References

Many of these sources can be found on the Internet using a search engine, and underground sites tend to move around anyway, so URLs have been omitted except where there appears to be a meaningful single location for a document. The spelling and capitalization of author names/handles in the original sources has been preserved.

[1] E. L. Abel and B. E. Buckley. *The Handwriting on the Wall: Toward a Sociology and Psychology of Graffiti*. Greenwood Press, 1977.

[2] B. Acohido and J. Swartz. Going price for network of zombie PCs: $2,000–$3,000. USA Today, 8 September 2004.

[3] L. M. Adleman. An abstract theory of computer viruses. In *Advances in Cryptology – CRYPTO '88 (LNCS 403)*, pages 354–374, 1990.

[4] P.-M. Agapow. Computational brittleness and evolution in machine language. *Complexity International*, 3, 1996.

[5] A. V. Aho and M. J. Corasick. Efficient string matching: An aid to bibliographic search. *Communications of the ACM*, 18(6):333–340, 1975.

[6] A. V. Aho, M. Ganapathi, and S. W. K. Tjiang. Code generation using tree matching and dynamic programming. *Journal of the ACM*, 11(4):491–516, 1989.

[7] I. A. Al-Kadi. Origins of cryptology: the Arab contributions. *Cryptologia*, XVI(2):97–126, 1992.

[8] Aleph One. Smashing the stack for fun and profit. *Phrack*, 7(49), 1996.

[9] $\aleph_0$. Darwin. *Software – Practice and Experience*, 2:93–96, 1972.

[10] M. Allen. The use of 'social engineering' as a means of violating computer systems. SANS Information Security Reading Room, 13 August 2001.

[11] J. P. Anderson. Computer security threat monitoring and surveillance, 15 April 1980.

[12] J. P. Anderson. Computer security technology planning study: Volume II, October 1972. ESD-TR-73-51, Vol. II.

[13] Anonymous. Understanding encryption and polymorphism. Written by J. Wells?

[14] Anonymous. Double trouble. *Virus Bulletin*, page 5, April 1992.

[15] Anonymous. Peach virus targets Central Point. *Virus Bulletin*, pages 17–18, May 1992.

[16] Anonymous. Disabling technologies – a critical assessment. *Jane's International Defense Review*, 27(7), 1994.

[17] Anonymous. Winword.Concept. *Virus Bulletin*, page 3, October 1995.

[18] anonymous. Once upon a free()... . *Phrack*, 0x0b(0x39), 2001.

[19] W. A. Arbaugh, W. L. Fithen, and J. McHugh. Windows of vulnerability: A case study analysis. *IEEE Computer*, 33(12):52–59, 2000.

[20] S. Axelsson. Aspects of the modelling and performance of intrusion detection. Licentiate thesis, Department of Computer Engineering, Chalmers University of Technology, 2000.

[21] J. Aycock and K. Barker. Creating a secure computer virus laboratory. In *13th Annual EICAR Conference*, 2004. 13pp.

[22] J. Aycock, R. deGraaf, and M. Jacobson, Jr. Anti-disassembly using cryptographic hash functions. Technical Report 2005-793-24, University of Calgary, Department of Computer Science, 2005.

[23] J. Aycock and N. Friess. Spam zombies from outer space. Technical Report 2006-808-01, University of Calgary, Department of Computer Science, 2006.

[24] B. S. Baker, U. Manber, and R. Muth. Compressing differences of executable code. In *ACM SIGPLAN Workshop of Compiler Support for System Software*, 1999.

[25] V. Bala, E. Duesterwald, and S. Banerjia. Dynamo: A transparent dynamic optimization system. In *Proceedings of the ACM SIGPLAN '00 Conference on Programming Language Design and Implementation (PLDI)*, pages 1–12, 2000.

[26] B. Barber. Cheese worm: Pros and cons of a "friendly" worm. SANS Information Security Reading Room, 2001.

[27] A. Bartolich. The ELF virus writing HOWTO, 15 February 2003.

[28] L. E. Bassham and W. T. Polk. Threat assessment of malicious code and human threats. Technical Report IR 4939, NIST, October 1992.

[29] J. Bates. Trojan horse: AIDS information introductory diskette version 2.0. *Virus Bulletin*, pages 3–6, January 1990.

[30] BBC News. Passwords revealed by sweet deal, 20 April 2004.

[31] BBC News. How to sell your self for a song, 24 March 2005.

[32] J. R. Bell. Threaded code. *Communications of the ACM*, 16(6):370–372, 1973.

[33] G. Benford. *Worlds Vast and Various*. EOS, 2000.

[34] J. L. Bentley. *Writing Efficient Programs*. Prentice-Hall, 1982.

[35] A. Bissett and G. Shipton. Some human dimensions of computer virus creation and infection. *International Journal of Human-Computer Studies*, 52:899–913, 2000.

[36] blexim. Basic integer overflows. *Phrack*, 0x0b(0x3c), 2002.

[37] H. Bögeholz. At your disservice: How ATA security functions jeopardize your data. c't 8/2005, S. 172: Hard Disk Security, 1 April 2005.

[38] V. Bontchev. Possible virus attacks against integrity programs and how to prevent them. In *Virus Bulletin Conference*, pages 131–141, 1992.

[39] V. Bontchev. Analysis and maintenance of a clean virus library. In *Virus Bulletin Conference*, pages 77–89, 1993.

[40] V. Bontchev. Are "good" computer viruses still a bad idea? In *Proceedings of the 3rd Annual EICAR Conference*, pages 25–47, 1994.

[41] V. Bontchev. Future trends in virus writing, 1994.

[42] V. Bontchev. Possible macro virus attacks and how to prevent them. *Computers & Security*, 15(7):595–626, 1996.

[43] V. Bontchev. Macro virus identification problems. *Computers & Security*, 17(1):69–89, 1998.

[44] V. Bontchev. Anti-virus spamming and the virus-naming mess: Part 2. *Virus Bulletin*, pages 13–15, July 2004.

[45] V. Bontchev. The real reason for the decline of the macro virus. *Virus Bulletin*, pages 14–15, January 2006.

[46] V. V. Bontchev. *Methodology of Computer Anti-Virus Research*. PhD thesis, University of Hamburg, 1998.

[47] Jordi Bosveld. Online malware scan. http://virusscan.jotti.org/.

[48] T. M. Breuel. Lexical closures for C++. In *USENIX C++ Conference Proceedings*, pages 293–304, 1988.

[49] D. Bristow. Asia: grasping information warfare? Jane's Intelligence Review, 1 December 2000.

[50] J. Brunner. *The Shockwave Rider*. Ballantine, 1975.

[51] Bulba and Kil3r. Bypassing StackGuard and StackShield. *Phrack*, 0xa(0x38), 2000.

[52] CA. eTrust PestPatrol vendor appeal process. CA Spyware Information Center, 25 April 2005. Version 1.1.

[53] CARO. A new virus naming convention, c. 1991.

[54] K. Carr. Sophos anti-virus detection: a technical overview, October 2002.

[55] CERT. Cert incident note IN-2001-09. http://www.cert.org/incident_notes/IN-2001-09.html, 6 August 2001.

[56] K. Cesare. Prosecuting computer virus authors: The need for an adequate and immediate international solution. *The Transnational Lawyer*, 14:135–170, 2001.

[57] S. Cesare. Linux anti-debugging techniques (fooling the debugger), 1999.

[58] S. Cesare. Unix viruses, Undated, post-October 1998.

[59] D. A. Chambers. Method and apparatus for detection of computer viruses. United States Patent #5,398,196, 14 March 1995.

[60] B. Chan, J. Denzinger, D. Gates, K. Loose, and J. Buchanan. Evolutionary behavior testing of commercial computer games. In *Proceedings of the 2004 IEEE Congress on Evolutionary Computation (CEC)*, pages 125–132, 2004.

[61] E. Y. Chen, J. T. Ro, M. M. Deng, and L. M. Chi. System, apparatus and method for the detection and removal of viruses in macros. United States Patent #5,951,698, 14 September 1999.

[62] S. Chen and S. Ranka. Detecting Internet worms at early stage. *IEEE Journal on Selected Areas in Communications*, 23(10):2003–2012, 2005.

[63] X. Chen and J. Heidemann. Detecting early worm propagation through packet matching. Technical Report ISI-TR-2004-585, University of Southern California, Information Sciences Institute, 2004.

[64] D. M. Chess. Virus verification and removal. *Virus Bulletin*, pages 7–11, November 1991.

[65] D. M. Chess, R. Ford, J. O. Kephart, and M. G. Swimmer. System and method for detecting and repairing document-infecting viruses using dynamic heuristics. United States Patent #6,711,583, 23 March 2004.

[66] D. M. Chess, J. O. Kephart, and G. B. Sorkin. Automatic analysis of a computer virus structure and means of attachment to its hosts. United States Patent #5,485,575, 16 January 1996.

[67] B. Cheswick. An evening with Berferd in which a cracker is lured, endured, and studied. In *Proceedings of the Winter USENIX Conference*, 1992.

[68] W. R. Cheswick and S. M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, 1994.

[69] D. Chi. Detection and elimination of macro viruses. United States Patent #5,978,917, 2 November 1999.

[70] E. Chien and P. Ször. Blended attacks exploits, vulnerabilities and buffer-overflow techniques in computer viruses. In *Virus Bulletin Conference*, pages 72–106, 2002.

[71] Chosun Ilbo. N. Korea's hackers rival CIA, expert warns. Digital Chosunilbo (English Edition), 2 June 2005.

[72] CIAC. Information about hoaxes. http://hoaxbusters.ciac.org/HBHoaxInfo.html.

[73] Cisco Systems, Inc. Cisco threat defense system guide: How to provide effective worm mitigation, April 2004.

[74] F. Cohen. Computer viruses: Theory and experiments. *Computers & Security*, 6(1):22–35, 1987.

[75] F. B. Cohen. *A Short Course on Computer Viruses*. Wiley, second edition, 1994.

[76] C. Collberg, C. Thomborson, and D. Low. A taxonomy of obfuscating transformations. Technical Report 148, University of Auckland, Department of Computer Science, 1997.

[77] Computer Associates. Security advisor center glossary. http://www3.ca.com/securityadvisor/glossary.aspx, 2005.

[78] M. Conover and w00w00 Security Team. w00w00 on heap overflows, 1999.

[79] E. Cooke, F. Jahanian, and D. McPherson. The zombie roundup: Understanding, detecting, and disrupting botnets. In *USENIX SRUTI Workshop*, 2005.

[80] C. Cowan, M. Barringer, S. Beattie, and G. Kroah-Hartman. FormatGuard: Automatic protection from `printf` format string vulnerabilities. In *Proceedings of the 10th USENIX Security Symposium*, 2001.

[81] CrackZ. Anti-debugging & software protection advice, 25 April 2003.

[82] M. L. Cramer and S. R. Pratt. Computer virus countermeasures – a new type of electronic warfare. In L. J. Hoffman, editor, *Rogue Programs: Viruses, Worms, and Trojan Horses*, chapter 20, pages 246–260. Van Nostrand Reinhold, 1990.

[83] I. Daniloff. Fighting talk. *Virus Bulletin*, pages 10–12, December 1997.

[84] I. Dawson. Blind buffer overflows in ISAPI extensions. SecurityFocus, 25 January 2005.

[85] T. de Raadt. Exploit mitigation techniques. AUUG'2004 Annual Conference.

[86] M. de Villiers. Computer viruses and civil liability: A conceptual framework. *Tort Trial & Insurance Practice Law Journal*, 40:1:123–179, 2004.

[87] J. Dellinger. Re: Prize for most useful computer virus. *Risks Digest*, 12(30), 1991.

[88] N. Desai. Intrusion prevention systems: the next step in the evolution of IDS. SecurityFocus, 27 February 2003.

[89] t. detristan, t. ulenspiegel, yann_malcom, and m. s. von underduk. Polymorphic shellcode engine using spectrum analysis. *Phrack*, 0x0b(0x3d), 2003.

[90] R. B. K. Dewar. Indirect threaded code. *Communications of the ACM*, 18(6):330–331, 1975.

[91] A. K. Dewdney. In the game called Core War hostile programs engage in a battle of bits. *Scientific American*, 250(5):14–22, 1984.

[92] A. K. Dewdney. A Core War bestiary of viruses, worms and other threats to computer memories. *Scientific American*, 252(3):14–23, 1985.

[93] U. Drepper. Security enhancements in Red Hat Enterprise Linux (beside SELinux), 16 June 2004.

[94] P. Ducklin. Counting viruses. In *Virus Bulletin Conference*, pages 73–85, 1999.

[95] T. Duff. Experience with viruses on UNIX systems. *Computing Systems*, 2(2):155–171, 1989.

[96] EICAR. The anti-virus test file. http://www.eicar.org/anti_virus_test_file.htm, 1 May 2003.

[97] M. W. Eichin and J. A. Rochlis. With microscope and tweezers: An analysis of the Internet virus of November 1988. In *Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pages 326–343, 1989.

[98] I. K. El Far, R. Ford, A. Ondi, and M. Pancholi. On the impact of short-term email message recall on the spread of malware. In *Proceedings of the 14th Annual EICAR Conference*, pages 175–189, 2005.

[99] B. W. Ellis. The international legal implications and limitations of information warfare: What are our options? USAWC Strategy Research Report, 10 April 2001.

[100] J. Erickson. *Hacking: The Art of Exploitation*. No Starch Press, 2003.

[101] F. Esponda, S. Forrest, and P. Helman. A formal framework for positive and negative detection schemes. *IEEE Transactions on Systems, Man, and Cybernetics*, 34(1):357–373, 2004.

[102] H. Etoh. Stack protection schemes: (propolice, StackGuard, XP SP2). PacSec/core04 Conference, 2004.

[103] D. Ferbrache. *A Pathology of Computer Viruses*. Springer-Verlag, 1992.

[104] P. Ferrie and F. Perriot. Detecting complex viruses. SecurityFocus, 6 December 2004.

[105] P. Ferrie and H. Shannon. It's Zell(d)ome the one you expect. *Virus Bulletin*, pages 7–11, May 2005.

[106] P. Ferrie and P. Ször. Zmist opportunities. *Virus Bulletin*, pages 6–7, March 2001.

[107] E. Filiol. Strong cryptography armoured computer viruses forbidding code analysis: The Bradley virus. In *Proceedings of the 14th Annual EICAR Conference*, pages 216–227, 2005.

[108] C. Fischer. TREMOR analysis (PC). *VIRUS-L Digest*, 6(88), 1993.

[109] N. FitzGerald. A virus by any other name – virus naming updated. *Virus Bulletin*, pages 7–9, January 2003.

[110] H. Flake. Structural comparison of executable objects. In *Workshop on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2004.

[111] B. Flint and M. Hughes. Fast virus scanning using session stamping. United States Patent #6,735,700, 11 May 2004.

[112] E. Florio. Backdoor.Ryknos. Symantec Security Response, 22 November 2005.

[113] R. Ford and J. Michalske. Gatekeeper II: New approaches to generic virus prevention. In *Virus Bulletin Conference*, pages 45–50, 2004.

[114] R. Ford and H. H. Thompson. The future of proactive virus detection. In *13th Annual EICAR Conference*, 2004. 11pp.

[115] R. Foulkes and J. Morris. Fighting worms in a large corporate environment: A design for a network anti-worm solution. In *Virus Bulletin Conference*, pages 56–66, 2002.

[116] L. Gamertsfelder. Anti-virus technologies – filtering the legal issues. In *Virus Bulletin Conference*, pages 31–35, 2003.

[117] S. Garfink and M. Landesman. Lies, damn lies and computer virus costs. In *Virus Bulletin Conference*, pages 20–23, 2004.

[118] D. Gerrold. *When Harlie Was One*. Nelson Doubleday, 1972.

[119] P. Gillingwater. Re: Where did they come from ? (PC). comp.virus, 27 November 1989.

[120] S. Gordon. Faces behind the masks, 1994.

[121] S. Gordon. The generic virus writer. In *Virus Bulletin Conference*, 1994.

[122] S. Gordon. What a (Winword.)Concept. *Virus Bulletin*, pages 8–9, September 1995.

[123] S. Gordon. The generic virus writer II. In *Virus Bulletin Conference*, 1996.

[124] S. Gordon. Spyware 101: Exploring spyware and adware risk assessment. In *14th Annual EICAR Conference*, pages 204–215, 2005.

[125] S. Gordon and R. Ford. Cyberterrorism? *Computers & Security*, 21(7):636–647, 2002.

[126] S. Gordon, R. Ford, and J. Wells. Hoaxes & hypes. In *Virus Bulletin Conference*, 1997.

[127] D. Gragg. A multi-level defense against social engineering. SANS Information Security Reading Room, 2002.

[128] S. Granger. Social engineering fundamentals, part I: Hacker tactics. SecurityFocus, 18 December 2001.

[129] S. Granger. Social engineering fundamentals, part II: Combat strategies. SecurityFocus, 9 January 2002.

[130] L. T. Greenberg, S. E. Goodman, and K. J. Soo Hoo. *Information Warfare and International Law*. National Defense University Press, 1998.

[131] GriYo. EPO: Entry-point obscuring. *29A e-zine*, 4, c. 2000.

[132] grugq and scut. Armouring the ELF: Binary encryption on the UNIX platform. *Phrack*, 0x0b(0x3a), 2001.

[133] D. O. Gryaznov. Scanners of the year 2000: Heuristics. In *Virus Bulletin Conference*, pages 225–234, 1995.

[134] A. Gupta and D. C. DuVarney. Using predators to combat worms and viruses: A simulation-based study. In *20th Annual Computer Security Applications Conference*, 2004.

[135] M. Handley, V. Paxson, and C. Kreibich. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics. In *Proceedings of the 10th USENIX Security Symposium*, 2001.

[136] Harl. People hacking: The psychology of social engineering. Access All Areas III, 1997.

[137] D. Harley, R. Slade, and U. E. Gattiker. *Viruses Revealed.* Osborne/McGraw-Hill, 2001.

[138] C. G. Harrison, D. M. Chess, and A. Kershenbaum. Mobile agents: Are they a good idea? IBM Research Report, 28 March 1995.

[139] R. Hasson. Anti-debugging tips. http://www.soft-analysts.com/debugging.php, 13 February 2003.

[140] Headquarters, Department of the Army. Information operations. Field manual No. 100-6, 27 August 1996. United States Army.

[141] H. J. Highland. A macro virus. *Computers & Security*, 8(3):178–188, 1989.

[142] N. Hindocha and E. Chien. Malicious threats and vulnerabilities in instant messaging. In *Virus Bulletin Conference*, pages 114–124, 2003.

[143] S. A. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion detection using sequences of system calls. *Journal of Computer Security*, 6:151–180, 1998.

[144] G. Hoglund and J. Butler. *Rootkits: subverting the Windows kernel.* Addison-Wesley, 2006.

[145] T. Holz and F. Raynal. Defeating honeypots: System issues, part 1. SecurityFocus, 23 March 2005.

[146] R. N. Horspool and N. Marovac. An approach to the problem of detranslation of computer programs. *The Computer Journal*, 23(3):223–229, 1980.

[147] M. Howard. Reviewing code for integer manipulation vulnerabilities. MSDN Library, 28 April 2003.

[148] J. W. Hunt and M. D. McIlroy. An algorithm for differential file comparison. Technical Report 41, Bell Laboratories, Computer Science, 1976.

[149] M. Hyppönen. Retroviruses – how viruses fight back. In *Virus Bulletin Conference*, 1994.

[150] M. Hypponen. Santy. F-Secure Virus Descriptions, 21 December 2004.

[151] C. Itshak, N. Vitaly, and M. Taras. Virus detection system. Canadian Patent Application #2,460,607, 27 March 2003.

[152] W. Jansen and T. Karygiannis. Mobile agent security. NIST Special Publication 800-19, 1999.

[153] Japan Times. Bug in antivirus software hits LANs at JR East, some media, 24 April 2005.

[154] M. Jordan. Dealing with metamorphism. *Virus Bulletin*, pages 4–6, October 2002.

[155] R. Joshi, G. Nelson, and K. Randall. Denali: a goal-directed superoptimizer. In *Proceedings of the ACM SIGPLAN 2002 Conference on Programming language design and implementation*, pages 304–314, 2002.

[156] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan. Fast portscan detection using sequential hypothesis testing. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, pages 211–225, 2004.

[157] J. E. Just and M. Cornwall. Review and analysis of synthetic diversity for breaking monocultures. In *Proceedings of the 2004 ACM Workshop on Rapid Malcode*, pages 23–32, 2004.

[158] S. P. Kanuck. Information warfare: New challenges for public international law. *Harvard International Law Journal*, 37(1):272–292, 1996.

[159] E. Kaspersky. Dichotomy: Double trouble. *Virus Bulletin*, pages 8–9, December 1994.

[160] E. Kaspersky. RMNS – the perfect couple. *Virus Bulletin*, pages 8–9, May 1995.

[161] Kaspersky Lab. Virus.DOS.Whale, 2000. *Whale appeared c. 1990.*

[162] Kaspersky Lab. Virus.Win16.Apparition.a, 2000. *Apparition appeared c. 1998.*

[163] J. O. Kephart, A. G. G. Morin, G. B. Sorkin, and J. W. Wells. Efficient detection of computer viruses and other data traits. United States Patent #6,016,546, 18 January 2000.

[164] V. Kiriansky, D. Bruening, and S. Amarasinghe. Secure execution via program shepherding. In *Proceedings of the 11th USENIX Security Symposium*, 2002.

[165] S. Kirsner. Sweating in the hot zone. *Fast Company*, 99, October 2005.

[166] P. Klint. Interpretation techniques. *Software – Practice and Experience*, 11:963–973, 1981.

[167] klog. The frame pointer overwrite. *Phrack*, 9(55), 1999.

[168] D. E. Knuth. *The Art of Computer Programming, Volume 3: Sorting and Searching.* Addison-Wesley, second edition, 1998.

[169] C. W. Ko. Method and apparatus for detecting a macro computer virus using static analysis. United States Patent #6,697,950, 24 February 2004.

[170] V. Kouznetsov and A. Ushakov. System and method for efficiently managing computer virus definitions using a structured virus database. United States Patent #6,622,150, 16 September 2003.

[171] J. Koziol, D. Aitel, D. Litchfield, C. Anley, S. Eren, N. Mehta, and R. Hassell. *The Shellcoder's Handbook: Discovering and Exploiting Security Holes.* Wiley, 2004.

[172] Krakowicz. Krakowicz's kracking korner: The basics of kracking II, c. 1983.

[173] N. Krawetz. Anti-honeypot technology. *IEEE Security & Privacy*, pages 76–79, January/February 2004.

[174] S. Kumar and E. H. Spafford. A generic virus scanner in C++. In *Proceedings of the 8th Computer Security Applications Conference*, pages 210–219, 1992.

[175] C. J. Kuo, J. Koltchev, D.-C. Zheng, and J. Peter. Method of treating whitespace during virus detection. United States Patent #6,230,288, 8 May 2001.

[176] J. Kuo and D. Beck. The common malware enumeration (CME) initiative. *Virus Bulletin*, pages 14–15, September 2005.

[177] Z. M. Laguerta. TROJ_CAGER.A. Trend Micro Virus Encyclopedia, 6 September 2005.

[178] A. Lakhotia, A. Kapoor, and E. U. Kumar. Are metamorphic viruses really invincible? part 1. *Virus Bulletin*, pages 5–7, December 2004.

[179] B. W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973.

[180] E. E. Landy and J. M. Steele. Graffiti as a function of building utilization. *Perceptual and Motor Skills*, 25:711–712, 1967.

[181] T. Laundrie. All we need is love. rec.humor.funny ILOVEYOU digest, joke attributed to M. Barker, 8 May 2000.

[182] A. J. Lee. Hunting the unicorn. *Virus Bulletin*, pages 13–16, May 2004.

[183] J. R. Levine. *Linkers and Loaders*. Morgan Kaufmann, 2000.

[184] J. Leyden. Americans are pants at password security. The Register, 6 May 2005.

[185] Y. Liu. Avkiller.Trojan. Symantec Security Response, 17 May 2002.

[186] R. W. Lo, K. N. Levitt, and R. A. Olsson. MCF: a malicious code filter. *Computers & Security*, 14(6):541–566, 1995.

[187] M. Ludwig. *The Giant Black Book of Computer Viruses*. American Eagle, second edition, 1998.

[188] LURHQ. Sobig.a and the spam you received today, 21 April 2003.

[189] J. Lyman. Name that worm – how computer viruses get their names. NewsFactor Technology News, 8 January 2002.

[190] J. Ma, G. M. Voelker, and S. Savage. Self-stopping worms. In *Proceedings of the 2005 ACM Workshop on Rapid Malcode*, pages 12–21, 2005.

[191] N. Macdonald. *The Graffiti Subculture: Youth, Masculinity and Identity in London and New York*. Palgrave, 2001.

[192] G. M. Mallén-Fullerton. The minimum size of virus identification signatures. In *Fifth International Computer Virus & Security Conference*, pages 813–817, 1992.

[193] O. Mann. Method for recovery of a computer program infected by a computer virus. United States Patent #5,408,642, 18 April 1995.

[194] Marc. Re: Blind remote buffer overflow. VULN-DEV List, 28 April 2000.

[195] A. Marinescu. Win32/CTX virus description. RAV AntiVirus, 15 November 1999 (detection date).

[196] H. Massalin. Superoptimizer: a look at the smallest program. In *Proceedings of the Second International Conference on Architectual Support for Programming Languages and Operating Systems*, pages 122–126, 1987.

[197] A. Matrawy, P. C. van Oorschot, and A. Somayaji. Mitigating network denial-of-service through diversity-based traffic management. In *Proceedings of the 3rd International Conference on Applied Cryptography and Network Security*, LNCS 3531, pages 104–121, 2005.

[198] McAfee Inc. ZeroHunt. Virus Information Library, 15 December 1990.

[199] McAfee Inc. Den Zuk. Virus Information Library, 1988.

[200] McAfee Inc. WM/Colors.D;M;P. Virus Information Library, 1997.

[201] M. D. McIlroy, R. Morris, and V. A. Vyssotsky. Letter to $\aleph_0$, c/o C. A. Lang, editor, *Software – Practice and Experience*. http://www.cs.dartmouth.edu/~doug/darwin.pdf, 29 June 1971.

[202] M. K. McKusick, K. Bostic, M. J. Karels, and J. S. Quarterman. *The Design and Implementation of the 4.4BSD Operating System*. Addison-Wesley, 1996.

[203] MessageLabs. *MessageLabs Intelligence Annual Email Security Report 2004*, 2004.

[204] E. Messmer. Threat of 'infowar' brings CIA warnings. Network World, 13 September 1999.

[205] Methyl. Tunneling with single step mode, Undated, post-1989.

[206] Z. Michalewicz and D. B. Fogel. *How to Solve It: Modern Heuristics*. Springer-Verlag, 2000.

[207] J. Middleton. Virus writers get behind Gigabyte. vnunet.com, 13 May 2002.

[208] MidNyte. An introduction to encryption, part I, April 1999.

[209] B. P. Miller, L. Fredriksen, and B. So. Study of the reliability of UNIX utilities. *Communications of the ACM*, 33(12):32–44, 1990.

[210] G. Molnár and G. Szappanos. Casualties of war: W32/Ganda. *Virus Bulletin*, pages 7–10, May 2003.

[211] D. Moore and C. Shannon. The spread of the code-red worm (crv2). CAIDA analysis, c. 2001.

[212] D. Moore, C. Shannon, and J. Brown. Code-Red: a case study on the spread and victims of an Internet worm. In *2nd Internet Measurement Workshop*, 2002.

[213] P. Morley. The biggie. *Virus Bulletin*, pages 10–11, November 1998.

[214] I. Muttik. Stripping down an AV engine. In *Virus Bulletin Conference*, pages 59–68, 2000.

[215] C. Nachenberg. Antivirus accelerator. United States Patent #6,021,510, 1 February 2000.

[216] C. Nachenberg. Behavior blocking: The next step in anti-virus protection. SecurityFocus, 19 March 2002.

[217] C. Nachenberg. Computer virus-antivirus coevolution. *Communications of the ACM*, 40(1):46–51, 1997.

[218] C. Nachenberg. Emulation repair system. United States Patent #6,067,410, 23 May 2000.

[219] C. S. Nachenberg. Data driven detection of viruses. United States Patent #6,851,057, 1 February 2005.

[220] C. S. Nachenberg. Dynamic heuristic method for detecting computer viruses using decryption exploration and evaluation phases. United States Patent #6,357,008, 12 March 2002.

[221] C. S. Nachenberg. Polymorphic virus detection module. United States Patent #5,826,013, 20 October 1998.

[222] C. S. Nachenberg. Histogram-based virus detection. Canadian Patent Application #2,403,676, 20 September 2001.

[223] C. S. Nachenberg. State-based cache for antivirus software. United States Patent #5,999,723, 7 December 1999.

[224] R. Naraine. Microsoft's security response center: How little patches are made. eWeek, 8 June 2005.

[225] K. Natvig. Sandbox technology inside AV scanners. In *Virus Bulletin Conference*, pages 475–488, 2001.

[226] K. Natvig. Sandbox II: The Internet. In *Virus Bulletin Conference*, pages 125–141, 2002.

[227] G. Navarro and M. Raffinot. *Flexible Pattern Matching in Strings*. Cambridge, 2002.

[228] G. Navarro and J. Tarhio. LZgrep: a Boyer-Moore string matching tool for Ziv-Lempel compressed text. *Software – Practice and Experience*, 35(12):1107–1130, 2005.

[229] J. Nazario. *Defense and Detection Strategies against Internet Worms*. Artech House, 2004.

[230] J. Nazario, J. Anderson, R. Wash, and C. Connelly. The future of Internet worms. In *Blackhat Briefings*, 2001.

[231] Nergal. The advanced return-into-lib(c) exploits: PaX case study. *Phrack*, 0x0b(0x3a), 2001.

[232] K. O'Brien and J. Nusbaum. Intelligence gathering on asymmetric threats – part one. Jane's Intelligence Review, 1 October 2000.

[233] H. O'Dea. Trapping worms in a virtual net. In *Virus Bulletin Conference*, pages 176–186, 2004.

[234] L. Oudot. Fighting Internet worms with honeypots. SecurityFocus, 23 October 2003.

[235] L. Oudot and T. Holz. Defeating honeypots: Network issues, part 1. SecurityFocus, 28 September 2004.

[236] M. Overton. Worm charming: Taking SMB-Lure to the next level. In *Virus Bulletin Conference*, 2003.

[237] R. C. Owens. Turning worms: Some thoughts on liabilities for spreading computer infections. *Canadian Journal of Law and Technology*, 3(1):33–47, 2004.

[238] M. C.-H. Pak, A. Ouchakov, K. N. Pham, D. O. Gryaznov, and V. Kouznetsov. System and method for executing computer virus definitions containing general purpose programming language extensions. United States Patent #6,718,469, 6 April 2004.

[239] Panda Software. Elkern.C. Virus Encyclopedia, 2005.

[240] Panda Software. PGPCoder.A. Virus Encyclopedia, 2005.

[241] Panda Software. A Trojan digitally encrypts files and asks for a ransom. Press release, 25 May 2005.

[242] paperghost. We're calm like a bomb: The antivirus virus. Vitalsecurity.org, 1 June 2005.

[243] V. Paxson. Bro: A system for detecting network intruders in real-time. In *Proceedings of the 7th USENIX Security Symposium*, 1998.

[244] J. Pearce. Antivirus virus on the loose. ZDNet Australia, 20 January 2003.

[245] T. J. Pennello. Very fast LR parsing. In *Proceedings of the SIGPLAN '86 Symposium on Compiler Construction*, pages 145–151, 1986.

[246] C. Percival. Naive differences of executable code, 2003.

[247] F. Perriot. Defeating polymorphism through code optimization. In *Virus Bulletin Conference*, pages 142–159, 2003.

[248] F. Perriot and P. Ferrie. Principles and practise of X-raying. In *Virus Bulletin Conference*, pages 51–66, 2004.

[249] F. Perriot, P. Ferrie, and P. Ször. Striking similarities. *Virus Bulletin*, pages 4–6, May 2002.

[250] F. Perriot and D. Knowles. W32.Welchia.Worm. Symantec Security Response, 28 July 2004.

[251] R. Perry. Extensions to CVDL, the CyberSoft virus description language. CyberSoft White Paper, 11 August 2001.

[252] R. Perry. CyberSoft CVDL tutorial. CyberSoft White Paper, 16 September 2001.

[253] phantasmal phantasmagoria. On polymorphic evasion. BugTraq, 2 October 2004.

[254] V. Pless. *Introduction to the Theory of Error-Correcting Codes*. Wiley, 1982.

[255] N. Provos and P. Honeyman. ScanSSH – scanning the Internet for SSH servers. In *Proceedings of the LISA 2001 15th Systems Administration Conference*, pages 25–30, 2001.

[256] T. H. Ptacek and T. N. Newsham. Insertion, evasion, and denial of service: Eluding network intrusion detection. Secure Networks, Inc., 1998.

[257] J. Purisma. To do or not to do: Anti-virus accessories. In *Virus Bulletin Conference*, pages 125–130, 2003.

[258] P. Radatti. Computer viruses in Unix networks, 1995.

[259] P. V. Radatti. The CyberSoft virus description language. CyberSoft White Paper, 1996.

[260] E. S. Raymond, ed. The jargon file, version 4.4.7, 2003.

[261] C. Renert. Proactive detection of code injection worms. In *Virus Bulletin Conference*, pages 147–158, 2004.

[262] E. Rescorla. Security holes... who cares? In *Proceedings of the 12th USENIX Security Symposium*, pages 75–90, 2003.

[263] Reuters. Looking into the mind of a virus writer. CNN.com, 19 March 2003.

[264] Reuters. Computer worm traps child porn offender in Germany. reuters.com, 20 December 2005.

[265] J. Riordan and B. Schneier. Environmental key generation towards clueless agents. In *Mobile Agents and Security (LNCS 1419)*, pages 15–24, 1998.

[266] W. Robertson, C. Kruegel, D. Mutz, and F. Valeur. Run-time detection of heap-based overflows. In *Proceedings of the 17th Large Installation Systems Administration Conference*, pages 51–59, 2003.

[267] E. C. Rosen. Vulnerabilities of network control protocols: An example. *ACM SIGCOMM Computer Communication Review*, 11(3):10–16, 1981.

[268] J. B. Rosenberg. *How Debuggers Work: Algorithms, Data Structures, and Architecture*. Wiley, 1996.

[269] C. H. Rowland. Covert channels in the TCP/IP protocol suite. *First Monday*, 2(5), 1997.

[270] RSA Security. Internet identity theft threatens to be the next crime wave to hit Britain. Press release, 20 April 2004.

[271] M. Russinovich. Sony, rootkits and digital rights management gone too far. Mark's SysInternals Blog, 31 October 2005.

[272] O. Ruwase and M. S. Lam. A practical dynamic buffer overflow detector. In *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, pages 159–169, 2004.

[273] T. Sabin. Comparing binaries with graph isomorphisms. BindView white paper, 2004.

[274] A. Saita. Security no match for theater lovers. SearchSecurity.com, 24 March 2005.

[275] I. Schaechter. Definitions of terrorism. http://www.unodc.org/unodc/terrorism_definitions.html, 2000.

[276] S. E. Schechter, J. Jung, and A. W. Berger. Fast detection of scanning worm infections. In *Seventh International Symposium on Recent Advances in Intrusion Detection (RAID)*, LNCS 3224, pages 59–81, 2004.

[277] S. E. Schechter and M. D. Smith. Access for sale: A new class of worm. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, pages 19–23, 2003.

[278] P. Schmehl. Past its prime: Is anti-virus scanning obsolete? SecurityFocus, 2002.

[279] B. Schneier. *Applied Cryptography*. Wiley, second edition, 1996.

[280] B. Schneier. Insurance and the computer industry. *Communications of the ACM*, 44(3):114–115, 2001.

[281] J. Schnurer and T. J. Klemmer. Computer virus trap. Canadian Patent Application #2,191,205, 7 December 1995.

[282] K. Schöldström. How to use live viruses as an education tool. In *Virus Bulletin Conference*, pages 251–261, 2002.

[283] M. G. Schultz, E. Eskin, E. Zadok, and S. J. Stolfo. Data mining methods for detection of new malicious executables. In *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, pages 38–49, 2001.

[284] scut. Exploiting format string vulnerabilities, version 1.2, 1 September 2001.

[285] H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, and D. Boneh. On the effectiveness of address-space randomization. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pages 298–307, 2004.

[286] L. Sherer. Keeping pace in a war of worms. *Virus Bulletin*, page 2, May 2004.

[287] J. F. Shoch and J. A. Hupp. The "worm" programs – early experience with a distributed computation. *Communications of the ACM*, 25(3):172–180, 1982.

[288] E. Skoudis and L. Zeltser. *Malware: Fighting Malicious Code*. Prentice Hall, 2004.

[289] R. Skrenta. Elk cloner. http://www.skrenta.com/cloner.

[290] F. Skulason. New Zealand – causing chaos worldwide. *Virus Bulletin*, pages 9–10, May 1990.

[291] F. Skulason. More about UVDs. comp.virus, 28 January 1990.

[292] Solar Designer. Getting around non-executable stack (and fix). Bugtraq, 10 August 1997.

[293] Solar Designer. JPEG COM marker processing vulnerability in Netscape browsers. OW-002-netscape-jpeg, revision 1, 25 July 2000.

[294] D. A. Solomon and M. E. Russinovich. *Inside Microsoft Windows 2000.* Microsoft Press, third edition, 2000.

[295] J. T. Soma, T. F. Muther, Jr., and H. M. L. Brissette. Transnational extradition for computer crimes: Are new treaties and laws needed? *Harvard Journal on Legislation*, 34:317–371, 1997.

[296] A. N. Sovarel, D. Evans, and N. Paul. Where's the FEEB? The effectiveness of instruction set randomization. In *Proceedings of the 14th USENIX Security Symposium*, pages 145–160, 2005.

[297] Sowhat. Multiple antivirus reserved device name handling vulnerability. BugTraq, 19 October 2004.

[298] E. H. Spafford. The Internet worm program: An analysis. Technical Report CSD-TR-823, Purdue University, Department of Computer Sciences, 1988.

[299] E. H. Spafford. Computer viruses as artificial life. *Journal of Artificial Life*, 1(3):249–265, 1994.

[300] Spammer-X. *Inside the SPAM Cartel.* Syngress, 2004.

[301] L. Spitzner. *Honeypots: Tracking Hackers.* Addison-Wesley, 2003.

[302] N. Stampf. Worms of the future: Trying to exorcise the worst. SecurityFocus, 2 October 2003.

[303] S. Staniford, D. Moore, V. Paxson, and N. Weaver. The top speed of flash worms. In *Proceedings of the 2004 ACM Workshop on Rapid Malcode*, pages 33–42, 2004.

[304] S. Staniford, V. Paxson, and N. Weaver. How to 0wn the Internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, 2002.

[305] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton. Analysis of end user security behaviors. *Computers & Security*, 24(2):124–133, 2005.

[306] Symantec. Symantec norton protected recycle bin exposure. SYM06-002, 10 January 2006.

[307] Symantec. Understanding heuristics: Symantec's Bloodhound technology. Symantec White Paper Series, Volume XXXIV, 1997.

[308] P. Szor. Generic disinfection. In *Virus Bulletin Conference*, 1996.

[309] P. Szor. Win95.Memorial, 1997.

[310] P. Ször. Memory scanning under Windows NT. In *Virus Bulletin Conference*, pages 325–346, 1999.

[311] P. Szor. W95.Zperm.A, 2000.

[312] P. Szor. *The Art of Computer Virus Research and Defense.* Addison-Wesley, 2005.

[313] P. Szor. W2K.Stream. Symantec Security Response, 7 September 2000.

[314] P. Ször and P. Ferrie. Hunting for metamorphic. In *Virus Bulletin Conference*, pages 123–144, 2001.

[315] P. Ször and F. Perriot. Slamdunk. *Virus Bulletin*, pages 6–7, March 2003.

[316] J. Tarala. Virii generators: Understanding the threat. SANS Information Security Reading Room, 2002.

[317] R. F. Templeton. Method of managing computer virus infected files. United States Patent #6,401,210, 4 June 2002.

[318] G. Tesauro, J. O. Kephart, and G. B. Sorkin. Neural networks for computer virus recognition. *IEEE Expert*, 11(4):5–6, 1996.

[319] The Honeynet Project & Research Alliance. Know your enemy: Tracking botnets, 13 March 2005.

[320] The Mental Driller. Metamorphism in practice. *29A e-zine*, 6, March 2002.

[321] T. L. Thomas. Russian views on information-based warfare. *Airpower Journal*, pages 25–35, 1996.

[322] K. Thompson. Reflections on trusting trust. *Communications of the ACM*, 27(8):761–763, 1984.

[323] H. Toyoizumi and A. Kara. Predators: Good will mobile codes combat against computer viruses. In *Proceedings of the 2002 Workshop of New Security Paradigms*, pages 11–17, 2002.

[324] N. Tuck, T. Sherwood, B. Calder, and G. Varghese. Deterministic memory-efficient string matching algorithms for intrusion detection. In *IEEE INFOCOM 2004*, volume 4, pages 2628–2639, 2004.

[325] J. Twycross and M. M. Williamson. Implementing and testing a virus throttle. In *Proceedings of the 12th USENIX Security Symposium*, pages 285–294, 2003.

[326] United States Attorney's Office. Former computer network administrator at New Jersey high-tech firm sentenced to 41 months for unleashing $10 million computer 'time bomb'. News release, 26 February 2002.

[327] United States of America v. Roger Duronio, Indictment, United States District Court, District of New Jersey, 2002.

[328] United States v. Lloyd, 269 F.3d 228 (3rd Cir. 2001).

[329] United States v. Morris, 928 F.2d 504 (2nd Cir. 1991).

[330] United States of America v. Jeffrey Lee Parson, Plea agreement, United States District Court, Western District of Washington at Seattle, Case 2:03-cr-00379-mjp, 2004.

[331] Ferry van het Groenewoud. Info wanted on spy-ware. comp.sys.ibm.pc.hardware.networking (cross-posted), 5 November 1994.

[332] F. Veldman. Generic decryptors: Emulators of the future. IVPC Conference, 1998.

[333] VGrep. How is the vgrep database created?, 2005.

[334] R. Vibert. A day in the life of an anti-virus lab. SecurityFocus, 2000.

[335] A. Vidström. Computer forensics and the ATA interface. Technical Report FOI-R–1638–SE, Swedish Defense Research Agency, Command and Control Systems, 2005.

[336] Virgil. *The Aeneid*. 19 BCE. Translation by J. Dryden, P. F. Collier & Son, 1909.

[337] T. Vogt. Simulating and optimising worm propagation algorithms. SecurityFocus, 29 September 2003.

[338] R. Vossen. Win95 source marketing. comp.programming, 16 October 1995.

[339] P. Wagle and C. Cowan. StackGuard: Simple stack smash protection for GCC. In *Proceedings of the GCC Developers Summit*, pages 243–255, 2003.

[340] J. Walker. The animal episode. Open letter to A. K. Dewdney, 1985.

[341] J. E. Walsh and E. H. A. Altberg. Method and apparatus for protecting data files on a computer from virus infection. United States Patent #5,956,481, 21 September 1999.

[342] M. Weber, M. Schmid, M. Schatz, and D. Geyer. A toolkit the detecting and analyzing malicious software. In *18th Annual Computer Security Applications Conference*, 2002.

[343] J. Wells. A radical new approach to virus scanning. CyberSoft White Paper, 1999.

[344] J. White. Mobile agents white paper. General Magic, 1996.

[345] D. Whyte, E. Kranakis, and P. C. van Oorschot. DNS-based detection of scanning worms in an enterprise network. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, 2005.

[346] B. Wiley. Curious Yellow: The first coordinated worm design. http://blanu.net/curious_yellow.html.

[347] M. M. Williamson. Design, implementation and test of an email virus throttle. In *19th Annual Computer Security Applications Conference*, 2003.

[348] M. M. Williamson, A. Parry, and A. Byde. Virus throttling for instant messaging. In *Virus Bulletin Conference*, pages 38–44, 2004.

[349] S. Wu and U. Manber. A fast algorithm for multi-pattern searching. Technical Report 94-17, University of Arizona, Department of Computer Science, 1994.

[350] P. E. Yee. Internet VIRUS alert. comp.protocols.tcp-ip, 3 November 1988.

[351] T. Yetiser. Polymorphic viruses: Implementation, detection, and protection, 1993.

[352] A. Young and M. Yung. Cryptovirology: Extortion-based security threats and countermeasures. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pages 129–140, 1996.

[353] z0mbie. Vmware has you, 13 June 2002.

[354] D. Zenkin. Fighting against the invisible enemy. *Computers & Security*, 20(4):316–321, 2001.

Index