Major Area Exam Reading List

Gianluca Stringhini

1 Botnet Analysis and Mitigation

[33, 45, 12, 3, 4, 21, 12, 27, 19, 42, 69, 103, 76, 97, 13, 51, 89, 7, 80, 16, 5, 70, 11, 34, 91, 35, 84, 24, 105, 95, 107, 48, 25, 39, 88, 40, 101, 15, 77, 10, 100, 17]

2 E-mail Spam

[36, 41, 59, 2, 65, 58, 82, 74, 86, 1, 93, 26, 57, 79, 85, 94, 55, 75, 78, 82, 72, 53, 28, 20, 31, 87, 56, 43, 50, 92, 99, 71, 96, 81, 47]

3 Phishing and Malicious Web

[97, 68, 22, 102, 73, 37]

4 Social Network Spam

[30, 6, 52, 32, 8, 98, 104, 18]

5 Underground Economy

[64, 83, 44, 29, 60, 49, 46, 38, 61, 23, 14, 66, 67, 54, 62, 63, 9, 90]

References

[1] D. Anderson, C. Fleizach, S. Savage, and G. Voelker. Spamscatter: Characterizing internet scam hosting infrastructure. In *USENIX Security Symposium*, 2007.

[2] I. Androutsopoulos, J. Koutsias, K. Chandrinos, and C. Spyropoulos. An experimental comparison of naive Bayesian and keyword-based anti-spam filtering with personal e-mail messages. In *international ACM SIGIR conference on Research and development in information retrieval*, 2000.

[3] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster. Building a dynamic reputation system for DNS. In *USENIX Security Symposium*, 2010.

[4] M. Antonakakis, R. Perdisci, W. Lee, N. Vasiloglou, and D. Dagon. Detecting Malware Domains at the Upper DNS Hierarchy. In *USENIX Security Symposium*, 2011.

[5] G. Banks, A. Fattori, R. Kemmerer, C. Kruegel, and G. Vigna. Mishima: Multilateration of internet hosts hidden using malicious fast-flux agents. *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, 2011.

[6] F. Benvenuto, G. Magno, T. Rodrigues, and V. Almeida. Detecting spammers on twitter. In *Conference on Email and Anti-Spam (CEAS)*, 2010.

[7] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi. Exposure : Finding malicious domains using passive dns analysis. In *Symposium on Network and Distributed System Security (NDSS)*, 2011.

[8] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In *Wold Wide Web Conference (WWW)*, 2009.

[9] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. Measuring Pay-per-Install: The Commoditization of Malware Distribution. *USENIX Security Symposium*, 2011.

[10] J. Caballero, P. Poosankam, C. Kreibich, and D. Song. Dispatcher: Enabling active botnet infiltration using automatic protocol reverse-engineering. In *ACM Conference on Computer and Communications Security (CCS)*, 2009.

[11] C. Castelluccia, M. Kaafar, P. Manils, and D. Perito. Geolocalization of proxied services and its application to fast-flux hidden servers. In *ACM SIGCOMM Conference on Internet Measurement*, 2009.

[12] C. Cho, J. Caballero, C. Grier, V. Paxson, and D. Song. Insights from the inside: A view of botnet management from infiltration. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2010.

[13] C. Y. Cho, D. Babic, and D. Song. Inference and Analysis of Formal Models of Botnet Command and Control Protocols. In *ACM Conference on Computer and Communications Security (CCS)*, 2010.

[14] N. Christin, S. Yanagihara, and K. Kamataki. Dissecting one click frauds. In *ACM Conference on Computer and Communications Security (CCS)*, 2010.

[15] M. Christodorescu and S. Jha. Static analysis of executables to detect malicious patterns. In *USENIX Security Symposium*, 2003.

[16] M. Christodorescu, S. Jha, S. Seshia, D. Song, and R. Bryant. Semantics-aware malware detection. In *IEEE Symposium on Security and Privacy*, 2005.

[17] M. Christodoresu and S. Sha. Testing malware detectors. *International Symposium on Software Testing and Analysis (ISSTA)*, 2004.

[18] Z. Chu, S. Giannivecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In *Annual Computer Security Applications Conference (ACSAC)*, 2010.

[19] E. Cooke, F. Jahanian, and D. Mcpherson. The Zombie Roundup : Understanding , Detecting , and Disrupting Botnets. In *USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, 2005.

[20] G. Cormack and T. Lynam. On-line supervised spam filter evaluation. *ACM Transactions on Information Systems*, 2007.

[21] B. Coskun and S. Dietrich. Friends of An Enemy : Identifying Local Members of Peer-to-Peer Botnets Using Mutual Contacts Categories and Subject Descriptors. In *Annual Computer Security Applications Conference (ACSAC)*, 2010.

[22] M. Cova, C. Kruegel, and G. Vigna. Detection and analysis of drive-by-download attacks and malicious JavaScript code. In *International Conference on World Wide Web (WWW)*, 2010.

[23] T. Cymru. the underground economy : priceless. *Usenix login*, 2006.

[24] D. Dagon, G. Gu, C. P. Lee, and W. Lee. A Taxonomy of Botnet Structures. In *Annual Computer Security Applications Conference (ACSAC)*, 2007.

[25] D. Dagon, C. Zou, and W. Lee. Modeling botnet propagation using time zones. In *Symposium on Network and Distributed System Security (NDSS)*, 2006.

[26] H. Drucker, D. Wu, and V. N. Vapnik. Support vector machines for spam categorization. In *IEEE transactions on neural networks*, 1999.

[27] B. Enright, G. Voelker, S. Savage, C. Kanich, and K. Levchenko. Storm: When researchers collide. *Login, Usenix*, 2008.

[28] M. Felegyhazi, C. Kreibich, and V. Paxson. On the potential of proactive domain blacklisting. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2010.

[29] J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM Conference on Computer and Communications Security (CCS)*, 2007.

[30] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Zhao. Detecting and characterizing social spam campaigns. In *ACM SIGCOMM Conference on Internet Measurement*, 2010.

[31] H. Garcia-Molina and J. Pedersen. Combating Web Spam with TrustRank. In *International Conference on Very Large Data Bases (VLDB)*, 2004.

[32] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: the underground on 140 characters or less. In *ACM Conference on Computer and Communications Security (CCS)*, 2010.

[33] G. Gu, R. Perdisci, J. Zhang, and W. Lee. BotMiner: clustering analysis of network traffic for protocol-and structure-independent botnet detection. In *USENIX Security Symposium*, 2008.

[34] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. Bothunter: Detecting malware infection through ids-driven dialog correlation. In *USENIX Security Symposium*, 2007.

[35] G. Gu, J. Zhang, and W. Lee. BotSniffer: Detecting botnet command and control channels in network traffic. In *Symposium on Network and Distributed System Security (NDSS)*, 2008.

[36] S. Hao, N. Syed, N. Feamster, A. Gray, and S. Krasser. Detecting spammers with SNARE: Spatio-temporal network-level automatic reputation engine. In *USENIX Security Symposium*, 2009.

[37] M. Heiderich, T. Frosch, and T. Holz. Iceshield: Detection and mitigation of malicious websites with a frozen dom. *Symposium on Recent Advances in Intrusion Detection (RAID)*, 2011.

[38] C. Herley and D. Florêncio. Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. *Economics of Information Security and Privacy*, 2010.

[39] T. Holz, C. Gorecki, K. Rieck, and F. Freiling. Measuring and detecting fast-flux service networks. In *Symposium on Network and Distributed System Security (NDSS)*, 2008.

[40] X. Hu, M. Knysz, and K. Shin. Rb-seeker: Auto-detection of redirection botnets. In *Symposium on Network and Distributed System Security (NDSS)*, 2009.

[41] G. Hulten, A. Penta, G. Seshadrinathan, and M. Mishra. Trends in Spam Products and Methods Introduction Trends in Spam Summary References. In *Conference on Email and Anti-Spam (CEAS)*, 2004.

[42] J. John, A. Moshchuk, S. Gribble, and A. Krishnamurthy. Studying spamming botnets using Botlab. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2009.

[43] J. Jung. An empirical study of spam traffic and the use of DNS black lists. *ACM SIGCOMM Conference on Internet Measurement*, 2004.

[44] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *ACM Conference on Computer and Communications Security (CCS)*, 2008.

[45] C. Kanich, K. Levchenko, B. Enright, G. Voelker, and S. Savage. The Heisenbot uncertainty problem: Challenges in separating bots from chaff. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2008.

[46] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. Voelker, and S. Savage. Show Me the Money: Characterizing Spam-advertised Revenue. *USENIX Security Symposium*, 2011.

[47] C. Karlberger, G. Bayler, C. Kruegel, and E. Kirda. Exploiting redundancy in natural language to penetrate bayesian spam filters. *USENIX Workshop on Offensive Technologies (WOOT)*, 2007.

[48] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang. Effective and efficient malware detection at the end host. In *USENIX Security Symposium*, 2009.

[49] M. Konte, N. Feamster, and J. Jung. Dynamics of online scam hosting infrastructure. *Passive and Active Network Measurement*, 2009.

[50] C. Kreibich, B. Enright, G. M. Voelker, and S. Savage. On the spam campaign trail. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2008.

[51] C. Kreibich, C. Kanich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamcraft: An inside look at spam campaign orchestration. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2009.

[52] K. Lee, J. Caverlee, and S. Webb. Uncovering social spammers: social honeypots + machine learning. In *International ACM SIGIR Conference on Research and Development in Information Retrieval*, 2010.

[53] B. Leiba. DomainKeys Identified Mail (DKIM): Using digital signatures for domain verification. *Conference on Email and Anti-Spam (CEAS)*, 2007.

[54] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, and Others. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *IEEE Symposium on Security and Privacy*, 2011.

[55] J. R. Levine. Experiences with Greylisting. In *Conference on Email and Anti-Spam (CEAS)*, 2005.

[56] H. Liu, K. Levchenko, M. Félegyházi, C. Kreibich, G. Maier, G. Voelker, and S. Savage. On the Effects of Registrarlevel Intervention. *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2011.

[57] D. Lowd and C. Meek. Good word attacks on statistical spam filters. In *Conference on Email and Anti-Spam (CEAS)*, 2005.

[58] J. Ma, L. Saul, S. Savage, and G. Voelker. Beyond blacklists: learning to detect malicious web sites from suspicious urls. In *ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009.

[59] T. Meyer and B. Whateley. SpamBayes: Effective open-source, Bayesian based, email classification system. In *Conference on Email and Anti-Spam (CEAS)*, 2004.

[60] D. Molnar, S. Egelman, and N. Christin. This is your data on drugs: lessons computer security can learn from the drug war. In *Workshop on New security paradigms*, 2010.

[61] T. Moore and R. Clayton. *Annual eCrime Researchers Summit*, 2007.

[62] T. Moore and R. Clayton. The consequence of non-cooperation in the fight against phishing. *eCrime Researchers Summit*, 2008.

[63] T. Moore and R. Clayton. The impact of incentives on notice and take-down. *Managing Information Risk and the Economics of Security*, 2009.

[64] T. Moore, R. Clayton, and R. Anderso. The economics of online crime. *The Journal of Economic Perspectives*, 2009.

[65] T. Moore, R. Clayton, and H. Stern. Temporal correlations between spam and phishing websites. In *USENIX Workshop on Large-Scale Exploits and Emerging Threats (LEET)*, 2009.

[66] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. Voelker. An Analysis of Underground Forums. *ACM SIGCOMM Conference on Internet Measurement*, 2011.

[67] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and M. Voelker. Dirty Jobs: The Role of Freelance Labor in Web Service Abuse. In *USENIX Security Symposium*, 2011.

[68] Y. Niu, Y. Wang, H. Chen, M. Ma, and F. Hsu. A quantitative study of forum spamming using context-based analysis. In *Symposium on Network and Distributed System Security (NDSS)*, 2007.

[69] C. Nunnery, G. Sinclair, and B. Kang. Tumbling down the rabbit hole: exploring the idiosyncrasies of botmaster systems in a multi-tier botnet infrastructure. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2010.

[70] A. Pitsillidis, K. Levchenko, C. Kreibich, C. Kanich, G. Voelker, V. Paxson, N. Weaver, and S. Savage. Botnet judo: Fighting spam with itself. In *Symposium on Network and Distributed System Security (NDSS)*, 2010.

[71] P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta. PhishNet: Predictive Blacklisting to Detect Phishing Attacks. *IEEE INFOCOM*, 2010.

[72] M. Prince, B. Dahl, L. Holloway, A. Keller, and E. Langheinrich. Understanding how spammers steal your e-mail address: An analysis of the first six months of data from project honey pot. In *Conference on Email and Anti-Spam (CEAS)*, 2005.

[73] N. Provos, P. Mavrommatis, M. Abu Rajab, and F. Monrose. All your iframes point to us. In *USENIX Security Symposium*, 2008.

[74] Z. Qian, Z. Mao, Y. Xie, and F. Yu. Investigation of Triangular Spamming: a Stealthy and Efficient Spamming Technique. In *IEEE Symposium on Security and Privacy*, 2010.

[75] Z. Qian, Z. Mao, Y. Xie, and F. Yu. On network-level clusters for spam detection. *Symposium on Network and Distributed System Security (NDSS)*, 2010.

[76] A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multifaceted approach to understanding the botnet phenomenon. In *ACM SIGCOMM Conference on Internet Measurement*, 2006.

[77] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging. In *USENIX Workshop on Hot Topics in Understanding Botnet*, 2007.

[78] A. Ramachandran, D. Dagon, and N. Feamster. Can DNS-based blacklists keep up with bots? In *Conference on Email and Anti-Spam (CEAS)*, 2006.

[79] A. Ramachandran and N. Feamster. Understanding the network-level behavior of spammers. *ACM SIGCOMM Computer Communication Review*, 2006.

[80] A. Ramachandran, N. Feamster, and D. Dagon. Revealing botnet membership using DNSBL counter-intelligence. In *USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, 2006.

[81] A. Ramachandran, N. Feamster, and S. Vempala. Filtering spam with behavioral blacklisting. In *ACM Conference on Computer and Communications Security (CCS)*, 2007.

[82] M. Sahami, S. Dumais, D. Heckermann, and E. Horvitz. A Bayesian approach to filtering junk e-mail. *Learning for Text Categorization*, 1998.

[83] D. Samosseiko. THE PARTNERKA–WHAT IS IT, AND WHY SHOULD YOU CARE? In *Virus Bulletin Conference*, 2009.

[84] S. Shin, R. Lin, and G. Gu. Cross-Analysis of Botnet Victims: New Insights and Implications. *Symposium on Recent Advances in Intrusion Detection (RAID)*, 2011.

[85] S. Sinha, M. Bailey, and F. Jahanian. Shades of grey: On the effectiveness of reputation-based "blacklists". In *International Conference on Malicious and Unwanted Software*, 2008.

[86] S. Sinha, M. Bailey, and F. Jahanian. Improving spam blacklisting through dynamic thresholding and speculative aggregation. *Symposium on Network and Distributed System Security (NDSS)*, 2010.

[87] H. Stern and Others. A survey of modern spam tools. In *Conference on Email and Anti-Spam (CEAS)*, 2008.

[88] B. Stock, J. Göbel, M. Engelberth, F. Freiling, and T. Holz. Walowdac - Analysis of a Peer-to-Peer Botnet. *European Conference on Computer Network Defense*, 2009.

[89] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna. Your botnet is my botnet: Analysis of a botnet takeover. In *ACM Conference on Computer and Communications Security (CCS)*, 2009.

[90] B. Stone-Gross, M. Cova, C. Kruegel, and G. Vigna. Peering through the iframe. In *INFOCOM*, 2011.

[91] B. Stone-Gross, C. Kruegel, K. Almeroth, A. Moser, and E. Kirda. FIRE: FInding Rogue nEtworks. In *Annual Computer Security Applications Conference (ACSAC)*, 2009.

[92] B. Taylor. Sender reputation in a large webmail service. In *Conference on Email and Anti-Spam (CEAS)*, 2006.

[93] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song. Design and evaluation of a real-time URL spam filtering service. In *IEEE Symposium on Security and Privacy*, 2011.

[94] R. D. Twining, M. Williamson, M. Mowbray, and M. Rahmouni. Email Prioritization : reducing delays on legitimate mail caused by junk mail. *Technical Report*, 2004.

[95] M. van Eeten, J. Bauer, H. Asghari, S. Tabatabaie, and D. Rand. The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data. In *Workshop on the Economics of Information Security*, 2010.

[96] S. Venkataraman, S. Sen, O. Spatscheck, P. Haffner, and . Song. Exploiting network structure for proactive spam mitigation. In *USENIX Security Symposium*, 2007.

[97] R. Wash. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[98] S. Webb, J. Caverlee, , and C.Pu. Social honeypots: Making friends with a spammer near you. In *Conference on Email and Anti-Spam (CEAS)*, 2008.

[99] G. Wittel and S. Wu. On attacking statistical spam filters. In *Conference on Email and Anti-Spam (CEAS)*, 2004.

[100] P. Wurzinger, L. Bilge, T. Holz, J. Goebel, C. Kruegel, and E. Kirda. Automatically generating models for botnet detection. *European Symposium on Research in Computer Security (ESORICS)*, 2010.

[101] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston. Internet background radiation revisited. In *ACM SIGCOMM Conference on Internet Measurement*, 2010.

[102] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldszmidt, and T. Wobber. How dynamic are IP addresses? 2007.

[103] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov. Spamming botnets: Signatures and characteristics. *ACM SIGCOMM Computer Communication Review*, 2008.

[104] W. Xu, F. Zhang, and S. Zhu. Toward worm detection in online social networks. In *Annual Computer Security Applications Conference (ACSAC)*, 2010.

[105] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda. Panorama: capturing system-wide information flow for malware detection and analysis. In *ACM Conference on Computer and Communications Security (CCS)*, 2007.

[106] L. Zhuang, J. Dunagan, D. Simon, H. Wang, and J. Tygar. Characterizing botnets from email spam records. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2008.