Linux malware

From Wikipedia, the free encyclopedia

Linux malware includes viruses, trojans, worms and other types of malware that affect the Linux operating system. Linux, Unix and other Unix-like computer operating systems are generally regarded as very well-protected against, but not immune to, computer viruses.[1][2]

There has not yet been a widespread Linux malware infection of the type that Microsoft Windows software has; this is attributable generally to the malware's lack of root access and fast updates to most Linux vulnerabilities.[2]

Contents

Linux vulnerability

Like Unix systems, Linux implements a multi-user environment where users are granted specific privileges and there is some form of access control implemented. To gain control over a Linux system or to cause any serious consequences to the system itself, the malware would have to gain root access to the system.[2]

In the past, it has been suggested that Linux had so little malware because its low market share made it a less profitable target. Rick Moen, an experienced Linux system administrator, counters that:

> [That argument] ignores Unix's dominance in a number of non-desktop specialties, including Web servers and scientific workstations. A virus/trojan/worm author who successfully targeted specifically Apache httpd Linux/x86 Web servers would both have an extremely target-rich environment and instantly earn lasting fame, and yet it doesn't happen."[3]

The amount of malware targeting Linux has seen an increase in recent years, however. Shane Coursen, a senior technical consultant with Kaspersky Lab, claims, "The growth in Linux malware is simply due to its increasing popularity, particularly as a desktop operating system ... The use of an operating system is directly correlated to the interest by the malware writers to develop malware for that OS."[4]

Tom Ferris, a researcher with Security Protocols, commented on one of Kaspersky's reports, stating, "In people's minds, if it's non-Windows, it's secure, and that's not the case. They think nobody writes malware for Linux or Mac OS X. But that's not necessarily true,"[4]

Some Linux users do run Linux-based anti-virus software to scan insecure documents and email which comes from or is going to Windows users. SecurityFocus's Scott Granneman stated:

> ...some Linux machines definitely need anti-virus software. Samba or NFS servers, for instance, may store documents in undocumented, vulnerable Microsoft formats, such as Word and Excel, that contain and propagate viruses. Linux mail servers should run AV software in order to neutralize viruses before they show up in the mailboxes of Outlook and Outlook Express users.[1]

Because they are predominantly used on mail servers which may send mail to computers running other operating systems, Linux virus scanners generally use definitions for, and scan for, all known viruses for all computer platforms. For example the open source ClamAV "Detects ... viruses, worms and trojans, including Microsoft Office macro viruses, mobile malware, and other threats."[5]

Viruses and trojan horses

The viruses listed below pose a potential, although minimal, threat to Linux systems. If an infected binary containing one of the viruses were run, the system would be infected. The infection level would depend on which user with what privileges ran the binary. A binary run under the root account would be able to infect the entire system. Privilege escalation vulnerabilities may permit malware running under a limited account to infect the entire system.

It is worth noting that this is true for any malicious program that is run without special steps taken to limit its privileges. It is trivial to add a code snippet to any program that a user may download and let this additional code download a modified login server, an open mail relay, or similar program, and make this additional component run any time the user logs in. No special malware writing skills are needed for this. Special skill may be needed for tricking the user to run the (trojan) program in the first place.

The use of software repositories significantly reduces any threat of installation of malware, as the software repositories are checked by maintainers, who try to ensure that their repository is malware-free. Subsequently, to ensure safe distribution of the software, checksums are made available. These make it possible to reveal modified versions that may have been introduced by e.g. hijacking of communications using a man-in-the-middle attack or via a redirection attack such as ARP or DNS poisoning. Careful use of these digital signatures provides an additional line of defense, which limits the scope of attacks to include only the original authors, package and release maintainers and possibly others with suitable administrative access, depending on how the keys and checksums are handled.

Worms and targeted attacks

The classical threat to Unix-like systems is vulnerabilities in network daemons, such as SSH and web servers. These can be used by worms or for attacks against specific targets. As servers are patched quite quickly when a vulnerability is found, there have been only a few widespread worms of this kind. As specific targets can be

attacked through a vulnerability that is not publicly known there is no guarantee that a certain installation is secure. Also servers without such vulnerabilities can be successfully attacked through weak passwords.

Web scripts

Linux servers may also be used by malware without any attack against the system itself, where e.g. web content and scripts are insufficiently restricted or checked and used by malware to attack visitors. Typically a CGI script (meant for leaving comments) by mistake allows inclusion of code exploiting vulnerabilities in the web browser.

Buffer overruns

Older Linux distributions were relatively sensitive to buffer overrun attacks: if the program did not care about the size of the buffer itself, the kernel provided only limited protection, allowing an attacker to execute arbitrary code under the rights of the vulnerable application under attack. Programs that gain root access even when launched by a non-root user (via the setuid bit) were particularly attractive to attack. However as of 2009 most of the kernels include address space layout randomization (ASLR), enhanced memory protection and other extensions making such attacks much more difficult to arrange.

Cross-platform viruses

An area of concern identified in 2007 is that of cross-platform viruses, driven by the popularity of cross-platform applications. This was brought to the forefront of malware awareness by the distribution of an OpenOffice.org virus called Badbunny.

Stuart Smith of Symantec wrote the following:

> "What makes this virus worth mentioning is that it illustrates how easily scripting platforms, extensibility, plug-ins, ActiveX, etc, can be abused. All too often, this is forgotten in the pursuit to match features with another vendor... The ability for malware to survive in a cross-platform, cross-application environment has particular relevance as more and more malware is pushed out via Web sites. How long until someone uses something like this to drop a JavaScript infecter on a Web server, regardless of platform?"[6]

Social engineering

As is the case with any operating system, Linux is vulnerable to malware that tricks the user into installing it through social engineering. In December 2009 a malicious waterfall screensaver was discovered that contained a script that used the infected Linux PC in denial-of-service attacks.[7]

Anti-virus applications

There are a number of anti-virus applications available which will run under the Linux operating system. Most of these applications are looking for exploits which could affect users of Microsoft Windows.

For Microsoft Windows-specific threats

These applications are useful for computers (typically, servers) which will pass on files to MS Windows users. They do not look for Linux-specific threats.

- Avast! (proprietary; freeware version available)
- AVG (proprietary; freeware version available)
- Avira (proprietary; freeware version available)
- BitDefender (proprietary; freeware version available)
- Comodo (proprietary; freeware version available)[8]
- ClamAV (free and open source software)[9]
- Dr.Web (proprietary) [10]
- EScan for Linux (proprietary)
- F-Prot (proprietary; freeware version available)[11]
- F-Secure Linux (proprietary)
- Kaspersky Linux Security (proprietary)[12]
- McAfee VirusScan Enterprise for Linux (proprietary)[13]
- Panda Security for Linux (proprietary)[14]
- Symantec AntiVirus for Linux (proprietary)[15]
- Trend Micro ServerProtect for Linux (proprietary)

The ClamTk GUI for ClamAV running a scan on Ubuntu 8.04 Hardy Heron

For Linux-specific threats

These applications look for actual threats to the Linux computers on which they are running.

- chkrootkit (free and open source software)[16]
- ESET (proprietary) (detects OS X, Windows malware as well)[17][18][19]
- rkhunter (free and open source software)[20]
- Sophos (proprietary) (detects Windows malware, too)[21]

Linux malware can also be detected (and analyzed) using memory forensics tools, such as the following.

- Second Look (proprietary)[22]
- Volatility[23] (free and open source software)[24]

Threats

The following is a partial list of known Linux malware. However, few if any are in the wild, and most have been rendered obsolete by Linux updates or were never a threat. Known malware is not the only or even the most important threat: new malware or attacks directed to specific sites can use vulnerabilities previously unknown to the community or unused by malware.

Rootkits

- Snakso-A - 64-bit Linux webserver rootkit[25]

Trojans

- Hand of Thief - Banking trojan, 2013,[26][27]
- Kaiten - Linux.Backdoor.Kaiten trojan horse[28]
- Rexob - Linux.Backdoor.Rexob trojan[29]
- Waterfall screensaver backdoor - on gnome-look.org[30]

Viruses

- 42 [31][32]
- Arches [33]
- Alaeda - Virus.Linux.Alaeda[34]
- Bad Bunny - Perl.Badbunny[6][35]
- Binom - Linux/Binom[36]
- Bliss - requires root privileges
- Brundle[37]
- Bukowski[38]
- Caveat [39][40]
- Coin [41][42]
- Diesel - Virus.Linux.Diesel.962[43]
- Hasher [44][45]
- Kagob a - Virus.Linux.Kagob.a[46]
- Kagob b - Virus.Linux.Kagob.b[47]
- Lacrimae (aka Crimea) [48][49]
- MetaPHOR (also known as Simile)[50]
- Nuxbee - Virus.Linux.Nuxbee.1403[51]
- OSF.8759
- PiLoT[52][53]
- Podloso - Linux.Podloso (The iPod virus)[54][55]
- RELx [56]
- Rike - Virus.Linux.Rike.1627[57]
- RST - Virus.Linux.RST.a[58] (known for infecting Korean release of Mozilla Suite 1.7.6 and Thunderbird 1.0.2 in September 2005[59])
- Satyr - Virus.Linux.Satyr.a[60]
- Staog
- Vit - Virus.Linux.Vit.4096[61]
- Winter - Virus.Linux.Winter.341[62]
- Winux (also known as Lindose and PEElf)[63]
- Wit virus[64]
- ZipWorm - Virus.Linux.ZipWorm[65]

Worms

- Adm - Net-Worm.Linux.Adm[66]
- Adore[67]
- Cheese - Net-Worm.Linux.Cheese[68]
- Devnull
- Kork[69]
- Linux/Lion
- Linux.Darlloz - Targets home routers, set-top boxes, security cameras and industrial control systems.[70][71]
- Linux/Lupper.worm[72]
- Mighty - Net-Worm.Linux.Mighty[73]
- Millen - Linux.Millen.Worm[74]
- Ramen worm - targeted only Red Hat Linux distributions versions 6.2 and 7.0
- Slapper[75]
- SSH Bruteforce[76]

See also

- List of computer viruses

References

1. ^ *a b* Granneman, Scott (October 2003). "Linux vs. Windows Viruses" (http://www.securityfocus.com/columnists/188). Retrieved 2008-03-06.
2. ^ *a b c* Yeargin, Ray (July 2005). "The short life and hard times of a linux virus" (http://librenix.com/?inode=21). Retrieved 2008-06-24.
3. ^ "Virus Department" (http://linuxmafia.com/~rick/faq/index.php?page=virus). Retrieved 2009-10-11.
4. ^ *a b* Patrizio, Andy (April 2006). "Linux Malware On The Rise" (http://www.internetnews.com/dev-news/article.php/3601946). Retrieved 2008-03-08.

5. ^ ClamAV (2010). "Clam AntiVirus 0.96 User Manual" (http://www.clamav.net/doc/latest/clamdoc.pdf). Retrieved 2011-02-22.
6. ^ *a b* Smith, Stuart (June 2007). "Bad Bunny" (http://www.symantec.com/enterprise/security_response/weblog/2007/06/bad_bunny.html). Retrieved 2008-02-20.
7. ^ Kissling, Kristian (December 2009). "Malicious Screensaver: Malware on Gnome-Look.org" (http://www.ubuntu-user.com/Online/News/Malicious-Screensaver-Malware-on-Gnome-Look.org). Retrieved 2009-12-12.
8. ^ Comodo Group (2012). "Comodo Antivirus for Linux" (http://www.comodo.com/home/internet-security/antivirus-for-linux.php). Retrieved 17 October 2012.
9. ^ "ClamAV" (http://www.clamav.net/). Retrieved 2011-02-22.
10. ^ "Dr.Web anti-virus for Linux" (http://products.drweb.com/linux/). Dashke. Retrieved 2010-05-25.
11. ^ FRISK Software International (2011). "F-PROT Antivirus for Linux x86 / BSD x86" (http://www.f-prot.com/products/corporate_users/unix/). Retrieved 13 December 2011.
12. ^ "Kaspersky Linux Security - Gateway, mail and file server, workstation protection for Linux/FreeBSD" (http://www.kaspersky.com/linux). Kaspersky Lab. Retrieved 2009-02-11.
13. ^ "McAfee VirusScan Enterprise for Linux" (http://www.mcafee.com/us/products/virusscan-enterprise-for-linux.aspx). McAfee. Retrieved 2012-12-27.
14. ^ "Panda Security Antivirus Protection for Linux" (http://www.pandasecurity.com/spain/homeusers/solutions/linux/). Panda Security. Retrieved 2009-01-13.
15. ^ Symantec (January 2009). "System requirements for Symantec AntiVirus for Linux 1.0" (http://service1.symantec.com/SUPPORT/ent-security.nsf/ppfdocs/2005110716014248). Retrieved 2009-03-07.
16. ^ "Chkrootkit" (http://www.chkrootkit.org).
17. ^ "ESET File Security - Antivirus Protection for Linux, BSD, and Solaris" (http://www.eset.com/products/linux.php). Eset. Retrieved 2008-10-26.
18. ^ "ESET Mail Security - Linux, BSD, and Solaris mail server protection" (http://www.eset.com/products/linux_mail.php). Eset. Retrieved 2008-10-26.
19. ^ "ESET NOD32 Antivirus for Linux Gateway Devices" (http://www.eset.com/products/gateway.php). Eset. Retrieved 2008-10-26.
20. ^ "Root Kit Hunter" (http://www.rootkit.nl/projects/rootkit_hunter.html).
21. ^ "Botnets, a free tool and 6 years of Linux/Rst-B | Naked Security" (http://nakedsecurity.sophos.com/2008/02/13/botnets-a-free-tool-and-6-years-of-linuxrst-b/). Nakedsecurity.sophos.com. 2008-02-13. Retrieved 2013-08-11.
22. ^ "Second Look" (http://secondlookforensics.com).
23. ^ volatilesystems.com (http://www.volatilesystems.com/)
24. ^ "Volatility" (http://code.google.com/p/volatility/wiki/LinuxMemoryForensics).
25. ^ Leyden, John (21 November 2012), Evildoers can now turn all sites on a Linux server into silent hell-pits (http://www.theregister.co.uk/2012/11/21/powerful_linux_rootkit/), The Register, retrieved 21 November 2012
26. ^ https://blogs.rsa.com. "Thieves Reaching for Linux—"Hand of Thief" Trojan Targets Linux #INTH3WILD » Speaking of Security - The RSA Blog and Podcast" (https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild/). Blogs.rsa.com. Retrieved 2013-08-11.
27. ^ Vaughan, Steven J. "Linux desktop Trojan 'Hand of Thief' steals in" (http://www.zdnet.com/linux-desktop-trojan-hand-of-thief-steals-in-7000019175/). ZDNet. Retrieved 2013-08-11.
28. ^ Florio, Elia (February 2006). "Linux.Backdoor.Kaiten" (http://www.symantec.com/security_response/writeup.jsp?docid=2006-021417-0144-99). Retrieved 2008-03-08.
29. ^ Florio, Elia (December 2007). "Linux.Backdoor.Rexob" (http://www.symantec.com/security_response/writeup.jsp?docid=2007-072612-1704-99). Retrieved 2008-03-08.
30. ^ Vervloesem, Koen (December 2009). "Linux malware: an incident and some solutions" (http://lwn.net/Articles/367874/). Retrieved 2010-09-16.
31. ^ herm1t (August 2008). "Linux.42: Using CRC32B (SSE4.2) instruction in polymorphic decryptor" (http://vx.eof-project.net/viewtopic.php?pid=1049).
32. ^ Ferrie, Peter (September 2008). "Life, the Universe, and Everything" (http://blogs.technet.com/mmpc/archive/2008/09/10/life-the-universe-and-everything.aspx).
33. ^ herm1t (August 2006). "Infecting ELF-files using function padding for Linux" (http://vx.netlux.org/lib/vhe00.html).
34. ^ Kaspersky Lab (May 2007). "Virus.Linux.Alaeda" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21703). Retrieved 2008-03-08.
35. ^ Smith, Stuart (May 2007). "Perl.Badbunny" (http://www.symantec.com/security_response/writeup.jsp?docid=2007-052400-3656-99). Retrieved 2008-03-08.

36. ^ McAfee (December 2004). "Linux/Binom" (http://vil.nai.com/vil/content/v_130506.htm). Retrieved 2008-03-08.
37. ^ Rieck, Konrad and Konrad Kretschmer (August 2001). "Brundle Fly 0.0.1 - A Good-Natured Linux ELF Virus" (http://www.roqe.org/brundle-fly/). Retrieved 2008-03-08.
38. ^ de Almeida Lopes, Anthony (July 2007). "Project Bukowski" (http://sourceforge.net/projects/bukowski/). Retrieved 2008-03-08.
39. ^ herm1t (February 2008). "Caveat virus" (http://www.vxheavens.com/lib/vhe06.html).
40. ^ Ferrie, Peter (July 2009). "Can you spare a seg?" (http://vx.netlux.org/lib/apf29.html).
41. ^ herm1t (October 2007). "Reverse of a coin: A short note on segment alignment" (http://www.vxheavens.com/lib/vhe04.html).
42. ^ Ferrie, Peter (September 2009). "Heads or tails?" (http://vx.netlux.org/lib/apf31.html).
43. ^ Kaspersky Lab (February 2002). "Virus.Linux.Diesel.962" (http://www.viruslist.com/en/viruslist.html?id=3994&key=00001000050000200004). Retrieved 2008-03-08.
44. ^ herm1t (October 2007). "Hashin' the elves" (http://www.vxheavens.com/lib/vhe02.html).
45. ^ Ferrie, Peter (August 2009). "Making a hash of things" (http://vx.netlux.org/lib/apf30.html).
46. ^ Kaspersky Lab (April 2001). "Virus.Linux.Kagob.a" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21720). Retrieved 2008-03-08.
47. ^ Kaspersky Lab (undated). "Virus.Linux.Kagob.b" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21721). Retrieved 2008-03-08.
48. ^ herm1t (June 2008). "README" (http://vx.netlux.org/herm1t/Lacrimae_EN.txt).
49. ^ Ferrie, Peter (February 2008). "Crimea river" (http://vx.netlux.org/lib/apf12.html).
50. ^ The Mental Driller (February 2002). "Metamorphism in practice or "How I made MetaPHOR and what I've learnt" " (http://vx.netlux.org/lib/vmd01.html). Retrieved 2008-03-08.
51. ^ Kaspersky Lab (December 2001). "Virus.Linux.Nuxbee.1403" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21725). Retrieved 2008-03-08.
52. ^ herm1t (November 2007). "INT 0x80? No, thank you!" (http://www.vxheavens.com/lib/vhe05.html).
53. ^ Ferrie, Peter (September 2009). "Flying solo" (http://vx.netlux.org/lib/apf37.html).
54. ^ Ferrie, Peter (April 2007). "Linux.Podloso" (http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-040516-4947-99). Retrieved 2008-03-08.
55. ^ Ferrie, Peter (April 2007). "The iPod virus" (http://www.symantec.com/enterprise/security_response/weblog/2007/04/the_ipod_virus.html). Retrieved 2008-03-08.
56. ^ herm1t (December 2009). "From position-independent to self-relocatable viral code" (http://www.vxheavens.com/lib/vhe08.html).
57. ^ Kaspersky Lab (August 2003). "Virus.Linux.Rike.1627" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21733). Retrieved 2008-03-08.
58. ^ Kaspersky Lab (January 2002). "Virus.Linux.RST.a" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21734). Retrieved 2008-03-08.
59. ^ "The ways of viruses in Linux HOW SAFE?" (http://www.linux-magazine.com/w3/issue/62/Viruses_in_Linux.pdf). Retrieved 2009-08-21.
60. ^ Kaspersky Lab (March 2001). "Virus.Linux.Satyr.a" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21736). Retrieved 2008-03-08.
61. ^ Kaspersky Lab (March 2000). "Virus.Linux.Vit.4096" (http://www.viruslist.com/en/viruslist.html?id=3135&key=00001000050000200003). Retrieved 2008-03-08.
62. ^ Kaspersky Lab (October 2000). "Virus.Linux.Winter.341" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21756). Retrieved 2008-03-08.
63. ^ Rautiainen, Sami et al. (March 2001). "F-Secure Virus Descriptions: Lindose" (http://www.f-secure.com/v-descs/lindose.shtml). Retrieved 2008-03-08.
64. ^ "The Wit Virus: A virus built on the ViT ELF virus" (http://members.hellug.gr/nmav/papers/other/wit-virus.pdf). Retrieved 2008-12-31.
65. ^ Kaspersky Lab (January 2001). "Virus.Linux.ZipWorm" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=21759). Retrieved 2008-03-08.
66. ^ Kaspersky Lab (May 2001). "Net-Worm.Linux.Adm" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=23854). Retrieved 2008-03-08.
67. ^ Rautiainen, Sami (April 2001). "F-Secure Virus Descriptions: Adore" (http://www.f-secure.com/v-descs/adore.shtml). Retrieved 2008-03-08.

68. ^ Kaspersky Lab (May 2001). "Net-Worm.Linux.Cheese" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=23856). Retrieved 2008-03-08.
69. ^ Rautiainen, Sami (April 2001). "F-Secure Virus Descriptions: Kork" (http://www.f-secure.com/v-descs/kork.shtml). Retrieved 2008-03-08.
70. ^ Mohit Kumar (2013-11-30). "Linux worm targeting Routers, Set-top boxes and Security Cameras with PHP-CGI Vulnerability" (http://thehackernews.com/2013/11/Linux-ELF-malware-php-cgi-vulnerability.html). The Hacker News. Retrieved 2013-12-04.
71. ^ Joe Casad (3 December 2013). "New Worm Attacks Linux Devices" (http://www.linux-magazine.com/Online/News/New-Worm-Attacks-Linux-Devices). Linux Magazine. Retrieved 4 December 2013.
72. ^ McAfee (June 2005). "Linux/Lupper.worm Description" (http://vil.nai.com/vil/content/v_136821.htm). Retrieved 2010-10-10.
73. ^ Kaspersky Lab (October 2002). "Net-Worm.Linux.Mighty" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=23864). Retrieved 2008-03-08.
74. ^ Perriot, Frederic (February 2007). "Linux.Millen.Worm" (http://www.symantec.com/security_response/writeup.jsp?docid=2002-121114-1432-99). Retrieved 2008-03-08.
75. ^ Rautiainen, Sami et al. (September 2002). "F-Secure Virus Descriptions: Slapper" (http://www.f-secure.com/v-descs/slapper.shtml). Retrieved 2008-03-08.
76. ^ Voss, Joel (December 2007). "SSH Bruteforce Virus by AltSci Concepts" (https://www.altsci.com/concepts/virus/). Retrieved 2008-03-13.

External links

- Linuxvirus (https://help.ubuntu.com/community/Linuxvirus) on the Official Ubuntu Documentation

Retrieved from "http://en.wikipedia.org/w/index.php?title=Linux_malware&oldid=594762828"
Categories: Linux malware | Linux
