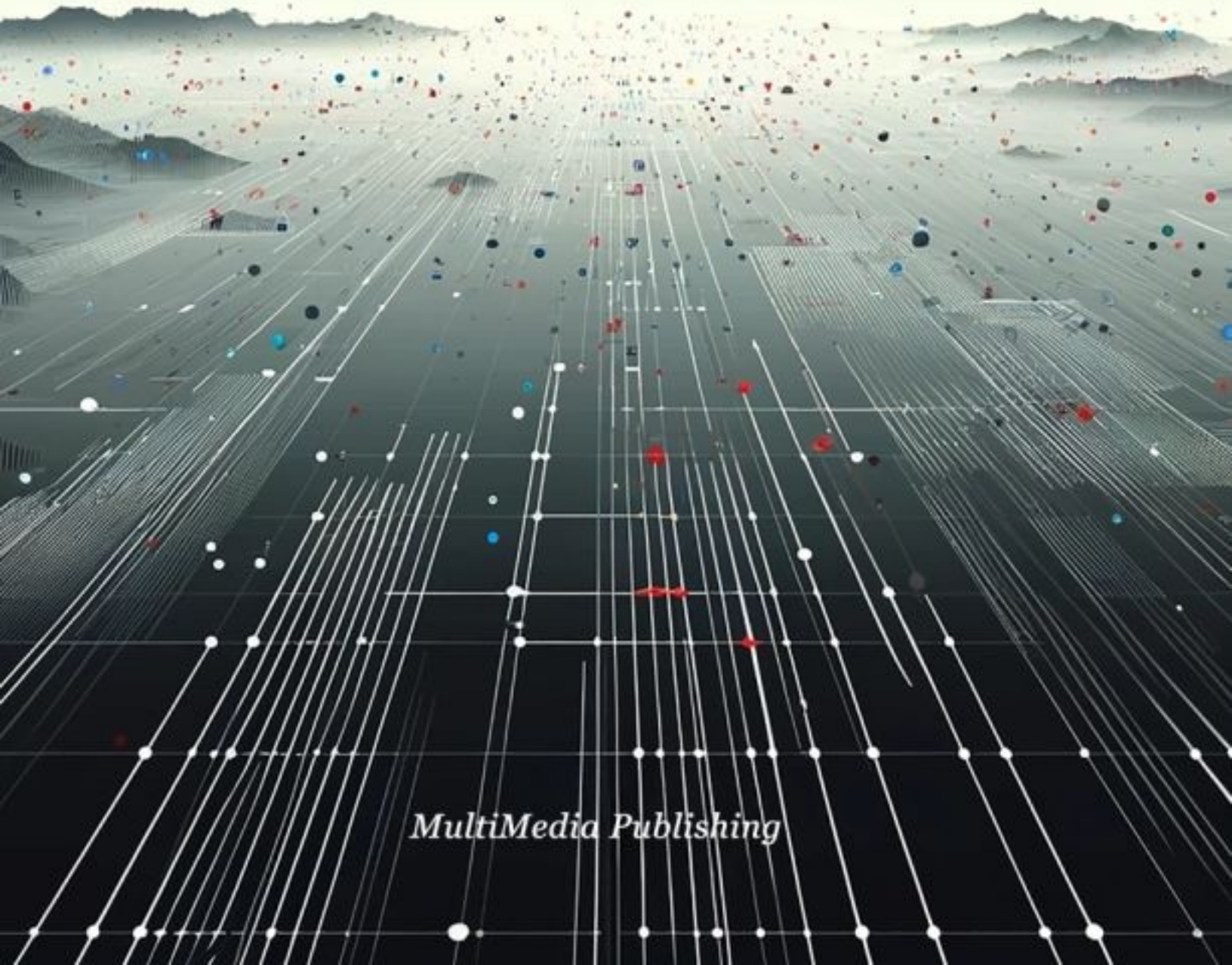
ADVANCED PERSISTENT THREATS IN CYBER SECURITY CYBER WARFARE

Nicolae Sfetcu



MultiMedia Publishing

Advanced Persistent Threats in Cybersecurity – Cyber Warfare

BOOK PREVIEW

Chapter: APT: Definition, History and Features

Nicolae SFETCU
nicolae@sfetcu.com[1]

Sfetcu, Nicolae (2024), *Advanced Persistent Threats in Cybersecurity – Cyber Warfare*, MultiMedia Publishing, ISBN 978-606-033-853-6, DOI: 10.58679/MM28378, https://www.telework.ro/en/e-books/advanced-persistent-threats-in-cybersecurity-cyber-warfare/

[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

Contents

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

report (Deloitte 2016), the key factors in combating APT are: constant risk assessment, offensive security, and staff training (Rot 2009).

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.

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

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

Bibliography

Adams, Chris. 2018. “Learning the Lessons of WannaCry.” *Computer Fraud & Security* 2018 (9): 6–9. https://doi.org/10.1016/S1361-3723(18)30084-8.

Adelaiye, Oluwasegun, Aminat Ajibola, and Faki Silas. 2019. "Evaluating Advanced Persistent Threats Mitigation Effects: A Review," February.

Aleroud, Ahmed, and Lina Zhou. 2017. "Phishing Environments, Techniques, and Countermeasures: A Survey." *Computers & Security* 68 (July):160–96. https://doi.org/10.1016/j.cose.2017.04.006.

Alperovitch, Dmitri. 2011. "Revealed: Operation Shady RAT - McAfee." https://icscsi.org/library/Documents/Cyber_Events/McAfee%20-%20Operation%20Shady%20RAT.pdf.

Al-Saraireh, Jaafer, and Ala' Masarweh. 2022. "A Novel Approach for Detecting Advanced Persistent Threats." *Egyptian Informatics Journal* 23 (4): 45–55. https://doi.org/10.1016/j.eij.2022.06.005.

Alshamrani, Adel, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. 2019. "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities." *IEEE Communications Surveys & Tutorials* 21 (2): 1851–77. https://doi.org/10.1109/COMST.2019.2891891.

Al-Yaseen, Wathiq Laftah, Zulaiha Ali Othman, and Mohd Zakree Ahmad Nazri. 2017. "Multi-Level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-Means for Intrusion Detection System." *Expert Systems with Applications* 67 (January):296–303. https://doi.org/10.1016/j.eswa.2016.09.041.

Amouri, Amar, Vishwa T. Alaparthy, and Salvatore D. Morgera. 2020. "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things." *Sensors* 20 (2): 461. https://doi.org/10.3390/s20020461.

Apruzzese, Giovanni, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti. 2017. "Detection and Threat Prioritization of Pivoting Attacks in Large Networks." *IEEE Transactions on Emerging Topics in Computing* PP (October):1–1. https://doi.org/10.1109/TETC.2017.2764885.

Arachchilage, Nalin, and Steve Love. 2014. "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective." *Computers in Human Behavior* 38 (September):304–12. https://doi.org/10.1016/j.chb.2014.05.046.

Arntz, Pieter. 2016. "Explained: Advanced Persistent Threat (APT) | Malwarebytes Labs." Malwarebytes. July 25, 2016. https://www.malwarebytes.com/blog/news/2016/07/explained-advanced-persistent-threat-apt/.

Ashford, Warwick. 2011. "How to Combat Advanced Persistent Threats: APT Strategies to Protect Your Organisation | Computer Weekly." ComputerWeekly.Com. 2011. https://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation.

Ask, M. 2013. "Advanced Persistent Threat (APT) Beyond the Hype Project Report in IMT 4582 Network Security at Gjøvik University College during Spring 2013." In . https://www.semanticscholar.org/paper/Advanced-Persistent-Threat-(-APT-)-Beyond-the-hype-Ask/a140cd962b136474685db82de60bb15f4fe1d7e1.

Axelsson, Stefan. 2000. "The Base-Rate Fallacy and the Difficulty of Intrusion Detection." *ACM Transactions on Information and System Security* 3 (3): 186–205. https://doi.org/10.1145/357830.357849.

Azaria, Amos, Ariella Richardson, Sarit Kraus, and V. Subrahmanian. 2014. "Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data." *IEEE*

Transactions on Computational Social Systems 1 (June):135–55. https://doi.org/10.1109/TCSS.2014.2377811.

Bai, Tim, Haibo Bian, Abbas Abou Daya, Mohammad Salahuddin, Noura Limam, and Raouf Boutaba. 2019. *A Machine Learning Approach for RDP-Based Lateral Movement Detection*. https://doi.org/10.1109/LCN44214.2019.8990853.

Balduzzi, Marco, Vincenzo Ciangaglini, and Robert McArdle. 2013. *Targeted Attacks Detection with SPuNge*. https://doi.org/10.1109/PST.2013.6596053.

BBC. 2009. "Major Cyber Spy Network Uncovered," March 29, 2009. http://news.bbc.co.uk/2/hi/americas/7970471.stm.

Bencsáth, B., Gábor Pék, L. Buttyán, and M. Félegyházi. 2012. "Duqu: Analysis, Detection, and Lessons Learned." In . https://www.semanticscholar.org/paper/Duqu%3A-Analysis%2C-Detection%2C-and-Lessons-Learned-Bencs%C3%A1th-P%C3%A9k/9974cdf65ffbdee47837574432b0f8b59ffbddd1.

Benjamin, Victor, Weifeng Li, and Thomas Holt. 2015. *Exploring Threats and Vulnerabilities in Hacker Web: Forums, IRC and Carding Shops*. https://doi.org/10.1109/ISI.2015.7165944.

Bere, Mercy, Fungai Bhunu Shava, Attlee Gamundani, and Isaac Nhamu. 2015. "How Advanced Persistent Threats Exploit Humans." *IJCSI*, November.

Bertino, Elisa, and Gabriel Ghinita. 2011. "Towards Mechanisms for Detection and Prevention of Data Exfiltration by Insiders: Keynote Talk Paper." In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 10–19. Hong Kong China: ACM. https://doi.org/10.1145/1966913.1966916.

Bhatt, Parth, Edgar Toshiro Yano, and Per Gustavsson. 2014. "Towards a Framework to Detect Multi-Stage Advanced Persistent Threats Attacks." In *2014 IEEE 8th International Symposium on Service Oriented System Engineering*, 390–95. https://doi.org/10.1109/SOSE.2014.53.

Bowen, Brian M., Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. 2009. "Baiting Inside Attackers Using Decoy Documents." In *Security and Privacy in Communication Networks*, edited by Yan Chen, Tassos D. Dimitriou, and Jianying Zhou, 51–70. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-05284-2_4.

Brewer, Ross. 2014. "Advanced Persistent Threats: Minimising the Damage." *Network Security* 2014 (April):5–9. https://doi.org/10.1016/S1353-4858(14)70040-6.

Bro, Rasmus, and Age K. Smilde. 2014. "Principal Component Analysis." *Analytical Methods* 6 (9): 2812–31. https://doi.org/10.1039/C3AY41907J.

Brogi, Guillaume, and Elena Di Bernardino. 2019. "Hidden Markov Models for Advanced Persistent Threats." *International Journal of Security and Networks* 14 (4): 181. https://doi.org/10.1504/IJSN.2019.103147.

Brogi, Guillaume, and Valerie Viet Triem Tong. 2016. "TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking." *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, November, 1–5. https://doi.org/10.1109/NTMS.2016.7792480.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–48. https://doi.org/10.2307/25750690.

Busby, J. S., B. S. S. Onggo, and Y. Liu. 2016. "Agent-Based Computational Modelling of Social Risk Responses." *European Journal of Operational Research* 251 (3): 1029–42. https://doi.org/10.1016/j.ejor.2015.12.034.

Chaitanya, Krishna T., HariGopal Ponnapalli, Dylan Herts, and Juan Pablo. 2012. "Analysis and Detection of Modern Spam Techniques on Social Networking Sites." *2012 Third International Conference on Services in Emerging Markets*, December, 147–52. https://doi.org/10.1109/ICSEM.2012.28.

Chandola, Varun, Arindam Banerjee, and Vipin Kumar. 2009. "Anomaly Detection: A Survey." *ACM Comput. Surv.* 41 (July). https://doi.org/10.1145/1541880.1541882.

Chandra Jadala, Dr, Challa Narasimham, and Sai Kiran Pasupuleti. 2020. "Detection of Deceptive Phishing Based on Machine Learning Techniques." In , 13–22. https://doi.org/10.1007/978-981-15-2407-3_2.

Chen, Ping, Lieven Desmet, and Christophe Huygens. 2014. "A Study on Advanced Persistent Threats." In *Communications and Multimedia Security*, edited by Bart De Decker and André Zúquete, 63–72. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-44885-4_5.

Chen, Zhiyan, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, H.T. Mouftah, and Petar Djukic. 2022. "Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats." *ACM Computing Surveys* 55 (April). https://doi.org/10.1145/3530812.

Chu, Wen-Lin, Chih-Jer Lin, and Ke-Neng Chang. 2019. "Detection and Classification of Advanced Persistent Threats and Attacks Using the Support Vector Machine." *Applied Sciences* 9 (21): 4579. https://doi.org/10.3390/app9214579.

Cisco. 2023. "What Is an Advanced Persistent Threat (APT)?" Cisco. 2023. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.

CloudStrike. 2023. "Cyber Attacks on SMBs: Current Stats and How to Prevent Them." Crowdstrike.Com. 2023. https://www.crowdstrike.com/solutions/small-business/cyber-attacks-on-smbs/.

Cobb, Michael. 2013. "The Evolution of Threat Detection and Management." https://docs.media.bitpipe.com/io_10x/io_109837/item_691345/EMC_sSecurity_IO%23109837_E-Guide_060513.pdf.

Cobb, Stephen. 1996. *The NCSA Guide to PC and LAN Security*. McGraw-Hill.

Cole, Eric. 2013. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Syngress.

Conti, Mauro, Luigi V. Mancini, Riccardo Spolaor, and Nino Vincenzo Verde. 2015. "Can't You Hear Me Knocking: Identification of User Actions on Android Apps via Traffic Analysis." In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 297–304. CODASPY '15. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2699026.2699119.

Coppolino, L., Michael Jäger, Nicolai Kuntze, and Roland Rieke. 2012. "A Trusted Information Agent for Security Information and Event Management." In , 6–12.

Crouse, Michael, Bryan Prosser, and Errin Fulp. 2015. *Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses*. https://doi.org/10.1145/2808475.2808480.

CSS. 2019. "Trend Analysis - The Israeli Unit 8200 An OSINT-Based Study." CSS CYBER DEFENSE PROJECT. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf.

Daly, Michael K. 2009. "The Advanced Persistent Threat (or Informa5onized Force Opera5ons)." https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf.

De Vries, Johannes, Hans Hoogstraaten, Jan Van Den Berg, and Semir Daskapan. 2012. "Systems for Detecting Advanced Persistent Threats: A Development Roadmap Using Intelligent Data Analysis." *2012 International Conference on Cyber Security*, December, 54–61. https://doi.org/10.1109/CyberSecurity.2012.14.

Deloitte. 2016. "Cyber Espionage - The Harsh Reality of Advanced Security Threats." https://indianstrategicknowledgeonline.com/web/us_aers_cyber_espionage_07292011.pdf.

Denault, Michel, Dimitris Karagiannis, Dimitris Gritzalis, and Paul Spirakis. 1994. "Intrusion Detection: Approach and Performance Issues of the SECURENET System." *Computers & Security* 13 (6): 495–508. https://doi.org/10.1016/0167-4048(91)90138-4.

Denning, D.E. 1987. "An Intrusion-Detection Model." *IEEE Transactions on Software Engineering* SE-13 (2): 222–32. https://doi.org/10.1109/TSE.1987.232894.

Dijk, Marten van, Ari Juels, Alina Oprea, and Ronald L. Rivest. 2013. "FlipIt: The Game of 'Stealthy Takeover.'" *Journal of Cryptology* 26 (4): 655–713. https://doi.org/10.1007/s00145-012-9134-5.

EC-Council. 2023. "What Is Cyber Threat Modeling | Importance of Threat Modeling." *EC-Council* (blog). 2023. https://www.eccouncil.org/threat-modeling/.

Edwards, Benjamin, Tyler Moore, George Stelle, Steven Hofmeyr, and Stephanie Forrest. 2012. "Beyond the Blacklist: Modeling Malware Spread and the Effect of Interventions." *Proceedings New Security Paradigms Workshop*, February. https://doi.org/10.1145/2413296.2413302.

Eke, Hope Nkiruka, Andrei Petrovski, and Hatem Ahriz. 2019. "The Use of Machine Learning Algorithms for Detecting Advanced Persistent Threats." In *Proceedings of the 12th International Conference on Security of Information and Networks*, 1–8. SIN '19. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3357613.3357618.

ETDA. 2023. "Threat Group Cards: A Threat Actor Encyclopedia." 2023. https://apt.etda.or.th/cgi-bin/aptgroups.cgi.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32.Stuxnet Dossier." Symantec. https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf.

Feily, Maryam, Alireza Shahrestani, and Sureswaran Ramadass. 2009. "A Survey of Botnet and Botnet Detection." *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 268–73. https://doi.org/10.1109/SECURWARE.2009.48.

Ferrer, Zarestel, and Methusela Cebrian Ferrer. 2010. "In-Depth Analysis of Hydraq - The Face of Cyberwar Enemies Unfolds." http://cybercampaigns.net/wp-content/uploads/2013/05/Hydraq.pdf.

FireEye. 2019. "Cyber Threats to the Financial Services and Insurance Industries." https://web.archive.org/web/20190811091624/https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/ib-finance.pdf.

Fortinet. 2023. "What Is a Watering Hole Attack?" Fortinet. 2023. https://www.fortinet.com/resources/cyberglossary/watering-hole-attack.

Friedberg, Ivo, and Roman Fiedler. 2014. "Dealing with Advanced Persistent Threats in Smart Grid ICT Networks: 5th IEEE Innovative Smart Grid Technologies Conference." Edited by Florian Skopik. *Proceedings of the 5th IEEE Innovative Smart Grid Technologies Conference*, 1–6.

Friedberg, Ivo, Florian Skopik, Giuseppe Settanni, and Roman Fiedler. 2015. "Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection." *Computers & Security* 48 (February):35–57. https://doi.org/10.1016/j.cose.2014.09.006.

García-Teodoro, Pedro, Jesús Díaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. 2009. "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges." *Computers & Security* 28 (February):18–28. https://doi.org/10.1016/j.cose.2008.08.003.

Ghafir, Ibrahim, Mohammad Hammoudeh, Vaclav Prenosil, Liangxiu Han, Robert Hegarty, Khaled Rabie, and Francisco J. Aparicio-Navarro. 2018. "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis." *Future Generation Computer Systems* 89 (December):349–59. https://doi.org/10.1016/j.future.2018.06.055.

Ghafir, Ibrahim, Konstantinos Kyriakopoulos, Francisco Aparicio-Navarro, S. Lambotharan, Basil AsSadhan, and Hamad BinSalleeh. 2018. "A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection." *IEEE Access* PP (July):40008–23. https://doi.org/10.1109/ACCESS.2018.2855078.

Ghafir, Ibrahim, Konstantinos G. Kyriakopoulos, Sangarapillai Lambotharan, Francisco J. Aparicio-Navarro, Basil Assadhan, Hamad Binsalleeh, and Diab M. Diab. 2019. "Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats." *IEEE Access* 7:99508–20. https://doi.org/10.1109/ACCESS.2019.2930200.

Ghafir, Ibrahim, and Vaclav Prenosil. 2014. "Advanced Persistent Threat Attack Detection: An Overview." *International Journal Of Advances In Computer Networks And Its Security*, December, 154.

———. 2016. "Proposed Approach for Targeted Attacks Detection." In *Advanced Computer and Communication Engineering Technology*, edited by Hamzah Asyrani Sulaiman, Mohd Azlishah Othman, Mohd Fairuz Iskandar Othman, Yahaya Abd Rahim, and Naim Che Pee, 73–80. Lecture Notes in Electrical Engineering. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-24584-3_7.

Giura, P., and Wei Wang. 2012. "Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats." *Science*. https://www.semanticscholar.org/paper/Using-Large-Scale-Distributed-Computing-to-Unveil-Giura-Wang/75e702d56a4a90f9c773a0e1fd0074cbe6910ead.

Giura, Paul, and Wei Wang. 2012. "A Context-Based Detection Framework for Advanced Persistent Threats." In *2012 International Conference on Cyber Security*, 69–74. https://doi.org/10.1109/CyberSecurity.2012.16.

Greitzer, Frank L., and Deborah A. Frincke. 2010. "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation." In *Insider Threats in Cyber Security*, edited by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop, 85–113. Advances in Information Security. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-7133-3_5.

Grow, Brian, Keith Epstein, and Chi-Chu Tschang. 2008. "The New E-Spionage Threat." *BusinessWeek*. https://web.archive.org/web/20110418080952/http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm.

Gu, Guofei, Roberto Perdisci, Junjie Zhang, and Wenke Lee. 2008. *BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection*. *CCS'08*.

Guerra-Manzanares, Alejandro, Sven Nõmm, and Hayretdin Bahsi. 2019. "Towards the Integration of a Post-Hoc Interpretation Step into the Machine Learning Workflow for IoT Botnet Detection." In *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, 1162–69. https://doi.org/10.1109/ICMLA.2019.00193.

Gulati, Radha. 2003. "The Threat of Social Engineering and Your Defense Against It | SANS Institute." 2003. https://www.sans.org/white-papers/1232/.

Hachem, Nabil, Yosra Ben Mustapha, Gustavo Gonzalez Granadillo, and Herve Debar. 2011. "Botnets: Lifecycle and Taxonomy." In *2011 Conference on Network and Information Systems Security*, 1–8. https://doi.org/10.1109/SAR-SSI.2011.5931395.

Haddadpajouh, Hamed, Ali Dehghantanha, Raouf Khayami, and Kim-Kwang Raymond Choo. 2018. "A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting." *Future Generation Computer Systems* 85 (March). https://doi.org/10.1016/j.future.2018.03.007.

Hamilton, S., W. L. Miller, Allen Ott, and O. S. Saydjari. 2002. "Challenges in Applying Game Theory to the Domain of Information Warfare †." In . https://www.semanticscholar.org/paper/Challenges-in-Applying-Game-Theory-to-the-Domain-of-Hamilton-Miller/a65d0d3c8aae0f35a524c84d15748f85b01df7de.

Hartigan, John A. 1975. *Clustering Algorithms*. Wiley.

Hasan, Mahmudul, Md Islam, Ishrak Islam, and M.M.A. Hashem. 2019. "Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches," May, 100059. https://doi.org/10.1016/j.iot.2019.100059.

Hassannataj Joloudari, Javad, Mojtaba Haderbadi, Amir Mashmool, Mohammad Ghasemigol, Shahab Shamshirband, and Amir Mosavi. 2020. "Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning." *IEEE Access* 8 (October). https://doi.org/10.1109/ACCESS.2020.3029202.

Hejase, Ale, Hussin Hejase, and Jose Hejase. 2015. "Cyber Warfare Awareness in Lebanon: Exploratory Research." *International Journal of Cyber-Security and Digital Forensics* Vol 4 (September):482–97. https://doi.org/10.17781/P001892.

Hejase, Hussin, Hasan Kazan, and Imad Moukadem. 2020. *Advanced Persistent Threats (APT): An Awareness Review*. https://doi.org/10.13140/RG.2.2.31300.65927.

Hinton, Geoffrey. 2009. "Deep Belief Networks." *Scholarpedia* 4 (January):5947. https://doi.org/10.4249/scholarpedia.5947.

Hochreiter, Sepp, and Jürgen Schmidhuber. 1997. "Long Short-Term Memory." *Neural Computation* 9 (December):1735–80. https://doi.org/10.1162/neco.1997.9.8.1735.

Hodge, Victoria J., and Jim Austin. 2004. "A Survey of Outlier Detection Methodologies." *Artificial Intelligence Review* 22 (2): 85–126. https://doi.org/10.1007/s10462-004-4304-y.

Hofer-Schmitz, Katharina, Ulrike Kleb, and Branka Stojanović. 2021. "The Influences of Feature Sets on the Detection of Advanced Persistent Threats." *Electronics* 10 (6): 704. https://doi.org/10.3390/electronics10060704.

Hofkirchner, Wolfgang, and Mark Burgin. 2017. *Future Information Society, The: Social And Technological Problems*. World Scientific.

Holland, Rick. 2013. "Introducing Forrester's Cyber Threat Intelligence Research." 2013. https://web.archive.org/web/20140415054512/http://blogs.forrester.com/rick_holland/13-02-14-introducing_forresters_cyber_threat_intelligence_research.

Hudson, Barbara. 2013. "Advanced Persistent Threats: Detection, Protection and Prevention." https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Sophos_Advanced_Persistent_Threats.pdf.

Huh, Jun, John Lyle, Cornelius Namiluko, and Andrew Martin. 2011. "Managing Application Whitelists in Trusted Distributed Systems." *Future Generation Comp. Syst.* 27 (February):211–26. https://doi.org/10.1016/j.future.2010.08.014.

Hutchins, Eric, Michael Cloppert, and Rohan Amin. 2011. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare & Security Research* 1 (January).

IC Espionage. 2010. "Shadows In The Cloud: Investigating Cyber Espionage 2.0." https://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

ISACA. 2016. "Book Review: Advanced Persistent Threats." ISACA. 2016. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/advanced-persistent-threats-how-to-manage-the-risk-to-your-business.

IT Governance. 2023. "Advanced Persistent Threats (APTs)." 2023. https://itgovernance.co.uk/advanced-persistent-threats-apt.

Jeun, Inkyung, Youngsook Lee, and Dongho Won. 2012. "A Practical Study on Advanced Persistent Threats." In *Computer Applications for Security, Control and System Engineering*, edited by Tai-hoon Kim, Adrian Stoica, Wai-chi Fang, Thanos Vasilakos, Javier García Villalba, Kirk P. Arnett, Muhammad Khurram Khan, and Byeong-Ho Kang, 144–52. Communications in Computer and Information Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-35264-5_21.

Jia, Bin, Zhaowen Lin, and Yan Ma. 2015. *Advanced Persistent Threat Detection Method Research Based on Relevant Algorithms to Artificial Immune System*. Vol. 520. https://doi.org/10.1007/978-3-662-47401-3_29.

Johnson, Ariana. 2016. "Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation." *North Carolina Banking Institute* 20 (1): 277.

Johnson, John, and Emilie Hogan. 2013. *A Graph Analytic Metric for Mitigating Advanced Persistent Threat*. Vol. 129. https://doi.org/10.1109/ISI.2013.6578801.

Kaspersky. 2015. "The Duqu 2.0." https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

———. 2023a. "Targeted Cyberattacks Logbook." APT Kaspersky Securelist. 2023. https://apt.securelist.com.

———. 2023b. "What Is an Advanced Persistent Threat (APT)?" www.kaspersky.com. April 19, 2023. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.

Kaushik, Atul, Emmanuel Pilli, and R. Joshi. 2010. *Network Forensic System for Port Scanning Attack*. https://doi.org/10.1109/IADCC.2010.5422935.

Kholidy, Hisham A., Abdelkarim Erradi, Sherif Abdelwahed, and Abdulrahman Azab. 2014. "A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems."

2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, August, 14–19. https://doi.org/10.1109/DASC.2014.12.

Kim, Hyunjoo, Jonghyun Kim, Ikkyun Kim, and Tai-myung Chung. 2015. "Behavior-Based Anomaly Detection on Big Data." *Australian Information Security Management Conference*, January. https://doi.org/10.4225/75/57b69d1ed938e.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. "Advanced Social Engineering Attacks." *Journal of Information Security and Applications*, Special Issue on Security of Information and Networks, 22 (June):113–22. https://doi.org/10.1016/j.jisa.2014.09.005.

Kyriakopoulos, Kostas, Francisco J. Aparicio-Navarro, Ibrahim Ghafir, Sangarapillai Lambotharan, and Jonathon Chambers. 2018. *Multi-stage attack detection using contextual information*. Loughborough University. https://doi.org/10.1109/MILCOM.2018.8599708'].

Langner, Ralph. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security & Privacy* 9 (3): 49–51. https://doi.org/10.1109/MSP.2011.67.

Lee, Bernard, Manmeet (Mandy) Mahinderjit Singh, and Azizul Rahman Mohd Shariff. 2019. "APTGuard : Advanced Persistent Threat (APT) Detections and Predictions Using Android Smartphone: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018." In , 545–55. https://doi.org/10.1007/978-981-13-2622-6_53.

Lee, Martin. 2011. "Clustering Disparate Attacks: Mapping The Activities of The Advanced Persistent Threat." *21st Virus Bulletin International Conference*, October. https://www.academia.edu/2352875/CLUSTERING_DISPARATE_ATTACKS_MAPPING_THE_ACTIVITIES_OF_THE_ADVANCED_PERSISTENT_THREAT.

Lemay, Antoine, Joan Calvet, François Menet, and José M. Fernandez. 2018. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors." *Computers & Security* 72 (January):26–59. https://doi.org/10.1016/j.cose.2017.08.005.

Lim, Joo, Shanton Chang, Sean Maynard, and Atif Ahmad. 2009. "Exploring the Relationship between Organizational Culture and Information Security Culture." *Australian Information Security Management Conference*, December. https://doi.org/10.4225/75/57b4065130def.

Lin, Min, Qiang Chen, and Shuicheng Yan. 2013. "Network In Network." *CoRR*, December. https://www.semanticscholar.org/paper/Network-In-Network-Lin-Chen/5e83ab70d0cbc003471e87ec306d27d9c80ecb16.

Liu, Yali, Cherita Corbett, Ken Chiang, Rennie Archibald, Biswanath Mukherjee, and Dipak Ghosal. 2009. *SIDD: A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack*. *Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2009.390.

Lo, Chi-Chun, and Wan-Jia Chen. 2012. "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences between Controls." *Expert Systems with Applications* 39 (1): 247–57. https://doi.org/10.1016/j.eswa.2011.07.015.

Lockheed Martin. 2023. "Cyber Kill Chain®." Lockheed Martin. 2023. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Mahadevan, Vijay, Wei-Xin LI, Viral Bhalodia, and Nuno Vasconcelos. 2010. *Anomaly Detection in Crowded Scenes*. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. https://doi.org/10.1109/CVPR.2010.5539872.

Maloney, Sarah. 2018. "What Is an Advanced Persistent Threat (APT)?" 2018. https://www.cybereason.com/blog/advanced-persistent-threat-apt.

Mandiant. 2013. "APT1 | Exposing One of China's Cyber Espionage Units." Mandiant. 2013. https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units.

———. 2021. "Today's Top Cyber Trends & Attacks Insights | M-Trends 2021." Mandiant. 2021. https://www.mandiant.com/resources/reports/m-trends-2021.

Manhas, Jatinder, and Shallu Kotwal. 2021. "Implementation of Intrusion Detection System for Internet of Things Using Machine Learning Techniques." In , edited by Kaiser J. Giri, Shabir Ahmad Parah, Rumaan Bashir, and Khan Muhammad, 217–37. Algorithms for Intelligent Systems. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-8711-5_11.

Marchetti, Mirco, Fabio Pierazzi, Michele Colajanni, and Alessandro Guido. 2016. "Analysis of High Volumes of Network Traffic for Advanced Persistent Threat Detection." *Computer Networks* 109 (June). https://doi.org/10.1016/j.comnet.2016.05.018.

Matthews, Tim. 2019. "Operation Aurora – 2010's Major Breach by Chinese Hackers." Exabeam. January 8, 2019. https://www.exabeam.com/information-security/operation-aurora/.

McAfee. 2010a. "Protecting Your Critical Assets." https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

———. 2010b. "Protecting Your Critical Assets - Lessons Learned from 'Operation Aurora.'" https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

———. 2018. "The Economic Impact of Cybercrime No Slowing Down." https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

McDermott, Christopher D., Farzan Majdani, and Andrei V. Petrovski. 2018. "Botnet Detection in the Internet of Things Using Deep Learning Approaches." In *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–8. https://doi.org/10.1109/IJCNN.2018.8489489.

McHugh, John. 2000. "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory." *ACM Transactions on Information and System Security* 3 (4): 262–94. https://doi.org/10.1145/382912.382923.

McMahon, Dave, and Rafal Rohozinski. 2013. "The Dark Space Project: Defence R&D Canada – Centre for Security Science Contractor Report DRDC CSS CR 2013-007."

Merz, Terry. 2019. "A Context-Centred Research Approach to Phishing and Operational Technology in Industrial Control Systems | Journal of Information Warfare." 2019. https://www.jinfowar.com/journal/volume-18-issue-4/context-centred-research-approach-phishing-operational-technology-industrial-control-systems.

Messier, Ric. 2013. *GSEC GIAC Security Essentials Certification All-in-One Exam Guide*. McGraw Hill Professional.

Microsoft. 2022. "Threats - Microsoft Threat Modeling Tool - Azure - STRIDE." August 25, 2022. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Milajerdi, Sadegh M., Rigel Gjomemo, Birhanu Eshete, R. Sekar, and V.N. Venkatakrishnan. 2019. "HOLMES: Real-Time APT Detection through Correlation of Suspicious

Information Flows." In *2019 IEEE Symposium on Security and Privacy (SP)*, 1137–52. https://doi.org/10.1109/SP.2019.00026.

Mitnick, Kevin D., and William L. Simon. 2011. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

MITRE. 2021. "MiniDuke, Software S0051 | MITRE ATT&CK®." 2021. https://attack.mitre.org/software/S0051/.

Montgomery, Douglas C., Elizabeth A. Peck, and G. Geoffrey Vining. 2012. *Introduction to Linear Regression Analysis*. John Wiley & Sons.

Moon, Daesung, Hyungjin Im, Jae Dong Lee, and Jong Hyuk Park. 2014. "MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats." *Symmetry* 6 (4): 997–1010. https://doi.org/10.3390/sym6040997.

Muszyński, Józef, and Greg Shipley. 2008. "Narzędzia SIEM (Security Information and Event Management)." Computerworld. 2008. https://www.computerworld.pl/news/Narzedzia-SIEM-Security-Information-and-Event-Management,325855.html.

Nance, Kara, and Matt Bishop. 2017. *Introduction to Deception, Digital Forensics, and Malware Minitrack*. https://doi.org/10.24251/HICSS.2017.731.

Nar, Kamil, and S. Shankar Sastry. 2018. "An Analytical Framework to Address the Data Exfiltration of Advanced Persistent Threats." In *2018 IEEE Conference on Decision and Control (CDC)*, 867–73. https://doi.org/10.1109/CDC.2018.8619834.

Nicho, Mathew, and Christopher D. McDermott. 2019. "Dimensions of 'Socio' Vulnerabilities of Advanced Persistent Threats." In *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1–5. https://doi.org/10.23919/SOFTCOM.2019.8903788.

Nick. 2018. "Turla APT Group's Espionage Campaigns Now Employs Adobe Flash Installer and Ingenious Social Engineering." *Cyber Defense Magazine* (blog). January 16, 2018. https://www.cyberdefensemagazine.com/turla-apt-groups-espionage-campaigns-now-employs-adobe-flash-installer-and-ingenious-social-engineering/.

Nissim, Nir, Aviad Cohen, Chanan Glezer, and Yuval Elovici. 2015. "Detection of Malicious PDF Files and Directions for Enhancements: A State-of-the Art Survey." *Computers & Security* 48 (February):246–66. https://doi.org/10.1016/j.cose.2014.10.014.

NIST, Initiative Joint Task Force Transformation. 2011. "Managing Information Security Risk: Organization, Mission, and Information System View." NIST Special Publication (SP) 800-39. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39.

Nunes, Eric, Ahmad Diab, Andrew Gunn, Ericsson Marin, Vineet Mishra, Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, and Paulo Shakarian. 2016. *Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence*. https://doi.org/10.1109/ISI.2016.7745435.

Oehmen, Christopher, Elena Peterson, and Scott Dowson. 2010. "An Organic Model for Detecting Cyber-Events." In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1–4. CSIIRW '10. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1852666.1852740.

Paganini, Pierluigi. 2019. "Iran-Linked APT33 Updates Infrastructure Following Its Public Disclosure." Security Affairs. July 1, 2019. https://securityaffairs.com/87784/apt/apt33-updates-infrastructure.html.

Park, Seong-Taek, Guozhong Li, and Jae-Chang Hong. 2020. "A Study on Smart Factory-Based Ambient Intelligence Context-Aware Intrusion Detection System Using Machine Learning." *Journal of Ambient Intelligence and Humanized Computing* 11 (4): 1405–12. https://doi.org/10.1007/s12652-018-0998-6.

Parrish, Jr, James L., Janet L. Bailey, and James F. Courtney. 2009. "A Personality Based Model for Determining Susceptibility to Phishing Attacks." http://www.swdsi.org/swdsi2009/papers/9J05.pdf.

Peikert, Chris. 2016. "A Decade of Lattice Cryptography." *Foundations and Trends® in Theoretical Computer Science* 10 (4): 283–424. https://doi.org/10.1561/0400000074.

Pfleeger, Shari, Angela Sasse, and Adrian Furnham. 2014. "From Weakest Link to Security Hero: Transforming Staff Security Behavior." *Journal of Homeland Security and Emergency Management* 11 (December). https://doi.org/10.1515/jhsem-2014-0035.

Probst, Philipp, Marvin N. Wright, and Anne-Laure Boulesteix. 2019. "Hyperparameters and Tuning Strategies for Random Forest." *WIREs Data Mining and Knowledge Discovery* 9 (3): e1301. https://doi.org/10.1002/widm.1301.

PWC. 2014. "Managing Cyber Risks in an Interconnected World." https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Quintero-Bonilla, Santiago, and Angel Martín del Rey. 2020. "A New Proposal on the Advanced Persistent Threat: A Survey." *Applied Sciences* 10 (11): 3874. https://doi.org/10.3390/app10113874.

Rachmadi, Salman, Satria Mandala, and Dita Oktaria. 2021. "Detection of DoS Attack Using AdaBoost Algorithm on IoT System." In *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 28–33. https://doi.org/10.1109/ICoDSA53588.2021.9617545.

Radzikowski, Shem. 2015. "CyberSecurity: Origins of the Advanced Persistent Threat (APT)." Dr.Shem. October 8, 2015. https://DrShem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/.

Rafique, M. Zubair, Ping Chen, Christophe Huygens, and Wouter Joosen. 2014. "Evolutionary Algorithms for Classification of Malware Families through Different Network Behaviors." In *Proceedings of the 2014 Annual Conference on Genetic and Evolutionary Computation*, 1167–74. GECCO '14. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2576768.2598238.

Rass, Stefan, Sandra König, and Stefan Schauer. 2017. "Defending Against Advanced Persistent Threats Using Game-Theory." *PLOS ONE* 12 (1): e0168675. https://doi.org/10.1371/journal.pone.0168675.

Roldán, José, Juan Boubeta-Puig, José Luis Martínez, and Guadalupe Ortiz. 2020. "Integrating Complex Event Processing and Machine Learning: An Intelligent Architecture for Detecting IoT Security Attacks." *Expert Systems with Applications* 149 (July):113251. https://doi.org/10.1016/j.eswa.2020.113251.

Rot, Artur. 2009. "Enterprise Information Technology Security: Risk Management Perspective." *Lecture Notes in Engineering and Computer Science* 2179 (October).

———. 2016. "Zarządzanie Ryzykiem w Cyberprzestrzeni – Wybrane Zagadnienia Teorii i Praktyki." In , 35–50.

Rot, Artur, and Bogusław Olszewski. 2017. *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*. https://doi.org/10.15439/2017F488.

Rowe, Mark. 2013. "Advanced Persistent Threats: How to Manage the Risk to Your Business." Professional Security. October 11, 2013. https://professionalsecurity.co.uk/reviews/advanced-persistent-threats-how-to-manage-the-risk-to-your-business/.

Russell, Chelsa. 2002. "Security Awareness - Implementing an Effective Strategy | SANS Institute." 2002. https://www.sans.org/white-papers/418/.

SANS. 2013. "Assessing Outbound Traffic to Uncover Advanced Persistent Threat." SANS Technology Institute.

Santoro, Diego, Gines Escudero-Andreu, Kostas Kyriakopoulos, Francisco J. Aparicio-Navarro, David J. Parish, and M. Vadursi. 2017. "A hybrid intrusion detection system for virtual jamming attacks on wireless networks," January, 79–87. https://doi.org/10.1016/j.measurement.2017.05.034'].

Sasaki, Takayuki. 2011. "Towards Detecting Suspicious Insiders by Triggering Digital Data Sealing." In *2011 Third International Conference on Intelligent Networking and Collaborative Systems*, 637–42. Fukuoka, Japan: IEEE. https://doi.org/10.1109/INCoS.2011.157.

Schatz, Daniel, Rabih Bashroush, and Julie Wall. 2017. "Towards a More Representative Definition of Cyber Security." *Journal of Digital Forensics, Security and Law* 12 (2). https://doi.org/10.15394/jdfsl.2017.1476.

Schmid, M., F. Hill, and A.K. Ghosh. 2002. "Protecting Data from Malicious Software." *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 199–208. https://doi.org/10.1109/CSAC.2002.1176291.

Schubert, Erich, Jörg Sander, Martin Ester, Hans Kriegel, and Xiaowei Xu. 2017. "DBSCAN Revisited, Revisited: Why and How You Should (Still) Use DBSCAN." *ACM Transactions on Database Systems* 42 (July):1–21. https://doi.org/10.1145/3068335.

SecureList. 2013. "'Red October' Diplomatic Cyber Attacks Investigation." January 14, 2013. https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/.

Sexton, Joseph, Curtis Storlie, and Joshua Neil. 2015. "Attack Chain Detection." *Statistical Analysis and Data Mining: The ASA Data Science Journal* 8 (5–6): 353–63. https://doi.org/10.1002/sam.11296.

Shalaginov, Andrii, Katrin Franke, and Xiongwei Huang. 2016. *Malware Beaconing Detection by Mining Large-Scale DNS Logs for Targeted Attack Identification*.

Shamah, David. n.d. "Cyber Espionage Bug Attacking Middle East, but Israel Untouched — so Far." Accessed December 12, 2023. http://www.timesofisrael.com/new-cyber-bug-targeting-middle-east-but-israel-untouched-so-far/.

Sharma, Pradip Kumar, Seo Yeon Moon, Daesung Moon, and Jong Hyuk Park. 2017. "DFA-AD: A Distributed Framework Architecture for the Detection of Advanced Persistent Threats." *Cluster Computing* 20 (1): 597–609. https://doi.org/10.1007/s10586-016-0716-0.

Shenwen, Lin, Li Yingbo, and Du Xiongjie. 2015. "Study and Research of APT Detection Technology Based on Big Data Processing Architecture." *2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, May, 313–16. https://doi.org/10.1109/ICEIEC.2015.7284547.

Shevchenko, Nataliya, Timothy A. Chick, Paige O'Riordan, and Thomas Patrick Scanlon. 2018. "Threat Modeling: A Summary of Available Methods." https://apps.dtic.mil/sti/citations/AD1084024.

Shin, Seongjun, Seungmin Lee, Hyunwoo Kim, and Sehun Kim. 2013. "Advanced Probabilistic Approach for Network Intrusion Forecasting and Detection." *Expert Systems with Applications* 40 (January):315–22. https://doi.org/10.1016/j.eswa.2012.07.057.

Shirey, Rob. 2000. "Internet Security Glossary." Request for Comments RFC 2828. Internet Engineering Task Force. https://doi.org/10.17487/RFC2828.

Siddiqui, Sana, Salman Khan, K. Ferens, and Witold Kinsner. 2016. *Detecting Advanced Persistent Threats Using Fractal Dimension Based Machine Learning Classification*. https://doi.org/10.1145/2875475.2875484.

Sigholm, Johan, and Martin Bang. 2013. *Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats*. https://doi.org/10.1109/EISIC.2013.37.

SignalSense. 2015. "Using Deep Learning To Detect Threat, SignalSense, White Paper,." https://www.ten-inc.com/presentations/deep_learning.pdf.

Sim, Kevin, Emma Hart, and Ben Paechter. 2014. "A Lifelong Learning Hyper-Heuristic Method for Bin Packing." *Evolutionary Computation* 23 (February). https://doi.org/10.1162/EVCO_a_00121.

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

Singh, Abhishek, and Zheng Bu. 2014. "Hot Knives Through Butter: Bypassing Automated Analysis Systems (Black Hat USA 2013) - InfoconDB." 2014. https://infocondb.org/con/black-hat/black-hat-usa-2013/hot-knives-through-butter-bypassing-automated-analysis-systems.

Smart, Steven J. 2011. "Joint Targeting in Cyberspace." https://apps.dtic.mil/sti/citations/ADA555785.

Soong, T. T. 2004. "Fundamentals of Probability and Statistics for Engineers | Wiley." Wiley.Com. 2004. https://www.wiley.com/en-us/Fundamentals+of+Probability+and+Statistics+for+Engineers-p-9780470868157.

Sriram, S., R. Vinayakumar, Mamoun Alazab, and Soman KP. 2020. "Network Flow Based IoT Botnet Attack Detection Using Deep Learning." In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 189–94. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668.

Stevens, Tim. 2018. "Global Cybersecurity: New Directions in Theory and Methods." *Politics and Governance* 6 (2): 1–4. https://doi.org/10.17645/pag.v6i2.1569.

Swisscom. 2019. "Report on the Threat Situation | SME | Swisscom." 2019. https://www.swisscom.ch/en/business/sme/downloads/report-threat-situation-switzerland-2019.html.

Symantec. 2018a. "2018 Internet Security Threat Report." https://docs.broadcom.com/doc/istr-23-executive-summary-en.

———. 2018b. "Advanced Persistent Threats: A Symantec Perspective." https://web.archive.org/web/20180508161501/https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

Taddeo, Mariarosaria. 2012. "An Analysis for a Just Cyber Warfare." In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–10. https://ieeexplore.ieee.org/document/6243976.

Tanaka, Yasuyuki, Mitsuaki Akiyama, and Atsuhiro Goto. 2017. "Analysis of Malware Download Sites by Focusing on Time Series Variation of Malware." *Journal of Computational Science* 22 (September):301–13. https://doi.org/10.1016/j.jocs.2017.05.027.

Tankard, Colin. 2011. "Advanced Persistent Threats and How to Monitor and Deter Them." *Network Security* 2011 (8): 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1.

Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. 2009. "A Detailed Analysis of the KDD CUP 99 Data Set." In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1–6. https://doi.org/10.1109/CISDA.2009.5356528.

Tollefson, Rodika. 2020. "ICS/SCADA Malware Threats | Infosec." 2020. https://resources.infosecinstitute.com/topics/scada-ics-security/ics-scada-malware-threats/.

Townsend, Kevin. 2018. "Knowing Value of Data Assets Is Crucial to Cybersecurity Risk Management." SecurityWeek. December 3, 2018. https://www.securityweek.com/knowing-value-data-assets-crucial-cybersecurity-risk-management/.

Trend. 2012. "Spear-Phishing Email: Most Favored APT Attack Bait." https://documents.trendmicro.com/assets/wp/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

Ussath, Martin, David Jaeger, Feng Cheng, and Christoph Meinel. 2016. "Advanced Persistent Threats: Behind the Scenes." *2016 Annual Conference on Information Science and Systems (CISS)*, March, 181–86. https://doi.org/10.1109/CISS.2016.7460498.

Villeneuve, Nart, and James Bennett. 2012. "Detecting APT Activity with Network Traffic Analysis." https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf.

Villeneuve, Nart, and James T. Bennett. 2014. "XtremeRAT: Nuisance or Threat?" Mandiant. 2014. https://www.mandiant.com/resources/blog/xtremerat-nuisance-or-threat.

Virvilis, Nikos, and Dimitris Gritzalis. 2013. "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?" In *2013 International Conference on Availability, Reliability and Security*, 248–54. https://doi.org/10.1109/ARES.2013.32.

Virvilis, Nikos, Dimitris Gritzalis, and Theodoros Apostolopoulos. 2013. "Trusted Computing vs. Advanced Persistent Threats: Can a Defender Win This Game?" In *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, 396–403. https://doi.org/10.1109/UIC-ATC.2013.80.

Vukalovic, J., and Damir Delija. 2015. *Advanced Persistent Threats - Detection and Defense*. https://doi.org/10.1109/MIPRO.2015.7160480.

Wahla, Arfan, Lan Chen, Yali Wang, Rong Chen, and Fan Wu. 2019. "Automatic Wireless Signal Classification in Multimedia Internet of Things: An Adaptive Boosting Enabled Approach." *IEEE Access* PP (November):1–1. https://doi.org/10.1109/ACCESS.2019.2950989.

Wang, Xiali, and Xiang Lu. 2020. "A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices." *Wireless Communications and Mobile Computing* 2020 (October):1–13. https://doi.org/10.1155/2020/8838571.

Wang, Xu, Kangfeng Zheng, Xinxin Niu, Bin Wu, and Chunhua Wu. 2016. "Detection of Command and Control in Advanced Persistent Threat Based on Independent Access." In

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

Wang, Yuan, Yongjun Wang, Jing Liu, and Zhijian Huang. 2014. "A Network Gene-Based Framework for Detecting Advanced Persistent Threats." In *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 97–102. https://doi.org/10.1109/3PGCIC.2014.41.

Wang, Yuan, Yongjun Wang, Jing Liu, Zhijian Huang, and Peidai Xie. 2016. *A Survey of Game Theoretic Methods for Cyber Security*. https://doi.org/10.1109/DSC.2016.90.

Waqas, Muhammad, Kamlesh Kumar, Asif Ali Laghari, Umair Saeed, Muhammad Malook Rind, Aftab Ahmed Shaikh, Fahad Hussain, Athaul Rai, and Abdul Qayoom Qazi. 2022. "Botnet Attack Detection in Internet of Things Devices over Cloud Environment via Machine Learning." *Concurrency and Computation: Practice and Experience* 34 (4): e6662. https://doi.org/10.1002/cpe.6662.

Wright, John, Yi Ma, Julien Mairal, Guillermo Sapiro, Thomas S. Huang, and Shuicheng Yan. 2010. "Sparse Representation for Computer Vision and Pattern Recognition." *Proceedings of the IEEE* 98 (6): 1031–44. https://doi.org/10.1109/JPROC.2010.2044470.

Wu, Xindong, Vipin Kumar, J. Ross Quinlan, Joydeep Ghosh, Qiang Yang, Hiroshi Motoda, Geoffrey J. McLachlan, et al. 2008. "Top 10 Algorithms in Data Mining." *Knowledge and Information Systems* 14 (1): 1–37. https://doi.org/10.1007/s10115-007-0114-2.

Xu, Lei, Chunxiao Jiang, Jian Wang, Yong Ren, Jian Yuan, and Mohsen Guizani. 2015. "Game Theoretic Data Privacy Preservation: Equilibrium and Pricing." In *2015 IEEE International Conference on Communications (ICC)*, 7071–76. https://doi.org/10.1109/ICC.2015.7249454.

Yadav, Sandeep, Ashwath Kumar Krishna Reddy, A. L. Narasimha Reddy, and Supranamaya Ranjan. 2012. "Detecting Algorithmically Generated Domain-Flux Attacks With DNS Traffic Analysis." *IEEE/ACM Transactions on Networking* 20 (5): 1663–77. https://doi.org/10.1109/TNET.2012.2184552.

Yan, Xiaohuan, and J. Zhang. 2013. "A Early Detection of Cyber Security Threats Using Structured Behavior Modeling." In . https://www.semanticscholar.org/paper/A-Early-Detection-of-Cyber-Security-Threats-using-Yan-Zhang/92b0c21afbf1941cb27e707c50e51bd76a8b1d45.

Yang, Lu Xing, Pengdeng Li, Xiaofan Yang, and Yuan Yan Tang. 2017. "Security Evaluation of the Cyber Networks under Advanced Persistent Threats." *IEEE Access* 5 (8053761): 20111–23. https://doi.org/10.1109/ACCESS.2017.2757944.

Yasar, Kinza, and Linda Rosencrance. 2021. "What Is an Advanced Persistent Threat (APT)? | Definition from TechTarget." Security. 2021. https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT.

Zhang, Chongzhen, Yanli Chen, Yang Meng, Fangming Ruan, Runze Chen, Yidan Li, and Yaru Yang. 2021. "A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques." Edited by Savio Sciancalepore. *Security and Communication Networks* 2021 (January):1–15. https://doi.org/10.1155/2021/6610675.

Zhang, Ru, Yanyu Huo, Jianyi Liu, and Fangyu Weng. 2017. "Constructing APT Attack Scenarios Based on Intrusion Kill Chain and Fuzzy Clustering." *Security and Communication Networks* 2017 (December):e7536381. https://doi.org/10.1155/2017/7536381.

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-

Supervised Learning and Complex Networks Characteristics." *Future Generation Computer Systems* 106 (May):501–17. https://doi.org/10.1016/j.future.2020.01.032.

Zions Bancorporation. 2012. "A Case Study In Security Big Data Analysis." 2012. https://www.darkreading.com/cybersecurity-analytics/a-case-study-in-security-big-data-analysis.

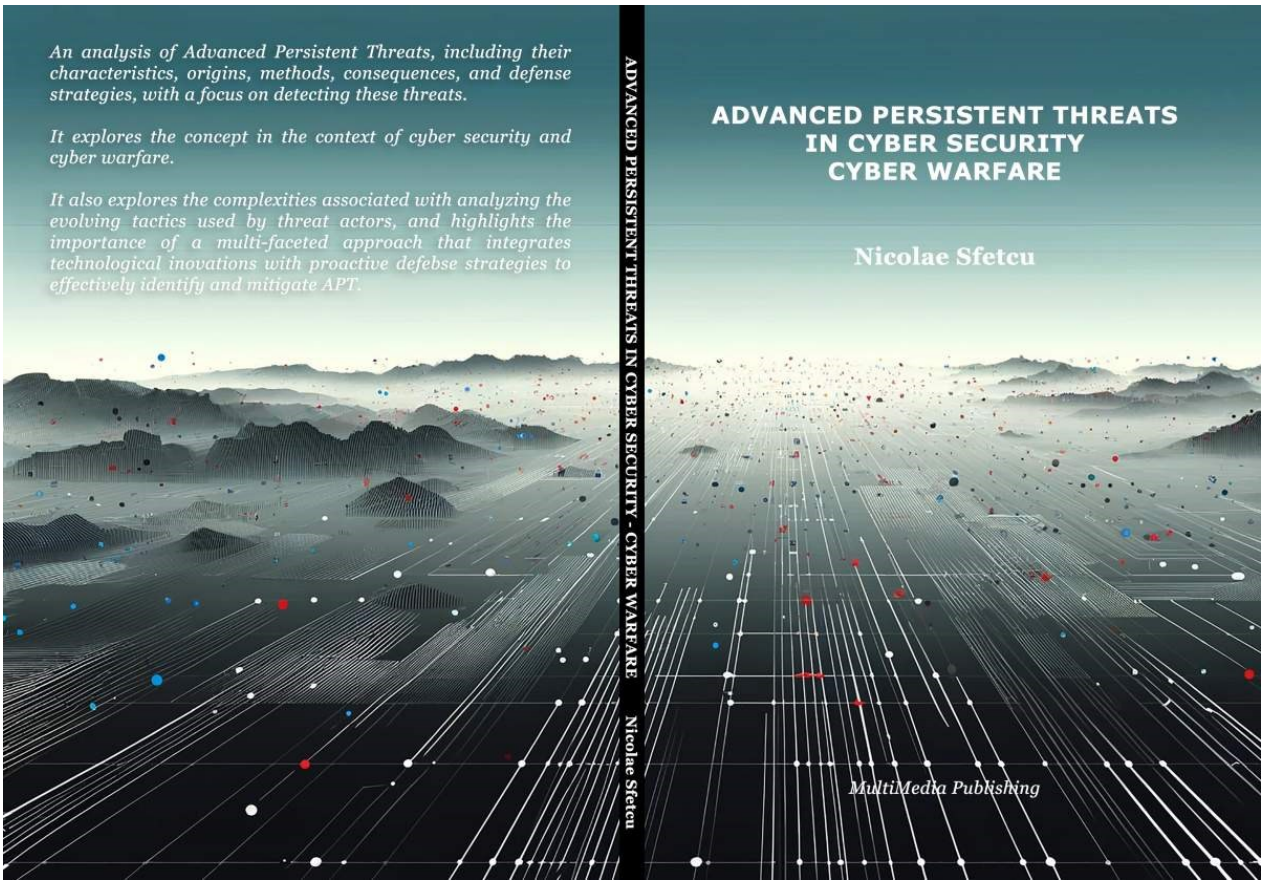
Zou, Qingtian, Xiaoyan Sun, Peng Liu, and Anoop Singhal. 2020. "An Approach for Detection of Advanced Persistent Threat Attacks," no. 12 (December), 92–26. https://doi.org/10.1109/MC.2020.3021548.

Content

Book

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 https://www.telework.ro/en/e-books/advanced-persistent-threats-in-cybersecurity-cyber-warfare/ https://www.cartilibrarie.com/carte/advanced-persistent-threats-in-cybersecurity-cyber-warfare/

Digital: EPUB (ISBN 978-606-033-851-2), Kindle (ISBN 978-606-033-852-9) PDF (ISBN 978-606-033-853-6)

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/