Security Spotlight
June 14, 2010

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

APPLE'S POPULARITY USHERS IN NEW SECURITY THREATS

A powerful presence in cyberspace is hard to miss. The introduction of revolutionary products, including the most recent launches of the iPad and iPhone 4, put the spotlight on Apple and its CEO Steve Jobs. The company's continuous rise to fame has made it a household name. Unfortunately, however, this has also made it an instant cybercriminal target.

Apple Ripens

Apple first gained the world's attention with the introduction of the iPod in 2001. This was then followed by the consecutive launch of numerous other products and services like the *iTunes Store*, the iMac, the MacBook Pro, the iPhone, and the iPod Touch.

Apple's continuous rise to fame has made it a household name. Unfortunately, however, this has also made it an instant cybercriminal target.

Figure 1. *Apple has become known for creating a new breed of technology consumers worldwide.*

The debut of one product from one year to the next earned Apple a high market capital that allowed it to surpass Dell. Despite the apparent growth, however, Microsoft still remained the most dominant force in the competition. In the third quarter of 2009, *The New York Times* reported that Apple accounted for 8% of the overall desktop and laptop PC market share in the United States. Though its share was still minute compared with Microsoft's, every time Apple grabs a point of market share from the leader, its stock price climbs.

A recent *Wired* article reported that Apple's market capital in the next few years is expected to reach US$241.5 billion, surpassing Microsoft's by US$2 billion. *The Wall Street Journal* noted a similar future trend for Apple's stock based on a Standard & Poor's (S&P) study.

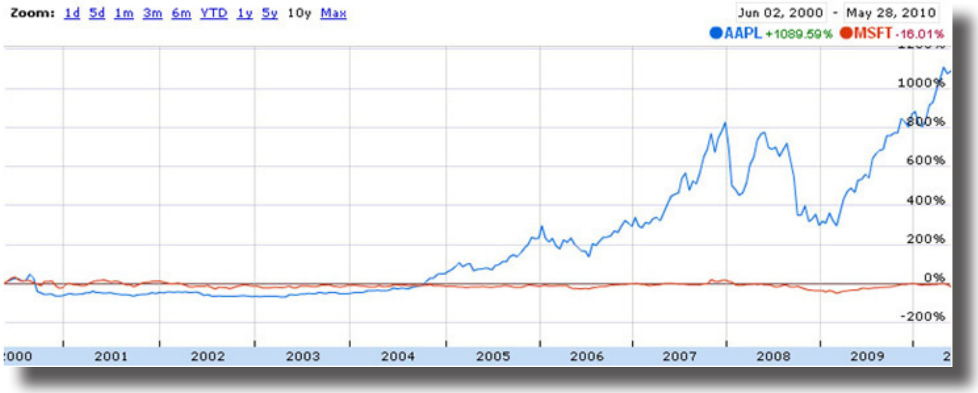

Figure 2. *Comparison of Microsoft and Apple's capital from 2001 to 2010*

Cybercriminals Aim for Apple

What was once an obscure name has been recently dubbed as the largest technology company in the world. It seems that the world has finally noticed Apple's products. In fact, blogs and news sites hardly ever fall short of articles mentioning the company and its latest products.

Apple's rise to fame could readily be attributed to its CEO Steve Jobs who single-handedly pushed products that were basically manifestations of his own eclectic thinking to the masses. In a sense, Jobs helped usher in a new technological era. Unfortunately, however, the popularity Apple products now enjoy has ushered in dangerous threats for their users.

The lack of visible attacks on an OS does not necessarily translate to OS invincibility. It could mean that cybercriminals would rather exert effort on initiatives that would bring them heftier returns.

PC Versus Mac: The Microsoft-Apple Tango

It is only natural for consumers to pit two seemingly equal products against each other to see which is better. In Microsoft and Apple's case, users have begun weighing which of the companies produced more secure products by pitting Microsoft's *Windows* against Apple's *Mac OS X.*

Many technology and security aficionados have attempted to clear up the confusion brought about by this age-old and longstanding debate, which inevitably cause heated exchanges between PC and Mac users. One *CNET News* article even featured various experts' opinions on the matter. Some of these were:

- Macs are less vulnerable to attacks today because Apple has significantly less market share than Microsoft.
- The lack of visible attacks on an OS does not necessarily translate to OS invincibility. It could mean that cybercriminals would rather exert effort on initiatives that would bring them heftier returns.
- Security does not have anything to do with what OS the user runs on his/her computer. It has more to do with the user himself/herself.

Note, however, that most experts recommended the Mac over the PC not because the former was more secure than the latter but because it had a lower market share.

Shooting One Apple Product at a Time

One should not be quick to dismiss that though *Windows* has had the greater number of reported vulnerabilities compared with *Mac OS X* and other OSs, that does not mean that the former is the greater evil of the two. When it comes to security, after all, one should realize that all software applications are vulnerable.

TrendLabs^{SM} has documented a number of threats targeting Apple users using a variety of social engineering ploys in the *TrendLabs Malware Blog*. The following lists some Apple products that have been used as bait by cybercriminals:

- ***QuickTime.*** In March 2007, a French band's *MySpace* page was found to host an exploit in the form of an invisible *QuickTime* movie (detected as TROJ_DLOADER.JHV) that plays whenever site visitors view the page. Note that *QuickTime* has a feature that allows users to include a URL or a JavaScript code in a movie. The movie file loads a malicious JavaScript (detected as JS_SPACESTALK.A) that later on downloads and executes another JavaScript, which is capable of stealing information from an affected system.

- ***iTunes.*** In February 2009, cybercriminals spammed users with an invoice that supposedly came from *itunes.com.* The spam advertised a Valentine's Day sale and enticed users to click embedded links that led to malicious pharmaceutical sites.

- **iPhone.** In July 2008, phishers rode the hype of the release of Apple's latest product then—the iPhone 3G—by sending out fake billing spammed messages. The spam contained a link that led recipients to a page that resembled a sleek-looking *Apple Store* page complete with a billing form that users could fill out.

- ***MobileMe.*** A month after the iPhone 3G-related phishing attack, phishers then turned their attention to *MobileMe* users. For this, they used more professional-looking spammed messages, which hardly looked fake. Some of the links in the message even led to legitimate Apple pages. Clicking the rogue link, however, led recipients to a spoofed *Apple Store* page, similar to that used in the iPhone 3G attack.

- ***OS X Snow Leopard.*** In August 2009, a few days before the release of *OS X Snow Leopard,* Trend Micro advanced threats researcher Feike Hacquebord found bogus sites purportedly giving out free copies of the said OS detected as OSX_JAHLAV.K. This malware downloads other malicious scripts that can alter the Domain Name System (DNS) configuration of an affected system, which can direct users to sites that host FAKEAV variants and/or their components.

- **iPad.** The announcement of the Apple iPad's launch in the United States in March 2010 spurred spammers to propagate messages purporting to be part of a word-of-mouth Apple marketing campaign. Interested recipients were asked to reply with their personal information.

One should not be quick to dismiss that though *Windows* has had the greater number of reported vulnerabilities compared with *Mac OS X* and other OSs, that does not mean that the former is the greater evil of the two.

Beyond social engineering, there is always the threat of information theft looming above the horizon for Apple product enthusiasts. True enough, just after the iPad was made available to the public, news of a security breach involving the product began to spread like wildfire. The breach was reported to have exposed iPad owners' email addresses and AT&T accounts. These people included big names in the military, finance, and media industries as well as politicians. Though it was later found that the compromise happened on AT&T's side via a brute-force attack, the article said it was still Apple's responsibility to ensure the security of its clients given that they are handing over sensitive information to activate and use products the company created.

Preventing Bites Off Apple Products and Services

If there is one key lesson that users should learn, it is the fact that making wise choices and practicing safe computing habits still make a lot of difference. With that in mind, Trend Micro implores users to ensure the maximum protection of their Apple products by following these guidelines:

If there is one key lesson that users should learn, it is the fact that making wise choices and practicing safe computing habits still make a lot of difference.

- **Keep security software up-to-date.** Regularly updated security software will catch most, if not all, kinds of threats. Using an effective security solution that stops threats before they even reach you is, of course, also a great idea.

- **Ensure that security updates are installed on all Apple products.** Apple products are vulnerable to malware attacks, too. Apply security updates to third-party software, which can act as attack vectors even if your OS is fully patched. Deploying vulnerability-scanning software on networks scheduled to run weekly is also a great idea. Automatic updates should also be enabled whenever possible.

- **Use only legitimate software and programs.** Downloading pirated software is illegal. Not only can it get you into trouble with the authorities, it also puts your devices, regardless of OS, at risk.

- **Download software only from trusted sites.** Applications may look harmless but turn out to have been actually compromised.

- **Be cautious of clicking links in email messages and of downloading file attachments.** Do not click embedded links nor download file attachments. Visit the sites themselves and download from there.

References:

- Apple Inc. (January 27, 2010). "Apple Launches iPad: Magical & Revolutionary Device at an Unbelievable Price." http://www.apple.com/pr/library/2010/01/27ipad.html (Retrieved June 2010).

- Apple Inc. (June 7, 2010). "Apple Presents iPhone 4: All-New Design with FaceTime Video Calling, Retina Display, 5 Megapixel Camera, & HD Video Recording—Thinnest Smartphone Ever." http://www.apple.com/pr/library/2010/06/07iphone.html (Retrieved June 2010).

- Bernadette Irinco. (August 26, 2009). *TrendLabs Malware Blog.* “Bogus *Snow Leopard* Update Sites Lead to DNS Changers.” http://blog.trendmicro.com/bogus-snow-leopard-update-sites-lead-to-dns-changers/ (Retrieved June 2010).

- Carolyn Guevarra. (March 19, 2007). *TrendLabs Malware Blog. “QuickTime* Movies Can Steal Your Identity!” http://blog.trendmicro.com/quicktime-movies-can-steal-your-identity21/ (Retrieved June 2010).

- Devin Leonard. (August 29, 2009). *The New York Times.* “Hey, PC, Who Taught You to Fight Back?” http://www.nytimes.com/2009/08/30/business/media/30ad.html?em (Retrieved June 2010).

- Dylan F. Tweney. (May 26, 2010). *Wired.* “Apple Passes Microsoft as World’s Largest Tech Company.” http://www.wired.com/epicenter/2010/05/apple-passes-microsoft/ (Retrieved June 2010).

- Elinor Mills. (February 1, 2010). *CNET News.* “In Their Words: Experts Weigh in on Mac Vs. PC Security.” http://news.cnet.com/8301-27080_3-10444561-245.html (Retrieved June 2010).

- Fatima Bancod. (July 4, 2008). *TrendLabs Malware Blog.* “Phishers Pose Fake Apple Billing Woes.” http://blog.trendmicro.com/phishers-pose-fake-apple-billing-woes/ (Retrieved June 2010).

- Gawker.TV. (June 15, 2010). *Valleywag.* “Apple’s Worst Security Breach: 114,000 iPad Owners Exposed.” http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed?skyline=true&s=i (Retrieved June 2010).

- Gregg Keizer. (June 10, 2010). *Computerworld.* “‘Brute Force’ Script Snatched iPad Email Addresses.” http://www.computerworld.com/s/article/9177921/_Brute_force_script_snatched_iPad_e_mail_addresses (Retrieved June 2010).

- Jeff Gamet. (January 16, 2006). *The Mac Observer.* “Apple Passes Dell’s Market Cap.” http://www.macobserver.com/stockwatch/2006/01/16.1.shtml (Retrieved June 2010).

- Jovi Umawing. (August 12, 2008). *TrendLabs Malware Blog.* “Phishers Cast a Seamless Attack on *MobileMe.”* http://blog.trendmicro.com/phishers-cast-a-seamless-attack-on-mobileme/ (Retrieved June 2010).

- Maria Alarcon. (February 6, 2009). *TrendLabs Malware Blog. “iTunes* Invoices and Valentine Ads Conceal Pharma Spam.” http://blog.trendmicro.com/itunes-invoices-and-valentines-ads-conceal-pharma-spam/ (Retrieved June 2010).

- Matt Phillips. (April 22, 2010). *The Wall Street Journal.* “Apple Edges Out Microsoft as #2 in S&P 500.” http://blogs.wsj.com/marketbeat/2010/04/22/apple-edges-out-microsoft-as-2-in-sp-500/ (Retrieved June 2010).

- Ria Rivera. (March 9, 2010). *TrendLabs Malware Blog.* “iPad Giveaway Gives Users’ Identities Away.” http://blog.trendmicro.com/ipad-giveaway-gives-users’-identities-away/ (Retrieved June 2010).

- Tom Hormby and Dan Knight. (October 14, 2005). *Low End Mac.* "A History of the iPod: 2000 to 2004." http://lowendmac.com/orchard/05/origin-of-the-ipod.html#1 (Retrieved June 2010).
- Trend Micro Incorporated. (March 17, 2007). *Threat Encyclopedia.* "JS_SPACESTALK.A." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=JS_SPACESTALK.A (Retrieved June 2010).
- Trend Micro Incorporated. (March 17, 2007). *Threat Encyclopedia.* "TROJ_DLOADER.JHV." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=TROJ_DLOADER.JHV (Retrieved June 2010).
- Trend Micro Incorporated. (August 26, 2009). *Threat Encyclopedia.* "OSX_JAHLAV.K." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=OSX_JAHLAV.K (Retrieved June 2010).
- Wikimedia Foundation Inc. (June 9, 2010). *Wikipedia.* "MacBook Pro." http://en.wikipedia.org/wiki/MacBook_Pro (Retrieved June 2010).
- Wikimedia Foundation Inc. (June 10, 2010). *Wikipedia. "iTunes Store."* http://en.wikipedia.org/wiki/ITunes_Store (Retrieved June 2010).
- Wikimedia Foundation Inc. (June 14, 2010). *Wikipedia.* "iMac." http://en.wikipedia.org/wiki/IMac (Retrieved June 2010).
- Wikimedia Foundation Inc. (June 14, 2010). *Wikipedia.* "iPhone." http://en.wikipedia.org/wiki/IPhone (Retrieved June 2010).
- Wikimedia Foundation Inc. (June 15, 2010). *Wikipedia.* "iPod Touch." http://en.wikipedia.org/wiki/IPod_Touch (Retrieved June 2010).