NETWORKWORLD

PRIVACY AND SECURITY FANATIC

By Ms. Smith

About |

Ms. Smith (not her real name) is a freelance writer and programmer

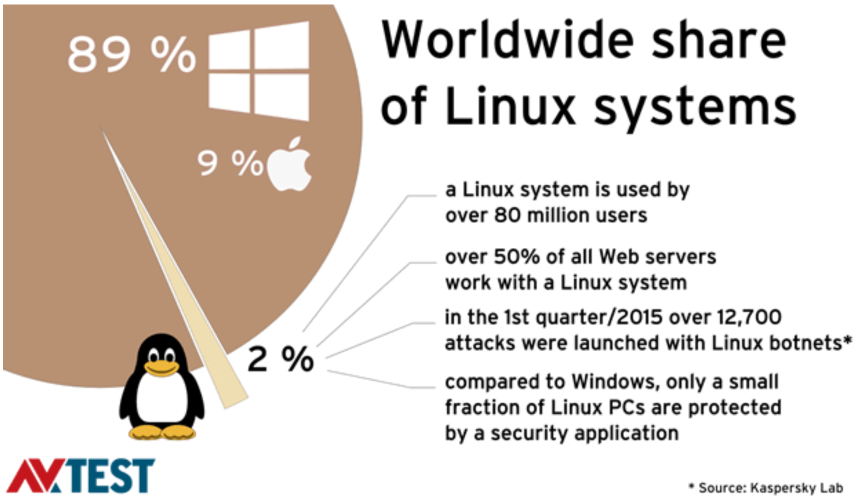
AV-Test Lab tests 16 Linux an

After testing 16 Linux antivirus pro
results.

Network World | Oct 5, 2015 7:53 AM PT

AV-Test, an independent IT-security institute, is well-known for testing Windows antivirus solutions, and the lab's findings are well respected, but this time AV-Test tested 16 Linux antivirus solutions to discover how well they did against Windows and Linux malware. The malware protection capabilities for some of the products were pathetic, as "85% of the Windows malware goes through unrecognized, and up to 75% of pure Linux malware remains undetected."

Linux may be safer than Windows, but "many Linux machines run in a network with Windows PCs." About half of all web servers run Linux, and those serve billions of web users. "That's why Web servers are a tempting target to be used as a bridgehead for Windows malware threats," AV-Test said in a blog post on the findings.



Malware might not damage a Linux machine, as it was expecting to infect Windows, but the malware could go after the apps running on a Linux PC, server, or "simply remain dormant, waiting for the opportunity to attack a Windows system. To do so, it is often sufficient to copy files from a Linux environment to Windows."

AV-Test checked the Linux antivirus products for three things: "the detection of Windows malware, the detection of Linux malware, and the test for false positives." Ubuntu 12.04 LTS 64-bit desktop version was used in the test environment when AV-Test tested the following 16 antivirus solutions:

1. Avast File Server Security
2. AVG Server Edition for Linux
3. Bitdefender Antivirus Scanner for Unices
4. ClamAV
5. Comodo Antivirus for Linux
6. Dr. Web Antivirus for Linux
7. eScan Antivirus for Linux Desktop
8. ESET NOD32 Antivirus for Linux Desktop
9. F-Prot Antivirus for Linux
10. F-Secure Linux Security
11. G Data Client Security Business for Linux
12. Kaspersky Anti-Virus for Linux File Server
13. Kaspersky Endpoint Security 8.0 for Linux
14. McAfee VirusScan Enterprise for Linux
15. Sophos for Linux
16. Symantec Endpoint Protection Manager

Detection of Windows malware by Linux antivirus products

The lab found:

> *A total of 8 out of 16 products detected between 99.7 and 99.9% of the 12,000 Windows attackers used in the test: Avast, F-Secure, Bitdefender, ESET, eScan, G Data, Kaspersky Lab (server version) and Sophos. Only the security package from Symantec achieved 100%.*
>
> *Noticeably weaker are the detection rates of McAfee with 85.1% and Comodo with 83%. Alarmingly feeble are the results of Dr. Web with 67.8%, F-Prot with 22.1% and ClamAV with only 15.3%!*

Detection of Linux malware

Regarding malware that specifically targets Linux, attackers count on user error. AV-Test's Markus Selinger wrote, "The most frequent case involves installing software or updates via third-party package sources. The user is often requested during installation to assign the software temporary root rights. If a user allows this to occur, important system components are swapped with manipulated versions. This enables an attacker to build a back door into the system and use it at will for a botnet."

AV-Test "unleashed on the systems 900 actually already-known attackers for Linux."

> *The result, however, looks significantly different than the detection rates under Windows. Only Kaspersky Endpoint Version achieved 100-percent detection under Linux. Following close behind with 99.7 percent was ESET – AVG still reached 99 percent. The server versions of Kaspersky Lab and Avast do in fact recognize over 98 percent of the attackers. Symantec, offering the best detection under Windows, only finds 97.2 percent of the malware under Linux. That's where the free fall begins.*
>
> *Coming in at the bottom of the list in detection of Linux malware threats are ClamAV, McAfee, Comodo and F-Prot. Their rates ranged between 66.1 and 23 percent. This means that in the worst case, 77 out of 100 threats simply remain undetected despite protection software under Linux.*

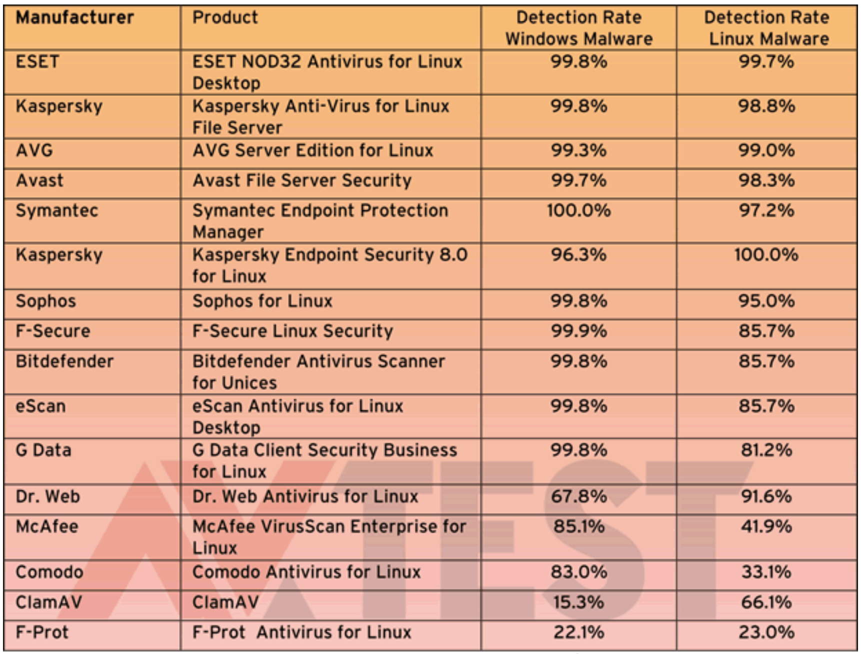
Testing for false positives

When testing for potential false positives, the lab had each product scan 210,000 clean Linux files. The false positive rate was great, as 15 solutions were error-free and "only Comodo issued a false alarm on just one file."

Best antivirus products?

It is wise to use antivirus protection for Linux to stop malware from sneaking through to the Windows side, but "you can skip the effort if every tenth malware threat gets through unscathed." Many Linux forums suggest private users should install Comodo, ClamAV, and F-Prot freeware versions, but "that is not good advice." Instead, as the test result showed, "users would be better advised to go with the freeware versions of Sophos for Linux or Bitdefender Antivirus Scanner for Unices. For server systems, there is even the freeware AVG Server Edition for Linux."

AV-Test Lab detection rates of Linux security packages show the best products, as well as some "blatant detection shortcomings."



Manufacturer	Product	Detection Rate Windows Malware	Detection Rate Linux Malware
ESET	ESET NOD32 Antivirus for Linux Desktop	99.8%	99.7%
Kaspersky	Kaspersky Anti-Virus for Linux File Server	99.8%	98.8%
AVG	AVG Server Edition for Linux	99.3%	99.0%
Avast	Avast File Server Security	99.7%	98.3%
Symantec	Symantec Endpoint Protection Manager	100.0%	97.2%
Kaspersky	Kaspersky Endpoint Security 8.0 for Linux	96.3%	100.0%
Sophos	Sophos for Linux	99.8%	95.0%
F-Secure	F-Secure Linux Security	99.9%	85.7%
Bitdefender	Bitdefender Antivirus Scanner for Unices	99.8%	85.7%
eScan	eScan Antivirus for Linux Desktop	99.8%	85.7%
G Data	G Data Client Security Business for Linux	99.8%	81.2%
Dr. Web	Dr. Web Antivirus for Linux	67.8%	91.6%
McAfee	McAfee VirusScan Enterprise for Linux	85.1%	41.9%
Comodo	Comodo Antivirus for Linux	83.0%	33.1%
ClamAV	ClamAV	15.3%	66.1%
F-Prot	F-Prot Antivirus for Linux	22.1%	23.0%

Note: Test under Ubuntu Desktop 12.04 LTS 64 bit; AV-Test 09/2015

AV-Test Institute

AV-Test Lab detection rates of Linux security packages

"In this test, the best detection rates in terms of Linux and Windows were exhibited by the desktop solution from ESET, followed by Symantec and Kaspersky Lab endpoint versions for company workstations," noted AV-Test. "Recommended for server protection are Kaspersky Anti-Virus for Linux File Server, AVG Server Edition for Linux and Avast File Server Security."

Jörg Luther, Editor-in-Chief of LinuxUser, noted that one might expect freeware ClamAV not to have a stellar detection rate, but F-Prot and Comodo solutions developed by commercial providers had an even poorer performance. McAfee business product finished below average, which served as an example of how using "renowned name and paid software" does not imply an automatic protection guarantee. "By contrast, AVG Server Edition for Linux 2013 and ESET NOD32 AV for Linux Desktop stand out with impeccable detection rates." He found it interesting to have it "confirmed in black and white" that "products running reliably under Windows also deliver solid results under Linux."

In the end, since antivirus provides "only the second line of defense in combating malware," it's up to users to be wise. Linux users have little to worry about regarding malware, Luther said, as long as they keep their system up-to-date, don't open up non-essential ports, install software only from reliable sources, don't allow their web browser to automatically execute active content, and don't "click on everything that has not disappeared on a count of three out of the mail client or from the desktop."

In conclusion, Luther wrote, "Those running a hybrid network have no other choice but to sift through in advance under Linux any data flowing to the Windows machines. When opting for a suitable tool, the current side-by-side test from AV-Test offers an invaluable decision-making asset."

Ms. Smith

OpenStack:Ready for prime time?

View Comments