FROM APPLICATION GUISES TO FAKEAV

The Evolution of Mac Malware

Threat Spotlight, our latest monthly offering, features expert views and findings on the current trends in the threat landscape. This maiden edition discusses the recent spate of FAKEAV for Macs. In a span of just one month, TrendLabs[SM] engineers came across several FAKEAV variants that targeted Mac users, prompting security experts to watch out for further attacks.

FAKEAV Malware Target Mac Users

The FAKEAV family is responsible for one of the most prevalent attack types to date. The family is one of the few malware types that utilizes a visual element, often worrying users the most. FAKEAV attacks traditionally targeted *Windows*-based system users until the recent emergence of a rogue antivirus software for *Mac OS X* known as *MACDefender*, detected by Trend Micro as OSX_FAKEDEF.M. This particular FAKEAV for Macs caused quite a stir in the security industry, as it prompted Apple to immediately release a security update to resolve the issue.

Sold for US$40–100 each, cybercriminals generate huge profits from the buyers of rogue antivirus software.

Figure 1. *Fake dialog box informing users that their systems are infected*

Like other FAKEAV variants, OSX_FAKEDEF.M displays fake scan results and virus notification prompts when executed. Affected users who try to fix the supposed malware infections are asked to purchase a license in order to obtain the full version of the rogue antivirus software, *MACDefender.* To do so, they are pointed to a malicious site that asks them to key in their personal credentials like credit card information. Sold for US$40–100 each, cybercriminals generate huge profits from the buyers of rogue antivirus software. They can also use the information they steal for other malicious activities.

TrendLabs engineers also spotted other variants of Mac FAKEAV in the wild. Some of these used names like *MacSecurity,* detected as OSX_FAKEAV.A, and *MacProtection.* This shows that the proliferation of more FAKEAV variants for Macs may become a trend.

Figure 2. *Typical FAKEAV for Macs infection diagram*

Blackhat SEO-FAKEAV Tandem: The *Mac OS X* Edition

Trend Micro senior threat researcher Nart Villeneuve blogged about a blackhat search engine optimization (SEO) attack that led affected users to either FAKEAV landing pages or to sites where the *Black Hole Exploit* pack can be found. This targeted users of both *Windows*- and *Mac OS X*-based systems. The cybercriminals behind this leveraged *Google's* image search feature to redirect users to FAKEAV landing pages. In just one month, the malicious landing pages obtained almost 300 million hits, 7.3 percent or approximately 21 million of which came from Mac users.

OSX_FAKEAV.A specifically used blackhat SEO as an arrival technique. Cybercriminals rigged search results to drive traffic to their specially crafted malicious sites.

Rogue Antivirus Software Spread via *Facebook*

FAKEAV for Macs also spread via popular social networking site, *Facebook.* Detected as OSX_DEFMA.B, the malware infects systems when users click malicious links spammed on *Facebook.* Like other FAKEAV for Macs, this shows fake scan results and alerts as well as urges users to avail of a rogue antivirus software in order to rid their systems of supposed infections. Users who are convinced to buy the software are redirected to *http://{BLOCKED}.217.79/mac.php* in order to make the purchase.

Figure 3. *Links to OSX_DEFMA.B download pages were spammed via* Facebook *posts*

Apple Immediately Releases a Security Patch

In response to the consecutive FAKEAV for Macs campaigns, Apple released a security update, which Trend Micro senior threat researcher Joey Costoya says not only addresses the threats *MACDefender* pose but also those other Mac malware such as OSX_RSPLUG.E, OSX_KROWI.A, and OSX_OPINIONSPY.A expose users to. Shortly after the patch's release, however, cybercriminals found a way to bypass Apple's solution, which again put users in danger.

Mac Malware Throughout the Years

Rogue antivirus software and other malware targeting *Mac OS X* users are not entirely new. In fact, the first-ever FAKEAV for Macs dubbed *MacSweeper,* detected as OSX_MACSWEEP.A, emerged as early as 2008. This prompts the display of a window to inform users of a certain "privacy violation." It then prompts the display of windows alerting them to supposed infections then convinces them to purchase *MacSweeper* to clean their systems. The existence of a legitimate antivirus software known as *Mac Sweeper* aided OSX_MACSWEEP.A into tricking users to purchase the rogue antivirus software.

A scareware for Macs known as *iMunizator* also appeared in the same year. This bore a lot of similarities to *MacSweeper,* except for download location.

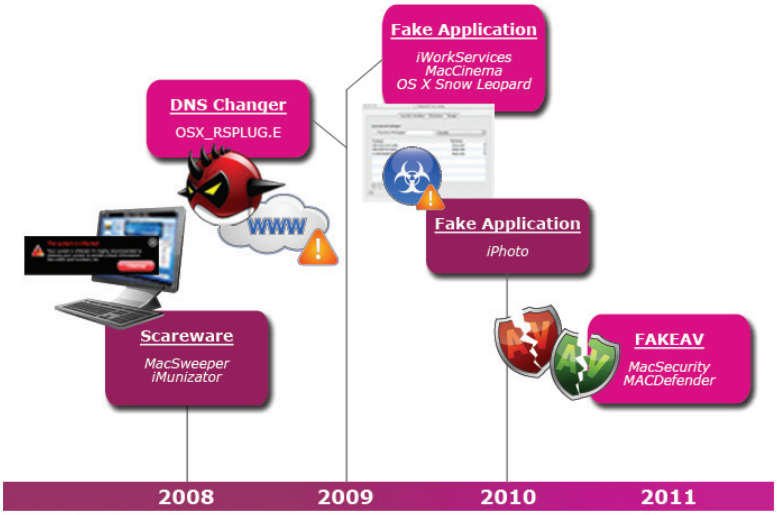

Figure 4. *Mac malware throughout the years*

Most Mac malware employ social engineering tactics, as these often come in the guise of legitimate applications. OSX_KROWI.A, for instance, posed as *iWorkServices* and came bundled with a pirated version of Apple's *iWork '09* suite. TrendLabs engineers also came across Mac malware that posed as a *MacCinema* installer, detected as OSX_JAHLAV.D, in 2009. Shortly after, two more Mac malware enticed users to download them in order to watch certain pornographic videos. In reality, however, these Trojans change the Domain Name System (DNS) server settings of infected systems, redirecting affected users to possibly malicious sites. In 2010, a malware posing as an *iPhoto* installer was found in the wild. Functioning as a backdoor application that allows remote users to access infected systems, this compromised affected users' security.

Typical Mac Malware Infection Vectors

Earlier *Mac OS X* malware often arrived as downloads from malicious sites and usually rode on the popularity of Mac applications. Cybercriminals have also been known to ride on new *Mac OS X* releases. Such was the case of OSX_JAHLAV.K, which posed as a free copy of *OS X Snow Leopard* even before the OS's official release in 2009.

FAKEAV for Macs, on the other hand, employed enhanced social engineering tactics, apart from social networking sites and blackhat SEO techniques, to spread.

Mac malware are clearly evolving to affect as many users as possible. The FAKEAV for Macs we recently spotted, for instance, not only spoofed legitimate applications, these also imitated their "look and feel" in order to appear more convincing. These also used a JavaScript to lead users who happen to click anywhere on a landing page to unknowingly download them. These used the same social engineering techniques *Windows*-based FAKEAV peddlers have become known for, urging our engineers to be on the lookout for more FAKEAV for Macs.

What's Next for FAKEAV for Macs?

Security researchers also see the possibility of seeing FAKEAV for iPhones, iPads, and iPod Touch devices, as the demand for these continues to surge. Consumer research firm, Nielsen, recently pegged Apple's share of the total U.S. smartphone market at 27 percent. Furthermore, market intelligence provider, Allied Business Intelligence Inc. (ABI), reported that the iPad accounts for an 85 percent share of the worldwide media tablet market. These figures are enticing cybercriminals to launch more and more attacks targeting Apple devices.

Security researchers see the possibility of seeing FAKEAV for iPhones, iPads, and iPod Touch devices, as the demand for these continues to surge.

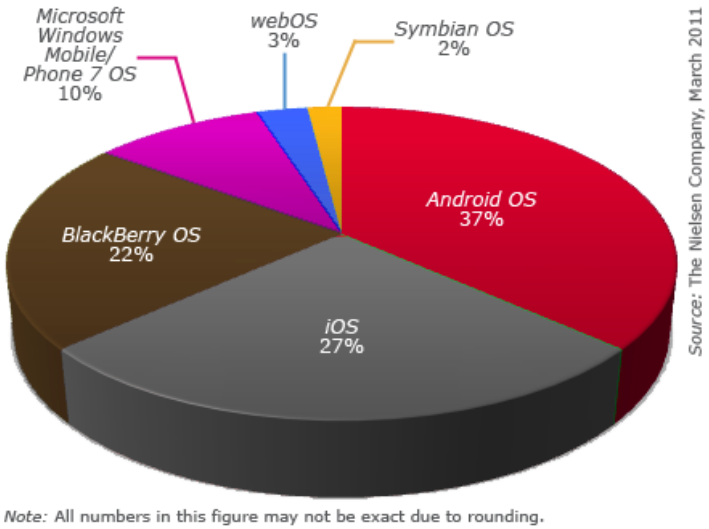

Figure 5. *U.S. 2011 smartphone OS market shares*

Trend Micro product manager Warren Tsai says FAKEAV scanning pages are essentially JavaScripts so any browser can easily render these. As such, iPhone, iPad, and iPod Touch users who unknowingly visit FAKEAV download pages may also see fake scans.

No Platform Is Malware Proof

Even though more malware target *Windows*-based systems, this does not mean that Macs are malware proof. In fact, we have been seeing malware targeting Macs since 2006. Research firm Gartner says *Mac OS X's* worldwide market share continues to grow. This may entice cybercriminals to go after its users even more.

The most recent FAKEAV for Macs had versions for various platforms. To determine what OSs and browsers are installed on systems, these utilized the *User-Agent* string that is present in all browsers. Doing so enabled the cybercriminals to serve users FAKEAV versions specific to their OSs.

As such, users, regardless of OS, should take utmost care when browsing the Web. They should keep in mind that there is no such thing as a malware-proof platform.

Defense Against FAKEAV

Users are strongly advised to refrain from visiting suspicious sites. They should never download and install applications from unknown sources. Clicking spammed links despite enticing subjects in email or chat messages and on social networking sites, regardless of sender, is also ill-advised. Keeping systems up-to-date by downloading the latest patches can also lessen the chances of suffering from malware infections. Last but not least, awareness is key. Users should stay abreast of the latest news and happenings in the threat landscape so as not to fall into cleverly crafted cybercriminal traps.

In addition, choosing to use a trusted and reliable security solution like *Trend Micro Smart Surfing for Mac* can protect Mac users from all kind of attacks, including FAKEAV. Blocking access to malicious sites helps prevent the download of malicious files and the threat of monetary and personal data theft.

References

Threat Encyclopedia

- "OSX_MACSWEEP.A." (January 20, 2008). http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_MACSWEEP.A (Retrieved June 2011).
- "OSX_KROWI.A." (February 9, 2009). http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_KROWI.A (Retrieved June 2011).
- "OSX_JAHLAV.D." (August 7, 2009). http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_JAHLAV.D (Retrieved June 2011).
- "OSX_RSPLUG.E." (October 10, 2009). http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_RSPLUG.E (Retrieved June 2011).
- "OSX_OPINIONSPY.A." (June 2, 2010). http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_OPINIONSPY.A (Retrieved June 2011).
- "OSX_JAHLAV.K." (October 10, 2009). http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_JAHLAV.K (Retrieved June 2011).
- "OSX_FAKEAV.A." (May 6, 2011). http://about-threats.trendmicro.com/Malware.aspx?language=us&name=OSX_FAKEAV.A (Retrieved June 2011).

- "OSX_FAKEDEF.M." (May 28, 2011). http://about-threats.trendmicro.com/Malware.aspx?language=us&name=OSX_FAKEDEF.M (Retrieved June 2011).
- "OSX_DEFMA.B." (June 2, 2011). http://about-threats.trendmicro.com/Malware.aspx?language=us&name=OSX_DEFMA.B (Retrieved June 2011).

TrendLabs Malware Blog

- Bernadette Irinco. (August 26, 2009). "Bogus *Snow Leopard* Update Sites Lead to DNS Changers." http://blog.trendmicro.com/bogus-snow-leopard-update-sites-lead-to-dns-changers/?wpmp_switcher=mobile (Retrieved June 2011).
- Carolyn Guevarra. (April 19, 2010). "Mac Malware Disguised as *iPhoto* Installer." http://blog.trendmicro.com/mac-malware-disguised-as-iphoto-installer/ (Retrieved June 2011).
- Det Caraig. (June 16, 2009). "Not One but Two New *OS X* Malware." http://blog.trendmicro.com/not-one-but-two-new-os-x-malware/ (Retrieved June 2011).
- Det Caraig. (August 11, 2009). *"Mac OS X* DNS-Changing Trojan in the Wild." http://blog.trendmicro.com/mac-os-x-dns-changing-trojan-in-the-wild/ (Retrieved June 2011).
- George Moore. (March 26, 2008). "Scareware Software Makes Its Second Round on *Mac O/S."* http://blog.trendmicro.com/scareware-software-makes-its-second-round-on-mac-os (Retrieved June 2011).
- Jamz Yaneza. (June 6, 2011). "What's in Apple *Security Update 2011-03?"* http://blog.trendmicro.com/whats-in-apple-security-update-2011-03/ (Retrieved June 2011).
- Joey Costoya. (June 8, 2011). "A Walk-Through of a FAKEAV Infection in *Mac OS X."* http://blog.trendmicro.com/a-walkthrough-of-a-fakeav-infection-in-mac-os-x/ (Retrieved June 2011).
- Karl Dominguez. (June 2, 2011). "More Malware for Mac." http://blog.trendmicro.com/more-malware-for-mac/ (Retrieved June 2011).
- Nart Villeneuve. (May 11, 2011). "Blackhat SEO Attack Uses *Google's* Image Search to Reach 300 Million Hits." http://blog.trendmicro.com/blackhat-seo-attack-uses-google's-image-search/ (Retrieved June 2011).
- Roderick Ordoñez. (January 18, 2008). "Rogue App Sweeps Mac." http://blog.trendmicro.com/rogue-app-sweeps-mac/ (Retrieved June 2011).

TrendWatch

- Erika Mendoza, Jasper Manuel, and Roland Dela Paz. (August 27, 2010). "Why FAKEAV Persist." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/66_why_fakeav_persist__august_27__2010_.pdf (Retrieved June 2011).

External Sources

- Allied Business Intelligence Inc. (April 20, 2011). *ABIresearch.* "Apple iPad Held 85% Media Tablet Market Share in 2010." http://www.abiresearch.com/press/3665-Apple+iPad+Held+85%25+Media+Tablet+Market+Share+in+2010 (Retrieved June 2011).
- Apple Inc. (May 31, 2011). *Apple Support.* "About *Security Update 2011-003."* http://support.apple.com/kb/HT4657 (Retrieved June 2011).
- Gartner Inc. (April 27, 2011). *Gartner Newsroom.* "Gartner Says Worldwide Operating System Software Market Grew to $30.4 Billion in 2010." http://www.gartner.com/it/page.jsp?id=1654914 (Retrieved June 2011).
- The Nielsen Company. (April 26, 2011). *nielsenwire.* "U.S. Smartphone Market: Who's the Most Wanted." http://blog.nielsen.com/nielsenwire/online_mobile/u-s-smartphone-market-whos-the-most-wanted/ (Retrieved June 2011).