Detecting Advanced Persistent Threats through Deception Techniques

Nikolaos Virvilis-Kollitiris

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business
76 Patission Ave., Athens GR-10434, Greece
nvir@aueb.gr

Abstract

The number and complexity of cyber-attacks has been increasing steadily in recent years. The major players in today's cyber conflicts are well organized and heavily funded teams with specific goals and objectives, working for or supported by a nation-state. A commonly used term to describe such teams/groups is Advanced Persistent Threat (APT). APT target the communication and information systems of government, military and industrial organizations and are willing to use vast amounts of money, time and expertise to reach their goals. A clear indication of the level of sophistication of APT is their impressive arsenal. The complexity and capabilities of recently discovered malware used to facilitate such attacks are remarkable: Stuxnet, Duqu, Flame, Red October, MiniDuke and more recently Regin are examples of highly sophisticated malware, the development of which required skillful individuals - in some cases (e.g. Stuxnet) with expertise in multiple technology fields - as well as substantial financial resources. In addition, serious insider attacks have occurred that resulted in the publication of several thousand classified documents, highlighting the fact that even in sensitive institutions, the effectiveness of the existing security safeguards is insufficient. Advances in attacker sophistication have not been matched by similar defensive advances. The concept of keeping the internal, trusted network separated from the external, untrusted one (i.e. boundary protection) has become obsolete. The use of blacklists or signatures for attack detection is practically useless against sophisticated attackers. The security industry, having spent decades developing security products such as anti-malware solutions and intrusion-detection/prevention systems, refuses to admit the shortcomings of these products. It is not uncommon for security companies to advertise that their products can detect and stop APT, even though the same products have been unable to detect such attacks for several years. Furthermore, C-level executives fail to understand the need for more robust security mechanisms, as they believe that by following vendor recommendations and making significant investments in traditional security solutions, they will keep their organization secure. However reality has proven them wrong, over and over again. In order to defend against such sophisticated adversaries, it is necessary to redesign our defenses and develop technologies focused more on detection than prevention. The purpose of this thesis is to offer a comprehensive view of the APT problem by analyzing the most common techniques, tools and attack paths that attackers are using, and highlighting the shortcomings of current security solutions. The use of deception techniques for attack detection is one of the integral focal points of this thesis. Based on this concept, a novel APT detection model is proposed, implemented and evaluated. The evaluation results highlight the significant efficacy of the model in detecting sophisticated attacks, with a very low false positive rate.

A dissertation submitted for the partial fulfillment of a Ph.D. degree

October 2015

References

1. Abrams, R., Barrera, O. & Pathak, J., 2013. *Browser Security Comparative Analysis*, Available at: https://www.nsslabs.com/reports/browser-security-comparative-analysis-phishing-protection.
2. Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P. & Lambrinoudakis, C., 2011. Cryptography goes to the cloud. In *Secure and Trust Computing, Data Management, and Applications*. Springer, pp. 190–197.
3. Akhawe, D. & Felt, A.P., 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Usenix Security*. pp. 257–272.
4. Alperovitch, D., 2011. *Revealed: operation shady RAT*, McAfee. Available at: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
5. Andreasson, K.J., 2011. *Cybersecurity: Public Sector Threats and Responses*, CRC Press.
6. Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou II, N. & Dagon, D., 2011. Detecting Malware Domains at the Upper {DNS} Hierarchy. In *{USENIX} Security Symposium*. p. 16.
7. Baggett, M., 2015. Detecting Mimikatz Use On Your Network. Available at: https://isc.sans.edu/forums/diary/Detecting+Mimikatz+Use+On+Your+Network/19311/.
8. Ball, J., Borger, J. & Greenwald, G., 2013. Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. Available at: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
9. Banu, M.N. & Banu, S.M., 2013. A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies*, 4(6), pp.783–786.
10. Barnes, J., 2013. What Bradley Manning Leaked. Available at: http://blogs.wsj.com/washwire/2013/08/21/what-bradley-manning-leaked/ [Accessed January 20, 2014].
11. Bejtlich, R., 2013. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* 1st ed., No Starch Press.
12. Bejtlich, R., 2010. Understanding the advanced persistent threat. Available at: http://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat.
13. Bencsáth, B. et al., 2015. *Duqu 2.0: A comparison to Duqu*, Available at: http://www.crysys.hu/duqu2/duqu2.pdf.
14. Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M., 2012a. Duqu: Analysis, detection, and lessons learned. In *ACM European Workshop on System Security (EuroSec)*.
15. Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M., 2012b. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, 4(4), pp.971–1003.
16. Berthier, R., Sanders, W.H. & Khurana, H., 2010. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. pp. 350–355.
17. Bertrand, N. & Kelley, M., 2015. "Complete takeover": Israel unleashed one of the world's most sophisticated cyberweapons on the Iran talks. *BusinessInsider*. Available at: http://www.businessinsider.com/israel-spying-on-the-iran-talks-2015-6.
18. Bian, R.M., 2013. *Alice in Battlefield: An Evaluation of the Effectiveness of Various {UI} Phishing Warnings*, Available at: https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/725mbian13.pdf.
19. Bilge, L., Kirda, E., Kruegel, C. & Balduzzi, M., 2011. {EXPOSURE}: Finding Malicious Domains Using Passive {DNS} Analysis. In *NDSS*.
20. Birnbaum, M., 2013. Germany looks at keeping its Internet, e-mail traffic inside its borders. *The Washington Post*. Available at: http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html.
21. Bodmer, S., Kilger, M., Carpenter, G. & Jones, J., 2012. *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, McGraw Hill Professional.

22. Bowen, B., Ben Salem, M., Hershkop, S., Keromytis, A. & Stolfo, S., 2013. Designing Host and Network Sensors to Mitigate the Insider Threat. *Journal of Security & Privacy IEEE*, 7, pp.22–29.
23. Bowen, B.M., Salem, M. Ben, Hershkop, S., Keromytis, A.D. & Stolfo, S., 2009. Designing host and network sensors to mitigate the insider threat. *IEEE Security & Privacy*, 7(6), pp.22–29.
24. Bowen, B.M., Salem, M. Ben, Keromytis, A.D. & Stolfo, S.J., 2010. Monitoring technologies for mitigating insider threats. In *Insider Threats in Cyber Security*. Springer, pp. 197–217.
25. Boxcryptor, 2015. Boxcryptor. Available at: https://www.boxcryptor.com.
26. Bradley, T., 2013. *Android Dominates Market Share, But Apple Makes All The Money*, Available at: http://goo.gl/B0ylqi.
27. Bro, 2015. The Bro Network Security Monitor. Available at: https://www.bro.org.
28. Broad, W.J., Markoff, J. & Sanger, D.E., 2011. Israel tests on worm called crucial in Iran nuclear delay. *New York Times*, 15, p.2011.
29. Brown, D.J., Suckow, B. & Wang, T., 2002. A Survey of Intrusion Detection Systems. *Department of Computer Science, University of California, San Diego*.
30. Caballero, J., Grier, C., Kreibich, C. & Paxson, V., 2011. Measuring Pay-per-Install: The Commoditization of Malware Distribution. In *{USENIX} Security Symposium*.
31. Cappelli, D., Moore, A.P., Trzeciak, R.F. & Shimeall, T., 2009. *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition*, Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50275.
32. Caputo, D., Maloof, M. & Stephens, G., 2009. Detecting insider theft of trade secrets. *IEEE Security and Privacy*, 7(6), pp.14–21.
33. Carrie, D., 2014. Kerry: Snowden a "Coward" and "Traitor." *NBC News*. Available at: http://www.nbcnews.com/politics/first-read/kerry-snowden-coward-traitor-n116366.
34. Chen, T. & Abu-Nimeh, S., 2011. Lessons from stuxnet. *Computer*, 44(4), pp.91–93. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5742014 [Accessed November 26, 2014].
35. Chien, E., OMurchu, L. & Falliere, N., 2012. W32. Duqu: the precursor to the next stuxnet. In *Proc. of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.
36. CIF, 2014. *Collective Intelligence Framework*, Available at: https://code.google.com/p/collective-intelligence-framework/.
37. Cisco, 2013. *Cisco Annual Security Report*, Available at: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.
38. Claise, B., 2004. Cisco systems NetFlow services export version 9.
39. Claise, B., Trammell, B. & Aitken, P., 2013. Specification of the IP Flow Information Export (IPFIX) protocol for the exchange of flow information. *draft-ietf-ipfix-protocol-rfc5101bis-08 (work in progress)*.
40. Clarke, R. & Knake, R., 2012. *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco.
41. Cloudfogger, 2015. cloudfogger. Available at: https://www.cloudfogger.com/.
42. Cohen, F., 1987. Computer viruses: theory and experiments. *Computers & security*, 6(1), pp.22–35.
43. Cole, E., 2012. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization* 1st ed., Syngress.
44. Colvin, R., 2011. *{SmartScreen} Application Reputation Building Reputation*, Available at: http://goo.gl/ChWEW.
45. Comparatives, A. V, 2012. *Anti-Phishing protection of popular web browsers*, Available at: http://www.av-comparatives.org/images/docs/avc_phi_browser_201212_en.pdf.
46. Cova, M., Leita, C., Thonnard, O., Keromytis, A.D. & Dacier, M., 2010. An analysis of rogue {AV} campaigns. In *Recent Advances in Intrusion Detection*. Springer, pp. 442–463.
47. Curtsinger, C., Livshits, B., Zorn, B.G. & Seifert, C., 2011. {ZOZZLE}: Fast and Precise In-Browser {JavaScript} Malware Detection. In *{USENIX} Security Symposium*. pp. 33–48.

48. Darwish, A. & Bataineh, E., 2012. Eye tracking analysis of browser security indicators. In *2012 International Conference on Computer Systems and Industrial Informatics ({ICCSII})*. pp. 1–6.

49. Dash, D. et al., 2006. When gossip is good: Distributed probabilistic inference for detection of slow network intrusions. In *Proceedings of the national conference on Artificial Intelligence*. p. 1115.

50. Denning, D.E., 1987. An intrusion-detection model. *Software Engineering, IEEE Transactions on*, (2), pp.222–232.

51. Denver, N., 2012. *Private: Bradley Manning, WikiLeaks, and the Biggest Exposure of Official Secrets in American History*, Chicago Review Press.

52. DoD, 2013. *Annual Report to Congress*, Available at: http://www.defense.gov/pubs/2013_china_report_final.pdf.

53. Dritsas, S. et al., 2005. Employing ontologies for the development of security critical applications. In *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government*. Springer, pp. 187–201.

54. Drummond, D., 2010. Official Google Blog: A new approach to China. Available at: http://googleblog.blogspot.gr/2010/01/new-approach-to-china.html#!/2010/01/new-approach-to-china.html [Accessed November 25, 2014].

55. Economist, 2010. War in the fifth domain. Available at: http://www.economist.com/node/16478792.

56. Edge, C., Barker, W., Hunter, B. & Sullivan, G., 2010. Network Scanning, Intrusion Detection, and Intrusion Prevention Tools. In *Enterprise Mac Security*. Springer, pp. 485–504.

57. Edwards, N., 2013. Hardware intrusion detection for supply-chain threats to critical infrastructure embedded systems.

58. Egelman, S. & Schechter, S., 2013. The Importance of Being Earnest [in Security Warnings]. In *Financial Cryptography and Data Security*. Springer, pp. 52–59.

59. Ewaida, B., 2010. *Pass-the-hash attacks: Tools and Mitigation*, Available at: https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283.

60. Field, S., 2006. An Introduction to Kernel Patch Protection - Windows Vista Security - Site Home - MSDN Blogs. Available at: http://blogs.msdn.com/b/windowsvistasecurity/archive/2006/08/11/695993.aspx [Accessed November 26, 2014].

61. FireEye, 2014. *APT28: A window into Russia's Cyber Espionage Operations?*, Available at: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

62. Fisher, D., 2012. *What have we learned: FLAME malware*,

63. Fogarty, K., 2014. Russian Cyberwar Force Intensifies 'net Arms Race. Available at: http://news.dice.com/2014/02/01/russian-cyberwar-force-intensifies-net-arms-race/.

64. Foreignpolicy, 2013. The Leading Global Thinkers of 2013. Available at: http://2013-global-thinkers.foreignpolicy.com/.

65. Forrest, S., Hofmeyr, S.A., Somayaji, A. & Longstaff, T.A., 1996. A sense of self for unix processes. In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*. pp. 120–128.

66. Freeman, S. & Edwards-Levy, A., 2013. Americans Still Can't Decide Whether Edward Snowden Is A "Traitor" Or A "Hero," Poll Finds. *Huffington Post*. Available at: http://www.huffingtonpost.com/2013/10/30/edward-snowden-poll_n_4175089.html.

67. Galperin, E., Schoen, S. & Eckersley, P., 2011. A Post Mortem on the Iranian DigiNotar Attack. Available at: https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack [Accessed April 12, 2014].

68. Gartner, 2013. *Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013*, Available at: https://www.gartner.com/newsroom/id/2665715.

69. Gartner, 2014a. Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware. Available at: https://www.gartner.com/newsroom/id/2828722 [Accessed November 29, 2014].

70. Gartner, 2012. Gartner Survey Highlights Top Five Daily Activities on Media Tablets. Available at: https://www.gartner.com/newsroom/id/2070515.

71. Gartner, 2014b. *Top 10 Strategic Technology Trends For 2014*, Available at: http://goo.gl/AdfeBN.

72. GCHQ, 2014. GCHQ. Available at: http://www.gchq.gov.uk/Pages/homepage.aspx.

73. Gebauer, M., 2012. Warfare with Malware: NATO Faced with Rising Flood of Cyberattacks. *Spiegel*.

74. Geers, K., Kindlund, D., Moran, N. & Rachwald, R., 2014. *WORLD WAR C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*,

75. Geftic, S., 2013. From SIEM to Security Analytics: The Path Forward. Available at: https://blogs.rsa.com/siem-security-analytics-path-forward/.

76. Gellman, B. & Markon, J., 2013. Edward Snowden says motive behind leaks was to expose "surveillance state" - The Washington Post. Available at: http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html [Accessed November 25, 2014].

77. Gellman, B. & Soltani, A., 2013. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Available at: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

78. Gibbs, S., 2015. Duqu 2.0: computer virus "linked to Israel" found at Iran nuclear talks venue. *The Guardian*. Available at: http://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks.

79. Goman, S. & Barnes, J., 2012. Iran Blamed for Cyberattacks. Available at: http://www.wsj.com/articles/SB10000872396390444657804578052931555576700.

80. Google, 2013. *Safe Browsing API*, Available at: https://developers.google.com/safe-browsing/.

81. Google, 2014. Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability. Available at: http://googleblog.blogspot.gr/2014/03/staying-at-forefront-of-email-security.html.

82. Gov.uk, 2014a. Cyber defence funding worth £2 million available to suppliers. Available at: https://www.gov.uk/government/news/cyber-defence-funding-worth-2-million-available-to-suppliers.

83. Gov.uk, 2014b. *The UK Cyber Security Strategy*, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.

84. Greenwald, G., 2013. NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

85. Greenwald, G. & MacAskill, E., 2013. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

86. Greenwald, G., MacAskill, E. & Poitras, L., 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, 9.

87. Gritzalis, D. et al., 2013. The Sphinx enigma in critical VoIP infrastructures: Human or botnet? In *Proc. of the 4th International Conference on Information, Intelligence, Systems and Applications (IISA-2013)*. pp. 1–6.

88. Gritzalis, D., Stavrou, V., Kandias, M. & Stergiopoulos, G., 2014. Insider Threat: Enhancing BPM through Social Media. In *Proc. of the 6th IFIP International Conference on New Technologies, Mobility and Security (NMTS-2014)*. UAE: Springer.

89. Guin, U. et al., 2014. Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proceedings of the IEEE*, 102(8), pp.1207–1228.

90. Gymnopoulos, L., Dritsas, S., Gritzalis, S. & Lambrinoudakis, C., 2003. GRID security review. In *Proc. of the MMM-ACNS-2003 2nd International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM '03)*. Springer.

91. Hadžiosmanović, D., Simionato, L., Bolzoni, D., Zambon, E. & Etalle, S., 2012. N-gram against the machine: On the feasibility of the n-gram network analysis for binary protocols. In *Research in Attacks, Intrusions, and Defenses*. Springer, pp. 354–373.

92. Healey, J. & Grindal, K., 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association.

93. Helman, P., Liepins, G. & Richards, W., 1992. Foundations of intrusion detection [computer security]. In *Computer Security Foundations Workshop V, 1992. Proceedings.* pp. 114–120.

94. Hendler, J. & Berners-Lee, T., 2010. From the Semantic Web to social machines: A research challenge for AI on the World Wide Web. *Artificial Intelligence*, 174(2), pp.156–161.

95. Heuer, R.J. & Herbig, K., 2001. The insider espionage threat. *Research on Mitigating the Insider Threat to Information Systems*, 2.

96. Hofmeyr, S.A., Forrest, S. & Somayaji, A., 1998. Intrusion detection using sequences of system calls. *Journal of computer security*, 6(3), pp.151–180.

97. Hosenball, M., 2013. NSA chief says Snowden leaked up to 200,000 secret documents | Reuters. Available at: http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114 [Accessed November 25, 2014].

98. Hudson, J., 2013. Deciphering How Edward Snowden Breached the NSA – Venafi. Available at: https://www.venafi.com/blog/post/deciphering-how-edward-snowden-breached-the-nsa/ [Accessed November 25, 2014].

99. ISACA, 2014. *The Growing Cybersecurity Skills Crisis*, Available at: http://www.isaca.org/cyber/Documents/Cybersecurity-Report_pre_Eng_0414.pdf.

100. Isikoff, M., 2013. Chinese hacked Obama, McCain campaigns, took internal documents, officials say - Investigations. Available at: http://investigations.nbcnews.com/_news/2013/06/06/18807056-chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say [Accessed December 2, 2014].

101. Jansson, K. & von Solms, R., 2013. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), pp.584–593.

102. Juels, A. & Rivest, R.L., 2013. Honeywords: Making password-cracking detectable. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. pp. 145–160.

103. Kammas, P., Komninos, T. & Stamatiou, Y.C., 2008. A queuing theory based model for studying intrusion evolution and elimination in computer networks. In *Information Assurance and Security, 2008. ISIAS'08. Fourth International Conference on*. pp. 167–171.

104. Kandias, M., Galbogini, K., Mitrou, L. & Gritzalis, D., 2013. Insiders trapped in the mirror reveal themselves in social media. In *Proc. of the 7th International Conference on Network and System Security (NSS 2013)*. Springer, pp. 220–235.

105. Kandias, M., Mylonas, A., Theoharidou, M. & Gritzalis, D., 2011. Exploitation of auctions for outsourcing security-critical projects. In *Proc. of the 16th IEEE Symposium on Computers and Communications (ISCC '11)*. pp. 646–651.

106. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M. & Gritzalis, D., 2010. An insider threat prediction model. In *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business (TrustBus-2010)*. Springer, pp. 26–37.

107. Kandias, M., Stavrou, V., Bozovic, N. & Gritzalis, D., 2013. Proactive insider threat detection through social media: The YouTube case. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*. pp. 261–266.

108. Kandias, M., Virvilis, N. & Gritzalis, D., 2013. The insider threat in Cloud computing. In *Proc. of the 6th International Conference on Critical Infrastructure Security (CRITIS-2011)*. Springer, pp. 93–103.

109. Kaspersky, 2013a. *Kaspersky Security Bulletin 2013. Overall Statistics for 2013*, Available at: http://goo.gl/30qqal.

110. Kaspersky, 2013b. “Red October” Diplomatic Cyber Attacks Investigation - Securelist. Available at: http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/ [Accessed November 26, 2014].

111. Kaspersky, 2012. Resource 207: Kaspersky Lab. Available at: http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected [Accessed November 26, 2014].

112. Kaspersky, 2015. *The Duqu 2.0*, Available at: https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

113. Kaspersky, 2014. The Regin Platform Nation-state ownage of GSM networks. Available at: http://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf.

114. Kelley, M., 2012. *The Stuxnet Virus at Iran’s Nuclear Facility was Planted by an Iranian Double Agent*,

115. Kelly, M., 2012. The Stuxnet Virus At Iran’s Nuclear Facility Was Planted By An Iranian Double Agent. Available at: http://www.businessinsider.com/stuxnet-virus-planted-by-iranian-double-agent-2012-4 [Accessed November 25, 2014].

116. Kijewski, P., 2004. ARAKIS-An early warning and attack identification system. In *Proc. of the 16th Annual First Conference, Dudapest, Hungary*.

117. Kirda, E. & Kruegel, C., 2005. Protecting users against phishing attacks with antiphish. In *Computer Software and Applications Conference, 2005. {COMPSAC} 2005. 29th Annual International*. IEEE, pp. 517–524.

118. Kokolakis, S., Gritzalis, D. & Katsikas, S., 1998. Generic security policies for healthcare information systems. *Health informatics journal*, 4(3-4), pp.184–195.

119. Kolter, J.Z. & Maloof, M.A., 2006. Learning to detect and classify malicious executables in the wild. *The Journal of Machine Learning Research*, 7, pp.2721–2744.

120. Komninos, T., Spirakis, P., Stamatiou, Y.C. & Vavitsas, G., 2007. A worm propagation model based on scale free network structures and people’s email acquaintance profiles. *International Journal of Computer Science and Network Security*, 7(2), pp.308–315.

121. Kotenko, I. & Skormin, V., 2010. *Computer Network Security: 5th International Conference, on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010, St. Petersburg, Russia, September 8-10, 2010, Proceedings*, Springer Science & Business Media.

122. Kotzanikolaou, P., Theoharidou, M. & Gritzalis, D., 2013a. Assessing n-order dependencies between critical infrastructures. *International Journal of Critical Infrastructures*, 9(1-2), pp.93–110.

123. Kotzanikolaou, P., Theoharidou, M. & Gritzalis, D., 2013b. Cascading effects of common-cause failures in critical infrastructures. In *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection (CIP-2013)*. Springer, pp. 171–182.

124. Krekel, B., 2009. *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Available at: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

125. Lagadec, P., 2006. Diode r{é}seau et ExeFilter: 2 projets pour des interconnexions s{é}curis{é}es. *Proc. of SSTIC06*, pp.1–15.

126. Lampson, B.W., 1973. A note on the confinement problem. *Communications of the ACM*, 16(10), pp.613–615.

127. Langner, R., 2011. Stuxnet: Dissecting a cyberwarfare weapon. *Security & Privacy, IEEE*, 9(3), pp.49–51.

128. Lee, H.L. & Whang, S., 2005. Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of production economics*, 96(3), pp.289–300.

129. Lekkas, D. & Gritzalis, D., 2007a. e-Passports as a means towards the first world-wide Public Key Infrastructure. In *Proc. of the 4th European PKI Workshop (EuroPKI ’07)*. Springer, pp. 34–48.

130. Lekkas, D. & Gritzalis, D., 2007b. Long-term verifiability of the electronic healthcare records authenticity. *international journal of medical informatics*, 76(5), pp.442–448.

131. Lemos, R., 2011. Stuxnet attack more effective than bombs | InfoWorld. Available at: http://www.infoworld.com/article/2625351/malware/stuxnet-attack-more-effective-than-bombs.html [Accessed November 26, 2014].

132. Leyden, J., 2014. GCHQ: We can't track crims any more thanks to Snowden. *The register*. Available at: http://www.theregister.co.uk/2014/12/23/gchq_criminal_tracking_post_snowden/.

133. Liao, Y. & Vemuri, V.R., 2002. Using Text Categorization Techniques for Intrusion Detection. In *USENIX Security Symposium*. pp. 51–59.

134. Libicki, M., Sentry, D. & Pollak, J., 2014. *An Examination of the Cybersecurity Labor Market*, Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf.

135. Liu, A., Martin, C., Hetherington, T. & Matzner, S., 2005. A comparison of system call feature for insider threat detection. In *Proc. of the 6th Annual IEEE Systems, Man & Cybernetics, Information Assurance Workshop*. pp. 341–347.

136. Locasto, M.E., Parekh, J.J., Keromytis, A.D. & Stolfo, S.J., 2005. Towards collaborative security and p2p intrusion detection. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*. pp. 333–339.

137. Love, D., 2013. *The Latest Jailbreak Statistics Are Jaw-Dropping*, Available at: http://www.businessinsider.com/jailbreak-statistics-2013-3.

138. Lu, L., Yegneswaran, V., Porras, P. & Lee, W., 2010. Blade: an attack-agnostic approach for preventing drive-by malware infections. In *Proceedings of the 17th {ACM} conference on Computer and communications security*. ACM, pp. 440–450.

139. Lynn, W.J., 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, pp.97–108.

140. Magklaras, G.B. & Furnell, S.M., 2005. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, 24(5), pp.371–380.

141. Mairh, A., Barik, D., Verma, K. & Jena, D., 2011. Honeypot in network security: a survey. In *Proceedings of the 2011 International Conference on Communication, Computing & Security*. pp. 600–605.

142. Mandiant, 2013. *Exposing One of China's Cyber Espionage Units*, Mandiant.

143. Manning, B., 2013. Bradley Manning's statement taking responsibility for releasing documents to WikiLeaks. Available at: http://www.chelseamanning.org/news/bradley-mannings-statement-taking-responsibility-for-releasing-documents-to-wikileaks.

144. Mavrommatis, N. & Monrose, M., 2008. All your iframes point to us. *17th USENIX Security Symposium*. Available at: https://www.usenix.org/legacy/event/sec08/tech/full_papers/provos/provos.pdf [Accessed January 22, 2015].

145. Maxion, R.A. & Tan, K.M.C., 2000. Benchmarking anomaly-based detection systems. In *Dependable Systems and Networks, 2000. DSN 2000. Proceedings International Conference on*. pp. 623–630.

146. Mayer, M., 2014. Our Commitment to Protecting Your Information. Available at: http://yahoo.tumblr.com/post/67373852814/our-commitment-to-protecting-your-information.

147. Mazher, N., Ashraf, I. & Altaf, A., 2013. Which web browser work best for detecting phishing. In *Information & Communication Technologies (ICICT), 2013 5th International Conference on*. pp. 1–5.

148. McAfee, 2014a. McAfee Labs Report Highlights Success of Phishing Attacks with 80 Percent of Business Users Unable to Detect Scams. Available at: http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx.

149. McAfee, 2014b. *McAfee Labs Threats report*, Available at: http://www.mcafee.com/mx/resources/reports/rp-quarterly-threat-q1-2014.pdf.

150. Mcafee, 2014. *Site Advisor*, Available at: https://www.siteadvisor.com/.

151. McAfee Labs, 2010. *Protecting Your Critical Assets - Lessons Learned from "Operation Aurora,"* Available at: http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

152. McDonald, G., Murchu, L.O., Doherty, S. & Chien, E., 2013. Stuxnet 0.5: The missing link. *Symantec Report*.

153. Melber, D., 2013. Securing and Auditing High Risk Files on Windows Servers. Available at: http://www.windowsecurity.com/articles-tutorials/windows_server_2008_security/securing-auditing-high-risk-files-windows-servers.html [Accessed November 25, 2014].

154. Microsoft, 2011. SmartScreen Filter - Microsoft Windows. *windows.microsoft.com*. Available at: http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/smartscreen-filter [Accessed November 15, 2014].

155. Microsoft, 2013. What is Protected View? Available at: https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653?ui=en-US&rs=en-US&ad=US [Accessed November 26, 2014].

156. Miller, J.F., 2013. *Supply Chain Attack Framework and Attack Patterns*,

157. Mitrou, L. & Karyda, M., 2006. Employees' privacy vs. employers' security: Can they be balanced? *Telematics and Informatics*, 23(3), pp.164–178.

158. Modi, C. et al., 2013. A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, 36(1), pp.42–57.

159. Moore, J., 2015. Anonymous's "Electronic Holocaust" Against Israel Falls Flat. Available at: http://europe.newsweek.com/anonymous-electronic-holocaust-against-israel-has-limited-success-320176.

160. Moskowitz, J., 2015. Cyberattack tied to Hezbollah ups the ante for Israel's digital defenses. Available at: http://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses.

161. Mozilla, 2014. Mozilla Support. Available at: https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work#w_how-does-phishing-and-malware-protection-work-in-firefox.

162. Mylonas, A., Dritsas, S., Tsoumas, B. & Gritzalis, D., 2012. On the feasibility of malware attacks in smartphone platforms. In *E-Business and Telecommunications*. Springer, pp. 217–232.

163. Mylonas, A., Gritzalis, D., Tsoumas, B. & Apostolopoulos, T., 2013. A qualitative metrics vector for the awareness of smartphone security users. In *Trust, Privacy, and Security in Digital Business*. Springer, pp. 173–184.

164. Mylonas, A., Kastania, A. & Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, pp.47–66.

165. Mylonas, A., Tsalis, N. & Gritzalis, D., 2013. Evaluating the manageability of web browsers controls. In *9th International Workshop on Security and Trust Management (STM-2013)*. United Kingdom: Springer, pp. 82–98.

166. Nakashima, E., 2014. U.S. cyberwarfare force to grow significantly, defense secretary says. Available at: http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html.

167. Nazario, J., 2009. Phoneyc: A virtual client honeypot. In *Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*. p. 6.

168. Netcraft, 2014. *Phishing Site Feed*, Available at: http://www.netcraft.com/anti-phishing/phishing-site-feed/.

169. Nguyen, N.T., Reiher, P.L. & Kuenning, G.H., 2003. Detecting Insider Threats by Monitoring System Call Activity. In *IAW*. pp. 45–52.

170. Oberheide, J., Cooke, E. & Jahanian, F., 2008. {CloudAV}: N-Version Antivirus in the Network Cloud. In *{USENIX} Security Symposium*. pp. 91–106.

171. Opendns, 2014. *OpenDNS*, Available at: http://www.opendns.com/.

172. OWASP, 2014. *Certificate and Public Key Pinning*, Available at: http://www.netcraft.com/anti-phishing/phishing-site-feed/.

173. Perdisci, R., Lanzi, A. & Lee, W., 2008. Classification of packed executables for accurate computer virus detection. *Pattern Recognition Letters*, 29(14), pp.1941–1946.

174. Perdisci, R., Lanzi, A. & Lee, W., 2008. McBoost: Boosting scalability in malware collection and analysis using statistical classification of executables. *Computer Security Applications …*. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4721567 [Accessed January 22, 2015].

175. Phishtank, 2014. *Join the fight against phishing*, Available at: https://www.phishtank.com/.

176. Pilkington, E., 2013. Bradley Manning a traitor who set out to harm US, prosecutors conclude. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jul/25/bradley-manning-traitor-wikileaks-prosecution.

177. Pitropakis, N., Darra, E., Vrakas, N. & Lambrinoudakis, C., 2013. It's All in the Cloud: Reviewing Cloud Security. In *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*. pp. 355–362.

178. Poitras, L., Rosenbach, M. & Holger, S., 2014. "A" for Angela: GCHQ and NSA Targeted Private German Companies and Merkel. *Spiegel*. Available at: http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

179. Polemi, D. et al., 2013. S-port: Collaborative security management of port information systems. In *Information, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference on*. pp. 1–6.

180. Prathapani, A., Santhanam, L. & Agrawal, D.P., 2009. Intelligent honeypot agent for blackhole attack detection in wireless mesh networks. In *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*. pp. 753–758.

181. Provos, N. et al., 2007. The ghost in the browser analysis of web-based malware. In *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*. p. 4.

182. Puleo, A.J., 2006. *Mitigating insider threat using human behavior influence models*,

183. Raiu, C., Soumenkov, I., Baumgartner, K. & Kamluk, V., 2013. *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor*, Available at: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf.

184. Rajab, M.A., Ballard, L., Lutz, N., Mavrommatis, P. & Provos, N., 2013. {CAMP}: Content-Agnostic Malware Protection. In *NDSS*. Citeseer.

185. RaniSahu, K. & Dubey, J., 2014. A Survey on Phishing Attacks. *International Journal of Computer Applications*, 88(10), pp.42–45.

186. Rasch, G., 1993. *Probabilistic models for some intelligence and attainment tests.*, ERIC.

187. Reed, T., 2007. *At the abyss: an insider's history of the Cold War*, Random House LLC.

188. Robertson, J. & Riley, M., 2014. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era. *Bloomberg*. Available at: http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html [Accessed December 15, 2014].

189. Rogers, M.K., 2001. *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. University of Manitoba.

190. Rosiello, A.P.E., Kirda, E., Kruegel, C. & Ferrandi, F., 2007. A layout-similarity-based approach for detecting phishing pages. In *Security and Privacy in Communications Networks and the Workshops, 2007. {SecureComm} 2007. Third International Conference on*. IEEE, pp. 454–463.

191. Ross, R.S., 2012. Guide for Conducting Risk Assessments (NIST SP-800-30rev1). *The National Institute of Standards and Technology (NIST), Gaithersburg*.

192. RSA, 2011. Anatomy of an Attack - Speaking of Security - The RSA Blog and Podcast. Available at: https://blogs.rsa.com/anatomy-of-an-attack/ [Accessed November 25, 2014].

193. RSA, 2014. *RSA Online fraud report*, Available at: http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf.

194. Ben Salem, M. & Stolfo, S., 2011. Decoy Document Deployment for Effective Masquerade Attack Detection. In T. Holz & H. Bos, eds. *Detection of Intrusions and Malware, and Vulnerability Assessment*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 35–54.

195. Sam Adams Award, 2014. Chelsea Manning. Available at: http://samadamsaward.ch/chelsea-manning/.

196. Schneier, B., 2013. More about the NSA's Tailored Access Operations Unit. Available at: https://www.schneier.com/blog/archives/2013/12/more_about_the.html.

197. Schneier, B., 2012. Schneier on Security: The Failure of Anti-Virus Companies to Catch Military Malware. Available at: https://www.schneier.com/blog/archives/2012/06/the_failure_of_3.html [Accessed November 26, 2014].

198. Schultz, E.E., 2002. A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), pp.526–531.

199. Schwartz, M., 2013. Google Aurora Hack Was Chinese Counterespionage Operation. Available at: http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

200. Shahzad, A., Hussain, M. & Khan, M.N.A., 2013. Protecting from Zero-Day Malware Attacks. *Middle-East Journal of Scientific Research*, 17(4), pp.455–464.

201. Shaw, E., Ruby, K. & Post, J., 1998. The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, 2(98), pp.1–10.

202. Sheng, S. et al., 2009. An empirical analysis of phishing blacklists. In *Sixth Conference on Email and Anti-Spam ({CEAS})*.

203. Shin, S., Xu, Z. & Gu, G., 2012. {EFFORT}: Efficient and effective bot malware detection. In *{INFOCOM}, 2012 Proceedings {IEEE}*. IEEE, pp. 2846–2850.

204. Silowash, G.J. et al., 2012. Common Sense Guide to Mitigating Insider Threats (4th Edition). *Software Engineering Institute*, (677).

205. Snapp, S.R. et al., 1991. DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype. In *Proceedings of the 14th national computer security conference*. pp. 167–176.

206. Snort, 2015. Snort. Available at: https://www.snort.org/.

207. Sobrier, J., 2014. *Google Safe Browsing v2 {API}: Implementation notes*, Available at: https://www.zscaler.com/research/Google.

208. Sommer, R. & Paxson, V., 2010. Outside the closed world: On using machine learning for network intrusion detection. In *Security and Privacy (SP), 2010 IEEE Symposium on*. pp. 305–316.

209. Soupionis, Y. & Benoist, T., 2014. Cyber attacks in Power Grid ICT systems leading to financial disturbance. In *9th International Conference on Critical Information Infrastructures Security (CRITIS-2014)*. Cyprus: Springer.

210. Soupionis, Y., Ntalampiras, S. & Giannopoulos, G., 2014. Faults and Cyber Attacks Detection in Critical Infrastructures. In *9th International Conference on Critical Information Infrastructures Security (CRITIS-2014)*. Cyprus: Springer.

211. Spiegel, 2013. Inside TAO: Documents Reveal Top NSA Hacking Unit. Available at: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

212. Spitzner, L., 2003. Honeypots: Catching the insider threat. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. pp. 170–179.

213. Spitzner, L., 2003. The Honeynet Project: Trapping the Hackers. *Security Privacy, IEEE*, 1(2), pp.15–23.

214. Stavrou, V., Kandias, M., Karoulas, G. & Gritzalis, D., 2014. Business Process Modeling for Insider threat monitoring and handling. In *Proc. of 11th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS-2014)*. Germany: Springer, pp. 119–131.

215. Stergiopoulos, G., Theoharidou, M. & Gritzalis, D., 2015. Using logical error detection in Remote-Terminal Units to predict initiating events of Critical Infrastructures failures. In *Proc. of the 3rd International Conference on Human Aspects of Information Security, Privacy and Trust (HCI-2015)*. USA: Springer.

216. Strobel, W., 2013. Analysis: Manning damage has fallen well short of worst U.S. fears. *Reuters*. Available at: http://www.reuters.com/article/2013/07/31/us-usa-wikileaks-manning-damage-analysis-idUSBRE96U00420130731.

217. Symantec, 2014a. *2014 Internet Security Threat Report*, Available at: http://www.symantec.com/security_response/publications/threatreport.jsp.

218. Symantec, 2014b. *Regin: Top-tier espionage tool enables stealthy surveillance*, Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf.

219. Symantec, 2014c. *Safe Web*, Available at: https://safeweb.norton.com.

220. Taborek, N. & Capaccio, T., 2013. Apple Mobile Devices Cleared for Use on U.S. Military Networks. *Bloomberg*. Available at: http://www.bloomberg.com/news/2013-05-17/apple-mobile-devices-cleared-for-use-on-u-s-military-networks.html [Accessed November 15, 2014].

221. Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E., 2005. The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), pp.472–484.

222. Theoharidou, M., Kotzanikolaou, P. & Gritzalis, D., 2011. Risk assessment methodology for interdependent critical infrastructures. *International Journal of Risk Assessment and Management*, 15(2-3), pp.128–148.

223. Theoharidou, M., Papanikolaou, N., Pearson, S. & Gritzalis, D., 2013. Privacy risks, security and accountability in the Cloud. In *Proc. of the 5th IEEE Conference on Cloud Computing Technology and Science (CloudCom-2013)*. United Kingdom: IEEE Press, pp. 177–184.

224. Theoharidou, M., Tsalis, N. & Gritzalis, D., 2013. In cloud we trust: risk-assessment-as-a-service. In *Proc. of the 7th IFIP International Conference on Trust Management (IFIP TM-2013)*. Spain: Springer, pp. 100–110.

225. Thompson, P., 2004. Weak models for insider threat detection. In *Defense and Security*. pp. 40–48.

226. Thonnard, O. & Dacier, M., 2008. A framework for attack patterns' discovery in honeynet data. *digital investigation*, 5, pp.S128–S139.

227. Timberg, C., 2013. Microsoft to encrypt data in its services in bid to prevent snooping. *The Washington Post*. Available at: http://www.washingtonpost.com/business/technology/microsoft-to-encrypt-data-in-its-services-in-bid-to-prevent-snooping/2013/12/04/f91f7b02-5d2c-11e3-bc56-c6ca94801fac_story.html.

228. Times, 2014. Time: The 100 most influential people in the world. *Time magazine*. Available at: http://time.com/time100-2014/.

229. Timm, T., 2014. Congress wants NSA reform after all. Obama and the Senate need to pass it. *The Guardian*. Available at: http://www.theguardian.com/commentisfree/2014/jun/20/congress-obama-nsa-reform-obama-senate.

230. Tivadar, M., Balazs, B. & Istrate, C., 2013. *A Closer Look at MiniDukele*, Available at: http://labs.bitdefender.com/wp-content/uploads/downloads/2013/04/MiniDuke_Paper_Final.pdf.

231. TOR, 2015. TOR. Available at: https://tor.eff.org/.

232. TrendMicro, 2015. *Operation Arid Viper*, Available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf.

233. Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y. & Lin, W.-Y., 2009. Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10), pp.11994–12000.

234. Vadrevu, P., Rahbarinia, B., Perdisci, R., Li, K. & Antonakakis, M., 2013. Measuring and Detecting Malware Downloads in Live Network Traffic. In *Computer Security–{ESORICS} 2013*. Springer, pp. 556–573.

235. Vidas, T. et al., 2013. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In *Financial Cryptography and Data Security*. Springer, pp. 52–69.

236. VirusTotal, 2014. *VirusTotal*, Available at: https://www.virustotal.com/.

237. Virvilis, N., Dritsas, S. & Gritzalis, D., 2011a. A cloud provider-agnostic secure storage protocol. In *Proc. of the 5th International Conference on Critical Information Infrastructure Security (CRITIS-2010)*. Springer, pp. 104–115.

238. Virvilis, N., Dritsas, S. & Gritzalis, D., 2011b. Secure cloud storage: Available infrastructures and architectures review and evaluation. In *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS-2011)*. Springer, pp. 74–85.

239. Virvilis, N. & Gritzalis, D., 2013. The big four-What we did wrong in advanced Persistent Threat detection? In *Proc. of the 8th International Conference on Availability, Reliability and Security (ARES-2013)*. IEEE, pp. 248–254.

240. Virvilis, N., Gritzalis, D. & Apostolopoulos, T., 2013. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? In *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing (ATC-2013)*. IEEE, pp. 396–403.

241. Virvilis, N. & Serrano, O., 2014. Changing the game: The art of deceiving sophisticated attackers. In *Proc. of the 6th International Conference on Cyber Conflict (CYCON-014)*. Estonia: IEEE, pp. 87–97.

242. Virvilis, N., Serrano, O. & Dandurand, L., 2014. Big Data analytics for sophisticated attack detection. *ISACA*, 3, pp.22–25.

243. Virvilis, N., Tsalis, N., Mylonas, A. & Gritzalis, D., 2014. Mobile devices: A phisher's paradise. In *Proc. of the 11th International Conference on Security and Cryptography (SECRYPT-2014)*. pp. 79–87.

244. Voris, J.A., Jermyn, J., Keromytis, A.D. & Stolfo, S.J., 2013. Bait and Snitch: Defending Computer Systems with Decoys.

245. Wang, P., Wu, L., Cunningham, R. & Zou, C.C., 2010. Honeypot detection in advanced botnet attacks. *International Journal of Information and Computer Security*, 4(1), pp.30–51.

246. Wang, W. et al., 2013. Detecting targeted attacks by multilayer deception. *Journal of Cyber Security and Mobility*, 2(2), pp.175–199.

247. Weiss, G.W., 1996. *The Farewell Dossier*,

248. Williams, Z., Lueg, J.E. & LeMay, S.A., 2008. Supply chain security: an overview and research agenda. *International Journal of Logistics Management, The*, 19(2), pp.254–281.

249. Wood, B., 2000. An insider threat model for adversary simulation. *SRI International, Research on Mitigating the Insider Threat to Information Systems*, 2, pp.1–3.

250. Wu, H., Schwab, S. & Peckham, R.L., 2008. Signature based network intrusion detection system and method.

251. Xu, Z. & Zhu, S., 2012. Abusing Notification Services on Smartphones for Phishing and Spamming. In *WOOT*. pp. 1–11.

252. Yadron, D., 2014. Symantec Develops New Attack on Cyberhacking. *The Wall Street Journal*. Available at: http://www.wsj.com/articles/SB10001424052702303417104579542140235850578.

253. Zetter, K., 2010. Google Hack Attack Was Ultra Sophisticated, New Details Show. Available at: http://www.wired.com/2010/01/operation-aurora/ [Accessed November 25, 2014].

254. Zhang, H., Liu, G., Chow, T.W.S. & Liu, W., 2011. Textual and visual content-based anti-phishing: a Bayesian approach. *Neural Networks, {IEEE} Transactions on*, 22(10), pp.1532–1546.

255. Zhang, J., Seifert, C., Stokes, J.W. & Lee, W., 2011. Arrow: Generating signatures to detect drive-by downloads. In *Proceedings of the 20th international conference on World wide web*. ACM, pp. 187–196.

256. Zhou, Y. & Jiang, X., 2012. Dissecting android malware: Characterization and evolution. In *Security and Privacy ({SP}), 2012 {IEEE} Symposium on*. IEEE, pp. 95–109.

257. Zhou, Y., Wang, Z., Zhou, W. & Jiang, X., 2012. Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets. In *19th Annual Symposium on Network and Distributed System Security (NDSS)*.