Information Security of Apple Devices

Mac’s and IPhone’s

By: Samuel Sanchez

April 10, 2016

Lately, in the past few years there has been a popular belief that the Mac OS X and the mobile IPhone are immune to viruses, worms, Trojans, etc. Apple, Inc. has repeatedly made advertisements stating that their devices are virus free and that anyone using a device other than an Apple product is vulnerable to hacking. This article will explain how this is now a proven myth and a few examples of known exploits used today.

It all started when Apple began advertising their new Mac OS X and displayed PC's as getting viruses all the time while the Mac's were virus free. For a long time, this was true, however not for the reasons Apple claims. At the time the Mac OS X 10.0 (Cheetah) was introduced on March 24, 2001 there were hardly any users. The Mac was still new to the market but was on the rise. According to the CVE (Common Vulnerabilities and Exposures) reports back in 2001 the Mac OS X wasn't even on the list for most vulnerabilities. At the time Linux and Windows held the top spot for most vulnerabilities, however that all changed very quickly. It wasn't till 2005 where the Mac OS X began to rise in vulnerabilities and now in the 2015 reports it holds the top spot.

When the Mac OS X first came out, it did not have a large impact in the market which caused it to not be an attractive target. There wasn't even an antivirus on the market for the Mac. A company by the name of F-Secure attempted to make an antivirus designed specifically for the Mac's, however the product never made it out because there was just no market for them. Mike Hypponen put it well, "They simply have not been a very interesting target for online criminals because there is a lot more money to be made from the much larger number of people using PCs." However, in the past year Mac OS X systems have grown exponentially in the market and are now starting to look like a more lucrative target to attackers.

Another popular Apple product is the mobile IPhone. The mobile IPhone was also under the same "immunity" myth as the Mac OS X. The very first IPhone was introduced on January 9th, 2007. The first IPhone ran the IOS 1 which at the time also did not have any known viruses. However, the IOS 1 was new to the smartphone market and only gave a really simply interface to users. At the time a company named Symbian was the top mobile operating system with roughly 50 percent of all smartphones running it. Wasn't until 2013 where the mobile IPhone rose to the top in yearly sales and also began getting attention by potential hackers. In 2013 the IPhone rose to 15th in the CVE vulnerabilities report.

Now the IPhone IOS and the Mac OS X are new to the computer world because their operating systems work completely different and are Unix based. The IPhone for example is very restricted in the applications that are allowed to run on them. No 3rd party applications are allowed to run on the IPhones unless approved by the vendor first and not all cell-phone carriers are allowed to be used with the device. These restrictions make it hard for attackers to develop a virus for this device. However recent studies show that some work around have been discovered.

The most recent GFI software reports show the Apple Mac OS X and Apple IPhone IOS at the top in known vulnerabilities, as shown in figure 1.

Figure 1. Top operating systems by vulnerabilities reported in 2014 by GFI

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0

In Figure 1, you will see the different operating systems listed in order of highest number of vulnerabilities to the lowest. Now the GFI reports are slightly different from the CVE reports in the sense that this chart shows how many of those vulnerabilities are considered critical threats versus minimal threats. As you can see in Figure 1, the Apple Mac OS X still holds the top spot for high threat vulnerabilities.

Now those are just statistics. Here are some known exploits that have been proven to work on Apple devices in the past 3 years. The “ThunderStrike 2 Bootkit – Mac OS X”, “Vilaca's Exploit – Mac OS X” and the, “AirDrop Exploit - IPhone IOS” are considered the top three vulnerabilities on Mac OS X and IPhone IOS.

The ThunderStike 2 Bootkit was an exploit developed by security engineer Trammell Hudson for the Mac OS X. The exploit uses an accessory item for the Mac called Thunderbolt. The Thunderbolt accessory is used as a host for the virus that, once plugged in and rebooted, will inject what’s known as an Option ROM into the extensible firmware interface (EFI). Once this is done, a rootkit is embedded into the hardware which makes it immune to reformats and operating system reinstallations as well as undetectable. This is considered an extremely critical vulnerability. However, this method does have one drawback. The exploit only works if the attacker has physical access to the device. This disadvantage causes this method to be used more in targeted attacks versus widespread attacks.

Vilaca’s exploit for the Mac OS X was discovered and developed by security researcher Pedro Vilaca. This method is proven to work on all Mac’s prior to mid-2014 and can be done remotely. Using Vilaca’s exploit, one would attack the BIOS protection of the Mac during a system reboot. For reasons unknown, Vilaca discovered that the BIOS protection is temporarily deactivated after a Mac wakes up from sleep. This BIOS protection is known as FLOCKDN and

once this protection is deactivated, an attacker can easily reflash the BIOS with its own malicious settings. The BIOS code is also stored in flash memory, not on the drive, which makes it survivable to reformats and OS reinstallations.

Lastly, the AirDrop exploit for the IPhone IOS was developed by a security researcher, Mark Dowd, who later privately reported it to Apple. This exploit works on all IPhones prior to IPhone 8.4.1 and exploits a directory traversal flaw that allows an attacker to write and overwrite files of their choice. All the attacker needs is to be within Bluetooth range to use this method. Now these were just some examples of the major exploits out there for the Mac OS X and IPhone IOS, nonetheless there are ways to mitigate these exploits.

The IPhone for example is considered secure because of the many restrictions put on the users that prevent viruses from acquiring any access. The issue is when people decide to “Jail Break” their phones which is essentially removing all those restrictions and gaining full administrative access. While there are many advantages to jailbreaking one’s phone there is one main disadvantage. When the user gains full administrative access through jailbreaking, they also remove any restrictions put in place to keep viruses from embedding themselves. For example, IPhone do not allow flash to be installed which prevent users from visiting certain websites. However, if one jailbreaks their phone they can install an app called Frash, which provides flash capabilities to the IPhone. Barmak Meftah said it best as quoted in the Smartphone Vulnerabilities article, “While Frash may look attractive to iPhone 4 and 3GS users wanting to surf to extra websites, the reality is that to install this software, users will have to jailbreak their handsets, so allowing the loading of apps from almost any source.” So the main idea is to not Jailbreak ones IPhone to keep all those restrictions that help protect its users.

In spite of this, Apple continues to advertise that their devices are virus proof and that its users have nothing to worry about. In fact, the Apple Mac OS X is about as secure as any PC running windows if not worse. A group of researchers wrote an article describing an experiment they performed on both the Mac OS X running Leopard OS and Windows XP-SP2. In this experiment both systems were monitored and subject to distributed denial of service (DDOS) attacks. The attacks used were, "Ping Flood Attack, Smurf Attack, ICMP Land Attack, TCP-SYN Attack, ARP Flood Attack, and UDP Flood Attack," as stated in the Information Security: A Global Perspective article. The results turned out to show, that after being subject to these attacks, the Mac OS X (Leopard) would crash while the Windows XP-SP2 was able to remain functional without crashing. This just proves that the Apple Mac OS X is not as impenetrable as they say.

Based on all the statistics and known exploits, the Apple Mac OS X and IPhone IOS prove to be just as vulnerable as any of the other computing devices out there today. On the other hand, the Apple product operating systems are extremely formidable and provide a lot of new revolutionary technology to the computer world. Nevertheless, the threat of viruses, exploits, bugs, etc. will forever be present, it's just a matter of time. Now Apple has proven to show due care by constantly updating its OS and patching most of these vulnerabilities as quickly as possible. Even though Apple has the highest amount of known vulnerabilities they also have the quickest rate of patch updates. Still, as compared to other devices on the market today, the myth that Mac's and IPhones are virus free is unfortunately just that, a myth. As technology gets more and more complex so do all the hacks and viruses that come with them.

References

Mansfield-Devine, Steve, ed. "Smartphone Vulnerabilities." Network Security 2010.7 (2010): N. pag. Web. * http://www.tandfonline.com.jproxy.lib.ecu.edu/doi/abs/10.1080/19393555.2011.569908

Sirisha Surisetty & Sanjeev Kumar (2011) Apple's Leopard Versus Microsoft's Windows XP: experimental Evaluation of Apple's Leopard Operating System with Windows XP-SP2 under Distributed Denial of Service Security Attacks, Information Security Journal: A Global Perspective, 20:3, 163-172, DOI:10.1080/19393555.2011.569908 * http://www.sciencedirect.com/science/article/pii/S135348581070088X

Hypponen, Mikko. "Are Apple Products Really More Secure?" Betanews. N.p., 2011. Web. http://betanews.com/2011/09/26/are-apple-products-really-more-secure/

Goodin, Dan. "New Exploit Leaves Most Macs Vulnerable to Permanent Backdooring." ArsTechnica. N.p., 1 June. 2015. Web. http://arstechnica.com/security/2015/06/new-remote-exploit-leaves-most-macs-vulnerable-to-permanent-backdooring/

Goodin, Dan. "Apple Mitigates but Doesn’t Fully Fix Critical IOS Airdrop Vulnerability." ArsTechnica. N.p., 16 Sept. 2015. Web. http://arstechnica.com/security/2015/09/apple-mitigates-but-doesnt-fully-fix-critical-ios-airdrop-vulnerability/

Cunningham, Andrew. "“Thunderstrike 2” Rootkit Uses Thunderbolt Accessories to Infect Mac Firmware [Updated]." ArsTechnica. N.p., 5 Aug. 2015. Web http://arstechnica.com/apple/2015/08/thunderstrike-2-rootkit-uses-thunderbolt-accessories-to-infect-mac-firmware/

Florian, Christian. "Most Vulnerable Operating Systems and Applications in 2014." GFI. N.p., 18 Feb. 2015. Web. http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/

"Top 50 Products by Total Number of "Distinct" Vulnerabilities in 2015." CVE Details. N.p., 18 Feb. 2015. Web. https://www.cvedetails.com/top-50-products.php?year=2015