FLAMING RETORT: All this new Mac malware - whose fault is it?

Blog Post from Paul Ducklin, Sophos

Flaming Retort is back, this time trying to Coole and Explayne Ye Flames we've had from some Mac users (and the discomfiture we know that many others have endured) in the past few days.

In a back-to-front way of making Mac fans feel better, I'll start by making everyone feel slightly worse, taking a small potshot at Windows, OS X and Linux fans alike.

My point here is not to prove that it issomebody'sfault, but simply to remind us that perennially finding someone else to blame for our computer security woes is a bad idea.

Let's start with Windows users.

Last year, Sophos bought a job-lot of USB keys from a rail company's annual lost property auction. Two-thirds of themcontained malware- all of it for Windows.

Not one file on any of the keys was encrypted, even though many of the files contained personal or business information.

This shouldn't be happening in the 2010s.Anydecent anti-virus softwarewould have made mincemeat of the malware infections on the keys we acquired.

And ourfree encryption tool[download link, Windows only, ungated] makes it easy to secure your files when you're taking them on the road.

Let's move on to OS X, which has beenunder the pumpover the last couple of weeks, as Apple has scrambled tocatch upwith its Java updates and to deliver some kind ofmitigation toolfor users who got hit by theFlashback malwareas a result.

It's easy to blame someone else. It's Apple's fault for not patching fast enough. It's Oracle's fault for the vulnerability in Java. It's Sophos's fault for making a conspiracy theory to boost sales of itsfree product. (No, I don't quite get that last complaint, either.)

Many of the Mac users who were hit by Flashback and who didn't have an anti-virus to help them out probably didn't even notice that anything untoward had happened. Mac users aren't much used to so-calleddrive-by installs.

That's where the crooks exploit a vulnerability so they can bypass the usual "do you want to download/this file comes from the internet/there is still time to save yourself" notifications from your browser, and sneak malware onto your computer without warning or consent.

But Flashback isn't the only malware out there for the Mac. According to SophosLabs, more than three-quarters of last week's malware reports from Sophos Anti-Virus for Mac were for other families of badware, including a lot of year-or-more-old stuff.

This shouldn't be happening in the 2010s.Any decent anti-virus software would have made mincemeat of that malware.

And finally, the Linux crew. Linux desktop users will get off the lightest here, because they haven't been targeted by widespread malware lately.

Perhaps that's the inherent superiority of the Linux platform? Or perhaps it's merely fortuitous, because Linux has just a 1% desktop market share? [*]

We'll go back to 2008 to take our first potshot at Linux users and security. Back then, SophosLabs found that a six-year-old Linux virus, Linux/RST-B, wasstill active and spreadingon and from more than 12,000 computers. Worse, those measurements only counted instances of the malware running as root (administrator), so the true total was almost certainly very much larger.

This shouldn't have happened, even back in the 2000s.Any decent anti-virus software would have made mincemeat of this malware.

And there was a malware fiasco, albeit not a widespread one, in the Linux world last year. Malware was discovered on the PC of at least one kernel maintainer, as well as on some of thekernel.org servers themselves. Kernel.org was down for about a month. (Yes, Linux malware. Not only in the wild, but on kernel.org, itself running Linux!)

This shouldn't have happened at all, ever.

What does all this mean?

If you want to get all Flaming Rhetorical about it, you might take a Biblical tone with those who attempt to point security fingers at everyone else, and try an observationlike this: "Hee that is without sinne among you, let him first cast a stone." [**]

Security is the responsibility of all of us: technologists, coders, mobile phone users, writers, video watchers, bloggers, Wikipedia readers, bank clerks, bicycle couriers, politicians, policemen and gardeners.

It's not yourfault. It's yourresponsibility.

[*]Don't shout at me! You can say it's more than 1%, if you dearly wish it to be. I'm currently using a simplistic desktop formula: Windows 90%, OS X 9%, Linux 0.9% and everything else 0.1%. Easy to remember and accurate enough by a physicist's yardstick. (One order of magnitude either way, plus or minus one order of magnitude.)

[**]That's the 1611 translation. It fits best, I think you will admit, with both the imagery and the orthography of the Flaming Retort graphic.