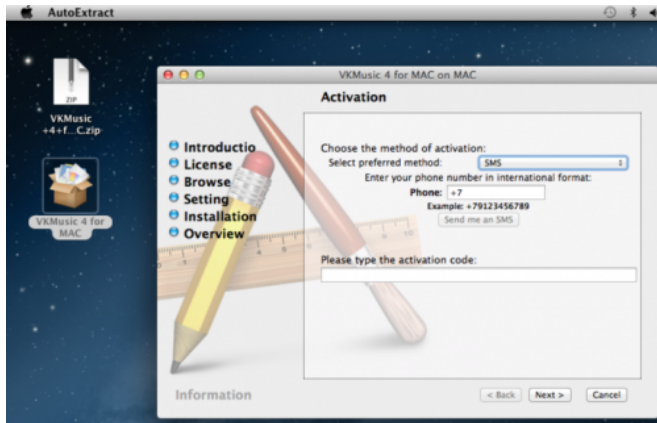


Apple kicks SMS scam fraudsters to the curb

14 December 2012, by Nancy Owano



(Phys.org)—Just what you never wanted. Mac-based malware, just ponder that phrase alone, not Windows-based but Mac-based, that tricks users into paying subscription fees. The malware masquerades as an installer for various software titles. The caper lies in the trick installer, which will tack fees on to the user's mobile phone account, so that the victim is stuck with unintended bills. The Trojan targeting Macs was discovered by Russia-based security company, Dr. Web. Its alert went out that this is malware targeting OS X systems. The Trojan is known as Trojan.SMSSend.3666, and Dr. Web said it was the first program of its kind to go after Mac OS X.

The ruse was in offering an installer for a program and the victim was asked for a phone number in order to register. Then the person was asked to respond to a subsequent [text message](#). "Fraudsters ask that the victim enter their cellphone number into an appropriate field and then specify the code found in a reply SMS. By performing these actions the user agrees to terms of a chargeable subscription and a fee will be debited from their mobile phone account on a

regular basis," according to Dr. Web.

The Trojan.SMSSend.3666 installer, according to CNET, is not a Java-based maneuver to gain backdoor system access but instead is built as a Mach-O [binary](#) that uses the OS X native runtime.

This sort of malicious installer scheme may sound familiar to Windows users who follow security alerts but this was news for Mac users. The good news for [Mac users](#) is that Apple sprang into [action](#) and out came a report that Apple quickly updated malware definitions to detect the scam Trojan. Apple added definitions for the malware to its "Xprotect.plist" blacklist, which is part of basic anti-malware tools that Apple launched with OS X [Snow Leopard](#) in 2009.

Nonetheless, the security scene is changing whereby more and more experts are warning users to get out of the comfort zone thinking [Apple computers](#) are not ever vulnerable. The recent discovery by Dr. Web of the installer scam indicates all computer platforms are fair game.

This advice was issued on the Doctor Web site, warning users "against installing programs if they are required to submit their phone number or send a text message—most likely, you will lose money and end up with nothing."

It pays, not costs, to use your search engine to try calling on the official site to take advantage of a free service, to avoid getting stuck with rogue installers.

More information:
threatpost.com/en_us/blogs/sms...pple-machines-121212
news.drweb.com/show/?i=3138

© 2012 Phys.org

APA citation: Apple kicks SMS scam fraudsters to the curb (2012, December 14) retrieved 24 February 2021 from <https://phys.org/news/2012-12-apple-sms-scam-fraudsters-curb.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.