REFERENCES

Acarali, D., Rajarajan, M., Komninos, N., Herwono, I., 2016. Survey of approaches and features for the identification of HTTP-based botnet traffic. Journal of Network and Computer Applications 76, 1–15. https://doi.org/10.1016/j.jnca.2016.10.007

Aiello, M., Mongelli, M., Papaleo, G., 2013. Basic classifiers for DNS tunneling detection, in: 2013 IEEE Symposium on Computers and Communications (ISCC). Presented at the 2013 IEEE Symposium on Computers and Communications (ISCC), IEEE, Split, Croatia, pp. 000880–000885. https://doi.org/10.1109/ISCC.2013.6755060

Almulhem, A., 2009. Network forensics: Notions and challenges, in: 2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). Presented at the 2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), IEEE, Ajman, United Arab Emirates, pp. 463–466. https://doi.org/10.1109/ISSPIT.2009.5407485

Białczak, P., Mazurczyk, W., 2020. Characterizing Anomalies in Malware-Generated HTTP Traffic. Security and Communication Networks 2020, 1–26. https://doi.org/10.1155/2020/8848863

Bortolameotti, R., Peter, A., Everts, M.H., Bolzoni, D., 2015. Indicators of Malicious SSL Connections, in: Qiu, M., Xu, S., Yung, M., Zhang, H. (Eds.), Network and System Security, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 162–175. https://doi.org/10.1007/978-3-319-25645-0_11

Buric, J., Delija, D., 2015. Challenges in network forensics, in: 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Presented at the 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, Opatija, Croatia, pp. 1382–1386. https://doi.org/10.1109/MIPRO.2015.7160490

cisco, 2018. As Encrypted Malicious Web Traffic Increases, Defenders Need Advanced Tools That Provide Visibility - Cisco Blogs [WWW Document].

URL https://blogs.cisco.com/security/as-encrypted-malicious-web-traffic-increases-defenders-need-advanced-tools-that-provide-visibility

Dai, R., Gao, C., Lang, B., Yang, L., Liu, H., Chen, S., 2019. SSL Malicious Traffic Detection Based On Multi-view Features, in: Proceedings of the 2019 the 9th International Conference on Communication and Network Security. Presented at the ICCNS 2019: 2019 the 9th International Conference on Communication and Network Security, ACM, Chongqing China, pp. 40–46. https://doi.org/10.1145/3371676.3371697

DFRWS USA 2001, 2001. A Road Map for Digital Forensic Research.

Eslahi, M., Rohmad, M.S., Nilsaz, H., Naseri, M.V., Tahir, N.M., Hashim, H., 2015. Periodicity classification of HTTP traffic to detect HTTP Botnets, in: 2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). Presented at the 2015 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), IEEE, Langkawi, Kedah, Malaysia, pp. 119–123. https://doi.org/10.1109/ISCAIE.2015.7298339

Ghafir, I., Prenosil, V., Hammoudeh, M., Han, L., Raza, U., 2017. Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence, in: Proceedings of the International Conference on Future Networks and Distributed Systems. Presented at the ICFNDS '17: International Conference on Future Networks and Distributed Systems, ACM, Cambridge United Kingdom. https://doi.org/10.1145/3102304.3102331

Gourley, D., Totty, B., Sayer, M., Aggarwal, A., Reddy, S., 2002a. HTTP: The Definitive Guide [Book]. O'Reilly Media, Inc., Chapter 4.1.

Gourley, D., Totty, B., Sayer, M., Aggarwal, A., Reddy, S., 2002b. HTTP: The Definitive Guide [Book]. O'Reilly Media, Inc., Chapter 3.

Hootsuite & We Are Social (2019), 2021. Digital 2021 April Statshot Report — DataReportal – Global Digital Insights [WWW Document]. URL https://datareportal.com/reports/digital-2021-april-global-statshot

Hwang, C., Kim, H., Lee, H., Lee, T., 2020. Effective DGA-Domain Detection and Classification with TextCNN and Additional Features. Electronics 9, 1070. https://doi.org/10.3390/electronics9071070

J. Clement, 2021. Top retail websites by global traffic 2020 | Statista [WWW Document]. URL https://www.statista.com/statistics/274708/online-retail-and-auction-ranked-by-worldwide-audiences/

Javadianasl, Y., Manaf, Azizah Abd, Zamani, M., 2017. A Practical Procedure for Collecting More Volatile Information in Live Investigation of Botnet Attack, in: Hassanien, A.E., Mostafa Fouad, M., Manaf, Azizah Abdul, Zamani, M., Ahmad, R., Kacprzyk, J. (Eds.), Multimedia Forensics and Security, Intelligent Systems Reference Library. Springer International Publishing, Cham, pp. 381–414. https://doi.org/10.1007/978-3-319-44270-9_17

Joshi, R.C., Pilli, E.S., 2016. Network Forensics, in: Fundamentals of Network Forensics, Computer Communications and Networks. Springer London, London, pp. 3–16. https://doi.org/10.1007/978-1-4471-7299-4_1

Kumar, G., 2016. Denial of service attacks – an updated perspective. Systems Science & Control Engineering 4, 285–294. https://doi.org/10.1080/21642583.2016.1241193

Lambion, D., Josten, M., Olumofin, F., De Cock, M., 2020. Malicious DNS Tunneling Detection in Real-Traffic DNS Data, in: 2020 IEEE International Conference on Big Data (Big Data). Presented at the 2020 IEEE International Conference on Big Data (Big Data), IEEE, Atlanta, GA, USA, pp. 5736–5738. https://doi.org/10.1109/BigData50022.2020.9378418

Law, F.Y.W., Chow, K.P., Lai, P.K.Y., Tse, H.K.S., 2010. A Host-Based Approach to BotNet Investigation?, in: Goel, S. (Ed.), Digital Forensics and Cyber Crime, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 161–170. https://doi.org/10.1007/978-3-642-11534-9_16

Leach, P.J., Berners-Lee, T., Mogul, J.C., Masinter, L., Fielding, R.T., Gettys, J., n.d. Hypertext Transfer Protocol -- HTTP/1.1 [WWW Document]. URL https://tools.ietf.org/html/rfc2616#section-1 (accessed 4.20.21).

Li, X., 2017. A Review of Motivations of Illegal Cyber Activities. Kriminol. soc. integr. (Online) 25, 110–126. https://doi.org/10.31299/ksi.25.1.4

Marnerides, A.K., 2014. Traffic Anomaly Diagnosis in Internet Backbone Networks: A Survey 22.

Microsoft, 2021. X.509 Public Key Certificates [WWW Document]. URL https://docs.microsoft.com/id-id/windows/win32/seccertenroll/about-x-509-public-key-certificates

Octa.com, 2021. Establishing a SSL/TLS Session - Transport Layer Security | Okta Developer [WWW Document]. URL https://developer.okta.com/books/api-security/tls/how/

Pilli, E.S., Joshi, R.C., Niyogi, R., 2010. A Generic Framework for Network Forensics. IJCA 1, 1–6. https://doi.org/10.5120/251-408

Plohmann, D., n.d. Botnets: Detection, Measurement, Disinfection & Defence 153.

P.Mockapetris, 1987. https://www.ietf.org/rfc/rfc1035.txt [WWW Document]. URL https://www.ietf.org/rfc/rfc1035.txt

Ren, F., Jiang, Z., Wang, X., Liu, J., 2020. A DGA domain names detection modeling method based on integrating an attention mechanism and deep neural network. Cybersecur 3, 4. https://doi.org/10.1186/s42400-020-00046-6

SonicWall, 2021. 2021 SonicWall Cyber Threat Report (No. 1.4). SonicWall.

Tang, R., Huang, C., Zhou, Y., Wu, H., Lu, X., Sun, Y., Li, Q., Li, J., Huang, W., Sun, S., Pei, D., 2020. A Practical Machine Learning-Based Framework to Detect DNS Covert Communication in Enterprises, in: Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N. (Eds.), Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer International Publishing, Cham, pp. 1–21. https://doi.org/10.1007/978-3-030-63095-9_1

The MITRE Corporation, 2015. MITRE ATT&CK® [WWW Document]. URL https://attack.mitre.org/

walter glenn, 2017. What Is the Service Host Process (svchost.exe) and Why Are So Many Running? [WWW Document]. URL https://www.howtogeek.com/howto/windows-vista/what-is-svchostexe-and-why-is-it-running/

what is tlu.dl.delivery.mp.microsoft.com? - Microsoft Community [WWW Document], 2019. URL https://answers.microsoft.com/en-

us/windows/forum/all/what-is-tludldeliverympmicrosoftcom/0c94d0e5-1e42-49ad-9d77-d13cb6567f9c

whatismybrowser.com, 2021. User Agents - Parser and API - Easily decode any user agent [WWW Document]. URL https://developers.whatismybrowser.com/