botnets using drift. *Transactions on Emerging Telecommunications Technologies* : e3505.

[46] HOLZ, T., GORECKI, C., RIECK, K. and FREILING, F.C. (2008) Measuring and detecting fast-flux service networks. In *NDSS*.

[47] NAZARIO, J. and HOLZ, T. (2008) As the net churns: Fast-flux botnet observations. In *MALWARE*: 24–31.

[48] SKRZEWSKI, M. (2011) Flow based algorithm for malware traffic detection. In *International Conference on Computer Networks* (Springer).

[49] SPAULDING, J., PARK, J., KIM, J. and MOHAISEN, A. (2018) Proactive detection of algorithmically generated malicious domains. In *Proceedings of the IEEE International Conference on Information Networking (ICOIN)*.

[50] SPAULDING, J., NYANG, D. and MOHAISEN, A. (2017) Understanding the effectiveness of typosquatting techniques. In *Proceedings of the ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*.

[51] ANTONAKAKIS, M., PERDISCI, R., DAGON, D., LEE, W. and FEAMSTER, N. (2010) Building a dynamic reputation system for dns. In *USENIX Sec. Symposium*.

[52] ANTONAKAKIS, M., PERDISCI, R., LEE, W., II, N.V. and DAGON, D. (2011) Detecting malware domains at the upper dns hierarchy. In *USENIX Sec. Symposium*.

[53] BILGE, L., KIRDA, E., KRUEGEL, C. and BALDUZZI, M. (2011) Exposure: Finding malicious domains using passive dns analysis. In *NDSS*.

[54] LANZI, A., SHARIF, M.I. and LEE, W. (2009) K-tracer: A system for extracting kernel malware behavior. In *NDSS*.

[55] PERDISCI, R., LANZI, A. and LEE, W. (2008) Mcboost: Boosting scalability in malware collection and analysis using statistical classification of executables. In *ACSAC*.

[56] LU, L., YEGNESWARAN, V., PORRAS, P. and LEE, W. (2010) Blade: an attack-agnostic approach for preventing drive-by malware infections. In *ACM CCS*: 440–450.

[57] EGELE, M., SCHOLTE, T., KIRDA, E. and KRUEGEL, C. (2008) A survey on automated dynamic malware-analysis techniques and tools. *ACM Comput. Surv.* **44**(2): 6:1–6:42. doi: 10.1145/2089125.2089126, URL http://doi.acm.org/10.1145/2089125.2089126.

[58] WRESSNEGGER, C., SCHWENK, G., ARP, D. and RIECK, K. (2013) A close look on n-grams in intrusion detection: anomaly detection vs. classification. In *Proceedings of the ACM workshop on Artificial intelligence and security* (ACM): 67–76.

[59] KOLTER, J.Z. and MALOOF, M.A. (2006) Learning to detect and classify malicious executables in the wild. *The Journal of Machine Learning Research* **7**: 2721–2744.

[60] SCHULTZ, M.G., ESKIN, E., ZADOK, F. and STOLFO, S.J. (2001) Data mining methods for detection of new malicious executables. In *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on* (IEEE): 38–49.

[61] STRAYER, W.T., LAPSLEY, D.E., WALSH, R. and LIVADAS, C. (2008) Botnet detection based on network behavior. In *Botnet Detection*.

[62] PERDISCI, R., LEE, W. and FEAMSTER, N. (2010) Behavioral clustering of http-based malware and signature generation using malicious network traces. In *USENIX NSDI*.

[63] BILGE, L., BALZAROTTI, D., ROBERTSON, W.K., KIRDA, E. and KRUEGEL, C. (2012) Disclosure: detecting botnet command and control servers through large-scale netflow analysis. In *ACSAC*.

[64] SHEN, F., DEL VECCHIO, J., MOHAISEN, A., KO, S.Y. and ZIAREK, L. (2017) Android malware detection using complexflows. In *ICDCS*.

[65] MEKKY, H., MOHAISEN, A. and ZHANG, Z.L. (2015) Separation of benign and malicious network events for accurate malware family classification. In *IEEE CNS*.

[66] — (2017), Detecting Encrypted Malware Traffic (Without Decryption), https://blogs.cisco.com/security/detecting-encrypted-malware-traffic-without-decryp

[67] — (2017), SSL/TLS-based malware attacks, https://www.zscaler.com/blogs/research/ssltls-based-malware-attacks.

[68] EFROS, A.A. and LEUNG, T.K. (1999) Texture synthesis by non-parametric sampling. In *Computer Vision, 1999. The Proceedings of the Seventh IEEE International Conference on* (IEEE), **2**: 1033–1038.

[69] MOHAISEN, A., ALRAWI, O. and LARSON, M. (2013) *AMAL: High-Fidelity, Behavior-based Automated Malware Analysis and Classification*. Tech. rep., Verisign Labs.

[70] ALPAYDIN, E. (2004) *Introduction to machine learning* (MIT press).

[71] BAYER, U., COMPARETTI, P.M., HLAUSCHEK, C., KRÜGEL, C. and KIRDA, E. (2009) Scalable, behavior-based malware clustering. In *NDSS*.

[72] — (2013), Yara Project: A malware identification and classification tool, http://bit.ly/3hbs3d.

[73] ARBOR NETWORKS (2010), Another family of DDoS bots: Avzhan, http://bit.ly/IJ7yCz.

[74] DAMBALLA (2010), The IMDDOS Botnet: Discovery and Analysis, http://bit.ly/1dRi2yi.

[75] DDOSPEDIA (2013), Darkness (Optima), http://bit.ly/1eR40Jc.

[76] JOSE NAZARIO (2007), BlackEnergy DDoS Bot Analysis, http://bit.ly/1bidVYB.

[77] ARBOR NETWORKS (2011), JKDDOS: DDoS bot with an interest in the mining industry?, http://bit.ly/18juHoS.

[78] MALWARE INTEL. (2010), n0ise Bot. Crimeware particular purpose for DDoS attacks, http://bit.ly/1kd24Mg.

[79] MCAFEE.COM (2011), Revealed: Operation Shady RAT, http://bit.ly/IJ9fQG.

[80] KELLY JACKSON HIGGINS (2013), Dropbox, WordPress Used As Cloud Cover In New APT Attacks, http://ubm.io/1cYMOQS.

[81] TREND MICRO (2011), Trend Micro Exposes LURID APT, http://bit.ly/18mX82e.

[82] — (2012), Sykipot is back, http://www.alienvault.com/open-threat-exchange/blog/sykipot-is-back.

[83] — (2011), ZeroAccess, http://bit.ly/IPxi0N.

[84] SOPHOS (2014), Volume of malware threatens security, http://bit.ly/17UVQ19.