REFERENCES

Abdulla, S., Ramadass, S., Altyeb, A.A., Al-Nassiri, A., 2014. Employing machine learning algorithms to detect unknown scanning and email worms. Int Arab J Inf Technol 11, 140–148.

Amidan, B.G., Ferryman, T.A., Cooley, S.K., 2005. Data outlier detection using the Chebyshev theorem, in: Aerospace Conference, 2005 IEEE. IEEE, pp. 3814–3819.

Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou II, N., Abu-Nimeh, S., Lee, W., Dagon, D., 2012. From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware., in: USENIX Security Symposium.

Ariyapperuma, S., Mitchell, C.J., 2007. Security vulnerabilities in DNS and DNSSEC, in: Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. IEEE, pp. 335–342.

Barford, P., Plonka, D., 2001. Characteristics of network traffic flow anomalies, in: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. ACM, pp. 69–73.

Bereziński, P., Jasiul, B., Szpyrka, M., 2015. An entropy-based network anomaly detection method. Entropy 17, 2367–2408.

Brauckhoff, D., Tellenbach, B., Wagner, A., May, M., Lakhina, A., 2006. Impact of packet sampling on anomaly detection metrics, in: Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement. ACM, pp. 159–164.

Bykova, M., Ostermann, S., Tjaden, B., 2001. Detecting network intrusions via a statistical analysis of network packet characteristics, in: System Theory, 2001. Proceedings of the 33rd Southeastern Symposium on. IEEE, pp. 309–314.

Caglayan, A., Toothaker, M., Drapeau, D., Burke, D., Eaton, G., 2009. Real-time detection of fast flux service networks, in: Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology. IEEE, pp. 285–292.

Callahan, T., Allman, M., Rabinovich, M., 2013. On modern DNS behavior and properties. ACM SIGCOMM Comput. Commun. Rev. 43, 7–15.

Cass, S., 2001. Anatomy of malice [computer viruses]. IEEE Spectr. 38, 56–60.

Chan, Y.-T.F., Shoniregun, C.A., Akmayeva, G.A., 2008. A netflow based internet-worm detecting system in large network, in: Digital Information Management, 2008. ICDIM 2008. Third International Conference on. IEEE, pp. 581–586.

Chandola, V., Banerjee, A., Kumar, V., 2009. Anomaly detection: A survey. ACM Comput. Surv. CSUR 41, 15.

Cisco [WWW Document], 2015. URL http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

Claise, B., 2004. Cisco systems netflow services export version 9 [WWW Document]. URL https://tools.ietf.org/html/rfc3954.txt

Clearswift, 2015. Insider Threat Index 22 [WWW Document]. URL http://pages.clearswift.com/FY16-CITI-Int-Report.html

CVE [WWW Document], 2017. URL https://www.cvedetails.com/browse-by-date.php

da Luz, P.M., 2013. Botnet Detection Using Passive DNS. Master Thesis/Pedro Marques da Luz.

Darodjat, I.H.A., Lim, C., Lukas, 2016. Detecting Advanced Persistent Threat Attack Based on DNS Network Traffic Using Bayesnet Algorithm. Swiss German University, Indonesia.

David, J., Thomas, C., 2015. DDoS Attack Detection Using Fast Entropy Approach on Flow-Based Network Traffic. Procedia Comput. Sci. 30–36.

Dietrich, C.J., Rossow, C., Freiling, F.C., Bos, H., Van Steen, M., Pohlmann, N., 2011. On Botnets that use DNS for Command and Control, in: Computer Network Defense (EC2ND), 2011 Seventh European Conference on. IEEE, pp. 9–16.

Etemad, F.F., Vahdani, P., 2012. Real-time botnet command and control characterization at the host level, in: Telecommunications (IST), 2012 Sixth International Symposium on. IEEE, pp. 1005–1009.

Etherington, D., Conger, K., 2016. Large DDoS attacks cause outages at Twitter, Spotify, and other sites [WWW Document]. URL http://social.techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

Farnham, G., Atlasis, A., 2013. Detecting DNS tunneling, in: SANS Institute InfoSec Reading Room. pp. 1–32.

Feinstein, L., Schnackenberg, D., Balupari, R., Kindred, D., 2003. Statistical approaches to DDoS attack detection and response, in: DARPA Information Survivability Conference and Exposition, 2003. Proceedings. IEEE, pp. 303–314.

Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., Maglaris, V., 2014. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput. Netw. 62, 122–136.

Grill, M., Nikolaev, I., Valeros, V., Rehak, M., 2015. Detecting DGA malware using NetFlow, in: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, pp. 1304–1309.

Gu, G., Perdisci, R., Zhang, J., Lee, W., others, 2008. BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection., in: USENIX Security Symposium. pp. 139–154.

Hands, N.M., Yang, B., Hansen, R.A., 2015. A Study on Botnets Utilizing DNS, in: Proceedings of the 4th Annual ACM Conference on Research in Information Technology. ACM, pp. 23–28.

Harris, B., Hunt, R., 1999. TCP/IP security threats and attack methods. Comput. Commun. 22, 885–897.

Hawkins, D.M., 1980. Identification of outliers. Springer.

Holz, T., Gorecki, C., Rieck, K., Freiling, F.C., 2008. Measuring and Detecting Fast-Flux Service Networks., in: NDSS.

Hsu, C.-H., Huang, C.-Y., Chen, K.-T., 2010. Fast-flux bot detection in real time, in: International Workshop on Recent Advances in Intrusion Detection. Springer, pp. 464–483.

Hunker, J., Probst, C.W., 2011. Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. JoWUA 2, 4–27.

IANA [WWW Document], 2017. URL https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml

Internet Live Stats [WWW Document], 2016. URL http://www.internetlivestats.com/internet-users/

ISC - Internet Systems Consortium [WWW Document], 2017. URL https://www.isc.org/network/survey/

Jiang, J., Papavassiliou, S., 2004. Detecting network attacks in the internet via statistical network traffic normality prediction. J. Netw. Syst. Manag. 12, 51–72.

Kambourakis, G., Moschos, T., Geneiatakis, D., Gritzalis, S., 2007. Detecting DNS amplification attacks, in: International Workshop on Critical Information Infrastructures Security. Springer, pp. 185–196.

Karasaridis, A., Meier-Hellstern, K., Hoeflin, D., 2006. Nis04-2: Detection of dns anomalies using flow data analysis, in: Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE. IEEE, pp. 1–6.

Khule, M., Singh, M., Kulhare, D., 2014. Enhanced worms detection by Netflow. Int. J. Eng. Comput. Sci. 3, 5123–7.

Kim, M.-S., Kong, H.-J., Hong, S.-C., Chung, S.-H., Hong, J.W., 2004. A flow-based method for abnormal network traffic detection, in: Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP. IEEE, pp. 599–612.

Kinable, J., 2008. Detection of network scan attacks using flow data, in: 9th Twente Student Conference on IT, 23th June. Citeseer.

Lakhina, A., Crovella, M., Diot, C., 2005. Mining anomalies using traffic feature distributions, in: ACM SIGCOMM Computer Communication Review. ACM, pp. 217–228.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G., Wolff, S., 2009. A brief history of the Internet. ACM SIGCOMM Comput. Commun. Rev. 39, 22–31.

Licklider, J.C., 1962. Intergalactic Computer Network.

Locky Developers Continue to Enhance Ransomware Delivery and Operation [WWW Document], 2016. URL https://blog.cyren.com/articles/2016-Q3_locky-developers-continue-to-enhance-ransomware-delivery-and-operation.html

Marchal, S., François, J., Wagner, C., State, R., Dulaunoy, A., Engel, T., Festor, O., 2012. DNSSM: A large scale passive DNS security monitoring framework, in: 2012 IEEE Network Operations and Management Symposium. IEEE, pp. 988–993.

Marchal, S., Jiang, X., State, R., Engel, T., 2014. A big data architecture for large scale security monitoring, in: Big Data (BigData Congress), 2014 IEEE International Congress on. IEEE, pp. 56–63.

Mendyk-Krajewska, T., Mazur, Z., 2010. Problem of network security threats, in: Human System Interactions (HSI), 2010 3rd Conference on. IEEE, pp. 436–443.

Mikle, O., Slanỳ, K., Veselỳ, J., Janoušek, T., Surỳ, O., 2011. Detecting hidden anomalies in DNS communication. Casalicchio E DNS EASY.

Mockapetris, P.V., 1987a. Domain names - concepts and facilities [WWW Document]. URL https://tools.ietf.org/html/rfc1034

Mockapetris, P.V., 1987b. Domain names - implementation and specification [WWW Document]. URL https://tools.ietf.org/html/rfc1035

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. 36, 42–57.

Mowbray, M., Hagen, J., 2014. Finding domain-generation algorithms by looking at length distribution, in: Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on. IEEE, pp. 395–400.

Nguyen, T.T., Armitage, G., 2008. A survey of techniques for internet traffic classification using machine learning. IEEE Commun. Surv. Tutor. 10, 56–76.

Oshima, S., Nakashima, T., Sueyoshi, T., 2010. DDoS detection technique using statistical analysis to generate quick response time, in: Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on. IEEE, pp. 672–677.

Plohmann, D., Yakdan, K., Klatt, M., Bader, J., Gerhards-Padilla, E., 2016. A Comprehensive Measurement Study of Domain Generating Malware, in: 25th USENIX Security Symposium (USENIX Security 16). USENIX Association, pp. 263–278.

Pukkawanna, S., Visoottiviseth, V., Pongpaibool, P., 2007. Lightweight detection of DoS attacks, in: Networks, 2007. ICON 2007. 15th IEEE International Conference on. IEEE, pp. 77–82.

Python [WWW Document], 2017. URL https://www.python.org/

Ray Bellis, 2010. DNS Transport over TCP - Implementation Requirements [WWW Document]. URL https://tools.ietf.org/html/rfc5966 (accessed 5.12.17).

Ren, P., Kristoff, J., Gooch, B., 2006. Visualizing DNS traffic, in: Proceedings of the 3rd International Workshop on Visualization for Computer Security. ACM, pp. 23–30.

Rincón, S.R., Vaton, S., Beugnard, A., Garlatti, S., 2015. Semantics based analysis of botnet activity from heterogeneous data sources, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International. IEEE, pp. 391–396.

Sadre, R., Sperotto, A., Pras, A., 2012. The effects of DDoS attacks on flow monitoring applications, in: Network Operations and Management Symposium (NOMS), 2012 IEEE. IEEE, pp. 269–277.

Santosa, K.I., Lim, C., Erwin, A., 2016. Analysis of educational institution DNS network traffic for insider threats, in: Computer, Control, Informatics and Its Applications (IC3INA), 2016 International Conference on. IEEE, pp. 147–152.

Singh, Y.K., 2006. Fundamental of research methodology and statistics. New Age International.

Sperotto, A., Vliek, G., Sadre, R., Pras, A., 2009. Detecting spam at the network level, in: Meeting of the European Network of Universities and Companies in Information and Communication Engineering. Springer, pp. 208–216.

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

Steinwart, I., Hush, D., Scovel, C., 2005. A classification framework for anomaly detection. J. Mach. Learn. Res. 6, 211–232.

Symantec, 2017. Internet Security Threat Report 22 [WWW Document]. URL https://www.symantec.com/security-center/threat-report

Takeuchi, Y., Yoshida, T., Kobayashi, R., Kato, M., Kishimoto, H., 2016. Detection of the DNS Water Torture Attack by Analyzing Features of the Subdomain Name. J. Inf. Process. 24, 793–801.

Vance, A., 2014. Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing, in: Problems of Infocommunications Science and Technology, 2014 First International Scientific-Practical Conference. IEEE, pp. 173–176.

Woolf, N., 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say [WWW Document]. URL https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Wu, H., Dang, X., Zhang, L., Wang, L., 2015. Kalman filter based DNS cache poisoning attack detection, in: Automation Science and Engineering (CASE), 2015 IEEE International Conference on. IEEE, pp. 1594–1600.

Xu, K., Zhang, Z.-L., Bhattacharyya, S., 2005. Profiling internet backbone traffic: behavior models and applications, in: ACM SIGCOMM Computer Communication Review. ACM, pp. 169–180.

Yadav, S., Reddy, A.K.K., Reddy, A.N., Ranjan, S., 2012. Detecting algorithmically generated domain-flux attacks with DNS traffic analysis. IEEEAcm Trans. Netw. 20, 1663–1677.

Yuan, J., Li, Z., Yuan, R., 2008. Information entropy based clustering method for unsupervised internet traffic classification, in: Communications, 2008. ICC'08. IEEE International Conference on. IEEE, pp. 1588–1592.

Zhao, G., Xu, K., Xu, L., Wu, B., 2015. Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis. IEEE Access 3, 1132–1142.