NEWSANALYSIS

The Linux Voice view on what's going on in the world of Free Software.

Opinion

Don't panic!

We should be grateful that MS has finally got its house in order. And angry that it took so long…

Simon Phipps is president of the Open Source Initiative and a board member of the Open Rights Group and of Open Source for America.

The action that law enforcement services have taken against the GameOver-Zeus malware syndicate is great news. In the UK, this was communicated with typical tabloid alarmism, framed as "two weeks to save the world" instead of "unusually effective action by law enforcement".

The BBC's instructions start with the statement "If your computer does not run Windows, stop right here." Users of other operating systems, like Linux or ChromeOS, have nothing to worry about this time, even if they are increasingly likely to be targeted elsewhere. I went scurrying to find a half-remembered explanation from my days at IBM to explain why Windows has suffered from so many virus attacks.

Before you write to the editor, note I am not saying that the only explanation for Windows viruses is this technical one; obviously the huge attack surface of the giant userbase attracts attackers, and the large legacy of sample code gives criminals a leg up. However, that leaving the door open for a decade hasn't helped, and is a major reason why the dominant form of malware on Windows is the virus and not the trojan.

All operating systems have bugs, and I suspect (although haven't found any data to confirm) that they occur at approximately the same frequency in all mature released operating systems. All operating systems that respect Shaw's Law are also vulnerable to malware. Malware depends on identifying exploits – defects of some sort in system security that can be "exploited" to permit infestation by the malware.

Not all bugs turn into security exploits, though. In particular, in Unix-like operating systems like OS X, Linux and Solaris, it's unusual for bugs to lead directly to security exploits; instead, most malware depends on user error or social engineering. For an exploit to exist, there has to be a way to use knowledge of the bug to gain access to a resource that would otherwise be forbidden. It happens on *ix systems, but the OS has checks in place to prevent the most common way of turning bugs into exploits.

Unauthorised pokes

The most common way for this to happen (although there are many others) is for the operating system to fail to differentiate between data and program code. By treating code and data as the same thing, a path is opened for malware to use a bug to push some data into a memory location (a "buffer over-run" or a "stack overflow" are examples of this) and then tell the computer to execute it. Hey presto – there's your exploit. All an attacker has to do is push code for a virus (or a virus bootstrap) into memory and ask for it to be executed, and your computer is compromised.

"Malware depends on identifying defects of some sort in system security that can be exploited."

Windows could have prevented this sort of thing from happening by using the ring protection offered by Intel x86 architecture from the 80186 chip onwards. A feature of Intel's x86 architecture makes it possible to prohibit execution of data unless the program in question is privileged ("at ring 0"), usually by being part of the operating system. Application code at ring 3 can be forbidden from executing data.

Indeed, Windows did use ring 0/ring 3 differentiation for some jobs (skipping rings 1 and 2 for cross-platform technical reasons). But access to ring 0 – "able to execute anything you want" – was never prohibited. Doing so would have prevented legacy DOS code from running, so (as I remember being told at the time) Microsoft chose not to implement ring 0/ring 3 protection in Windows NT until it was completely sure that deprecating DOS legacy support would no longer be a marketing issue. That was in Windows 8…

Credit where due

So actually it's somewhat appropriate to blame Windows versions prior to Windows 8 for being vulnerable to many viruses that exploited bugs in this way. The existence of the vulnerability was a conscious choice and a marketing decision; in OS/2, which had no legacy to accommodate, the ring 0 separation was enforced.

Yes, Windows also offers a larger attack "surface" because of its wide adoption, and yes, there are other exploit mechanisms. But this tolerated technical vulnerability is the root cause of a large number of exploits. Windows 8 has finally addressed this particular issue, but the criminal community that exploited it is now well-funded and capable, so the problem it caused isn't going away any time soon.

CATCHUP **Summarised:** the eight biggest news stories from the last month

1 First Tizen smartphone will go on sale in Russia

Privyet, Samsung Z! This is the first smartphone to run Tizen, a mobile operating system somewhat akin to Android in that it's based on the Linux kernel. Hardware-wise it sports a 2.3GHz quad-core CPU, 2GB RAM, and a 4.8-inch 720p AMOLED display. Tizen applications will be based on HTML5 technologies, so they should be easy to port to Firefox OS, Ubuntu Touch and other mobile platforms. The Samsung Z will go on sale in the third quarter for an as-yet unknown quantity of rubles.

2 systemd 213 released, now sets your clock

Yes, systemd is marching onwards in its quest to take over all aspects of the Linux boot process. The latest release, 213, features a new **systemd-timesyncd** (spot a pattern here?) daemon, which functions as an SNTP (Simple Network Time Protocol) client. Essentially, this gets the current time from another computer on your network – or the internet – to make sure your clock doesn't drift away from reality. What's to come in systemd next? Maybe we'll see "systemd-emacsd"...

3 Nginx overtakes Apache on top 10,000 websites

Nginx has been creeping up on the Apache web server for a while, and the latest adoption statistics tell a story. Of course, Nginx often functions as a reverse proxy or load balancer for Apache, so it's not an 'either-or' situation. See more at: **http://w3techs.com/technologies/cross/web_server/ranking**

4 Chinese government bans Windows 8, looks to Linux

As if Windows 8, with its widely-dissed "Metro" interface, wasn't having enough trouble. Now the Chinese government has banned Microsoft's latest operating system, citing vague energy consumption and security issues. Meanwhile, with support for Windows XP terminated, the government is taking a fresh look at Linux to upgrade its vast number of computers. After the Red Flag Linux project was shelved earlier in the year, however, it's unclear what will happen...

5 Mozilla adopts Adobe DRM scheme in Firefox

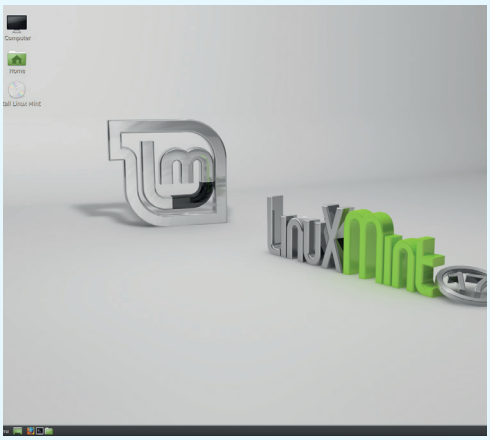
This is has made a lot of people upset. DRM – aka Digital Rights Management – is a ploy by media companies to restrict who can view or listen to their content. It's deeply unpopular in the FOSS world, but Mozilla has decided to implement a DRM system from Adobe in future Firefox releases (users will be prompted to install it if desired). The argument is that it keeps Firefox relevant, but detractors regard it as a capitulation – acceptance that DRM is here to stay.

6 OpenSSL receives two full-time developers

For years, major companies have been relying on OpenSSL without ever contributing anything back. Then Heartbleed comes along, and there's a mad rush to give OpenSSL some funding. Now the project will get two full-time developers, but given the horrific state of the source code (see **www.openssl rampage.org**), is this really going to help? Many argue that a full fork is needed, with developers willing to rip out all the old cruft, like the LibreSSL team from OpenBSD is doing.

7 Linux Mint 17 "Qiana" hits the mirrors

It's currently the most popular Linux flavour on DistroWatch, and now Mint 17 has been released. We have a full review on page 48, but here's a summary of the highlights: the Update Manager is faster and its GUI has been overhauled; the Driver Manager can install drivers from the boot media, without an internet connection; and the login screen now works better with multiple monitors. Mint 17 is a Long Term Support release, with updates until 2019.



8 EU supports "right to be forgotten" on Google

While this isn't Linux news per se, it's a major development in terms of online privacy. An EU court has ruled that Google should alter its search results to remove links to information about a person, should that person request it. So if there's a page on the web about you that you don't like, and you don't want it appearing in Google results when someone searches for your name, you can ask Google to remove the links via this page: **http://tinyurl.com/googleforget**