

Daftar Pustaka

- Acceptable Jitter and Latency. (n.d.). Retrieved June 29, 2019, from <https://getvoip.com/blog/2018/12/20/acceptable-jitter-latency/>
- Almohannadi, H., Awan, I., Al Hamar, J., Cullen, A., Disso, J. P., & Armitage, L. (2018). Cyber threat intelligence from honeypot data using elasticsearch. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 2018-May*, 900–906. <https://doi.org/10.1109/AINA.2018.00132>
- Branscombe, M. (n.d.). Why you need to care more about DNS. Retrieved from <https://www.cio.com/article/2948378/why-you-need-to-care-more-about-dns.html>
- Brumaghin, E., & Grady, C. (2017). Talos Blog || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Covert Channels and Poor Decisions: The Tale of DNSMessenger. Retrieved April 3, 2019, from <https://blog.talosintelligence.com/2017/03/dnsmessenger.html>
- Bruneau, G. (2010). *DNS Sinkhole*. Retrieved from <https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523>
- Dakhgan, A., Hadi, A., Sarairoh, J. Al, & Alrababah, D. (2018). Passive DNS Analysis Using Bro-IDS. *Proceedings - 2017 International Conference on New Trends in Computing Sciences, ICTCS 2017, 2018-Janua*, 121–126. <https://doi.org/10.1109/ICTCS.2017.47>
- Das, A., Shen, M. Y., Shashanka, M., & Wang, J. (2018). Detection of exfiltration and tunneling over DNS. *Proceedings - 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017, 2018-Janua*, 737–742. <https://doi.org/10.1109/ICMLA.2017.00-71>
- DNS Grind. (n.d.). Retrieved from <https://github.com/pentestmonkey/dns-grind>
- DNScat2 C&C tunneling tools. (n.d.). Retrieved from <https://github.com/iagox86/dnscat2>
- Elastic. (n.d.). Kibana Dashboard. Retrieved September 3, 2019, from <https://www.elastic.co/products/kibana>
- Elasticsearch. (n.d.). Elasticsearch: RESTful, Distributed Search & Analytics | Elastic. Retrieved April 3, 2019, from <https://www.elastic.co/products/elasticsearch>
- Farnham, G. (2013). *Detecting DNS Tunneling*.
- Homem, I., Papapetrou, P., & Dosis, S. (2017). *Entropy-based Prediction of Network*

- Protocols in the Forensic Analysis of DNS Tunnels*. Retrieved from <http://arxiv.org/abs/1709.06363>
- Iodine DNS tunneling Tools. (n.d.). Retrieved from <https://code.kryo.se/iodine/>
- Jaworski, S. (2019). *Using Splunk to Detect DNS Tunneling*.
- Leijenhorst, T. Van, Chin, K., & Lowe, D. (2008). *On the Viability and Performance of DNS Tunneling*.
- Liu, J., Li, S., Zhang, Y., Xiao, J., Chang, P., & Peng, C. (2017). Detecting DNS tunnel through binary-classification based on behavior features. *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems*, 339–346. <https://doi.org/10.1109/Trustcom/BigDataSE/ICCESS.2017.256>
- Mockapetris, P. (1987). *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION - RFC 1035*. Retrieved from <https://www.ietf.org/rfc/rfc1035.txt>
- Pearson. (1998). DNS Tunnel. Retrieved from http://archives.neohapsis.com/archives/bugtraq/1998_2/0079.html
- Pi-Hole. (2019). Pi-Hole, a DNS sinkhole that protects your devices from unwanted content. Retrieved from <https://docs.pi-hole.net/>
- Ramdhany, R., Babar, M. A., Edwards, M., Ullah, F., Chitchyan, R., & Rashid, A. (2017). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, 101(November 2017), 18–54. <https://doi.org/10.1016/j.jnca.2017.10.016>
- Sani, A. F., & Setiawan, M. A. (2019). *DNS Tunneling detection using Elasticsearch*.
- Skoudis, E. (2012). *No Title*. Retrieved from <https://blogs.sans.org/pentesting/files/2012/03/RSA-2012-EXP-108-Skoudis-Ullrich.pdf>
- Xu, K., Butler, P., Saha, S., & Yao, D. D. (2013). DNS for massive-scale command and control. *IEEE Transactions on Dependable and Secure Computing*, 10(3), 143–153. <https://doi.org/10.1109/TDSC.2013.10>