Mitigating Advanced Persistent Threats: A Comparative Evaluation Review

Aminat AJIBOLA[1,2], Innocent UJATA[1], Oluwasegun ADELAIYE[3], Noorihan Abdul RAHMAN[4]

[1] Computer Science Department, University of Abuja, Abuja, Nigeria,
e-mail: aminat.ajibola@uniabuja.edu.ng

[2] School of Computing and Engineering, University of Huddersfield, UK,
e-mail: ujatasuni@gmail.com

[3] Computer Science Department, Bingham University, Karu, Nigeria,
e-mail: oluwasegun.adelaiye@binghamuni.edu.ng

[4] Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Kelatan, Machang, Malaysia,
e-mail: noorihan@kelantan.uitm.edu.my

Abstract

Cyber threats have been an issue of great concern since the advent of the information (computer and internet) age. But of greater concern is the most recent class of threats, known as Advanced Persistent Threats (APTs). It has drawn increasing attention all over the world, from researchers, and the industrial security sector. APTs are sophisticated cyber-attacks executed by sophisticated and well-resourced adversaries targeting specific information in companies and government. APT is a long-term campaign involving different steps. This form of attack if successful has significant implications to countries and large organizations, which may be from financial to reputational damage. This work presents a comprehensive study on APT, characterizing its uniqueness and attack model, and analyzing techniques commonly seen in APT attacks. On evaluating mitigation effects proposed and developed by researches, the use of a multiple mitigation methods shows good signs in detecting and preventing APT. Anomaly detection and dynamic analysis show high accuracy levels in detecting APT. This work also highlights and recommends security tips as well as methods of implementing countermeasures that can help to mitigate APTs, thereby giving directions for future research.

Index terms: Information Security, phishing, social engineering, Zero-day, cyber warfare

References:

[1]. O. I. Adelaiye, A. Showole and S. A. Faki, "Evaluating Advanced Persistent Threats Mitigation Effects: A Review," International Journal of Information Security Science, vol. 7, (4), pp. 159-171, 2018.

[2]. I. Ghafir and V. Prenosil, "Advanced persistent threat attack detection: An overview," International Journal of Advances in Computer Networks and its Security (IJCNS), (I), 2014.

[3]. C. Levine, "Conceptualizing financial loses as a result of advanced persistent threats," 2013.

[4]. D. Lacey, Advanced Persistent Threats: How to Manage the Risk to Your Business. 2013.

[5]. D. Sullivan, "Beyond the hype: advanced persistent threats," Advanced Persistent Threats and Real Time Threat Management. The Essential Series. Realtime Publishers, 2011.

[6]. Y. Wang et al, "A network gene-based framework for detecting advanced persistent threats," in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference On, 2014.

[7]. I. Jeun, Y. Lee and D. Won, "A practical study on advanced persistent threats," Computer Applications for Security, Control and System Engineering, vol. 339, pp. 144-152, 2012.

[8]. J. B. Fraley, "Improved Detection for Advanced Polymorphic Malware," 2017.

[9]. D. Alperovitch, Revealed: Operation Shady RAT. 20113.

[10]. M. Ask et al, "Advanced persistent threat (APT) beyond the hype," Project Report in IMT4582 Network Security at Gjøvik University College, Springer, 2013.

[11]. M. Maskun, "The Crime of Aggression: Complexities in Definition and Elements of Crime," Mimbar Hukum-Fakultas Hukum Universitas Gadjah Mada, vol. 25, (2), pp. 366-375, 2013.

[12]. M. Rudner, "Cyber-threats to critical national infrastructure: An intelligence challenge," International Journal of Intelligence and CounterIntelligence, vol. 26, (3), pp. 453-481, 2013.

[13]. N. Virvilis, D. Gritzalis and T. Apostolopoulos, "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, 2013.

[14]. R. Mehresh and S. J. Upadhyaya, "Deception-based survivability," in Secure System Design and Trustable ComputingAnonymous 2016.

[15]. E. Cole, Advanced Persistent Threat: Understanding the Danger and how to Protect Your Organization. 2012.

[16]. P. Chen, L. Desmet and C. Huygens, "A study on advanced persistent threats," in IFIP International Conference on Communications and Multimedia Security, 2014.

[17]. M. Ussath et al, "Advanced persistent threats: Behind the scenes," in Information Science and Systems (CISS), 2016 Annual Conference On, 2016.

[18]. M. Marchetti et al, "Analysis of high volumes of network traffic for Advanced Persistent Threat detection," Computer Networks, vol. 109, pp. 127-141, 2016.

[19]. R. Brewer, "Advanced persistent threats: minimising the damage," Network Security, vol. 2014, (4), pp. 5-9, 2014.

[20]. S. Pfleeger and R. Cunningham, "Why measuring security is hard," IEEE Security & Privacy, vol. 8, (4), pp. 46-54, 2010.

[21]. D. Borbor et al, "Securing networks against unpatchable and unknown vulnerabilities using heterogeneous hardening options," in IFIP Annual Conference on Data and Applications Security and Privacy, 2017.

[22]. U. K. Singh and C. Joshi, "Scalable Approach Towards Discovery of Unknown Vulnerabilities." IJ Network Security, vol. 20, (5), pp. 827-835, 2018.

[23]. X. Zhou et al, "APT attack analysis in SCADA systems," in MATEC Web of Conferences, 2018.

[24]. M. Nicho, A. Oluwasegun and F. Kamoun, "Identifying vulnerabilities in APT attacks: A simulated approach," in New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference On, 2018.

[25]. G. Kim, C. Choi and J. Choi, "Ontology modeling for APT attack detection in an IoT-based power system," in Proceedings of the 2018 Conference on Research in Adaptive and Convergent Systems, 2018.

[26]. Y. Su et al, "A Framework of APT Detection Based on Dynamic Analysis," 2016.

[27]. G. Husari et al, "Learning APT chains from cyber threat intelligence," in Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security, 2019.

[28]. A. Ahmad et al, "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," Comput. Secur., 2019.

[29]. J. Vukalović and D. Delija, "Advanced persistent threats-detection and defense," in 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015.

[30]. C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, (8), pp. 16-19, 2011.

[31]. M. Nicho, O. Adelaiye and F. Kamoun, "Identifying vulnerabilities in apt attacks: A simulated approach," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.

[32]. L. Yang et al, "Security evaluation of the cyber networks under advanced persistent threats," IEEE Access, vol. 5, pp. 20111-20123, 2017.

[33]. I. Friedberg et al, "Combating advanced persistent threats: From network event correlation to incident detection," Comput. Secur., vol. 48, pp. 35-57, 2015.

[34]. P. Hu et al, "Dynamic defense strategy against advanced persistent threat with insiders," in Computer Communications (INFOCOM), 2015 IEEE Conference On, 2015.

[35]. K. Krombholz et al, "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113-122, 2015.

[36]. B. Binde, R. McRee and T. J. O'Connor, "Assessing outbound traffic to uncover advanced persistent threat," SANS Institute.Whitepaper, 2011.

[37]. V. S. Raj, R. Chezhian and M. Mrithulashri, "Advanced persistent threats & recent high profile cyber threat encounters," International Journal of Innovative Research in Computer & Communication Engineering, vol. 2, (1), 2014.

[38]. V. Benetis et al, "Advanced Persistent Threat Awareness," 2013.

[39]. D. L. Weed, Methodologic Guidelines for Review Papers, 1997.

[40]. D. L. Weed, "Weight of evidence: a review of concept and methods," Risk Analysis: An International Journal, vol. 25, (6), pp. 1545-1557, 2005.

[41]. I. Ghafir and V. Prenosil, "Advanced persistent threat attack detection: An overview," International Journal of Advances in Computer Networks and its Security (IJCNS), (I), 2014.

[42]. M. R. DeVore and S. Lee, "APT (Advanced Persistent Threat) S And Influence: Cyber Weapons And The Changing Calculus Of Conflict," The Journal of East Asian Affairs, pp. 39-64, 2017.

[43]. D. Higgins, "The growing challenge of Advanced Persistent Threats; The growing challenge of Advanced Persistent Threats," CSO Online, 2016.

[44]. V. F. Roth, "How to Fall Victim to Advanced Persistent Threats," unpublished.

[45]. I. Ghafir, M. Hammoudeh and V. Prenosil, Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat, 2017.

[46]. R. A. Grimes, "5 signs you've been hit with an advanced persistent threat (APT)," CSO Online, 2019.

[47]. R. Bruce, "5 stages of an advanced persistent threat attack on your network," 2014.

[48]. E. Messmer, "What is an 'Advanced Persistent Threat,' anyway?" 2011.

[49]. N. Virvilis and D. Gritzalis, "The big four-what we did wrong in advanced persistent threat detection?" in Availability, Reliability and Security (ARES), 2013 Eighth International Conference On, 2013.

[50]. P. Hernandez, "How to Stop Advanced Persistent Threats," eSecurity Planet, 2018.

[51]. C. Osborne, "Security in 2016: The death of advanced persistent threats," 2015.

[52]. Biztech, "APT Security: Protecting Against Advanced Persistent Threats," 2016.

[53]. L. L. Bann, M. M. Singh and A. Samsudin, "Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment," Procedia Computer Science, vol. 72, pp. 129-136, 2015.

[54]. C. Budd, "Have you been the victim of an APT?: Identifying and protecting against an attack," 2015, 2015.

[55]. P. Lamprakis et al, "Unsupervised detection of APT C&C channels using web request graphs," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2017.

[56]. S. Rass, S. König and S. Schauer, "Defending against advanced persistent threats using game-theory," PloS One, vol. 12, (1), pp. e0168675, 2017.

[57]. R. Luh et al, "Semantics-aware detection of targeted attacks: a survey," Journal of Computer Virology and Hacking Techniques, vol. 13, (1), pp. 47-85, 2017.

[58]. N. Virvilis, B. Vanautgaerden and O. S. Serrano, "Changing the game: The art of deceiving sophisticated attackers," in Cyber Conflict (CyCon 2014), 2014 6th International Conference On, 2014.