# Bibliography


[1] Vipin Kumar Varun Chandola Arindam Banerjee. *Anomaly Detection : A Survey*. Tech. rep. http://cucis.ece.northwestern.edu/projects/DMS/publications/AnomalyDetection.pdf. University of Minnesota, Sept. 2009.

[2] Levent Ertoz Aleksandar Lazarevic et al. *Anomaly Detection Schemes in Network Intrusion Detection*. Tech. rep. https://epubs.siam.org/doi/pdf/10.1137/1.9781611972733.3. University of Minnesota, 2003.

[3] Pang.n ing Tan et al. *Introduction to Data Mining*. http://www.uokufa.edu.iq/staff/ehsanali/Tan.pdf. 2006.

[4] Christopher Kruegel Giovanni Vigna. *Host-Based Intrusion Detection*. Tech. rep. . Reliable Software Group, Technical University Vienna, June 2005.

[5] Levent Ertoz Paul Dokas et al. *Data Mining for Network Intrusion Detection*. Tech. rep. https://www-users.cs.umn.edu/~kumar001/papers/nsf_ngdm_2002.pdf. University of Minnesota, 2002.

[6] Lian Duan. *Density-Based Clustering and Anomaly Detection*. Tech. rep. https://pdfs.semanticscholar.org/237b/19f1.pdf. University of Iowa, Feb. 2012.

[7] Jung-Min Park Animesh Patcha. *An overview of anomaly detection techniques: Existing solutions and latest technological trends*. Tech. rep. . Virginia Polytechnic Institute and State University, Feb. 2007.

[8] Frank Apap Salvatore J. Stolfo et al. "A Comparative Evaluation of Two Algorithms for Windows Registry Anomaly Detection". In: *Journal of Computer Security* (Oct. 2005). http://www.gatsby.ucl.ac.uk/~heller/CompareEval.pdf.

[9] Sander Dorigo. *Security Information and Event Management*. Tech. rep. Radboud University Nijmegen, Aug. 2012.

[10] Loai Zomlot Sandeep Bhatt Pratyusa K. Manadhata. "The Operational Role of Security Information and Event Management Systems". In: *IEEE Computer and Reliability Societies* (Oct. 2014). .

[11] Michael K. Daly. "The Advanced Persistent Threat (or Information-ized Force Operations)". In: *LISA'09* (Nov. 2009). http://static.usenix.org/event/lisa09/tech/slides/daly.pdf.

[12] Ned Moran. "Understanding Advanced Persistent Threats". In: *USENIX ;login:* (Aug. 2011). https://www.usenix.org/system/files/login/articles/105484-Moran.pdf.

[13] Christophe Huygens Ping Chen Lieven Desmet. *A Study on Advanced Persistent Threats*. Tech. rep. 15th IFIP International Conference on Communications and Multimedia Security (CMS), Sept. 2014.

[14] Lucian Carata Graeme Jenkinson et al. *Applying Provenance in APT Monitoring and Analysis*. Tech. rep. https://www.usenix.org/system/files/conference/tapp2017/tapp17%5Fpaper%5Fjenkinson.pdf. USENIX TaPP 2017, June 2017.

[15] Dorothy E. Denning. "An Intrusion-Detection Model". In: *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING* (Feb. 1987). .

[16] Abdolhossein Sarrafzadeh Sreenivas Tirumala Hira Sathu. "Free and open source intrusion detection systems: A study". In: *4th International Conference on Machine Learning and Cybernetics* (July 2015).

[17] Anand Nayyar. "The Best Open Source Network Intrusion Detection Tools". In: *OpenSource For U* (Apr. 2017). https://opensourceforu.com/2017/04/best-open-source-network-intrusion-detection-tools/.

[18] J. Diaz-Verdejoa P. Garcia-Teodoroa et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges". In: *ScienceDirect* (Aug. 2008). .

[19] *OWASP.ORG Intrusion Detection*. https://www.owasp.org/index.php/Intrusion_Detection. Accessed: 2010-08-10.

[20] Timothy N. Newsham Thomas H. Ptacek. *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*. Tech. rep. http://cs.unc.edu/~fabian/course_papers/PtacekNewsham98.pdf. Secure Networks, Inc., Jan. 1998.

[21] Somesh Jha Mihai Christodorescu. *Testing Malware Detectors*. Tech. rep. http://pages.cs.wisc.edu/~jha/jha-papers/security/ISSTA_2004.pdf. University of Wisconsin, July 2004.

[22] Hoon-Jae Lee Jonathan A.P. Marpaung Mangal Sain. *Survey on malware evasion techniques: state of the art and challenges*. Tech. rep. http://www.icact.org/upload/2012/0474/20120474_finalpaper.pdf. Dongseo University, Feb. 2012.

[23] Christos Xenakis Giorgos Poulios Christoforos Ntantogian. "ROPInjector: Using Return Oriented Programming for Polymorphism and Antivirus Evasion". In: *BlackHat USA 2015* (Aug. 2015). https://docs.huihoo.com/blackhat/usa-2015/us-15-Xenakis-ROPInjector-Using-Return-Oriented-Programming-For-Polymorphism-And-Antivirus-Evasion-wp.pdf.

[24] A. Shulman O. Maor. "SQL Injection Signatures Evasion". In: *BlackHat USA 2015* (Apr. 2004). https://www.imperva.com/docs/IMPERVA_HII_SQL-Injection-Signatures-Evasion.pdf.

[25] Yan Shoshitaishvili Alexandros Kapravelos et al. "Revolver: An Automated Approach to the Detection of Evasive Web-based Malware". In: *22nd USENIX Security Symposium* (Aug. 2013). https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/kapravelos.

[26] Giovanni Vigna Dhilung Kirat. *MalGene: Automatic Extraction of Malware Analysis Evasion Signature*. Tech. rep. http://www.cs.ucsb.edu/~vigna/publications/2015_CCS_MalGene.pdf. University of California, Santa Barbara, Oct. 2015.

[27] Hiroshi Fujinoki Matthew L. Bringer Christopher A. Chelmecki. "A Survey: Recent Advances and Future Trends in Honeypot Research". In: *MECS* (Sept. 2012). http://www.mecs-press.org/ijcnis/ijcnis-v4-n10/IJCNIS-V4-N10-7.pdf.

[28] K. G. Anagnostakis et al. "Detecting Targeted Attacks Using Shadow Honeypots". In: *14th USENIX Security Symposium* (Aug. 2005). http://static.usenix.org/publications/library/proceedings/sec05/tech/full_papers/anagnostakis/anagnostakis.pdf.

[29] Markus Koetter Paul Baecher et al. *The Nepenthes Platform: An Efficient Approach to Collect Malware*. Tech. rep. https://www.syssec.rub.de/media/emma/veroeffentlichungen/2012/08/07/Nepenthes-RAID06.pdf. University of Mannheim, Aug. 2012.

[30] Niels Provos. "A Virtual Honeypot Framework". In: *13th USENIX Security Symposium* (Aug. 2004). https://www.usenix.org/legacy/event/sec04/tech/full_papers/provos/provos_html/.

[31] Lance Spitzner. "The Honeynet Project: Trapping the Hackers". In: *IEEE Security & Privacy* (Apr. 2003). https://pdfs.semanticscholar.org/ec08/56d6.pdf.

[32] M. Dacier F. Pouget. "Honeypot-based Forensics". In: *AusCERT Asia Pacific Information technology Security Conference 2004* (May 2004). https://pdfs.semanticscholar.org/ec08/56d6.pdf.

[33] Abakash Saikia Namit Gupta. *Web Application Firewall*. Tech. rep. . Indian Institute Of Technology, Kanpur, Apr. 2007.

[34] *A Quick Guide to Runtime Application Self-Protection (RASP)*. Tech. rep. https://cdn2.hubspot.net/hubfs/376484/resources/170206_Guide_to_RASP_100.pdf. Prevoty, Inc. HQ, Feb. 2017.

[35] D. Miller. *Security information and event management (SIEM) implementation*. 2011.

[36] P.K. Manadhata S. Bhatt et al. "The Operational Role of Security Information and Event Management Systems". In: *IEEE security & Privacy* (2014). https://www.researchgate.net/profile/Loai_Zomlot/publication/273394505_The_Operational_Role_of_Security_Information_and_Event_Management_Systems/links/55aed64e08ae98e661a6f259/The-Operational-Role-of-Security-Information-and-Event-Management-Systems.pdf.

[37] N. Hu P.G. Bradford. "A layered approach to insider threat detection and proactive forensics". In: *Annual Computer Security Applications Conference* (Dec. 2005). https://www.researchgate.net/profile/Phillip_Bradford/publication/254390140_A_Layered_Approach_to_Insider_Threat_Detection_and_Proactive_Forensics/links/0a85e537d25e690e86000000.pdf.

[38] C. Kruegel A. Moser et al. *Limits of static analysis for malware detection*. Tech. rep. https://auto.tuwien.ac.at/~chris/research/doc/acsac07_limits.pdf. Technical University Vienna, 2007.

[39] D. Gritzalis N. Virvilis. "The big four-what we did wrong in advanced persistent threat detection?" In: *2013 International Conference on Availability, Reliability and Security* (201"). https://www.infosec.aueb.gr/Publications/ARES-2013%20APT%20Short.pdf.

[40] A. Chowdhary A. Alshamrani. "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities". In: *IEEE Communications Surveys & Tutorials* (Jan. 2019). https://www.researchgate.net/publication/330269772_A_Survey_on_Advanced_Persistent_Threats_Techniques_Solutions_Challenges_and_Research_Opportunities.

[41] G. Sykiotakis Z. Tzermias et al. "Combining static and dynamic analysis for the detection of malicious documents". In: *Proceedings of the Fourth European Workshop on System Security* (2011). https://dl.acm.org/doi/pdf/10.1145/1972551.1972555.

[42] J. Wook Jang H. Kang. "Detecting and classifying android malware using static analysis along with creator information". In: *International Journal of Distributed Sensor Networks* (2015). https://arxiv.org/ftp/arxiv/papers/1903/1903.01618.pdf.

[43] J. Weber-Jahnke S. Alharbi et al. "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review". In: *International Journal of Security and Its Applications* (Oct. 2011). https://www.researchgate.net/profile/Jens_Weber6/publication/220849931_The_Proactive_and_Reactive_Digital_Forensics_Investigation_Process_A_Systematic_Literature_Review/links/553a9a570cf245bdd7644679/The-Proactive-and-Reactive-Digital-Forensics-Investigation-Process-A-Systematic-Literature-Review.pdf.

[44] P. Poosankam H. Yin et al. "HookScout: Proactive Binary-Centric Hook Detection". In: *Detection of Intrusions and Malware, and Vulnerability Assessment, 7th International Conference* (July 2010). https://apps.dtic.mil/dtic/tr/fulltext/u2/a540503.pdf.

[45] Jared Myers. "How to Evolve Threat Hunting by Using the MITRE ATT&CK Framework". In: *RSA Conference 2019* (Mar. 2019). https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13712/SPO3-W03-How%20to%20Evolve%20Threat%20Hunting%20by%20Using%20the%20MITRE%20ATT&CK%20Framework.pdf.

[46] Vernon Habersetzer. "Threat Hunting Using 16th Century Math and Sesame Street". In: *RSA Conference 2019* (Mar. 2019). https://www.rsaconference.com/industry-topics/presentation/threat-hunting-using-16th-century-math-and-sesame-street.

[47] M. Durrin S. Davidoff. "Cloud Threat Hunting". In: *RSA Conference 2020* (Feb. 2020). https://www.rsaconference.com/industry-topics/presentation/cloud-threat-hunting.

[48] A. Dehghantanha H. Haddadpajouh et al. "A Deep Recurrent Neural Network Based Approach for Internet of Things Malware Threat Hunting". In: *Future Generation Computer Systems Volume 85* (Aug. 2018). https://www.researchgate.net/publication/323723430_A_Deep_Recurrent_Neural_Network_Based_Approach_for_Internet_of_Things_Malware_Threat_Hunting.

[49] Rob Lee Robert M. Lee. *The Who, What, Where, When, Why and How of Effective Threat Hunting*. Tech. rep. www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785. SANS Institute, Feb. 2016.

[50] Paul Löwenadler Theodor Liliengren. *Threat hunting, definition and framework*. Tech. rep. http://www.diva-portal.org/smash/get/diva2:1205812/FULLTEXT02.pdf. Halmstad University, May 2018.

[51] W. Robertson C. Kruegel et al. *Detecting Kernel-Level Rootkits Through Binary Analysis*. Tech. rep. http://security.poly.ro/acsac2004.pdf. Technical University Vienna, 2004.

[52] Teodor Sommestad Hannes Holm et al. *A quantitative evaluation of vulnerability scanning*. Tech. rep. http://www.diva-portal.org/smash/get/diva2:545791/FULLTEXT01.pdf. Royal Institute of Technology, Stockholm, 2011.

[53] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™)*. Tech. rep. https://attack.mitre.org/wiki/Main_Page. The MITRE Corporation, 2017.

[54] Inc MongoDB. *Compound Indexes*. Tech. rep. https://docs.mongodb.com/manual/core/index-compound/. Nov. 2020.

[55] Zhaoshun Wang Aaron Zimba. "Malware-Free Intrusions: Exploitation of Built-in Pre-Authentication Services for APT Attack Vectors". In: *Modern Education and Computer Science* (July 2017). www.mecs-press.org/ijcnis/ijcnis-v9-n7/IJCNIS-V9-N7-1.pdf.

[56] AECOM Global Security Operations Center Paul Speulstra. *Accessibility Features*. Tech. rep. https://attack.mitre.org/wiki/Technique/T1015. The MITRE Corporation, Jan. 2018.

[57] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Event Triggered Execution: Accessibility Features*. Tech. rep. https://attack.mitre.org/techniques/T1546/008/. The MITRE Corporation, 2020.

[58] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Boot or Logon Autostart Execution*. Tech. rep. https://attack.mitre.org/techniques/T1547/. The MITRE Corporation, 2020.

[59] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Create Account: Local Account*. Tech. rep. https://attack.mitre.org/techniques/T1136/001/. The MITRE Corporation, 2020.

[60] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder*. Tech. rep. https://attack.mitre.org/techniques/T1547/001/. The MITRE Corporation, 2021.

[61] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Adversary-in-the-Middle: LLMNR, NBT-NS Poisoning and SMB Relay*. Tech. rep. https://attack.mitre.org/techniques/T1557/001/. The MITRE Corporation, 2021.

[62] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Obfuscated Files or Information: Binary Padding*. Tech. rep. https://attack.mitre.org/techniques/T1027/001/. The MITRE Corporation, 2021.

[63] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Abuse Elevation Control Mechanism: Bypass User Account Control*. Tech. rep. https://attack.mitre.org/techniques/T1548/002/. The MITRE Corporation, 2021.

[64] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™), Boot or Logon Initialization Scripts*. Tech. rep. https://attack.mitre.org/techniques/T1037/. The MITRE Corporation, 2021.