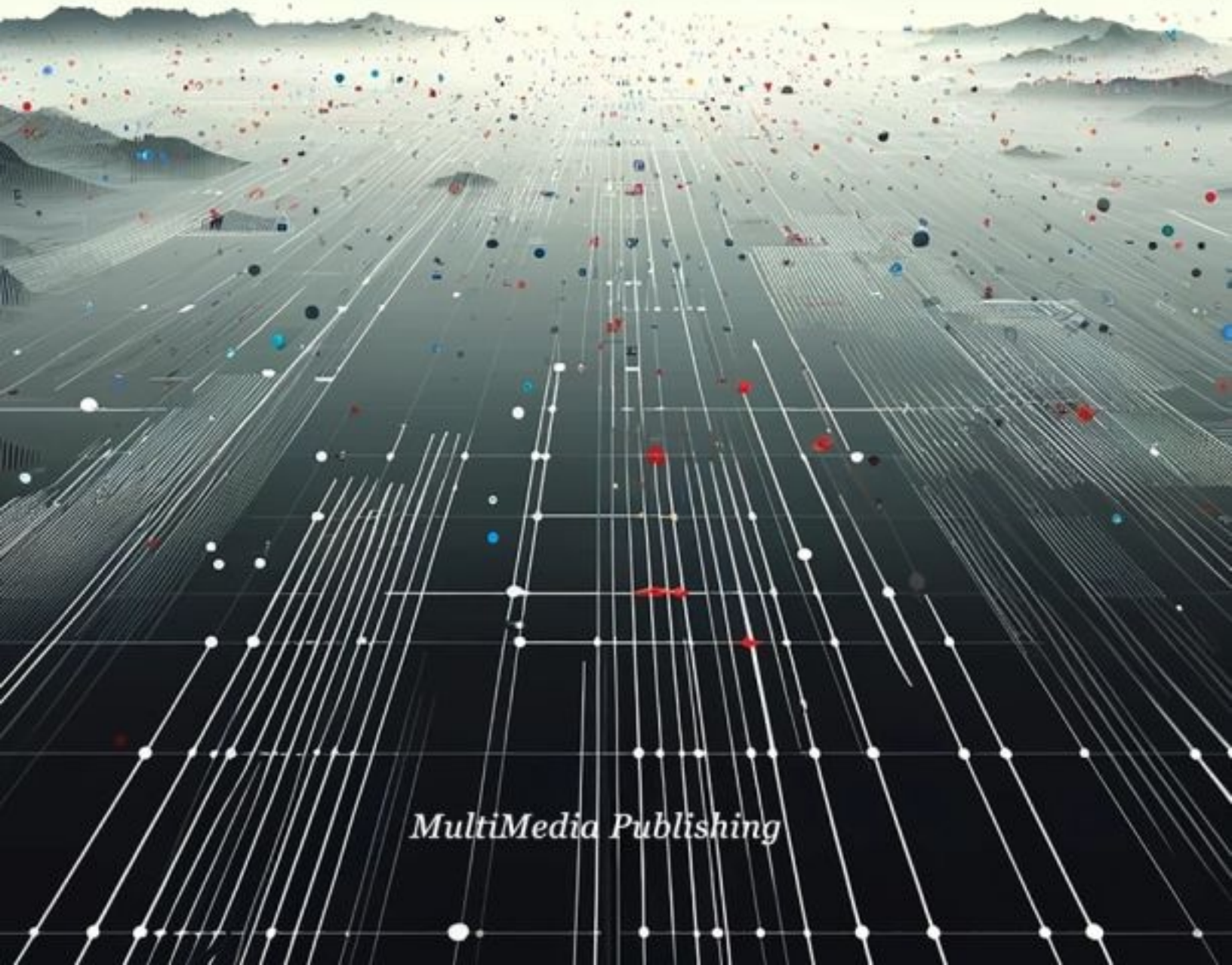
AMENINȚĂRILE PERSISTENTE AVANSATE ÎN SECURITATEA CIBERNETICĂ RĂZBOIUL CIBERNETIC

Nicolae Sfetcu



MultiMedia Publishing

Amenințările persistente avansate în securitatea cibernetică – Războiul cibernetic

Nicolae SFETCU
nicolae@sfetcu.com[1]

Sfetcu, Nicolae (2024), *Detectarea amenințărilor persistente avansate în securitatea cibernetică și războiul cibernetic*, MultiMedia Publishing, ISBN 978-606-033-828-4, DOI: 10.58679/MM92932, https://www.telework.ro/ro/e-books/amenintarile-persistente-avansate-in-securitatea-cibernetica-razboiul-cibernetic/

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

Cuprins

Amenințările persistente avansate în securitatea cibernetică – Războiul cibernetic

Nicolae SFETCU

Detection of Advanced Persistent Threats in Cyber Security and Cyber Warfare

Abstract

This essay 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. He 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. This 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. The essay 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, cyber security. cyber warfare, threat detection

Rezumat

Acest eseu își propune să ofere o analiză cuprinzătoare a Amenințărilor Persistente Avansate (Advanced Persistent Threats, APT), inclusiv caracteristicile, originile, metodele, consecințele și strategiile de apărare ale acestora, cu accent pe detectarea acestor amenințări. El explorează conceptul de amenințări persistente avansate în contextul securității cibernetice și al războiului cibernetic. APT reprezintă una dintre cele mai insidioase și provocatoare forme de amenințări cibernetice, caracterizate prin sofisticarea, persistența și natura lor țintită. Această lucrare analizează originile, caracteristicile și metodele folosite de actorii APT. De asemenea, explorează complexitățile asociate cu detectarea APT, analizând tacticile evolutive folosite de actorii amenințărilor și a progreselor corespunzătoare în metodologiile de detectare. Eseul subliniază importanța abordării cu mai multe fațete, care integrează inovații tehnologice cu strategii proactive de apărare pentru a identifica în mod eficient și atenua APT.

Cuvinte cheie: Amenințări Persistente Avansate, Advanced Persistent Threats, APT, securitate cibernetică. război cibernetic, detectarea amenințărilor

Amenințările Persistente Avansate (APT)

Amenințările persistente avansate (APT) sunt o clasă de amenințări cibernetice care reprezintă o provocare semnificativă pentru organizații și națiuni din întreaga lume. Ele sunt cunoscute pentru tacticile, tehnicile și procedurile lor avansate, precum și pentru capacitatea lor de a se infiltra și de a opera în mod persistent în sistemele țintă pentru perioade îndelungate.

APT sunt coordonate de obicei de un stat sau un grup sponsorizat de stat [23]. Motivațiile acestor actori de amenințare sunt de obicei de spionaj militar, geopolitice sau economice[4]. Aceste sectoare vizate includ guvernul, apărarea, serviciile financiare, serviciile juridice, industria, telecomunicațiile, bunurile de larg consum și multe altele[5].

„Timpul de contact" mediu, în care un atac APT trece nedetectat, a fost în medie în 2018 de 71 de zile în America de Nord, 177 de zile în EMEA, și 204 zile în APAC[6].

Amenințările persistente avansate combină o varietate de forme diferite de atac, de la inginerie socială la exploatări tehnice. În general în APT se folosesc vectori tradiționali de spionaj[7], inclusiv ingineria socială, inteligența umană și infiltrarea, pentru atacurile în rețea, instalând programe malware personalizate (software rău intenționat)[8]. Diversitatea și discreția APT le transformă într-o problemă centrală a securității sistemelor cibernetice, datorită caracterului asimetric al atacurilor, apelându-se adesea la teoria jocurilor pentru modelarea conflictului folosind jocuri matrice ca instrument de atenuare a riscurilor. Modelele APT teoretice ale jocurilor pot fi derivate direct din analiza vulnerabilității topologice, împreună cu evaluările riscurilor, în conformitate cu standardele comune de management al riscului, cum ar fi familia ISO 31000[9].

Creșterea eterogenității, conectivității și deschiderii sistemelor informaționale permit accesul într-un sistem prin multiple căi diferite. Pentru a asigura securitatea, se folosesc instrumente și tehnici semi-automatizate pentru a detecta și a atenua vulnerabilitățile, dar astfel de atacuri se adaptează rapid la aceste . configurații, astfel încât să rămână „sub radar".

[2] Kaspersky, „What Is an Advanced Persistent Threat (APT)?"
[3] Cisco, „What Is an Advanced Persistent Threat (APT)?"
[4] Cole, *Advanced Persistent Threat*.
[5] FireEye, „Cyber Threats to the Financial Services and Insurance Industries".
[6] Mandiant, „Today's Top Cyber Trends & Attacks Insights | M-Trends 2021".
[7] Ghafir și Prenosil, „Advanced Persistent Threat Attack Detection".
[8] Symantec, „Advanced Persistent Threats: A Symantec Perspective".
[9] Rass, König, și Schauer, „Defending Against Advanced Persistent Threats Using Game-Theory".

Contramăsurile au o latență mai mare, fiind ineficiente pentru schimbări bruște ale strategiilor de atac ale unui adversar invizibil[10].

Amenințările persistente avansate au apărut ca o versiune nouă și complexă a atacurilor în mai multe etape (multi-stage attacks, MSA)[11], în condițiile în care sistemele actuale de detectare a APT se concentrează mai degrabă pe apariția alertelor de detectare, decât pe prezicerea amenințărilor[12]. Prognoza etapelor APT nu numai că dezvăluie ciclul de viață APT în stadiile sale incipiente, dar ajută și la înțelegerea strategiilor și obiectivelor atacatorului. În plus, Internetul obiectelor (IoT) face ca dispozitivele conectate la internet să devină ținte ușoare pentru atacurile cibernetice[13]. Costul global al criminalității cibernetice a atins 600 de miliarde de dolari în 2018, conform unui raport McAfee[14].

Pentru a contracara atacurile cibernetice, analiștii folosesc de obicei sisteme de detectare a intruziunilor (Intrusion Detection Systems, IDS) prin potrivirea tiparelor de atacuri cunoscute (bazate pe semnături, prin compararea datelor cu o bază de date care conține o listă de semnături de atac cunoscute) sau observarea anomaliilor (abaterea de la un profil de referință)[15].Obiectivul vizat al APT este spionajul și exfiltrarea datelor. Atacul poate dura săptămâni sau ani, cu perioade foarte lungi între etapele atacului. făcând dificilă detectarea acestuia prin corelarea mai multor alerte în timpul ciclului de viață a APT[16]. Metodele tradiționale de potrivire a modelelor sunt ineficiente în cazul APT, întrucât nu există un tipar al ordinei și frecvențelor dintre etape, din cauza limitărilor tehnice ale mecanismelor statice ale instituției atacate sau a utilizării de către atacator a unor tehnici noi și dinamice. Un APT se desfășoară în mai multe etape, cu privilegii, informații și resurse cumulate ale atacatorului la fiecare etapă.

În 76% din organizațiile afectate de APT, software-ul antivirus și sistemele de detectare a amenințărilor au fost ineficiente. În cadrul conferinței Infosecurity Europe 2011, APT au fost incluse printre cele mai mari amenințări cibernetice ale lumii moderne[17]. Conform unui raport

[10] Rass, König, și Schauer.

[11] Kyriakopoulos et al., *Multi-stage attack detection using contextual information*.

[12] Ghafir et al., „Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats".

[13] Ghafir et al., „A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection".

[14] McAfee, „The Economic Impact of Cybercrime No Slowing Down."

[15] Santoro et al., „A hybrid intrusion detection system for virtual jamming attacks on wireless networks".

[16] Mandiant, „APT1 | Exposing One of China's Cyber Espionage Units".

[17] Rot și Olszewski, *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*.

Deloitte[18], factorii cheie în combaterea APT sunt: evaluarea constantă a riscurilor, o securitate ofensivă, și instruirea personalului[19].

Definiția APT

Un atac cibernetic obișnuit vizează exploatarea vulnerabilităților pentru a sustrage datele unor firme[20], determinând daune ne-critice. Un APT dispune de mult mai multe resurse și se concentrează asupra organizațiilor mari și instituțiilor guvernamentale, provocând daune grave, chiar critice.

Mulți consideră că termenul de APT este supraîncărcat, deoarece diferiți oameni se referă la el ca fiind lucruri diferite. Definiția dată de Institutul Național de Standarde și Tehnologie din SUA (NIST) afirmă că o APT este[21]:

„Un adversar care posedă niveluri sofisticate de expertiză și resurse semnificative care îi permit să creeze oportunități de a-și atinge obiectivele prin folosirea de mulți vectori de atac (de exemplu, cibernetic, fizic și înșelăciune). Aceste obiective includ, de obicei, stabilirea și extinderea punctelor de sprijin în cadrul infrastructurii tehnologiei informaționale a organizațiilor vizate în scopul extragerii de informații, subminarea sau împiedicarea aspectelor critice ale unei misiuni, program sau organizație; sau poziționându-se pentru a îndeplini aceste obiective în viitor. Amenințarea persistentă avansată: (i) își urmărește obiectivele în mod repetat pe o perioadă lungă de timp; (ii) se adaptează la eforturile apărătorilor de a-i rezista; și (iii) este decisă să mențină nivelul de interacțiune necesar pentru a-și îndeplini obiectivele”.

Principalele trăsături ale unei APT rezultă chiar din numele său:

- **Amenințare** – APT au atât capacitate, cât și intenție, fiind executate prin acțiuni coordonate, cu personal calificat, motivat, organizat și bine finanțat[2223].
- **Persistență** – Atacatorii folosesc o abordare „scăzută și lentă” în cadrul unei strategii coerente; dacă pierd accesul la ținta lor, vor încerca din nou să îl obțină. Obiectivele lor sunt de a menține accesul pe termen lung[2425].
- **Avansată** – Atacatorii dispun de un spectru larg de tehnici și instrumente de ultimă generație, unele chiar inovative, putând include și componente disponibile în mod obișnuit. Ei încearcă de obicei să stabilească mai multe puncte de intrare în rețelele vizate, și

[18] Deloitte, „Cyber Espionage - The harsh reality of advanced security threats”.
[19] Rot, „Enterprise Information Technology Security”.
[20] Chen, Desmet, și Huygens, „A Study on Advanced Persistent Threats”.
[21] NIST, „Managing Information Security Risk”.
[22] Maloney, „What Is an Advanced Persistent Threat (APT)?”
[23] IT Governance, „Advanced Persistent Threats (APTs)”.
[24] IT Governance.
[25] Arntz, „Explained”.

combină mai multe metode, instrumente și tehnici pentru a-și atinge obiectivele, a menține accesul și a compromite ținta[2627].

Specificitatea APT le permite să păstreze accesul chiar dacă activitatea rău intenționată este descoperită și este declanșat un răspuns la incident permițând apărătorilor securității cibernetice să închidă un compromis.

Istoria APT

Atacuri asupra securității cibernetice prin mesaje email direcționate, combinate cu ingineria socială și folosind troieni pentru a exfiltra informații, au fost folosite încă la începutul anilor 1990, fiind făcute cunoscute de CERT din Marea Britanie și SUA în 2005. Termenul „amenințare persistentă avansată" (Advanced Persistent Threat, APT) a fost folosit pentru prima dată în Forțele Aeriene ale Statelor Unite în 2006[28], de către colonelul Greg Rattray[29].

Prin proiectul Stuxnet, SUA a vizat hardware-ul computerului programului nuclear al Iranului, este un exemplu de atac APT[30].

PC World a raportat o creștere a APT cu 81% din 2010 până în 2011. Mai multe țări au folosit spațiul cibernetic pentru a colecta informații prin APT[31], prin grupuri afiliate sau agenți ai guvernelor statelor suverane[32].

Un studiu Bell Canada a descoperit prezența pe scară largă a APT în guvernul canadian și în infrastructura critică, atacurile fiind atribuite actorilor chinezi și ruși[33].

Google, Adobe Systems, Juniper Networks și Symantec au fost victime ale unui atac APT numit Operațiunea Aurora[34].

O serie de atacuri în sectoarele militar, financiar, energetic, nuclear, educație, aerospațial, telecomunicații, chimie și guvern au fost raportate în 2011[35]. Dintre atacurile APT cele mai mediatizate fac parte Stuxnet, Breșa RAS, Operațiunea Aurora, Duqu, Operațiunea Ke3chang, Flame, Snow Man, Red October și Mini duke, cu atacuri mai recente malware Ratankba, ActiveX

[26] Maloney, „What Is an Advanced Persistent Threat (APT)?"
[27] Arntz, „Explained".
[28] SANS, „Assessing Outbound Traffic to Uncover Advanced Persistent Threat".
[29] Holland, „Introducing Forrester's Cyber Threat Intelligence Research".
[30] Virvilis și Gritzalis, „The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?"
[31] Grow, Epstein, și Tschang, „The New E-spionage Threat".
[32] Daly, „The Advanced Persistent Threat (or Informa5onized Force Opera5ons)".
[33] McMahon și Rohozinski, „The Dark Space Project: Defence R&D Canada – Centre for Security Science Contractor Report DRDC CSS CR 2013-007".
[34] Matthews, „Operation Aurora – 2010's Major Breach by Chinese Hackers".
[35] Wang et al., *A Survey of Game Theoretic Methods for Cyber Security*.

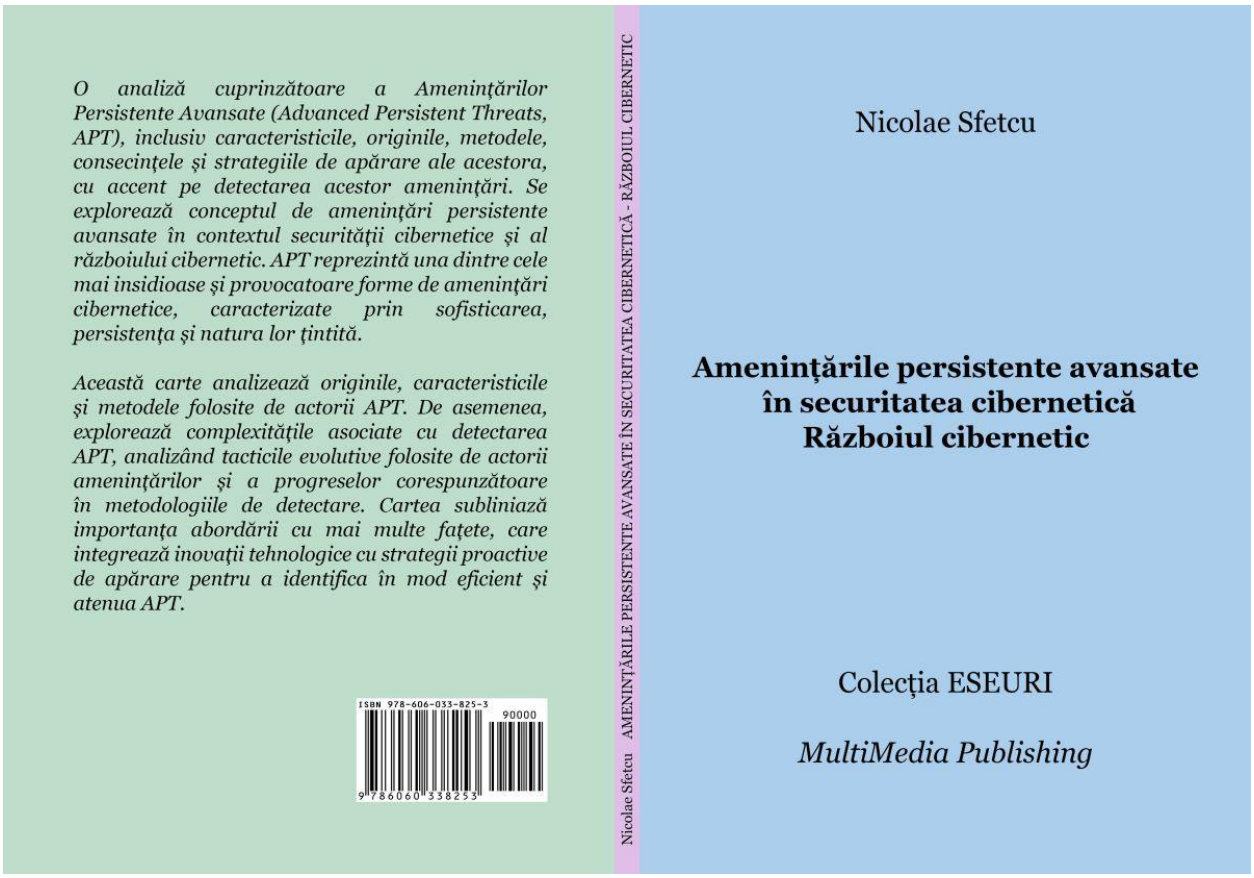
etc.[36]. Obiectivele obișnuite ale acestora sunt spionajul cibernetic cu interese în securitate națională și sabotarea infrastructurilor strategice.Atacurile folosesc dispozitive hardware și instrumente software, cu o abordare sistematică care se bazează adesea pe ingineria socială ca principal mecanism de obținere a accesului și exploatări zero-day[37].

Industroyer, un cadru de malware care a fost descoperit în 2016, a vizat rețeaua electrică din capitala Ucrainei, determinând o întrerupere a curentului pe termen scurt în acea zonă[38].

Cuprins

[36] Xu et al., „Game theoretic data privacy preservation".
[37] Adelaiye, Ajibola, și Silas, „Evaluating Advanced Persistent Threats Mitigation Effects".
[38] Tollefson, „ICS/SCADA Malware Threats | Infosec".

Cartea



O analiză cuprinzătoare a Amenințărilor Persistente Avansate (Advanced Persistent Threats, APT), inclusiv caracteristicile, originile, metodele, consecințele și strategiile de apărare ale acestora, cu accent pe detectarea acestor amenințări. El explorează conceptul de amenințări persistente avansate în contextul securității cibernetice și al războiului cibernetic. APT reprezintă una dintre cele mai insidioase și provocatoare forme de amenințări cibernetice, caracterizate prin sofisticarea, persistența și natura lor țintită. Această lucrare analizează originile, caracteristicile și metodele folosite de actorii APT. De asemenea, explorează complexitățile asociate cu detectarea APT, analizând tacticile evolutive folosite de actorii amenințărilor și a progreselor corespunzătoare în metodologiile de detectare. Eseul subliniază importanța abordării cu mai multe fațete, care integrează inovații tehnologice cu strategii proactive de apărare pentru a identifica în mod eficient și atenua APT.

MultiMedia Publishing https://www.telework.ro/ro/e-books/amenintarile-persistente-avansate-in-securitatea-cibernetica-razboiul-cibernetic/

- Digital: EPUB (ISBN 978-606-033-826-0), Kindle (ISBN 978-606-033-827-7) PDF (ISBN 978-606-033-828-4)

- Tipărit: Format A5, 210 x 148 x 7 mm, 166 g, 126 pagini, ISBN 978-606-033-825-3

DOI: 10.58679/MM92932

Data publicării: 06.01.2024

Bibliografie

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

Adelaiye, Oluwasegun, Aminat Ajibola, și Faki Silas. „Evaluating Advanced Persistent Threats Mitigation Effects: A Review”, 19 februarie 2019.

Aleroud, Ahmed, și Lina Zhou. „Phishing environments, techniques, and countermeasures: A survey”. *Computers & Security* 68 (1 iulie 2017): 160–96. https://doi.org/10.1016/j.cose.2017.04.006.

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

Al-Saraireh, Jaafer, și Ala’ Masarweh. „A novel approach for detecting advanced persistent threats”. *Egyptian Informatics Journal* 23, nr. 4 (1 decembrie 2022): 45–55. https://doi.org/10.1016/j.eij.2022.06.005.

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

Al-Yaseen, Wathiq Laftah, Zulaiha Ali Othman, și Mohd Zakree Ahmad Nazri. „Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system”. *Expert Systems with Applications* 67 (1 ianuarie 2017): 296–303. https://doi.org/10.1016/j.eswa.2016.09.041.

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

Apruzzese, Giovanni, Fabio Pierazzi, Michele Colajanni, și Mirco Marchetti. „Detection and Threat Prioritization of Pivoting Attacks in Large Networks”. *IEEE Transactions on Emerging Topics in Computing* PP (23 octombrie 2017): 1–1. https://doi.org/10.1109/TETC.2017.2764885.

Arachchilage, Nalin, și Steve Love. „Security awareness of computer users: A phishing threat avoidance perspective”. *Computers in Human Behavior* 38 (1 septembrie 2014): 304–12. https://doi.org/10.1016/j.chb.2014.05.046.

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

Ashford, Warwick. „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. „Advanced Persistent Threat (APT) Beyond the hype Project report in IMT 4582 Network security at Gjøvik University College during spring 2013", 2013. https://www.semanticscholar.org/paper/Advanced-Persistent-Threat-(-APT-)-Beyond-the-hype-Ask/a140cd962b136474685db82de60bb15f4fe1d7e1.

Axelsson, Stefan. „The base-rate fallacy and the difficulty of intrusion detection". *ACM Transactions on Information and System Security* 3, nr. 3 (1 august 2000): 186–205. https://doi.org/10.1145/357830.357849.

Azaria, Amos, Ariella Richardson, Sarit Kraus, și V. Subrahmanian. „Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data". *IEEE Transactions on Computational Social Systems* 1 (1 iunie 2014): 135–55. https://doi.org/10.1109/TCSS.2014.2377811.

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

Balduzzi, Marco, Vincenzo Ciangaglini, și Robert McArdle. *Targeted attacks detection with SPuNge*, 2013. https://doi.org/10.1109/PST.2013.6596053.

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

Bencsáth, B., Gábor Pék, L. Buttyán, și M. Félegyházi. „Duqu: Analysis, Detection, and Lessons Learned", 2012. 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, și Thomas Holt. *Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops*, 2015. https://doi.org/10.1109/ISI.2015.7165944.

Bere, Mercy, Fungai Bhunu Shava, Attlee Gamundani, și Isaac Nhamu. „How Advanced Persistent Threats Exploit Humans". *IJCSI*, 1 noiembrie 2015.

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

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

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

Brewer, Ross. „Advanced persistent threats: Minimising the damage". *Network Security* 2014 (1 aprilie 2014): 5–9. https://doi.org/10.1016/S1353-4858(14)70040-6.

Bro, Rasmus, și Age K. Smilde. „Principal Component Analysis”. *Analytical Methods* 6, nr. 9 (10 aprilie 2014): 2812–31. https://doi.org/10.1039/C3AY41907J.

Brogi, Guillaume, și Elena Di Bernardino. „Hidden Markov models for advanced persistent threats”. *International Journal of Security and Networks* 14, nr. 4 (2019): 181. https://doi.org/10.1504/IJSN.2019.103147.

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

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

Busby, J. S., B. S. S. Onggo, și Y. Liu. „Agent-based computational modelling of social risk responses”. *European Journal of Operational Research* 251, nr. 3 (16 iunie 2016): 1029–42. https://doi.org/10.1016/j.ejor.2015.12.034.

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

Chandola, Varun, Arindam Banerjee, și Vipin Kumar. „Anomaly Detection: A Survey”. *ACM Comput. Surv.* 41 (1 iulie 2009). https://doi.org/10.1145/1541880.1541882.

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

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

Chen, Zhiyan, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, H.T. Mouftah, și Petar Djukic. „Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats”. *ACM Computing Surveys* 55 (19 aprilie 2022). https://doi.org/10.1145/3530812.

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

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

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

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

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

Conti, Mauro, Luigi V. Mancini, Riccardo Spolaor, și Nino Vincenzo Verde. „Can't You Hear Me Knocking: Identification of User Actions on Android Apps via Traffic Analysis". În *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, 2015. https://doi.org/10.1145/2699026.2699119.

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

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

CSS. „Trend Analysis - The Israeli Unit 8200 An OSINT-based study". CSS CYBER DEFENSE PROJECT, 2019. 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. „The Advanced Persistent Threat (or Informa5onized Force Opera5ons)", 2009. https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf.

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

Deloitte. „Cyber Espionage - The harsh reality of advanced security threats", 2016. https://indianstrategicknowledgeonline.com/web/us_aers_cyber_espionage_07292011.pdf.

Denault, Michel, Dimitris Karagiannis, Dimitris Gritzalis, și Paul Spirakis. „Intrusion detection: Approach and performance issues of the SECURENET system". *Computers & Security* 13, nr. 6 (1 ianuarie 1994): 495–508. https://doi.org/10.1016/0167-4048(91)90138-4.

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

Dijk, Marten van, Ari Juels, Alina Oprea, și Ronald L. Rivest. „FlipIt: The Game of "Stealthy Takeover"". *Journal of Cryptology* 26, nr. 4 (1 octombrie 2013): 655–713. https://doi.org/10.1007/s00145-012-9134-5.

EC-Council. „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, și Stephanie Forrest. „Beyond the Blacklist: Modeling Malware Spread and the Effect of Interventions". *Proceedings New Security Paradigms Workshop*, 17 februarie 2012. https://doi.org/10.1145/2413296.2413302.

Eke, Hope Nkiruka, Andrei Petrovski, și Hatem Ahriz. „The use of machine learning algorithms for detecting advanced persistent threats". În *Proceedings of the 12th International Conference on Security of Information and Networks*, 1–8. SIN '19. New York, NY, USA: Association for Computing Machinery, 2019. https://doi.org/10.1145/3357613.3357618.

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

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

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

Ferrer, Zarestel, și Methusela Cebrian Ferrer. „In-depth Analysis of Hydraq - The face of cyberwar enemies unfolds”, 2010. http://cybercampaigns.net/wp-content/uploads/2013/05/Hydraq.pdf.

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

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

Friedberg, Ivo, și Roman Fiedler. „Dealing with Advanced Persistent Threats in Smart Grid ICT Networks: 5th IEEE Innovative Smart Grid Technologies Conference”. Ediție de Florian Skopik. *Proceedings of the 5th IEEE Innovative Smart Grid Technologies Conference*, 2014, 1–6.

Friedberg, Ivo, Florian Skopik, Giuseppe Settanni, și Roman Fiedler. „Combating advanced persistent threats: From network event correlation to incident detection”. *Computers & Security* 48 (1 februarie 2015): 35–57. https://doi.org/10.1016/j.cose.2014.09.006.

García-Teodoro, Pedro, Jesús Díaz-Verdejo, Gabriel Maciá-Fernández, și Enrique Vázquez. „Anomaly-based network intrusion detection: Techniques, systems and challenges”. *Computers & Security* 28 (1 februarie 2009): 18–28. https://doi.org/10.1016/j.cose.2008.08.003.

Ghafir, Ibrahim, Mohammad Hammoudeh, Vaclav Prenosil, Liangxiu Han, Robert Hegarty, Khaled Rabie, și Francisco J. Aparicio-Navarro. „Detection of advanced persistent threat using machine-learning correlation analysis”. *Future Generation Computer Systems* 89 (1 decembrie 2018): 349–59. https://doi.org/10.1016/j.future.2018.06.055.

Ghafir, Ibrahim, Konstantinos Kyriakopoulos, Francisco Aparicio-Navarro, S. Lambotharan, Basil AsSadhan, și Hamad BinSalleeh. „A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection”. *IEEE Access* PP (11 iulie 2018): 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, și Diab M. Diab. „Hidden Markov Models and Alert Correlations for the Prediction of Advanced Persistent Threats”. *IEEE Access* 7 (2019): 99508–20. https://doi.org/10.1109/ACCESS.2019.2930200.

Ghafir, Ibrahim, și Vaclav Prenosil. „Advanced Persistent Threat Attack Detection: An Overview”. *International Journal Of Advances In Computer Networks And Its Security*, 27 decembrie 2014, 154.

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

Giura, P., și Wei Wang. „Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats”. *Science*, 2012. https://www.semanticscholar.org/paper/Using-Large-Scale-

Distributed-Computing-to-Unveil-Giura-Wang/75e702d56a4a90f9c773a0e1fd0074cbe6910ead.

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

Greenberg, Andy. „The Full Story of the Stunning RSA Hack Can Finally Be Told”. *Wired*. Data accesării 11 decembrie 2023. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.

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

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

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

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

Gulati, Radha. „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, și Herve Debar. „Botnets: Lifecycle and Taxonomy”. În *2011 Conference on Network and Information Systems Security,* 1–8, 2011. https://doi.org/10.1109/SAR-SSI.2011.5931395.

Haddadpajouh, Hamed, Ali Dehghantanha, Raouf Khayami, și Kim-Kwang Raymond Choo. „A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting”. *Future Generation Computer Systems* 85 (4 martie 2018). https://doi.org/10.1016/j.future.2018.03.007.

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

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

Hassannataj Joloudari, Javad, Mojtaba Haderbadi, Amir Mashmool, Mohammad Ghasemigol, Shahab Shamshirband, și Amir Mosavi. „Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning”. *IEEE Access* 8 (6 octombrie 2020). https://doi.org/10.1109/ACCESS.2020.3029202.

Hejase, Ale, Hussin Hejase, și Jose Hejase. „Cyber Warfare Awareness in Lebanon: Exploratory Research”. *International Journal of Cyber-Security and Digital Forensics* Vol 4 (20 septembrie 2015): 482–97. https://doi.org/10.17781/P001892.

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

Hochreiter, Sepp, și Jürgen Schmidhuber. „Long Short-term Memory". *Neural computation* 9 (1 decembrie 1997): 1735–80. https://doi.org/10.1162/neco.1997.9.8.1735.

Hodge, Victoria J., și Jim Austin. „A Survey of Outlier Detection Methodologies". *Artificial Intelligence Review* 22, nr. 2 (1 octombrie 2004): 85–126. https://doi.org/10.1007/s10462-004-4304-y.

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

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

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

Huh, Jun, John Lyle, Cornelius Namiluko, și Andrew Martin. „Managing application whitelists in trusted distributed systems". *Future Generation Comp. Syst.* 27 (1 februarie 2011): 211–26. https://doi.org/10.1016/j.future.2010.08.014.

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

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

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

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

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

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

Johnson, John, și Emilie Hogan. *A graph analytic metric for mitigating advanced persistent threat*. Vol. 129, 2013. https://doi.org/10.1109/ISI.2013.6578801.

Kaspersky. „Targeted Cyberattacks Logbook". APT Kaspersky Securelist, 2023. https://apt.securelist.com.

———. „The Duqu 2.0”, 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

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

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

Kholidy, Hisham A., Abdelkarim Erradi, Sherif Abdelwahed, și Abdulrahman Azab. „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 2014, 14–19. https://doi.org/10.1109/DASC.2014.12.

Kim, Hyunjoo, Jonghyun Kim, Ikkyun Kim, și Tai-myung Chung. „Behavior-based anomaly detection on big data”. *Australian Information Security Management Conference*, 1 ianuarie 2015. https://doi.org/10.4225/75/57b69d1ed938e.

Krombholz, Katharina, Heidelinde Hobel, Markus Huber, și Edgar Weippl. „Advanced social engineering attacks”. *Journal of Information Security and Applications*, Special Issue on Security of Information and Networks, 22 (1 iunie 2015): 113–22. https://doi.org/10.1016/j.jisa.2014.09.005.

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

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

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

Lee, Martin. „Clustering Disparate Attacks: Mapping The Activities of The Advanced Persistent Threat.” *21st Virus Bulletin International Conference*, 1 octombrie 2011. https://www.academia.edu/2352875/CLUSTERING_DISPARATE_ATTACKS_MAPPING_THE_ACTIVITIES_OF_THE_ADVANCED_PERSISTENT_THREAT.

Lemay, Antoine, Joan Calvet, François Menet, și José M. Fernandez. „Survey of publicly available reports on advanced persistent threat actors”. *Computers & Security* 72 (1 ianuarie 2018): 26–59. https://doi.org/10.1016/j.cose.2017.08.005.

Leonhard, Woody. „Internet Explorer «SnowMan» Zero-Day Spreading: Use Alternative or Patch with KB 2934088”. InfoWorld, 26 februarie 2014. https://www.infoworld.com/article/2610582/internet-explorer--snowman--zero-day-spreading--use-alternative-or-patch-with-kb-293408.html.

Lim, Joo, Shanton Chang, Sean Maynard, și Atif Ahmad. „Exploring the Relationship between Organizational Culture and Information Security Culture”. *Australian Information Security Management Conference*, 1 decembrie 2009. https://doi.org/10.4225/75/57b4065130def.

Lin, Min, Qiang Chen, și Shuicheng Yan. „Network In Network”. *CoRR*, 16 decembrie 2013. https://www.semanticscholar.org/paper/Network-In-Network-Lin-Chen/5e83ab70d0cbc003471e87ec306d27d9c80ecb16.

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

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

Lockheed Martin. „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, și Nuno Vasconcelos. *Anomaly Detection in Crowded Scenes. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2010. https://doi.org/10.1109/CVPR.2010.5539872.

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

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

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

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

Marchetti, Mirco, Fabio Pierazzi, Michele Colajanni, și Alessandro Guido. „Analysis of high volumes of network traffic for Advanced Persistent Threat detection". *Computer Networks* 109 (1 iunie 2016). https://doi.org/10.1016/j.comnet.2016.05.018.

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

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

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

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

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

McHugh, John. „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, nr. 4 (Noiembrie 2000): 262–94. https://doi.org/10.1145/382912.382923.

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

Merz, Terry. „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. *GSEC GIAC Security Essentials Certification All-in-One Exam Guide*. McGraw Hill Professional, 2013.

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

Milajerdi, Sadegh M., Rigel Gjomemo, Birhanu Eshete, R. Sekar, și V.N. Venkatakrishnan. „HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows”. În *2019 IEEE Symposium on Security and Privacy (SP)*, 1137–52, 2019. https://doi.org/10.1109/SP.2019.00026.

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

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

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

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

Muszyński, Józef, și Greg Shipley. „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, și Matt Bishop. *Introduction to Deception, Digital Forensics, and Malware Minitrack*, 2017. https://doi.org/10.24251/HICSS.2017.731.

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

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

Nick. „Turla APT Group’s Espionage Campaigns Now Employs Adobe Flash Installer and Ingenious Social Engineering”. *Cyber Defense Magazine* (blog), 16 ianuarie 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, și Yuval Elovici. „Detection of Malicious PDF Files and Directions for Enhancements: A State-of-the Art Survey”. *Computers & Security* 48 (februarie 2015): 246–66. https://doi.org/10.1016/j.cose.2014.10.014.

NIST, Initiative Joint Task Force Transformation. „Managing Information Security Risk: Organization, Mission, and Information System View”. National Institute of Standards and Technology, 1 martie 2011. 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, și Paulo Shakarian. *Darknet and deepnet*

mining for proactive cybersecurity threat intelligence, 2016. https://doi.org/10.1109/ISI.2016.7745435.

Oehmen, Christopher, Elena Peterson, și Scott Dowson. „An organic model for detecting cyber-events". În *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, 2010. https://doi.org/10.1145/1852666.1852740.

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

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

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

Peikert, Chris. „A Decade of Lattice Cryptography". *Foundations and Trends® in Theoretical Computer Science* 10, nr. 4 (1 martie 2016): 283–424. https://doi.org/10.1561/0400000074.

Pfleeger, Shari, Angela Sasse, și Adrian Furnham. „From Weakest Link to Security Hero: Transforming Staff Security Behavior". *Journal of Homeland Security and Emergency Management* 11 (1 decembrie 2014). https://doi.org/10.1515/jhsem-2014-0035.

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

PWC. „Managing cyber risks in an interconnected world", 2014. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

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

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

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

Rafique, M. Zubair, Ping Chen, Christophe Huygens, și Wouter Joosen. „Evolutionary algorithms for classification of malware families through different network behaviors". În *Proceedings of the 2014 Annual Conference on Genetic and Evolutionary Computation*, 1167–74. GECCO '14. New York, NY, USA: Association for Computing Machinery, 2014. https://doi.org/10.1145/2576768.2598238.

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

Roldán, José, Juan Boubeta-Puig, José Luis Martínez, și Guadalupe Ortiz. „Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks". *Expert Systems with Applications* 149 (1 iulie 2020): 113251. https://doi.org/10.1016/j.eswa.2020.113251.

Rot, Artur. „Enterprise Information Technology Security: Risk Management Perspective". *Lecture Notes in Engineering and Computer Science* 2179 (1 octombrie 2009).

———. „Zarządzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki", 35–50, 2016.

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

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

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

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

Santoro, Diego, Gines Escudero-Andreu, Kostas Kyriakopoulos, Francisco J. Aparicio-Navarro, David J. Parish, și M. Vadursi. „A hybrid intrusion detection system for virtual jamming attacks on wireless networks", 1 ianuarie 2017, 79–87. https://doi.org/10.1016/j.measurement.2017.05.034'].

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

Schatz, Daniel, Rabih Bashroush, și Julie Wall. „Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law* 12, nr. 2 (30 iunie 2017). https://doi.org/10.15394/jdfsl.2017.1476.

Schmid, M., F. Hill, și A.K. Ghosh. „Protecting data from malicious software". *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, 199–208. https://doi.org/10.1109/CSAC.2002.1176291.

Schubert, Erich, Jörg Sander, Martin Ester, Hans Kriegel, și Xiaowei Xu. „DBSCAN revisited, revisited: Why and how you should (still) use DBSCAN". *ACM Transactions on Database Systems* 42 (31 iulie 2017): 1–21. https://doi.org/10.1145/3068335.

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

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

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

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

Sharma, Pradip Kumar, Seo Yeon Moon, Daesung Moon, și Jong Hyuk Park. „DFA-AD: A Distributed Framework Architecture for the Detection of Advanced Persistent Threats".

Cluster Computing 20, nr. 1 (1 martie 2017): 597–609. https://doi.org/10.1007/s10586-016-0716-0.

Shenwen, Lin, Li Yingbo, și Du Xiongjie. „Study and research of APT detection technology based on big data processing architecture". *2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, mai 2015, 313–16. https://doi.org/10.1109/ICEIEC.2015.7284547.

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

Shin, Seongjun, Seungmin Lee, Hyunwoo Kim, și Sehun Kim. „Advanced probabilistic approach for network intrusion forecasting and detection". *Expert Systems with Applications* 40 (31 ianuarie 2013): 315–22. https://doi.org/10.1016/j.eswa.2012.07.057.

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

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

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

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

Sim, Kevin, Emma Hart, și Ben Paechter. „A Lifelong Learning Hyper-heuristic Method for Bin Packing". *Evolutionary computation* 23 (10 februarie 2014). https://doi.org/10.1162/EVCO_a_00121.

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

Singh, Abhishek, și Zheng Bu. „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. „Joint Targeting in Cyberspace", 2011. https://apps.dtic.mil/sti/citations/ADA555785.

Soong, T. T. „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, și Soman KP. „Network Flow based IoT Botnet Attack Detection using Deep Learning". În *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 189–94, 2020. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668.

Stevens, Tim. „Global Cybersecurity: New Directions in Theory and Methods". *Politics and Governance* 6, nr. 2 (11 iunie 2018): 1–4. https://doi.org/10.17645/pag.v6i2.1569.

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

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

———. „Advanced Persistent Threats: A Symantec Perspective”, 2018. 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. „An analysis for a just cyber warfare”. În *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–10, 2012. https://ieeexplore.ieee.org/document/6243976.

Tanaka, Yasuyuki, Mitsuaki Akiyama, și Atsuhiro Goto. „Analysis of malware download sites by focusing on time series variation of malware”. *Journal of Computational Science* 22 (1 septembrie 2017): 301–13. https://doi.org/10.1016/j.jocs.2017.05.027.

Tankard, Colin. „Advanced Persistent threats and how to monitor and deter them”. *Network Security* 2011, nr. 8 (1 august 2011): 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1.

Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, și Ali A. Ghorbani. „A detailed analysis of the KDD CUP 99 data set”. În *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1–6, 2009. https://doi.org/10.1109/CISDA.2009.5356528.

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

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

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

Ussath, Martin, David Jaeger, Feng Cheng, și Christoph Meinel. „Advanced persistent threats: Behind the scenes”. *2016 Annual Conference on Information Science and Systems (CISS)*, martie 2016, 181–86. https://doi.org/10.1109/CISS.2016.7460498.

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

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

Villeneuve, Nart, James T. Bennett, Ned Moran, Thoufique Haq, Mike Scott, și Kenneth Geers. *Operation "Ke3chang: Targeted Attacks Against Ministries of Foreign Affairs*. FireEye, Incorporated, 2013.

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

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

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

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

Wang, Xiali, și Xiang Lu. „A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices". *Wireless Communications and Mobile Computing* 2020 (5 octombrie 2020): 1–13. https://doi.org/10.1155/2020/8838571.

Wang, Xu, Kangfeng Zheng, Xinxin Niu, Bin Wu, și Chunhua Wu. „Detection of command and control in advanced persistent threat based on independent access". În *2016 IEEE International Conference on Communications (ICC)*, 1–6, 2016. https://doi.org/10.1109/ICC.2016.7511197.

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

Wang, Yuan, Yongjun Wang, Jing Liu, Zhijian Huang, și Peidai Xie. *A Survey of Game Theoretic Methods for Cyber Security*, 2016. 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, și Abdul Qayoom Qazi. „Botnet Attack Detection in Internet of Things Devices over Cloud Environment via Machine Learning". *Concurrency and Computation: Practice and Experience* 34, nr. 4 (2022): e6662. https://doi.org/10.1002/cpe.6662.

Wright, John, Yi Ma, Julien Mairal, Guillermo Sapiro, Thomas S. Huang, și Shuicheng Yan. „Sparse Representation for Computer Vision and Pattern Recognition". *Proceedings of the IEEE* 98, nr. 6 (iunie 2010): 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. „Top 10 Algorithms in Data Mining". *Knowledge and Information Systems* 14, nr. 1 (1 ianuarie 2008): 1–37. https://doi.org/10.1007/s10115-007-0114-2.

Xu, Lei, Chunxiao Jiang, Jian Wang, Yong Ren, Jian Yuan, și Mohsen Guizani. „Game theoretic data privacy preservation: Equilibrium and pricing". În *2015 IEEE International Conference on Communications (ICC)*, 7071–76, 2015. https://doi.org/10.1109/ICC.2015.7249454.

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

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

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

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

Zhang, Ru, Yanyu Huo, Jianyi Liu, și Fangyu Weng. „Constructing APT Attack Scenarios Based on Intrusion Kill Chain and Fuzzy Clustering". *Security and Communication Networks* 2017 (27 decembrie 2017): e7536381. https://doi.org/10.1155/2017/7536381.

Zimba, Aaron, Hongsong Chen, Zhaoshun Wang, și Mumbi Chishimba. „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 (1 mai 2020): 501–17. https://doi.org/10.1016/j.future.2020.01.032.

Zions Bancorporation. „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, și Anoop Singhal. „An Approach for Detection of Advanced Persistent Threat Attacks", nr. 12 (1 decembrie 2020): 92–26. https://doi.org/10.1109/MC.2020.3021548.