New Apple Mac Trojan Called OSX/Dockster Found in the Wild

Published on 12/04/12

New Apple Mac Trojan Called OSX/Dockster Found in the Wild on Tibetan Website. A sample of
a new Mac spyware called OSX/Dockster.A was found on VirusTotal on Friday, possibly as part of a test before pushing it to the public. This trojan has backdoor functionality,
i
protects users from this malware with malware definitions dated November 30, 2012 or later.

London, United Kingdom - Malware: OSX/Dockster. Risk: Low; the threat is not known to be widespread and the vulnerability targeted by the exploit code is corrected by the latest version of Java.

Description: A sample of a new Mac spyware called OSX/Dockster.A was found on VirusTotal on Friday, possibly as part of a test before pushing it to the public. This trojan has
b
typing.

This malware is now known to be in the wild, on a website dedicated to the Dalai Lama that has been compromised to deliver the same exploit code as used by SabPab to push Dockster. (This Java vulnerability was also the same one used by Flashback.)

I
i
v
Monitor. It creates a launch agent called mac.Dockset.deman so that the trojan will restart each time an affected user logs in. Once the trojan is active, it tries to contact the remote address itsec.eicp.net to await instructions.

The backdoor functionality of this trojan is quite basic. It provides a simple remote
s
download additional files, and it logs keystrokes.

Means of protection: VirusBarrier X6 protects users from this malware with malware
d
detect the exploit code as OSX/SabPab.A and OSX/Dockster.A when it is dropped, and its Anti-Spyware protection will block any connections to remote servers if a user has installed the Trojan horse.

VirusBarrier Express and VirusBarrier Plus, available exclusively from the Mac App Store, detect this malware with malware definitions dated November 30, 2012 or later, but these programs do not have a real-time scanner due to limitations imposed by the Mac App Store; users should scan their Macs after they have updated to the latest malware definitions, or manually scan any installer packages they have downloaded if they seem suspicious.

For additional protection against this threat, update to the latest version of Java, which has fixed this vulnerability.

Intego:
http://www.intego.com

VirusBarrier X6:
http://Http://www.intego.com/virusbarrier/

Intego develops and sells desktop Internet security and privacy software for Macs. 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.

###

Marco Fiori
Account Manager
+44 (0)845 2577116

Marco@bamboopr.co.uk

****
Link To Article: https://prmac.com/release-id-51613.htm
****