ADVANCED PERSISTENT THREATS IN CYBER SECURITY
CYBER WARFARE

Nicolae Sfetcu

MultiMedia Publishing
Advanced Persistent Threats in Cybersecurity – Cyber Warfare

BOOK PREVIEW

Chapter: APT: Definition, History and Features

Nicolae SFETCU
nicolae@sfetcu.com


© 2024 Nicolae Sfetcu.

1 Researcher - Romanian Academy - Romanian Committee of History and Philosophy of Science and Technology (CRIFST), Division of History of Science (DIS), ORCID: 0000-0002-0162-9973
Advanced Persistent Threats in Cybersecurity – Cyber Warfare

Nicolae SFETCU

Abstract

This book aims to provide a comprehensive analysis of Advanced Persistent Threats (APTs), including their characteristics, origins, methods, consequences, and defense strategies, with a focus on detecting these threats. It explores the concept of advanced persistent threats in the context of cyber security and cyber warfare. APTs represent one of the most insidious and challenging forms of cyber threats, characterized by their sophistication, persistence, and targeted nature. The paper examines the origins, characteristics and methods used by APT actors. It also explores the complexities associated with APT detection, analyzing the evolving tactics used by threat actors and the corresponding advances in detection methodologies. It highlights the importance of a multi-faceted approach that integrates technological innovations with proactive defense strategies to effectively identify and mitigate APT.

Keywords: Advanced Persistent Threats, APT, cybersecurity, cyber warfare, threat detection, cyberattack

Advanced Persistent Threats

Advanced persistent threats (APTs) are a class of cyber threats that pose a significant challenge to organizations and nations around the world. They are known for their advanced tactics, techniques, and procedures, as well as their ability to infiltrate and operate persistently on target systems for long periods of time.

APTs are usually coordinated by a state or a state-sponsored group (Kaspersky 2023b) (Cisco 2023). The motivations of these threat actors are usually military, geopolitical, or economic espionage (Cole 2013). These targeted sectors include government, defense, financial services, legal services, industrial, telecommunications, consumer goods, and more (FireEye 2019).

The average "contact time," in which an APT attack goes undetected, averaged 71 days in North America, 177 days in EMEA, and 204 days in APAC in 2018 (Mandiant 2021).

Advanced persistent threats combine a variety of different forms of attack, from social engineering to technical exploits. APTs generally use traditional espionage vectors (Ghafir and Prenosil 2014), including social engineering, human intelligence, and infiltration, for network attacks by installing custom malware (malicious software) (Symantec 2018b). The diversity and
stealth of APTs make them a central issue in cyber security due to the asymmetric nature of attacks, often turning to game theory to model conflict using matrix games as a risk mitigation tool. Game-theoretic APT models can be derived directly from topological vulnerability analysis, together with risk assessments, according to common risk management standards such as the ISO 31000 family (Rass, König, and Schauer 2017).

Increasing heterogeneity, connectivity and openness of information systems allow access to a system through multiple different paths. To ensure security, semi-automated tools and techniques are used to detect and mitigate vulnerabilities, but such attacks quickly adapt to these configurations so that they stay "under the radar". Countermeasures have a higher latency, being ineffective for sudden changes in attack strategies of an invisible adversary (Rass, König, and Schauer 2017).

Advanced persistent threats have emerged as a new and complex version of multi-stage attacks (MSA) (Kyriakopoulos et al. 2018), while current APT detection systems focus more on the emergence of alerts of detection, than on predicting threats (Ghafir et al. 2019). APT stage forecasting not only reveals the APT lifecycle in its early stages, but also helps in understanding the attacker's strategies and objectives. In addition, the Internet of Things (IoT) makes Internet-connected devices easy targets for cyberattacks (Ghafir, Kyriakopoulos, et al. 2018). The global cost of cybercrime reached $600 billion in 2018, according to a McAfee report (McAfee 2018).

To counter cyberattacks, analysts typically use Intrusion Detection Systems (IDS) by matching known (signature-based) attack patterns by comparing the data to a database containing a list of known attack signatures), or observing anomalies (deviation from a reference profile) (Santoro et al. 2017). The targeted objective of APT is espionage and data exfiltration. The attack can last for weeks or years, with very long periods between the stages of the attack, making it difficult to detect by correlating multiple alerts during the APT lifecycle (Mandiant 2013). Traditional pattern matching methods are ineffective in the case of APT, as there is no pattern of order and frequencies between stages, due to technical limitations of the static mechanisms of the attacked institution or the attacker's use of new and dynamic techniques. An APT unfolds in several stages, with the attacker's privileges, information, and resources accumulating at each stage.

In 76% of organizations affected by APTs, antivirus software and threat detection systems were ineffective. At the Infosecurity Europe 2011 conference, APTs were included among the biggest cyber threats of the modern world (Rot and Olszewski 2017). According to a Deloitte
Definition of APT

A common cyberattack aims to exploit vulnerabilities to steal data from companies (P. Chen, Desmet, and Huygens 2014), causing non-critical damage. An APT has far more resources and focuses on large organizations and government institutions, causing serious, even critical, damage.

Many feel that the term APT is overloaded because different people refer to it as different things. The definition given by the US National Institute of Standards and Technology (NIST) states that an APT is (NIST 2011):

“An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.”

The main features of an APT follow from its name itself:

- **Threat** – APTs have both capability and intent, being executed through coordinated actions, with qualified, motivated, organized and well-funded personnel (Maloney 2018) (IT Governance 2023).
- **Persistence** – Attackers use a "low and slow" approach within a coherent strategy; if they lose access to their target, they will try again to get it. Their goals are to maintain long-term access (IT Governance 2023) (Arntz 2016).
- **Advanced** – Attackers have a wide range of state-of-the-art techniques and tools, some even innovative, and may include commonly available components. They typically attempt to establish multiple entry points into targeted networks, and combine multiple methods, tools, and techniques to achieve their goals, maintain access, and compromise the target (Maloney 2018) (Arntz 2016).

The specificity of APTs allows them to retain access even if malicious activity is discovered and an incident response is triggered allowing cybersecurity defenders to close a compromise.
History of APT

Attacks on cybersecurity via targeted email combined with social engineering and using trojans to exfiltrate information have been used as far back as the early 1990s, being made known by UK and US CERTs in 2005. The term "advanced persistent threat" was first used in the United States Air Force in 2006 (SANS 2013), by Colonel Greg Rattray (Holland 2013).

Through the Stuxnet project, the US targeted the computer hardware of Iran's nuclear program, an example of an APT attack (Virvilis and Gritzalis 2013).

PC World reported an 81% increase in APTs from 2010 to 2011. Several countries have used cyberspace to collect information through APTs (Grow, Epstein, and Tschang 2008), through affiliated groups or agents of sovereign state governments (Daly 2009).

A Bell Canada study found widespread APT presence in Canadian government and critical infrastructure, with attacks attributed to Chinese and Russian actors (McMahon and Rohozinski 2013).

Google, Adobe Systems, Juniper Networks and Symantec were victims of an APT attack called Operation Aurora (Matthews 2019).

Several attacks in the military, financial, energy, nuclear, education, aerospace, telecommunications, chemical, and government sectors were reported in 2011 (Y. Wang et al. 2016). The most publicized APT attacks include Stuxnet, RAS Breach, Operation Aurora, Duqu, Operation Ke3chang, Flame, Snow Man, Red October and Mini duke, with more recent malware attacks Ratankba, ActiveX, etc. (Xu et al. 2015). Their usual objectives are cyber espionage with national security interests and sabotage of strategic infrastructures. Attacks use hardware devices and software tools, with a systematic approach that often relies on social engineering as the main mechanism to gain access and zero-day exploits (Adelaiye, Ajibola, and Silas 2019).

Industroyer, a malware framework that was discovered in 2016, targeted the power grid in the capital of Ukraine, causing a short-term power outage in that area (Tollefson 2020).

Features of APT

Advanced persistent threats are characterized by persistence (remaining undetected in a target environment for long periods, sometimes even years), pinpoint targeting (selective, tailoring their attacks to the vulnerabilities or weaknesses of targets), and sophistication (advanced and
cutting-edge techniques generation, some even innovative, often using zero-day exploits, social engineering, and other sophisticated methods).

The distinctive characteristics of APT are (P. Chen, Desmet, and Huygens 2014):

**Specific targets and clear objectives.** The targets of APT attacks are specific, usually governments, organizations, or countries' militaries, limiting their attack range. Their purpose is mostly strategic benefits in national security and obtaining secret information.

**Expert, organized and resourceful attackers.** Attackers are usually skilled hackers working in a coordinated manner, employed in a government/military cyber unit (Mandiant 2013) or cyber mercenaries, prepared to operate for extended periods of time and exploit zero-day vulnerabilities. Sometimes they can even operate with the support of military or state intelligence services.

**Long-term attacks and, if necessary, repeated attempts.** APT campaigns go undetected for months or years. APT actors are constantly adapting their efforts to changing conditions or to overcome a particular difficulty.

**Stealth and evasive techniques.** APT attacks can remain undetected, hiding in network traffic and interacting minimally, only to achieve defined objectives. They can use zero-day exploits to avoid signature-based detection, and encryption to spoof network traffic.

<table>
<thead>
<tr>
<th></th>
<th>Traditional Attacks</th>
<th>APT Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>Mostly single person</td>
<td>Highly organized, sophisticated, determined, and well-resourced group</td>
</tr>
<tr>
<td>Target</td>
<td>Unspecified, mostly individual systems</td>
<td>Specific organizations, governmental institutions, commercial enterprises</td>
</tr>
<tr>
<td>Purpose</td>
<td>Financial benefits, demonstrating abilities</td>
<td>Competitive advantages, strategic benefits</td>
</tr>
<tr>
<td>Approach</td>
<td>Single run, “smash and grab”, short period</td>
<td>Repeated attempts, stays low and slow, adapts to resist defenses, long term</td>
</tr>
</tbody>
</table>

Table 1: Comparison of traditional and APT attacks. Source (P. Chen, Desmet, and Huygens 2014)

**Bibliography**


NICOLAE SFETCU: ADVANCED PERSISTENT THREATS IN CYBERSECURITY – CYBER WARFARE


Singer, Peter W., and Allan Friedman. 2014. Cybersecurity: What Everyone Needs to Know. OUP USA.


2016 IEEE International Conference on Communications (ICC), 1–6. https://doi.org/10.1109/ICC.2016.7511197.


Zimba, Aaron, Hongsong Chen, Zhaoshun Wang, and Mumbi Chishimba. 2020. “Modeling and Detection of the Multi-Stages of Advanced Persistent Threats Attacks Based on Semi-


**Content**

Abstract

Introduction

- Cybersecurity
  - Challenges in cyber security
  - Solutions in cyber security
- Cyber warfare
  - Challenges in maintaining cybersecurity
  - Implications of cyber warfare

Advanced Persistent Threats

- Definition of APT
- History of APT
- Features of APT
- APT methods, techniques, and models
  - APT life cycle
  - Consequences of APT attacks
- Defense strategies
- Related works
- Case studies
  - Titan Rain
  - Sykipot
  - GhostNet
  - Stuxnet
  - Operation Aurora
This book aims to provide a comprehensive analysis of Advanced Persistent Threats (APTs), including their characteristics, origins, methods, consequences, and defense strategies, with a focus on detecting these threats. It explores the concept of advanced persistent threats in the context of cyber security and cyber warfare. APTs represent one of the most insidious and challenging forms of cyber threats, characterized by their sophistication, persistence, and targeted nature. The paper examines the origins, characteristics and methods used by APT actors. It also explores the complexities associated with APT detection, analyzing the evolving tactics used by threat actors and the corresponding advances in detection methodologies. It highlights the
importance of a multi-faceted approach that integrates technological innovations with proactive defense strategies to effectively identify and mitigate APT.

MultiMedia Publishing  


Print: Format 6' x 9

DOI: 10.58679/MM28378

Publishing date: 22.06.2024

Contact

About author

Owner and manager with MultiMedia SRL and MultiMedia Publishing House.

Project Coordinator for European Teleworking Development Romania (ETD)
Member of Rotary Club Bucuresti Atheneum
Cofounder and ex-president of the Mehedinti Branch of Romanian Association for Electronic Industry and Software
Initiator, cofounder and president of Romanian Association for Telework and Teleactivities
Member of Internet Society
Initiator, cofounder and ex-president of Romanian Teleworking Society
Cofounder and ex-president of the Mehedinti Branch of the General Association of Engineers in Romania

Physicist engineer - Bachelor of Science (Physics, Major Nuclear Physics). Master of Philosophy.

Researcher - Romanian Academy - Romanian Committee for the History and Philosophy of Science and Technology (CRIFST), History of Science Division (DIS), ORCID: 0000-0002-0162-9973

Contact

Nicolae Sfetcu

Email: nicolae@sfetcu.com
MultiMedia: https://www.telework.ro/