Intego Security Memo - November 18, 2008

Published on 11/21/08

A new variant of the RSPlug Trojan horse has been found on several pornographic web sites. While this new variant currently performs the same actions as the RSPlug.A Trojan horse, its installer is different: it is a downloader, and it contacts a remote server to download the files it installs. This means that, in the future, the downloader may be able to install other payloads than the one it currently installs.

Description: A new variant of the RSPlug Trojan horse has been found on several pornographic web sites. (See Intego's Internet Security Memo of October 31, 2007 for more on this Trojan horse.) While this new variant currently performs the same actions as the RSPlug.A Trojan horse, its installer is different: it is a downloader, and it contacts a remote server to download the files it installs. This means that, in the future, the downloader may be able to install other payloads than the one it currently installs.

Exploit: OSX.RSPlug.D Trojan Horse
Discovered: November 18, 2008
Risk: Medium

This new variant, like the initial RSPlug.A Trojan horse, has been found on pornographic web sites. When visiting such a site, a user is alerted that there is a "Video ActiveX Object Error" and is told that their "Browser cannot play this video file." The alert instructs the user to download the "missing Video ActiveX Object".

If the user clicks OK, a disk image called cleanlive.dmg downloads (this name may be different in the future; with the first version of the RSPlug Trojan horse, a number of different names were found). Depending on the user's browser settings, this disk image may mount and launch automatically commencing installation.

If the user clicks Cancel when the Video ActiveX Object alert displays, however, they receive another alert saying, "Please install new version of Video ActiveX Object." This alert only allows the user to click OK, returning them to the first alert. The only way to get rid of these alerts is either to download the infected disk image, or quit the browser.

Means of protection: The best way to protect against this exploit is to run Intego VirusBarrier X5; the program's behavioral analysis feature detects the activity of this Trojan horse. VirusBarrier X5's virus definitions dated November 18, 2008 detect more specifically this downloader.

Intego VirusBarrier X5 eradicates the malicious code and prevents the Trojan horse from being installed. Intego recommends that users never download and install software from untrusted sources or questionable web sites. Users should be especially careful if such alert loops appear and disk images are downloaded; users should delete any unknown disk image that they find in their Downloads folder. We invite any users who find suspicious disk images to send them to Intego's Virus Monitoring Center.

Intego:
http://www.intego.com

I
http://www.intego.com/news/ism0705.asp

Intego's Virus Monitoring Center:

http://sample@virusbarrier.com

Intego develops and sells desktop Internet security and privacy software for Macintosh. Intego provides the widest range of software to protect users and their Macs from the dangers of the Internet. Intego's multilingual software and support repeatedly receives awards from Mac magazines, and protects more than one million users in over 60 countries. Intego has headquarters in the USA, France and Japan.

###

Rosaline Mills
PR Consultant
+44 (0)845 2577115

rosaline@bamboopr.co.uk

****
Link To Article: https://prmac.com/release-id-3443.htm
****