References

[1] TestDisk - CGSecurity. http://www.cgsecurity.org/wiki/TestDisk.

[2] M. Accetta, R. Baron, W. Bolosky, D. Golub, R. Rashid, A. Tevanian, and M. Young. Mach: A new kernel foundation for UNIX development. *contract*, 39(85-C):1034, 1986.

[3] A. Acharya and M. Raje. MAPbox: using parameterized behavior classes to confine untrusted applications. In *Proceedings of the 9th conference on USENIX Security Symposium-Volume 9*, page 11, 2000.

[4] A. Alexandrov, P. Kmiec, and K. Schauser. *Consh: A confined execution environment for internet computations.* Citeseer, 1998.

[5] J. Anderson. Computer security technology planning study vol i. *Prepared for Electronic Systems Division, October*, page 758206, 1972.

[6] E. Bachaalany. VMDetect: detect if your program is running inside a virtual machine - CodeProject. http://www.codeproject.com/KB/system/VmDetect.aspx, 2005.

[7] G. Banga, P. Druschel, and J. C. Mogul. Resource containers: A new facility for resource management in server systems. *Operating Systems Review*, 33:4558, 1998.

[8] P. Barford and V. Yegneswaran. An inside look at botnets. *Malware Detection*, page 171191, 2007.

[9] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In *ACM SIGOPS Operating Systems Review*, volume 37, page 164177, 2003.

[10] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel. A view on current malware behaviors. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2009.

[11] F. Bellard. QEMU, a fast and portable dynamic translator. In *Proceedings of the USENIX Annual Technical Conference, FREENIX Track*, page 4146, 2005.

[12] M. Ben-Yehuda, M. D. Day, Z. Dubitzky, M. Factor, N. Har'El, A. Gordon, A. Liguori, O. Wasserman, and B. A. Yassour. The turtles project: design and implementation of nested virtualization. In *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, page 16, 2010.

[13] M. Ben-Yehuda, J. Mason, O. Krieger, J. Xenidis, L. Van Doorn, A. Mallick, J. Nakajima, and E. Wahlig. Utilizing IOMMUs for virtualization in linux and xen. In *Proceedings of the 2006 Ottawa Linux Symposium*, 2006.

[14] A. Berman, V. Bourassa, and E. Selberg. TRON: process-specific file protection for the UNIX operating system. In *Proceedings of the USENIX 1995 Technical Conference Proceedings on USENIX 1995 Technical Conference Proceedings*, page 1414, 1995.

[15] M. Bernaschi, E. Gabrielli, and L. Mancini. REMUS: a security-enhanced operating system. *ACM Transactions on Information and System Security (TISSEC)*, 5(1):3661, 2002.

[16] D. J. Bernstein. *Cache-timing attacks on AES.* Citeseer, 2005.

[17] S. Biggs and S. Vidalis. Cloud computing storms. *International Journal of Intelligent Computing Research (IJICR)*, March 2010.

[18] S. Bratus, N. D'Cunha, E. Sparks, and S. Smith. TOCTOU, traps, and trusted computing. *Trusted Computing-Challenges and Applications*, page 1432, 2008.

[19] s. Brian Carrier. The sleuth kit (TSK) & autopsy: Open source digital investigation tools. http://www.sleuthkit.org/.

[20] V. Broucek and P. Turner. Bridging the divide: Rising awareness of forensic issues amongst systems administrators. In *3rd International System Administration and Networking Conference. Maastricht, The Netherlands*, 2002.

[21] R. Buyya, C. S. Yeo, and S. Venugopal. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *The 10th IEEE international conference on high performance computing and communications*, page 513, 2008.

[22] G. Carraro and F. Chong. Software as a service (saas): An enterprise perspective. Last accessed November, 28th 2010 at: http://msdn.microsoft.com/en-us/library/aa905332.aspx., October 2006.

[23] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, and J. Nazario. Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware. In *Dependable Systems and Networks With FTCS and DCC, 2008. DSN 2008. IEEE International Conference on*, page 177186, 2008.

[24] I. Citrix Systems. Citrix systems citrix XenServer: efficient server virtualization software. http://www.citrix.com/English/ps2/products/product.asp?contentID=683148.

[25] C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield. Live migration of virtual machines. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*, page 273286, 2005.

[26] A. T. Claudio Guarnieri, Dario Fernandes. Cuckoo sandbox user's guide. http://www.cuckoobox.org/documentation.php, Nov 2011.

[27] A. V. Cleeff, W. Pieters, and R. J. Wieringa. Security implications of virtualization: A literature study. In *2009 International Conference on Computational Science and Engineering*, page 353358, 2009.

[28] cloudtweaks. Thunder in the cloud: $6 cloud-based denial-of-service attack | CloudTweaks.com - the cloud computing community. `http://www.cloudtweaks.com/2010/08/`

thunder-in-the-cloud-6-cloud-based-denial-of-service-attack/, 2010.

[29] A. Dan, A. Mohindra, R. Ramaswami, and D. Sitaram. *Chakra vyuha (cv): a sandbox operating system environment for controlled execution of alien code*. IBM TJ Watson Research Center, 1997.

[30] B. des Ligneris. Virtualization of linux based computers: the linux-VServer project. In *High Performance Computing Systems and Applications, 2005. HPCS 2005. 19th International Symposium on*, page 340346, 2005.

[31] A. Dinaburg, P. Royal, M. Sharif, and W. Lee. Ether: malware analysis via hardware virtualization extensions. In *Proceedings of the 15th ACM conference on Computer and communications security*, page 5162, 2008.

[32] W. Dolle and C. Wegener. Virtualizing rootkits - linux magazine online. http://www.linux-magazine.com/Issues/2008/90/Virtualizing-Rootkits/(offset)/3, 2008.

[33] J. Elliott. Distributed denial of service attacks and the zombie ant effect. *IT PROF*, 2(2):5557, 2000.

[34] Emsi Software EmbH. Definition: Zombies, dictionary of computer security terms. AvailableOnlineat:http://www.emsisoft.com/en/kb/articles/tec080424/, January 2010.

[35] U. Erlingsson and F. Schneider. SASI enforcement of security policies: A retrospective. In *Proceedings of the 1999 workshop on New security paradigms*, page 8795, 1999.

[36] U. Erlingsson and F. Schneider. IRM enforcement of java stack inspection. In *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, page 246255, 2000.

[37] L. Farrar. How safe is cloud computing? - CNN.com. http://edition.cnn.com/2010/TECH/03/12/cloud.computing.security/index.html, March 2010.

[38] T. Garfinkel. Virtual machine monitors: Current technology and future trends.

[39] T. Garfinkel. Traps and pitfalls: Practical problems in system call interposition based security tools. In *Proceedings of the Network and Distributed Systems Security Symposium*, 2003.

[40] T. Garfinkel, B. Pfaff, and M. Rosenblum. Ostia: A delegating architecture for secure system call interposition. In *Proc. Network and Distributed Systems Security Symposium*, 2004.

[41] T. Garfinkel, M. Rosenblum, and D. Boneh. Flexible OS support and applications for trusted computing. In *Proceedings of the 9th conference on Hot Topics in Operating Systems-Volume 9*, page 2525, 2003.

[42] D. Ghormley, D. Petrou, S. Rodrigues, and T. Anderson. SLIC: an extensibility system for commodity operating systems. In *Proceedings of the annual conference on USENIX Annual Technical Conference*, page 44, 1998.

[43] I. Goldberg, D. Wagner, R. Thomas, and E. A. Brewer. A secure environment for untrusted helper applications confining the wily hacker. In *Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography-Volume 6*, page 11, 1996.

[44] R. Grapes. Transitioning to cloud computing | cloud computing journal. http://cloudcomputing.sys-con.com/node/1272246, Feb. 2010.

[45] I. Guidance Software. EnCase | cyber security | computer forensics | network security | E-Discovery | eDiscovery | forensics | forensic. http://www.guidancesoftware.com/.

[46] U. Gurav and R. Shaikh. Virtualization: a key feature of cloud computing. In *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*, pages 227–229, 2010.

[47] T. Halfhill. ARM dons armor: TrustZone security extensions strengthen ARMv6 architecture. *Microprocessor Report*, 17(34):2023, 2003.

[48] S. Hand, A. Warfield, K. Fraser, E. Kotsovinos, and D. Magenheimer. Are virtual machine monitors microkernels done right? In *Proceedings of the 10th conference on Hot Topics in Operating Systems-Volume 10*, page 11, 2005.

[49] M. Hogan, F. Liu, A. Sokol, and J. Tong. Nist cloud computing standards roadmap. *NIST Special Publication*, page 35, 2011.

[50] G. Hunt and J. Larus. Singularity: rethinking the software stack. *ACM SIGOPS Operating Systems Review*, 41(2):3749, 2007.

[51] ilook forensics.org. ILook investigator computer forensics software. http://www.ilook-forensics.org/.

[52] D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, and K. Nakao. Malware behavior analysis in isolated miniature network for revealing malware's network activity. In *Communications, 2008. ICC'08. IEEE International Conference on*, page 17151721, 2008.

[53] S. Ioannidis, S. Bellovin, and J. Smith. Sub-operating systems: A new approach to application security. In *Proceedings of the 10th workshop on ACM SIGOPS European workshop*, page 108115, 2002.

[54] I. Ivanov. API hooking revealed. *The Code Project*, 2002.

[55] K. Jackson. Cloud computing 101. xmind - social brainstorming and mind mapping. Technical report, XMind - Social Brainstorming and Mind Mapping available at `http://www.xmind.net/share/_embed/kvjacksn/cloud-computing-101/`, 2010.

[56] K. Jain and R. Sekar. User-level infrastructure for system call interposition: A platform for intrusion detection and confinement. *ISOC Network and Distributed System Security*, 1(1), 2000.

[57] M. Jensen and N. Gruschka. Flooding attack issues of web services and Service-Oriented architectures. In *Proceedings of the Workshop on Security for Web Services and Service-Oriented Architectures (SWSOA, held at GI Jahrestagung 2008*, page 117122, 2008.

[58] M. Jensen, N. Gruschka, and N. Luttenberger. The impact of flooding attacks on network-based services. In *The Third International Conference on Availability, Reliability and Security*, page 509513, 2008.

[59] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono. On technical security issues in cloud computing. In *2009 IEEE International Conference on Cloud Computing*, page 109116, 2009.

[60] M. Kaashoek, D. Engler, G. Ganger, H. Briceno, R. Hunt, D. Mazieres, T. Pinckney, R. Grimm, J. Jannotti, and K. Mackenzie. Application performance and flexibility on exokernel systems. In *ACM SIGOPS Operating Systems Review*, volume 31, page 5265, 1997.

[61] P. Kamp and R. Watson. Jails: Confining the omnipotent root. In *Proceedings of the 2nd International SANE Conference*, 2000.

[62] L. M. Kaufman. Data security in the world of cloud computing. *Security & Privacy, IEEE*, 7(4):61–64, 2009.

[63] S. T. King, P. M. Chen, Y. M. Wang, C. Verbowski, H. J. Wang, and J. R. Lorch. SubVirt: implementing malware with virtual machines. 2006.

[64] S. T. King, P. M. Chen, Y. M. Wang, C. Verbowski, H. J. Wang, and J. R. Lorch. SubVirt: implementing malware with virtual machines. 2006.

[65] J. Kirch. Virtual machine security guidelines. *The Center for Internet Security*, 2007.

[66] J. Kirch. Virtual machine security guidelines version 1.0. Technical report, The Center for Internet Security (CIS), September 2007.

[67] V. Kiriansky, D. Bruening, and S. Amarasinghe. Secure execution via program shepherding. In *Proceedings of the 11th USENIX security symposium*, page 191206, 2002.

[68] V. Kiriansky, D. Bruening, and S. Amarasinghe. Secure execution via program shepherding. In *Proceedings of the 11th USENIX security symposium*, page 191206, 2002.

[69] T. Klein. Jerry.c - VMware fingerprinter. http://www.trapkit.de/research/vmm/jerry/index.html, 2005.

[70] T. Klein. ScoopyNG - the VMware detection tool. http://www.trapkit.de/research/vmm/scoopyng/index.html, 2006.

[71] C. Ko, G. Fink, and K. Levitt. Automated detection of vulnerabilities in privileged programs by execution monitoring. In *Computer Security*

Applications Conference, 1994. Proceedings., 10th Annual, page 134144, 1994.

[72] C. Ko, T. Fraser, L. Badger, and D. Kilpatrick. Detecting and countering system intrusions using software wrappers. In *Proceedings of the 9th conference on USENIX Security Symposium-Volume 9*, page 1111, 2000.

[73] K. Kolyshkin. Virtualization in linux. *White paper, OpenVZ*, 2006.

[74] R. L. Krutz and R. D. Vines. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing.* Wiley Publishing, Inc., Indianapolis, Indiana, 1 edition, 2010.

[75] C. Labs. Public cloud computing with opennebula 1.4. Technical report, C12G Labs, June 2010.

[76] B. Lau and V. Svajcer. Measuring virtual machine detection in malware using DSD tracer. *Journal in Computer Virology*, 6(3):181195, 2010.

[77] C. Li, W. Jiang, and X. Zou. Botnet: Survey and case study. *Fourth International Conference on Innovative Computing, Information and Control, IEEE Computer Society*, page 11841187, 2009.

[78] T. Lindholm and F. Yellin. *Java virtual machine specification.* Addison-Wesley Longman Publishing Co., Inc., 1999.

[79] M. Lindorfer, C. Kolbitsch, and P. Milani Comparetti. Detecting environment-sensitive malware. In *Recent Advances in Intrusion Detection*, page 338357, 2011.

[80] T. Liston and E. Skoudis. On the cutting edge: Thwarting virtual machine detection. In *SANSFIRE'06 Conference*, 2006.

[81] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf. NIST cloud computing reference architecture. *NIST Special Publication*, 500:292, 2011.

[82] F. Lombardi and R. D. Pietro. Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, In Press, Corrected Proof, June 2010.

[83] J. C. Luis M. Vaquero, Luis Rodero-Merino and M. Lindner. A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, 39:50–55, 2009.

[84] T. Mappings. CWE-362: race condition. *CWE Version 1.5*, page 387, 2009.

[85] M. Mare\vs and B. Blackham. A new contest sandbox. *Olympiads in Informatics*, 6:100109, 2012.

[86] P. Mell and T. Grance. The nist definition of cloud computing. Technical report, National Institute of Standards and Technology, Information Technology Laboratory, July 2009.

[87] P. B. Menage. Adding generic process containers to the linux kernel. In *Proceedings of the Linux Symposium*, volume 2, page 4557, 2007.

[88] B. Michelson. Cloud slam: Songnian zhou, platoform, cloud moving into the enterprise. Technical report, TechTarget, available at `http://www.ebizq.net/blogs/bda/2009/04/cloud_slam_songnian_zhou_platf.php`, April 2009.

[89] S. Microsystem. The k virtual machine (KVM). *White Paper*, 1999.

[90] R. Mikkilineni and V. Sarathy. Cloud computing and the lessons from the past. In *2009 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*, page 5762, 2009.

[91] T. Mitchem, R. Lu, and R. O'Brien. Using kernel hypervisors to secure applications. In *Computer Security Applications Conference, 1997. Proceedings., 13th Annual*, page 175181, 1997.

[92] W. Moss and B. Richardson. Zombies in the clouds. 2010.

[93] R. Naraine. VMWare: virtual machine security flaw very serious - security - news & reviews - eWeek.com. `http://www.eweek.com/c/a/Security/VMWare-Virtual-Machine-Security-Flaw-Very-Serious/`, December 2005.

[94] National Vulnerability Database. National vulnerability database (NVD) (CVE-2010-1225). http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1225, April 2010.

[95] National Vulnerability Database. National vulnerability database (NVD) (CVE-2010-3699). http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3699, December 2010.

[96] D. Osvik, A. Shamir, and E. Tromer. Cache attacks and countermeasures: The case of AES. *Topics in CryptologyCT-RSA 2006*, page 120, 2006.

[97] R. Perez, L. van Doorn, and R. Sailer. Virtualization and hardware-based security. *Security & Privacy, IEEE*, 6(5):24–31, 2008.

[98] B. Pfitzmann, J. Riordan, C. Stble, M. Waidner, and A. Weber. The PERSEUS system architecture. 2001.

[99] S. Potter, J. Nieh, and M. Selsky. Secure isolation of untrusted legacy applications. In *Proceedings of the 21st conference on Large Installation System Administration Conference*, page 114, 2007.

[100] N. Provos. Improving host security with system call policies. In *Proceedings of the 12th conference on USENIX Security Symposium-Volume 12*, page 1818, 2003.

[101] T. R. Rajarshi Chakraborty, Srilakshmi Ramireddy and H. R. Rao. The information assurance practices of cloud computing vendors. *IEEE Computer Society*, 2010.

[102] J. S. Reuben. A survey on virtual machine security. *Helsinki University of Technology*, 2007.

[103] J. Rittinghouse and J. F. Ransome. *Cloud computing: implementation, management, and security.* CRC Press Taylor & Francis Group, 2009.

[104] J. Robin and C. Irvine. Analysis of the intel pentium's ability to support a secure virtual machine monitor. In *Proceedings of the 9th conference on USENIX Security Symposium-Volume 9*, page 1010, 2000.

[105] J. Rutkowska. invisiblethings.org - red pill. http://www.ouah.org/Red_%20Pill.html, 2004.

[106] J. Rutkowska. Subverting VistaTM kernel for fun and profit. *Black Hat Briefings*, 2006.

[107] F. Schneider, G. Morrisett, and R. Harper. A language-based approach to security. In *Informatics*, page 86101, 2001.

[108] K. Scott and J. Davidson. Safe virtual execution using software dynamic translation. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, page 209218, 2002.

[109] Search Security, Online Information Security Magazine. What is pulsing zombie? `AvailableOnlineat:http://searchsecurity.techtarget.com/sDefinition/0sid14/gci558213.00.html`.

[110] Security Focus. VMWare remote arbitrary code execution vulnerability. `http://www.securityfocus.com/bid/15998/info`, 2006.

[111] Security Focus. RETIRED: VMware hosted products VMSA-2010-0007 multiple remote and local vulnerabilities. `http://www.securityfocus.com/bid/39345/info`, 2010.

[112] D. Shands, J. Jacobs, R. Yee, and E. Sebes. Secure virtual enclaves: Supporting coalition use of distributed application technologies. *ACM Transactions on Information and System Security*, 4(2):103133, 2001.

[113] Z. Shen and Q. Tong. The security of cloud computing system enabled by trusted computing technology. In *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, volume 2, page V211, 2010.

[114] C. B. W. Shirlei Aparecida de Chaves and F. R. Lamin. Sla perspective in security management for cloud computing. *Sixth International Conference on Networking and Services*, 2010.

[115] K. Skapinetz. Virtualisation as a blackhat tool. *Network Security*, 2007(10):47, 2007.

[116] J. Smith and R. Nair. The architecture of virtual machines. *Computer*, 38(5):3238, 2005.

[117] J. E. Smith and R. Nair. The architecture of virtual machines. *Computer*, 38(5):3238, 2005.

[118] N. Solutions. *Norman sandbox whitepaper.* 2003.

[119] D. X. Song, D. Wagner, and X. Tian. Timing analysis of keystrokes and timing attacks on SSH. In *Proceedings of the 10th conference on USENIX Security Symposium-Volume 10*, page 2525, 2001.

[120] L. Stein. SBOX: put CGI scripts in a box. In *USENIX Annual Technical Conference, General Track*, page 145155, 1999.

[121] W. Sun, Z. Liang, R. Sekar, and V. Venkatakrishnan. One-way isolation: An effective approach for realizing safe execution environments. In *Proceedings of the Network and Distributed System Security Symposium*, page 265278, 2005.

[122] D. Talbot. Vulnerability seen in amazon's cloud-computing. *MIT Technology Review*, October 2009.

[123] H. S. Thomas Ristenpart, Eran Tromer and S. Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. *Proc. 16th ACM Conf. Computer and Communications Security*, pages 199–212, November 2009.

[124] Trend Micro. Cloud computing security: Making virtual machines cloud-ready. Technical report, Trend Micro, May 2010.

[125] P. Tullmann. *The Alta operating system.* PhD thesis, Citeseer, 1999.

[126] A. Vasudevan and R. Yerraballi. Cobra: Fine-grained malware analysis using stealth localized-executions. In *Security and Privacy, 2006 IEEE Symposium on*, page 15pp, 2006.

[127] O. Virtualbox. Virtualbox. `http://www.virtualbox.org/wiki/VirtualBox`, 2009.

[128] VirtualBox.org. Oracle VirtualBox. http://www.virtualbox.org/.

[129] Virtuatopia.com. Configuring VirtualBox virtual machine settings - virtuatopia. `http://www.virtuatopia.com/index.php/Configuring_VirtualBox_Virtual_Machine_Settings`, 2009.

[130] A. Viswanathan and B. Neuman. A survey of isolation techniques. 2007.

[131] E. S. X. VMWare. Server. *GSX Server, product documentation*, 2005.

[132] VMware Security Announcements. [Security-announce] VMSA-2010-0007 VMware hosted products, vCenter server and ESX patches resolve multiple security issues. http://lists.vmware.com/pipermail/security-announce/2010/000090.html, 2010.

[133] D. Wagner. *Janus: an approach for confinement of untrusted applications*. PhD thesis, Department of Electrical Engineering and Computer Sciences, University of California, 1999.

[134] R. Wahbe, S. Lucco, T. Anderson, and S. Graham. Efficient software-based fault isolation. In *ACM SIGOPS Operating Systems Review*, volume 27, page 203216, 1994.

[135] Z. Wang and R. B. Lee. New cache designs for thwarting software cache-based side channel attacks. In *Proceedings of the 34th annual international symposium on Computer architecture*, page 494505, 2007.

[136] Webopedia. What is zombie? - a word definition from the webopedia computer dictionary. `http://www.webopedia.com/TERM/Z/zombie.html`.

[137] J. Wei and C. Pu. TOCTTOU vulnerabilities in UNIX-style file systems: an anatomical study. In *FAST*, volume 5, page 1212, 2005.

[138] L. Whitney. Amazon ec2 cloud service hit by botnet,outage. `http://news.cnet.com/8301-1009_3-10413951-83.html`, December 2009.

[139] S. Wijerathna. Cloud computing: Evaluation of security issues to be concerned. pages 100–120, July 2010.

[140] C. Willems, T. Holz, and F. Freiling. Toward automated dynamic malware analysis using cwsandbox. *IEEE Security & Privacy*, page 3239, 2007.

[141] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov. Spamming botnets: Signatures and characteristics. *ACM SIGCOMM Computer Communication Review*, 38(4):171182, 2008.

[142] K. Yoshioka, Y. Hosobuchi, T. Orii, and T. Matsumoto. Your sandbox is blinded: Impact of decoy injection to public malware analysis systems. *Journal of Information Processing*, 19(0):153168, 2011.

[143] K. Yoshioka, T. Kasama, and T. Matsumoto. Sandbox analysis with controlled internet connection for observing temporal changes of malware behavior. In *The Fourth Joint Workshop on Information Security (JWIS 2009)*, 2009.