Criminals gain control over Mac with BackDoor.Olyx

news.drweb.com/show/

Doctor Web

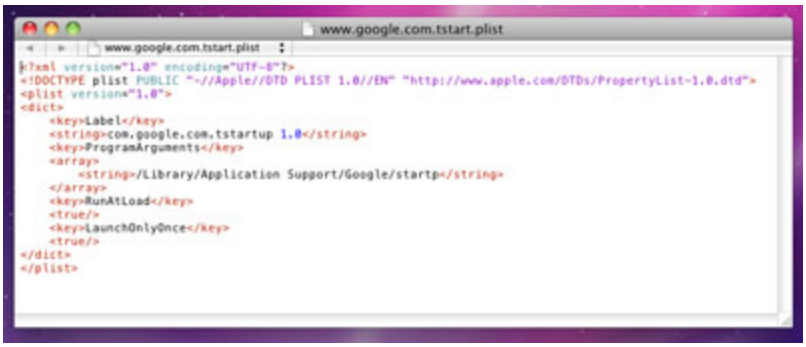
Back to news

June 22, 2011

Doctor Web—the leading Russian developer of anti-virus software —informs users that its virus analysts have discovered a new threat to computers running Mac OS X. BackDoor.Olyx is the second known backdoor for the operating system. If a machine is compromised by the malware, attackers get an opportunity to covertly control the computer. The backdoor receives commands from a remote server to create, transfer, rename, delete various files, as well as some other instructions.

The number of malicious programs for MAC OS X is small, especially compared with the number of threats to Windows. Until recently only one backdoor program for the OS was known—BackDoor.DarkHole. Versions of this malware exist for Mac OS X and for Windows. When launched, it enables hackers to open web pages in the default browser on the infected machine, restart the computer remotely and perform various operations with files. Now, in the Dr.Web virus database contains entries for both BackDoor.DarkHole and **BackDoor.Olyx**.

The program gets to a user's computer as an application designed for Macs featuring the Intel-compatible architecture, **BackDoor.Olyx** creates the /Library/Application Support/google/ directory on the disk to which it saves a file named startp. Then **BackDoor.Olyx** places the file /Library/ LaunchAgents/www.google.com.tstart.plist into the home directory, and uses the file to launch the malicious object after a system reboot.



After that the program moves itself to a temporary folder named google.tmp to delete the executable from its original location. As the name implies, **BackDoor.Olyx** operates in an infected system as a backdoor which includes downloading and running malicious files on infected machines and executing various commands in the /bin/bash shell. Thus, attackers can gain control over an infected computer without the user's knowledge.

Users of Dr.Web for Mac OS X can rest assured about the security of their computers, since the signature of the malware has already been added to the Dr.Web virus database. To prevent **BackDoor.Olyx** from infecting systems, users of Dr.Web for Mac OS X are recommended to enable automatic updating and scan their hard drives regularly.

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments