



Article Side

The Mac Malware is Back by [Eccuni](#)

Article published on December 12th 2011 | [Internet](#)

This year is probably one of the busiest years according to researchers, cyber security experts and computer forensics when asked about the Mac malware. So why do you think these people point that out? The reason is pretty simple really; it is the report from Apple, one of the leaders in the IT industry.

This report has opened a new update regarding a list of malware that is known to invade many desktops and devices with Mac operating systems. Among those malware is the Trojan dropper experts' call as Revir and including in the report is the new Trojan they call as Flashback. If Revir disguises itself as some sort of PDF file, the Flashback will cloak itself as some sort of update for the Flash Player. Intego, the security firm of Mac believes that the Trojan Flashback was not as widespread at start, but now there has been an increase in number of incidences and reports of Flashback infections.

Experts from Intego believe that this Trojan is slowly spreading its terror across different systems and it is spread through many malicious Websites. Whenever internet users visit the malicious websites, they will suddenly notice a particular message saying that their plug-in has crashed and that there are suspected errors in the plug-in. After these false messages, a screen will suddenly pop-up offering the user to fix the problem by installing the Adobe Flash installer. Unknown to the user, this installer is not an Adobe Flash installer but an installer for a Trojan horse, the Flashback. And if the user's browser is in Safari mode, then their computer will automatically download the said "safe" downloadable and a window for the installer will automatically open.

In the event that the user will install the said "safe" software, the Trojan horse Flashback will automatically deactivate the software needed for network security. The code in this particular malware will deactivate some security software only like Little Snitch, and luckily it has no effect in software like Intego VirusBarrierX6. Once the package has been installed, it will automatically delete the installation package. This malware will also automatically install a dynamic loader or dyld library and also an auto-launch code that allows the malware to inject its code into any applications the user will launch. This malware will also install a backdoor in the system where it will try to communicate to a remote server where it will send all the data it has stolen and this data will be in an RC4 encryption.

Experts who have completed cyber security training and computer forensics training believe that this malware infection is a fruit of genius social engineering. Most Mac users aren't easily fooled by this method because an installer for Mac will never appear this way. Unfortunately, there are two things that make this approach believable. Devices with Mac OS X Lion does not come in with a Flash Player package, so if they want to view Flash content found on the Internet they must install the software themselves. Second reason is that their Flash Player must have been set to automatically update itself and this might look like an update alert. These two reasons could easily trick or fool Mac users; they would unwittingly download a malicious malware that would compromise their important data.

However, the report did not mention how Internet users are being drawn into these malicious websites. But according to some experts who have completed computer forensic course, it is easy to imagine how the users are drawn to these sites. One example is creating viral videos and spreading them like wildfire. Crooks may use these viral videos like a video about a trending topic or

a scandalous video or nude video of an artist or any known person. When Internet users will try to view the video, they are prompted to install a fake Adobe Flash update – a false update that is instead an installation of the said Trojan. In fact, this method has worked well in many Windows as well as Mac users for the past years.

Indeed, there are more malware that is written and intended for Windows users compared to Mac OS X. Still it doesn't mean that Mac computers and devices should be left unprotected.

Article Source:

<http://www.articleside.com/internet-articles/the-mac-malware-is-back.htm> - [Article Side](#)

[Eccuni](#) - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in computer forensics.

More information about EC-Council is available at www.eccouncil.org, a [computer forensics](#), a [computer forensics training](#), a [computer forensic course](#).

Article Keywords:

Mac Malware, computer forensics, computer forensics training, computer forensic course, Windows computer, cyber security, Apple, IT industry, Trojan dropper, Flashback, security firm, malicious Websites, Adobe Flash, security software, VirusBarrierX6, Mac

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!