Macintosh Malware Erupts

by Jeremy Legendre
BSCSIA Student, Norwich University
&
M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

MK writes: Norwich University student Jeremy Legendre sent me an interesting essay which prompted a close collaboration between the two of us on this article.

* * *

History

Sophos antimalware expert Graham Cluley< http://www.linkedin.com/in/grahamcluley >, who has a long and distinguished career in the field, has written a summary of malicious software affecting Macintosh computers.[1] In comparison to the history of Windows malware,[2] Macintosh systems have been far less susceptible to malware than Windows systems. For example, in 2005, Mark H. Anbinder and colleagues published a review of Macintosh computer malware in which (in the version available through the EBSCO library database provided by Norwich University) *Macworld* editors started the review with this note: "Most Mac users gaze on smugly as reports of each new Windows security crisis break. And they have good reason: At press time, research from Sophos (a maker of antivirus software) showed that 68 viruses have affected the Mac while 97,467 have affected Windows. Of those 68, most are a decade old or older and don't directly affect OS X."

Despite the disparity in the number of viruses affecting Windows and Macintosh systems, Anbinder *et al.* challenged the belief that "Mac users don't need to worry about viruses." The authors warned readers that "We've enjoyed a long, glorious stretch without serious malware affecting our platform. But that doesn't mean we can afford to let down our collective guard. If there is a virus attack, those of us who have good, up-to-date antivirus software installed will have the best odds of escaping unscathed." They urged Mac users to keep updated antimalware tools – and back in 2005, it was reasonable to suggest, "Weekly updates should be adequate for most users, but if your computing involves accessing lots of files from lots of sources—whether via e-mail, file servers, or Web downloads—then daily updates might be a better idea."

Changes

However, malware specifically designed for Mac is on the rise. Cluley's historical summary shows progressively more and more serious malware in 2009, 2010 and 2011. Apple products have been increasing their market share for laptops and workstations but especially for tablets and phones. Writing in the *Wall Street* Journal, Nick Winfield pointed out that "Some research firms have even started to look at tablets as part of the PC market when determining market share, which significantly changes Apple's position. Canalys Ltd., for example, now calls Apple the second-largest PC vendor, after Hewlett Packard Co. Adding in iPads as well as Macs –

which only accounted for about 5% of global shipments – the firm estimates that Apple accounted for 13.6% in world-wide PC shipments in the second quarter, up from 8.2% a year earlier, and just a bit behind H-P's 15.7% share."[4]

It seems reasonable to predict that black hats would to follow the trend in market share, and recently, evidence has surfaced of new Macintosh operating system malware. Ed Bott reported on an interview with an anonymous AppleCare support representative who told him in May 2011 about increasing calls to AppleCare support because of malware.[5] Apparently the "Mac Defender"[6] virus was causing four to five times as many calls as usual.

Jeremy personally reverse-engineered and analyzed Mac Defender to see what the fuss was all about. As it turns out, this piece of malware is very simple and could be easily stopped by Apple with a service package or update. If this simple little program is causing such an increase in AppleCare calls, what is going to happen when more advanced malware comes out?

On May 2nd, 2011, a Danish security company named CSIS Security Group announced something that has never been seen before: the first do-it-yourself crimeware kit for the Mac.[7] It has been put up for sale on a few underground forums. Not all the details on what the crimeware kit can do have been released yet, but Brian Krebs interviewed the author of the malware: "The seller of this crimeware kit claims his product supports form-grabbing in Firefox and Chrome, and says he plans to develop a Linux version and one for the iPad in the months ahead. The price? $1,000, with payment accepted only through virtual currencies Liberty Reserve or WebMoney."[8] Krebs includes a link to a YouTube video showing details of the crimeware's user interface.

Apple posted instructions on "How to avoid or remove Mac Defender malware" in June 2011.[9]

Concluding Remarks from Jeremy

One of the reasons Mac OS X is perceived as superior to Windows is because of its appearance of having integrated security; for example, requiring user credentials before running any system changing software or claiming that "With virtually no effort on your part, OS X defends against viruses and other malicious applications, or malware. For example, it thwarts hackers through a technique called "sandboxing" — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch."[10]

Although the design may be sound, the operating system does *not* prevent people from being swayed into *thinking* that the malicious software they are downloading is safe. Although a user cannot install a program on a Mac without user permission, an unsuspecting user may easily allow malware to run. From this point of view, Mac OS X is *not* fundamentally safer than Windows or Linux. I do not say this as someone who is anti-Mac: I use my Macbook Pro every day and I love it, but I am still cautious about what I install on it. But without adapting to the changing threat picture, Apple will be in the same position of malware vulnerability that Microsoft has reached.

So, in conclusion, Macs are starting to become more popular and a wider range of people are using their systems. Apple will have to concentrate more on security and vulnerability within their operating system. They are going to have to have more security updates and patches and may have to stop their "It doesn't get PC viruses" ad campaign from which I quoted in the first

paragraph of these concluding remarks.

Although Apple may not like having to admit that their systems are susceptible to viruses, awareness of the changing malware situation gives them a chance to get ahead of the curve by strengthening the operating system and find additional ways to prevent further malware attacks.

Notes

[1] (Cluley 2011)
[2] (Leonhard 2011)
[3] (Anbinder, et al. 2005)
[4] (Wingfield 2011)
[5] (Bott, An AppleCare support rep talks: Mac malware is "getting worse" 2011)
[6] (Bott, What a Mac malware attack looks like 2011)
[7] (Kruse 2011)
[8] (Krebs 2011)
[9] (Apple, How to avoid… 2011)
[10] (Apple, Why you'll love… 2011)

Works Cited

Anbinder, Mark H, Jeff Carlson, Glenn Fleishman, Jeffery Battersby, and Kirk McElhearn. "Mac Security: Fact and Fiction." *Macworld* 22, no. 3 (2005-02-18): 54-64. http://www.macworld.com/article/42964/2005/02/macsecuritymain.html (accessed 2011-12-07).

Apple. How to avoid or remove Mac Defender malware. 2011-06-08. http://support.apple.com/kb/HT4650 (accessed 2011-11-22).

—. "Why you'll love a Mac -- It doesn't get PC viruses." Apple Inc. 2011. http://www.apple.com/why-mac/better-os/#viruses (accessed 2011-12-07).

Bott, Ed. An AppleCare support rep talks: Mac malware is "getting worse". 2011-05-11. http://www.zdnet.com/blog/bott/an-applecare-support-rep-talks-mac-malware-is-getting-worse/3342 (accessed 2011-11-21).

—. What a Mac malware attack looks like. 2011-05-06. http://www.zdnet.com/blog/bott/what-a-mac-malware-attack-looks-like/3269?tag=content;siu-container (accessed 2011-11-21).

Cluley, Graham. The short history of Mac malware: 1982 - 2011. 2011-10-03. http://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/ (accessed 2011-11-21).

Krebs, Brian. 'Weyland-Yutani' Crime Kit Targets Macs for Bots. 2011-05-11. http://krebsonsecurity.com/tag/weyland-yutani-bot/ (accessed 2011-11-21).

Kruse, Peter. Crimekit for MacOSX launched. 2011-05-02. http://www.csis.dk/en/csis/blog/3195/ (accessed 2011-11-21).

Leonhard, Woody. 20 years of innovative Windows malware -- Ingenuity to nefarious ends: The evolution of groundbreaking Windows malware sheds light on what's to come. 2011-02-28. http://www.infoworld.com/d/security/20-years-innovative-windows-malware-021 (accessed 2011-11-21).

Wingfield, Nick. "Microsoft Faces the Post-PC World -- Now 25 Years Old, Windows Sales Slow as iPad Gains; Lowest Market Share in Two Decades -- 82%." *The Wall Street Journal*, 2011-08-15: B1. http://online.wsj.com/article/SB10001424053111903885604576486343139938136.html (Subscription required; accessed through Norwich University Kreitzberg Library databases 2011-12-07).

* * *

Jeremy Legendre has been programming since he was 14; he is now is one of our most gifted freshmen in the BSCSIA program at Norwich University. He is currently collaborating with one of our professors on a textbook for an upper-level malware forensics course.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >