VIPRE® BusinessPremium™

Antivirus: The Hippest New Apple Accessory

I'm a Mac Malware. Nice to Meet You.

Running antivirus software is second nature to the average PC user, but Apple devotees are a different story entirely. Only 20% of Mac users believe their machines are vulnerable to malware, while the vast majority of PC users know the risks they face online, according to Alex Stamos, a security analyst with iSEC Partners.

Feeling invulnerable to the dangers of malware and viruses, most Mac users give little thought to deploying antivirus tools or updating and patching their machines. Unlike PC users and IT admins from the Windows world, they have yet to learn that prevention is better than remediation, and that is something that needs to change.

Cyber-attacks on Macs are becoming commonplace as Mac use continues to increase. By April 2012, hundreds of thousands of Macs had been infected by malware. Meanwhile, the skyrocketing popularity of Apple devices such as iPhones and iPads has made them "fair game" for hackers who historically have focused on Windows machines.

This is a source of major concern for organizations that have deployed fleets of Macs and iPads. To protect private data and intellectual property, businesses, large enterprises and educational institutions must take the same steps to safeguard Apple devices as they have for PCs. They need to educate users and deploy technology to prevent cyber-attacks. Experts say antivirus alone would have averted most of the Mac infections that have taken place so far.

Low-Risk Perception

Users have lulled themselves into believing in the invulnerability of the Mac because it was rarely attacked until recently. Apple capitalized on this belief, using it as a marketing tool. It's one of the reasons – in addition to a very effective image-building campaign – that users have flocked to the Mac since the mid 2000s.

Mac users and the IT admins supporting them have been lulled into believing the invulnerability of the Mac to malware because it was rarely ever attacked.

The year 2012 was a wake-up call for Mac users – or should have been – with a string of cyber-attacks that infected Apple machines around the world. Most notoriously, the Flashback or Flashfake Trojan infected at least 700,000 Mac computers by April 2012.

IT admins need antivirus for the Macs on their networks and Mobile Device Management (MDM) for the iPads and iPhones used by employees.

As a result, Apple's PC market share reached 14% in 2012, substantially higher than its 4% share in 2006, according to research firm Gartner.

Once believed to be on the verge of extinction, Apple has become the third largest PC platform in the United States. On the mobile front, Apple has fared even better, with iPad sales accounting for about 87% of the tablet market, and with the iconic iPhone capturing close to half of all smartphone sales.

The Cost of Success

As the Apple brand gains more and more cachet, it also attracts unwanted attention from cybercriminals.

"Macs have become a larger target for malware writers, due to their newfound popularity," security and Mac expert Thomas Reed told ZDNet in December 2012.

The brand has become too conspicuous for hackers to ignore. Always keen on finding new channels to spread mischief, they have started to target the Mac OS and iOS more and more. And who can blame them? Put yourself in their position and you'll understand how irresistible a target all those vulnerable Macs have become.

> Macs have become a larger target for malware writers, due to their newfound popularity.[2]

Cyber-attacks on Apple devices reached numbers high enough in 2012 to force Apple – after being accused of taking too long to fix a Java vulnerability – to take decisive action. The company even hired famed hacker and former Microsoft employee Kristin Paget to look into beefing up Mac OS security.

A String of Mac Attacks

The year 2012 was a wake-up call for Mac users – or should have been – with a string of cyber-attacks that infected Apple machines around the world. Most notoriously, the Flashback or Flashfake Trojan, which first appeared in 2011, infected at least 700,000 Mac computers by April 2012.

Hackers used the Trojan to steal information from computers and manipulate some machines to deliver attacks on others. Scientific American's Larry Greenemeier called Flashback " by far the largest and most public scar sullying" Apple's aura of invincibility.

Flashback was successful for two primary reasons:

1) It exploited a well-documented Java vulnerability that experts say Apple was too slow to patch.

2) It took advantage of Mac users' apathetic approach to security.

Unaccustomed to cyber threats, Mac users also became easy phishing and spam targets.

In one case, an official-looking email purporting to be from American Express drew users to a compromised website that downloaded malware to their machines. The site, wrote ZDNet's Ed Bott, served up a variant of the "Blackhole" exploit "capable of installing a very nasty data-stealing Trojan on a PC or Mac that's running outdated versions of Java, Adobe Shockwave, Adobe Acrobat and Reader, and other third-party software."

Another Mac bug, dubbed "Dockster," exploits the Java framework to capture the keystrokes of infected machines. It downloads and executes additional malware after the initial infection. Dockster was one of several exploits that targeted Dalai Lama supporters who were tricked into opening infected Word documents or URLs sent to them by email.

In December 2012, a Trojan that had made the rounds on Windows networks called Trojan.SMSSend.3666 started showing up in Mac OS X machines. The Trojan, according to ZDNet, "is a fake installer application that claims to play music across Russian social network VK.com, which can be downloaded from a variety of sources, and attempts to deceive the user into entering a cell number to activate the software. In doing so, it subscribes the cell user to a chargeable subscription service that debits mobile phone accounts regularly."

While it infected only Russian computers, the Trojan was believed to be headed beyond Russia's borders because its text is in English.

In earlier attacks, the Mac Defender Trojan – also known as Mac Security Trojan, Mac Protector Trojan, Mac Guard Trojan and Mac Shield Trojan – used an authentic-looking popup warning that a virus had been detected on a user's machine. It then prompted users to download fake antivirus software. Users who took the bait were asked to add credit card information to pay for the software, essentially giving away their account information.

Dose of Reality

With the sheen of invulnerability now peeled off the Mac, the question is, "What happened?" Security experts, some of whom had predicted the Mac would eventually become a preferred target, say Mac OS X's perceived imperviousness to cyber threats was pure myth.

"We've been saying for five, six, seven years that Mac is not more immune to computer viruses than Windows PCs or even Linux boxes," Nicolas Christin, associate director of Carnegie Mellon University's Information Networking Institute, told Scientific American. "The only reason Macs were not massively targeted is that

> ...Mac is not more immune to computer viruses than Windows PCs or even Linux boxes.[3]

they didn't have enough of a market share to make them interesting for a hacker to devote resources to try to compromise those machines. Now that they've acquired a fairly sizeable market share, it makes sense that the bad guys would focus some attention on the Mac platform."

Adding insult to injury for Mac fans, the Java vulnerabilities that hackers exploited to infect Apple products had already been addressed in Windows operating systems. Since Mac attacks were so rare, security vulnerabilities presumably weren't addressed because the danger wasn't perceived to be as high. iSEC Partners' Alex Stamos said networked Macs at one point were easier to hack than Windows PCs because of poor authentication by Mac OS X servers.

Changing Minds

The recent string of Mac attacks proves that businesses and organizations using Macs can no longer remain blissfully unaware of the risks. Now that cybercriminals have whet their appetites on Macs, they are bound to come looking for more.

As is the case with Windows-based networks, Macs need protection from hackers. Since Macs typically are deployed in mixed environments that also include Windows machines, the potential for cross-infections is real and growing. An unsecured Mac is a potential carrier – or wide open door for a skilled cybercriminal – for malware intended for PCs and network servers.

To protect themselves, organizations should start by raising awareness among users about the risks of using Macs and how they are not immune to cyber-attacks. Organizations must inform users about malware dangers and the latest known threats. Users need information about hackers' tricks to bait them and the consequences of clicking infected links.

Organizations also must include Macs in their antivirus protection. They should deploy comprehensive AV and scanning technologies with the following capabilities:

- Sophisticated scanning engines that analyze and detect potential viruses and malware before they infect machines
- Automated monitoring and protection that minimizes manual intervention
- Malicious web filtering and behavioral analysis to block bad URLs before they can infect a network

In environments such as school campuses, where iPads have been cannibalizing PCs, IT departments must securely manage those tablets. They need to leverage an antivirus solution with integrated Mobile Device Management (MDM) that addresses iPads and iPhones, creating a more secure environment across PCs, Macs and mobile devices.

VIPRE Business Premium is the small-footprint antivirus software that enables IT administrators to protect their Mac devices as well as their PCs from one central console. In addition to Macs, VIPRE also provides integrated Mobile Device Management (MDM) for Android devices as well as iPhones and iPads, helping users defend themselves against these increasingly popular malware targets.

Visit **www.ThreatTrackSecurity.com/VIPRE** to evaluate VIPRE Business Premium free for 30 days.

Conclusion

Experts agree that Mac attacks are bound to continue. And as Mac, iPad and iPhone use increases in education and corporate environments, Apple's mobile devices are just one more target for cybercriminals.

With that in mind, organizations that deploy fleets of Apple products cannot be cavalier about cyber-threats. They must educate users about the risks, and implement antivirus technology that will bring them peace of mind and spare them costly remediation efforts.

[1] MacRumors, Apple Hits New High with 13.6% Share of U.S. PC Shipments in 3Q 2012, Lenovo Captures Worldwide Title, October 2012
http://www.macrumors.com/2012/10/10/apple-hits-new-high-with-13-6-share-of-u-s-pc-shipments-in-3q-2012/

[2] ZDNet, Latest Mac malware adds to 'troubling trend,' says security expert, December 2012
http://www.zdnet.com/latest-mac-malware-adds-to-troubling-trend-says-security-expert-7000008814/

[3] Scientific American, Big Mac Attack: Apple Security Bruised after OS X Infections, April 2012
http://www.scientificamerican.com/article.cfm?id=flashback-mac-security-attack

[4] ZDNet, New wave of phishing attacks serves malware to PCs and Macs, March 2012
http://www.zdnet.com/blog/bott/new-wave-of-phishing-attacks-serves-malware-to-pcs-and-macs/4648

[5] ZDNet, Latest Mac malware adds to 'troubling trend,' says security expert
http://www.zdnet.com/latest-mac-malware-adds-to-troubling-trend-says-security-expert-7000008814/

Feb 2013