to target thousands of users, hoping that some will fall for the scam by clicking on a link or attachment, thus initiating the breach. In contrast, APTs, while capable of using spam, often concentrate on specific individual systems. Their infiltration process is meticulously targeted rather than relying on the automated methods commonly seen in non-APTs attacks.

2 - Discovery

Upon gaining access, attackers begin to systematically survey the organization's systems, searching for sensitive information or, in specific cases like some Advanced Persistent Threats (APTs), looking for operational commands and capabilities. This stage often involves identifying unsecured data and networks, as well as pinpointing any vulnerabilities in software and hardware. It also includes the search for exposed credentials and paths that might lead to further resources or entry points. Unlike more common opportunistic attacks, APTs proceed in a highly structured manner and go to great lengths to remain undetected.

APT attacks are characterized by the use of multiple methods for discovery. Once the attacker has managed to install malware on the system, they can then introduce additional tools as necessary to probe for weaknesses in software, hardware, and networks.

One of the primary objectives for APTs is to stay concealed within the organization to continuously steal data over time. To achieve this, discovery activities are meticulously planned to avoid detection. An example of this is the Hydraq malware (also known as the Aurora or Google attacks), which employed complex obfuscation techniques to stay hidden, including the use of convoluted code to complicate the analysis and detection of the malware.

Alongside these activities, attackers also engage in thorough research and analysis of the systems and data they find. This can include studying network structures, user IDs, passwords, and more.

When an APT is discovered, the immediate question is often how long it has been in the system. This is not typically a concern with standard targeted attacks, where the timing of the breach can usually be determined relatively easily based on when specific data was compromised. However, with APTs, it can be extremely challenging to pinpoint when the intrusion occurred. Victims may find themselves needing to sift through extensive log files or even resort to discarding hardware to fully understand the scope of the breach due to the stealthy nature of the incursion and exploration phases.

In some cases, the APT kill-chain may be quite easy to find. But appearances can be deceptive. The obvious kill-chain may be intentionally launched to distract the victim while the perpetrators proceed undetected to their actual objectives.

3 - Capture

During the capture phase, attackers gain immediate access to sensitive data held on unguarded systems. Additionally, they might covertly install rootkits on selected systems and network access points. These rootkits are designed to intercept data and commands moving throughout the organization. An example of such targeted malware is Duqu, believed to be a precursor to a more aggressive Stuxnet-like attack. Duqu's main objective was intelligence gathering to facilitate future attacks. Though not widespread, Duqu specifically targeted suppliers connected to industrial operations.

Long-term Engagement

APTs aim for prolonged infiltration to continuously gather information. One notable instance is GhostNet, a cyber espionage network uncovered in March 2009, which penetrated computer systems across 103 countries. This network affected embassies, foreign ministries, various government entities, and locations associated with the Tibetan exile community. The Information Warfare Monitor's report highlights that GhostNet began its data collection activities on May 22, 2007, and was active until at least March 12, 2009. On average, systems remained compromised by an APT for 145 days, with the longest instance reaching 660 days.

Control and Sabotage

In some scenarios, APTs can remotely control or even shut down automated software and hardware systems. This risk becomes particularly significant as more physical devices are operated by embedded microprocessors, creating opportunities for significant disruption. Stuxnet, for example, was designed not merely for espionage. It aimed to reprogram industrial control systems — the computer systems that manage industrial processes like power generation, oil refining, and gas pipelines. Its objective was to manipulate physical equipment controlled by these systems, causing the equipment to operate in a manner determined by the attackers, which could diverge significantly from its intended function.

4 - Exfiltration

After gaining control over the targeted systems, intruders might start to exfiltrate intellectual property or other sensitive information.

Data Transmission

The stolen data is transmitted back to the attackers' headquarters following specific command-and-control directives. This transmission could occur openly (such as via Webmail) or be more concealed, using encryption or being packaged into password-protected zip files. For instance, the Hydraq malware employed innovative methods to send information back. It used Port 443, commonly associated with secure web traffic, as a main conduit for data exfiltration. Additionally, it mimicked the initial stages of an SSL key exchange, creating the appearance of a secure connection without actually establishing one. Hydraq also utilized custom encryption to protect the data as it was exfiltrated from compromised organizations.

Ongoing Analysis

Unlike the immediate sale of stolen credit card details common in other forms of cyberattacks, information obtained by Advanced Persistent Threats (APTs) undergoes extensive analysis. This analysis seeks to uncover strategic insights from the captured data. Experts might manually examine the stolen information to uncover trade secrets, forecast competitors' future actions, and develop strategic responses. This careful scrutiny of data underscores the sophisticated and strategic nature of APTs, emphasizing their focus on long-term impact and advantage.

Authors

Oussama Ben Hadj Dahman, also known as cybereagle2001, is a cybersecurity expert and instructor. Holding certifications as an ISO 27001 Lead Implementer, CDFE, and CPT from ICSI, UK, as well as CC from ISC², AI-900 and SC-900 from Microsoft, Oussama has demonstrated his commitment to excellence in the field. With a background as an esteemed member of Securinets INSAT and former Chairman of Securinets Tek-UP, he has played pivotal roles in various cybersecurity communities. Used to serve as the Cybersecurity Manager at Engineers Spark, Faculty of Science of Tunis, Oussama brings a wealth of experience and knowledge to his role. His dedication to educating others is evident through his previous positions as a cybersecurity instructor at GOMYCODE Tunisia and his contributions to the international Securzy community.

Nouha Ben Brahim, is a prominent figure in the cybersecurity industry, revered for her exceptional expertise and innovative leadership as the CEO of No-Breach. Nouha's journey to becoming a cybersecurity luminary began with her fervent dedication to mastering the craft. Certified by EC-COUNCIL as a Bug Bounty Hunter, Web Exploitation Expert, and Dark Web Operator, she possesses a rare combination of technical prowess and strategic insight. Her certifications from Cisco as a Network Expert further solidify her status as a formidable force in cybersecurity.

Oussama Ben Hadj Dahman

also known as cybereagle2001, is a cybersecurity expert and instructor. Holding certifications as an ISO 27001 Lead Implementer, CDFE, and CPT from ICSI, UK, as well as CC from ISC², AI-900 and SC-900 from Microsoft, Oussama has demonstrated his commitment to excellence in the field. With a background as an esteemed member of Securinets INSAT and former Chairman of Securinets Tek-UP, he has played pivotal roles in various cybersecurity communities. Used to serve as the Cybersecurity Manager at Engineers Spark, FST, Oussama brings a wealth of experience and knowledge to his role. His dedication to educating others is evident through his previous positions as a cybersecurity instructor at GOMYCODE Tunisia and his contributions to the international Securzy community.

Nouha Ben Brahim

is a prominent figure in the cybersecurity industry, revered for her exceptional expertise and innovative leadership as the CEO of No-Breach. Nouha's journey to becoming a cybersecurity luminary began with her fervent dedication to mastering the craft. Certified by EC-COUNCIL as a Bug Bounty Hunter, Web Exploitation Expert, and Dark Web Operator, she possesses a rare combination of technical prowess and strategic insight. Her certifications from Cisco as a Network Expert further solidify her status as a formidable force in cybersecurity.