[137] Perdisci R, Lanzi A, Lee W. Mcboost: Boosting scalability in malware collection and analysis using statistical classification of executables. In: Proc. of the ACSAC. 2008. 301−310.

[138] Marko D, Atzeni S, Ugrina L, Rakamaric Z. Evaluation of Android malware detection based on system calls. In: Proc. of the ACM on Int'l Workshop on Security and Privacy Analytics (IWSPA). New Orlean, 2016. 1−8.

[139] Xiao X, Wang Z, Li Q, Xia S, Jiang Y. Back-propagation neural network on Markov chains from system call sequences: A new approach for detecting android malware with system call sequences. In: Proc. of the IET Information Security. 2017. 8−15.

[140] Qiao YC, Yun XC, Zhang YZ, Li SH. Based on transfer custom malicious code automation homology determination method. Acta Electronica Sinica, 2016,44(10):2410−2414 (in Chinese with English abstract).

[141] Ki Y, Kim E, Kim HK. A novel approach to detect malware based on API call sequence analysis. Int'l Journal of Distributed Sensor Networks, 2015,11(6):No.659101.

[142] Zhou H, Zhang W, Wei F, Chen Y. Analysis of Android malware family characteristic based on isomorphism of sensitive API call graph. In: Proc. of the 2017 2nd IEEE Int'l Conf. on Data Science in Cyberspace (DSC). IEEE, 2017. 319−327.

[143] Alam S, Riley R, Sogukpinar I, Carkaci N. Droidclone: Detecting android malware variants by exposing code clones. In: Proc. of the 2016 6th Int'l Conf. on Digital Information and Communication Technology and its Applications (DICTAP). IEEE, 2016. 79−84.

[144] Alam S, Horspool RN, Traore I. MAIL: Malware analysis intermediate language—A step towards automating and optimizing malware detection. In: Proc. of the SIN. ACM SIGSAC, 2013. 233−240.

[145] Aho AV, Lam MS, Sethi R, Ullman JD. Compilers: Principles, Techniques, and Tools. 2nd ed., Boston: Addison-Wesley Longman Publishing Co., Inc., 2006.

[146] Crussell J, Gibler C, Chen H. Attack of the clones: Detecting cloned applications on android markets. In: Proc. of the European Symp. on Research in Computer Security. Berlin, Heidelberg: Springer-Verlag, 2012. 37−54.

[147] Sun X, Zhongyang YB, Xin Z, Mao B, Xie L. Detecting code reuse in Android applications using component-based control flow graph. In: Proc. of the ICT. Springer-Verlag, 2014. 142−155.

[148] Chan PPK, Song WK. Static detection of Android malware by using permissions and API calls. In: Proc. of the 2014 Int'l Conf. on Machine Learning and Cybernetics (ICMLC). IEEE, 2014. 82−87.

[149] Zhu J, Guan Z, Yang Y, Yu L, Sun H, Chen Z. Permission-Based abnormal application detection for Android. In: Proc. of the Information and Communications Security. Springer-Verlag, 2012. 228−239.

[150] Faruki P, Laxmi V, Bharmal A, Gaur MS, Ganmoor V. AndroSimilar: Robust signature for detecting variants of Android malware. Journal of Information Security and Applications, 2015,22:66−80.

[151] Liu X, Liu J, Wang W. Exploring sensor usage behaviors of Android applications based on data flow analysis. In: Proc. of the 2015 34th IEEE Int'l Performance Computing and Communications Conf. (IPCCC). IEEE, 2015. 1−8.

[152] Arp D, Spreitzenbarth M, Hubner M, Gascon H, Rieck K. DREBIN: Effective and explainable detection of Android malware in your pocket. In: Proc. of the 21th Annual Network and Distributed System Security Symp. (NDSS). 2014. 23−26.

[153] Roussev V. Building a better similarity trap with statistically improbable features. In: Proc. of the 2009 42nd Hawaii Int'l Conf. on System Sciences (HICSS 2009). IEEE, 2009. 1−10.

[154] Wang C, Qin Z, Zhang J, Yin H. A malware variants detection methodology with an opcode based feature method and a fast density based clustering algorithm. In: Proc. of the 2016 12th Int'l Conf. on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD). IEEE, 2016. 481−487.

[155] Wu L, Ping R, Ke L, Hai D. Behavior-Based malware analysis and detection. In: Proc. of the 2011 1st Int'l Workshop on Complexity and Data Mining (IWCDM). New York: IEEE, 2011. 39−42.

[156] Santos I, Penya YK, Devesa J, Bingas PG. *N*-grams-based file signatures for malware detection. In: Proc. of the 2009 Int'l Conf. on Enterprise Information Systems (ICEIS), Volume AIDSS. 2009. 317−320.

[157] A biologically inspired immune system for computers. In: Proc. of the Artificial Life IV: 4th Int'l Workshop on the Synthesis and Simulation of Living Systems. MIT Press, 2011. 130−139.

[158] Kolosnjaji B, Zarras A, Webster G, Eckert C. Deep learning for classification of malware system call sequences. In: Proc. of the Australasian Joint Conf. on Artificial Intelligence. Cham: Springer-Verlag, 2016. 137−149.

[159] Dahl GE, Stokes JW, Deng L, Yu D. Large-scale malware classification using random projections and neural networks. In: Proc. of the 2013 IEEE Int'l Conf. on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2013. 3422−3426.

[160] Fang Y, Yu B, Tang Y, Liu L, Lu Z, Wang Y. A new malware classification approach based on malware dynamic analysis. In: Proc. of the Australasian Conf. on Information Security and Privacy. Cham: Springer-Verlag, 2017. 173−189.

[161] Aoyama H. On the chi-square test for weighted samples. Annals of the Institute of Statistical Mathematics, 1953,5(1):25−28.

[162] Cesare S, Xiang Y, Member S. Control flow-based malware variant detection. IEEE Trans. on Dependable Secure Computing, 2014,11(4):304−317.

[163] Awad RA, Sayre KD. Automatic clustering of malware variants. In: Proc. of the 2016 IEEE Conf. on Intelligence and Security Informatics (ISI). IEEE, 2016. 298−303.

[164] Hanna S, Huang L, Wu E, Li S, Chen C, Song D. Juxtapp: A scalable system for detecting code reuse among Android applications. In: Proc. of the 9th Conf. on Detection of Intrusions and Malware & Vulnerability Assessment. 2012.

[165] Allix KFT, Jerome BQ, Klein J, State R, Traon YL. Empirical assessment of machine learning-based malware detectors for Android. Empir Software Engineering, 2016,21:183−211.

[166] The Phrack Staff. "Phrack" 14(68). 2012. http://phrack.org/issues/68/1.html

[167] Xu Z, Ren K, Qin S, Craciun F. CDGDroid: Android malware detection based on deep learning using CFG and DFG. In: Proc. of the Int'l Conf. on Formal Engineering Methods. Cham: Springer-Verlag, 2018. 177−193.

[168] Crussell J, Gibler C, Chen H. Andarwin: Scalable detection of semantically similar Android applications. In: Proc. of the European Symp. on Research in Computer Security. Springer, Berlin, Heidelberg, 2013. 182−199.

[169] Yang W, Li J, Zhang Y, Li Y, Shu J, Gu D. APKLancet: Tumor payload diagnosis and purification for Android applications. In: Proc. of the 9th ACM Symp. on Information, Computer and Communications Security. ACM Press, 2014. 483−494.

[170] Karbab EMB, Debbabi M, Mouheb D. Fingerprinting Android packaging: Generating DNAs for malware detection. Digital Investigation, 2016,18:S33−S45.

[171] Cesare S, Xiang Y, Zhou W. Control flow-based malware variant detection. IEEE Trans. on Dependable and Secure Computing, 2014,11(4):307−317.

[172] Kim J, Kim TG, Im EG. Structural information based malicious app similarity calculation and clustering. In: Proc. of the 2015 Conf. on Research in Adaptive and Convergent Systems. ACM Press, 2015. 314−318.

[173] Feizollah A, Anuar NB, Salleh R, Amalina F. Comparative study of *k*-means and mini batch *k*-means clustering algorithms in Android malware detection using network traffic analysis. In: Proc. of the 2014 Int'l Symp. on Biometrics and Security Technologies (ISBAST). IEEE, 2014. 193−197.

[174] Niu Z, Qin Z, Zhang J, Yin H. Malware variants detection using density based spatial clustering with global opcode matrix. In: Proc. of the Int'l Conf. on Security, Privacy and Anonymity in Computation, Communication and Storage. Cham: Springer-Verlag, 2017. 757−766.

[175] Xu XL, Yun XC, Zhou YL, Kang XB. Online analytical model of massive malware based on feature clusting. Journal on Communications, 2013,34(8):146−153 (in Chinese with English abstract).

[176] Moran N, Bennett J. Supply chain analysis: From quarter master to sunshop. Technical Report, Fire Eye Labs, 2013. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf

[177] Antiy CERT. White elephant dance—Cyber attacks from the south Asian subcontinent. 2016 (in Chinese). https://mp.weixin.qq.com/s/XGZGaylS1B84v-NWaevLEw

[178] Mandiant. Tracking malware import hashing. 2014. https://www.mandiant.com/blog/tracking-malware-import-hashing

[179] Bencsáth B, Pék G, Buttyán L, *et al*. Duqu: A stuxnet-like malware found in the wild. CrySyS Lab Technical Report, Vol.14, 2011. 1−60. https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

[180] MCAFEE. Android malware appears linked to Lazarus cybercrime group. 2017. https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/

[181] Li DH. Malicious sample analysis handbook—Traceability. 2018 (in Chinese). http://blog.nsfocus.net/trace-source/

[182] Venustech. Hedwig (Haiwei) Organization analysis report: A game that cannot be ended. 2016 (in Chinese). http://www.freebuf.com/news/92945.html

[183] 360CERT. QQKEY hacking Trojan new variant traceability analysis. 2018 (in Chinese). https://www.anquanke.com/post/id/147591

[184] 360CERT. Take advantage of a variety of office OLE features for sample analysis and traceability. 2018 (in Chinese). https://www.anquanke.com/post/id/101722

[185] FireEye iSIGHT Intelligence. APT28: At the center of the storm. 2017. https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html

[186] 360CERT. 2017 China advanced persistent threat (APT). 2018. http://www.360doc.com/content/18/0227/06/43535834_732761511.shtml

[187] AVLTeam. Antiy mobile security's "Dvmap" Android malware analysis report. 2017. http://www.freebuf.com/articles/terminal/137015.html

[188] Peng GJ, Wang TG, *et al*. Unknown Trojan Detection System Based on Host Behavior Perception. [referred to as: XDetector]v1.0. [Registration number:2014SR113893], China, 2014 (in Chinese).

[189] Liang Y, Fu JM, Peng GJ, Peng BC. S-tracker: Shellcode detection method based on stack anomaly. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2014,42(11):39−46 (in Chinese with English abstract).

[190] Sha LT, Fu JM, Chen J, Huang SY. A sensitivity measurement for sensitive information processing. Journal of Computer Research and Development, 2014,51(5):1050−1060 (in Chinese with English abstract).

[191] Fu JM, Sha LT, Li PW, Peng GJ. Kernel data active protection method using hardware virtualization. Journal of Sichuan University (Enigineering Science Edition), 2014,46(1):8−13 (in Chinese with English abstract).

[192] Cheng BL, Ming J, Fu JM, Peng GJ, Chen T, Zhang XS, Marion JY. Towards paving the way for large-scale windows malware analysis: Generic binary unpacking with orders-of-magnitude performance boost. In: Proc. of the 25th ACM Conf. on Computer and Communications Security. Toronto, 2018.

[193] Lin YD, Lai YC, Chen CH, Tsai HC. Identifying Android malicious repackaged applications by thread-grained system call sequences. Computers and Security, 2013,39:340−350.

[194] Yang C, Xu Z, Gu G, Yegneswaran V, Porras P. Droidminer: Automated mining and characterization of fine-grained malicious behaviors in Android applications. In: Proc. of the Computer Security (ESORICS 2014). Springer-Verlag, 2014. 163−182.

[195] Chen K, Wang P, Lee Y, *et al*. Finding unknown malice in 10 seconds: Mass vetting for new threats at the Google-play scale. In: Proc. of the USENIX Security Symp. 2015. 658−674.

[196] Roman Unuchek. Dvmap: The first Android malware with code injection. 2017. https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/2017.8

[197] Villanueva MJ. JS_POWMET.DE. 2017. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/js_powmet.de

[198] Peng GJ, Tao F. Malicious Code Forensics. Beijing: Science Press, 2009 (in Chinese).

[199] Fu JM, Peng GJ, Zhang HG. Computer Virus Analysis and Confrontation. 2nd ed., Wuhan: Wuhan University Press, 2009 (in Chinese).

[200] Qiao YC, Yun XC, Zhang YZ. Fast reused function retrieval method based on simhash and inverted index. In: Proc. of the 2016 IEEE Trustcom/BigDataSE/I SPA. IEEE, 2016. 937−944.

附中文参考文献:

[17] AVLTeam.移动端动端 C#病毒"东山再起",利用知名应用通信实现远控隐私窃取.2017.12−28. https://bbs.pediy.com/thread-223596.htm

[24] 360 天眼实验室.OceanLotus(海莲花)APT 报告摘要.2015. http://blogs.360.cn/blog/oceanlotus-apt/

[25] 孔德光,谭小彬,奚宏生,宫涛,帅建梅.提升多维特征检测迷惑恶意代码.软件学报,2010,22(3):522−533. http://www.jos.org.cn/1000-9825/3727.htm [doi: 10.3724/SP.J.1001.2011.03727]

[31] 王蕊,冯登国,杨轶,苏璞睿.基于语义的恶意代码行为特征提取及检测方法.软件学报,2012,23(2):378−393. http://www.jos.org.cn/1000-9825/3953.htm [doi: 10.3724/SP.J.1001.2012.03953]

[46] 彭国军,傅建明,梁玉.软件安全.武汉:武汉大学出版社,2015.262−264.

[55] 邵思豪,高庆,马森,段富尧,马骁,张世琨,胡津华.缓冲区溢出漏洞分析技术研究进展.软件学报,2018,29(5):1179−1198. http://www.jos.org.cn/1000-9825/5504.htm [doi: 10.13328/j.cnki.jos.005504]
[57] 安天发布:潜伏的象群——越过世界屋脊的攻击.2017. https://mp.weixin.qq.com/s/nnrDVgH-mEzZ8cytaUEUVg
[58] 360 追日团队,360CERT,3602 天眼实验室.2017 中国高级持续性威胁(APT)研究报告.2018. https://mp.weixin.qq.com/s/Su3IFORhc55Py7oXOn32ng
[91] 钱雨村,彭国军,王滢,梁玉.恶意代码同源性分析及家族聚类.计算机工程与应用,2015,51(18):76−81.
[100] 乔延臣,云晓春,庹宇鹏,张永铮.基于 simhash 与倒排索引的复用代码快速溯源方法.通信学报,2016,37(11):104−113.
[112] 左黎明,刘二根,徐保根,汤鹏志.恶意代码族群特征提取与分析技术.华中科技大学学报(自然科学版),2010,38(4):46−49.
[114] 韩晓光,曲武,姚宣霞,郭长友,周芳.基于纹理指纹的恶意代码变种检测方法研究.通信学报,2017,35(8):125−136.
[133] 赵炳麟,孟曦,韩金,王婧,刘福东.基于图结构的恶意代码同源性分析.通信学报,2017,38(Z2):86−93.
[134] 葛雨玮,康绯,彭小详.基于动态 BP 神经网络的恶意代码同源性分析.小型微型计算机系统,2016,37(11):2527−2531.
[140] 乔延臣,云晓春,张永铮,李书豪.基于调用习惯的恶意代码自动化同源判定方法.电子学报,2016,44(10):2410−2414.
[175] 徐小琳,云晓春,周勇林,康学斌.基于特征聚类的海量恶意代码在线自动分析模型.通信学报,2013,34(8):146−153.
[177] 安天实验室安全研究与应急处理中心.白象的舞步——来自南亚次大陆的网络攻击.2016. https://mp.weixin.qq.com/s/XGZGaylS1B 84v-NWaevLEw
[181] 李东宏.恶意样本分析手册——溯源篇.2018. http://blog.nsfocus.net/trace-source/
[182] 启明星辰.海德薇(Hedwig)组织分析报告:一场无法结束的博弈.2016. http://www.freebuf.com/news/92945.html
[183] 360CERT.QQKEY 盗号木马新型变种溯源分析.2018. https://www.anquanke.com/post/id/147591
[184] 360CERT.利用了多种 Office OLE 特性的免杀样本分析及溯源.2018. https://www.anquanke.com/post/id/101722
[188] 彭国军,王泰格,等.基于主机行为感知的未知木马检测系统[简称:XDetector]v1.0[登记号:2014SR113893],中国,2014.
[189] 梁玉,傅建明,彭国军,彭碧琛.S-Tracker:基于栈异常的 shellcode 检测方法.华中科技大学学报(自然科学版),2014,42(11):39−46.
[190] 沙乐天,傅建明,陈晶,黄诗勇.一种面向敏感信息处理的敏感度度量方法.计算机研究与发展,2014,51(5):1050−1060.
[191] 傅建明,沙乐天,李鹏伟,彭国军.一种采用硬件虚拟化的内核数据主动保护方法.四川大学学报(工程科学版),2014,46(1):8−13.
[198] 彭国军,陶芬.恶意代码取证.北京:科学出版社,2009.
[199] 傅建明,彭国军,张焕国.计算机病毒分析与对抗.第 2 版,武汉:武汉大学出版社,2009.

宋文纳(1989－),女,河南平顶山人,博士生,主要研究领域为信息安全.

张焕国(1945－),男,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,可信计算,密码学.

彭国军(1979－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为恶意代码检测,可信软件.

陈施旅(1994－),男,硕士,主要研究领域为信息安全.

傅建明(1969－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为系统安全,网络安全.