The Economist

Babbage

Computer security

A digital fortress?

Qubes is the most secure operating system you have never heard of

Babbage Mar 28th 2014 | by J.M.P.|MONTEVIDEO

WINDOWS "is spyware with an operating system attached" according to the old sysadmin joke. Riddled with unpatched security vulnerabilities ("zero-days") that let criminal hackers and intel agencies take control of the operating system, Windows is a computer security professional's nightmare.

Measuring the severity of the problem is difficult because of the lucrative black market in zero-day exploits. A handful of boutique exploit providers—Endgame

Systems, Exodus Intelligence, Netragard, ReVuln and VUPEN—control the market, and buyers, according to Stefan Frei of NSS Lab (https://www.nsslabs.com/reports/known-unknowns-0) s, pay on average $40,000 to $160,000 for an exploit (depending on the software affected and the reach of the zero-day offers).

Mr Frei's research suggests that, on any given day from 2011-2013, privileged groups had access to at least 58 vulnerabilities targeting Microsoft, Apple, Oracle, or Adobe—and these are just the known ones. In 2013 alone, according to documents provided by Edward Snowden (http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities), the NSA spent more than $25 million on zero-days. Other governments and criminal hackers are also known to be stockpiling these digital armaments.

How many zero-days are there? Who knows about them? What software do they affect? These are, as Mr Frei puts it, "known unknowns."

Nor is the problem confined to Windows, which bears the brunt of these attacks because of its popularity. Mac OSX, Linux, Android and many other operating systems suffer from zero-days. As Micah Lee, CTO of the Freedom of the Press

Foundation advises national security journalists, such as Glenn Greenwald, on how to evade government spying. He points out that "all non-trivial software contains bugs, some of which are security vulnerabilities". Computers can be hacked simply by users watching a Flash video or using javascript in a web browser, or even just by viewing a JPG or GIF.

Worse, there is usually no way to defend against a zero-day. And once a system has been hacked, malware can steal secrets, record keystrokes, capture camera and microphone feeds, and even inject arbitrary keystrokes or mouse movements to impersonate the owner—often without their knowledge—until the operating system is reinstalled or the computer gets replaced. That is until the exploited zero-day is patched (assuming it gets discovered at all).

The solution, argues Joanna Rutkowska of Invisible Things Lab (http://invisiblethingslab.com) , is to "assume breach." A former offensive security researcher, she grew frustrated with how easy it was for her to subvert the operating systems she tested. So in 2010 she decided to build her own: Qubes OS (qubes-os.org) . Rather than try to create a bug-free operating system, she assumes in advance that every part of the operating system contains zero-days, and designs the system accordingly.

In Qubes, hardware control, networking, and applications are all kept separate. Based on the Xen hypervisor (a virtual machine manager), Qubes allows the creation of multiple VMs (virtual machines): one for work, one for personal, and one for online banking, say. By separating one's digital life into multiple domains, an attacker who compromises, say, the web browser, will not have access to sensitive work files. Qubes supports both Linux and Windows VMs.

Five leading computer security experts named the operating system a finalist for the Access Innovation Prize for Endpoint Security (https://www.accessnow.org/blog/2014/02/13/endpoint-security-prize-finalists-announced) . Mr Lee jokes that Qubes is like "a digital fortress."

Sound too good to be true? There is a catch. Computer security is equal parts tools

and digital "street smarts." Qubes relies on the user to make security decisions, and cannot offer protection to those who make foolhardy choices. This is a challenge Ms Rutkowska hopes to overcome in the next release of Qubes by automating some of its functions.

Qubes's hardware support can also be finicky. For maximum security it requires CPU virtualisation. The system is also resource intensive, and users will get best results with a minimum of 4GB (preferably 8GB) of RAM.

So who is the ideal Qubes user? Sysadmins? National security journalists? Criminals? Spies? Ms Rutkowska reckons corporations will be its primary market.

By separating work and personal domains on a corporate workstation, "Qubes could significantly increase the level of protection of corporate secrets and IP." Ms Rutkowska expects to see real-world commercial deployments starting sometime within the next year.

No device can be trusted in a world of zero-days. But assuming one’s system has been compromised should not cause despair. Dealing with the uncertainty of computer security requires finding the right mental attitude: assume breach, but put up your best defense, regardless. For those willing to put in the effort, Qubes is more secure than almost any other operating system available today.