

Flashback: Trojaner hat über eine halbe Million Macs unter Kontrolle

Beitrag von „JugoX“ vom 5. April 2012, 12:16

Quelle: <http://www.golem.de/news/flash...kontrolle-1204-90992.html>

Ich erinnere mich, dass sich der Flasplayer erst vor kurzem updaten wollte.
Gibt es irgendeine Möglichkeit zu prüfen, ob mein Mac infiziert ist?

//

Bin gerade dabei das Sicherheitsupdate zu installieren.

Beitrag von „Forenfinder“ vom 5. April 2012, 13:20

Das Java für OS X 2012-001-Update 1 erhöht die Kompatibilität, Sicherheit und Verlässlichkeit durch die Aktualisierung von Java SE 6 auf 1.6.0_31. Installieren.
Und es bleibt uns ggf. nur die Möglichkeit mal einen V-Scanner für Mac OS zu nutzen. Hier gibt es [den Besten](#) für Free!

Beitrag von „“ vom 5. April 2012, 18:34

Scheint viele ja nicht zu interessieren. *kopfschüttel*

Beitrag von „Griven“ vom 5. April 2012, 19:00

Was wohl daran liegt, dass immer noch viele dem Irrglauben verfallen sind, dass es keine Viren für UNIX Systeme gibt und sich somit sicher fühlen....

Beitrag von „Dr. Ukeman“ vom 6. April 2012, 02:46

Findet ihn der sophos? Lücke ist zugemacht mit dem sicherheitsupdate. Jetzt muss ich bur noch checken obs clean ist.

Gesendet vom iPhone via
Tapatalk

Beitrag von „“ vom 6. April 2012, 11:19

So alles geprüft und alles OK. 😊

Beitrag von „Griven“ vom 6. April 2012, 12:29

Sophos findet ihn und prüfen ob man bereits befallen ist kann man mit folgenden einfachen Befehlen im Terminal:

Code

1. defaults read /Applications/Safari.app/Contents/Info LSEnvironment
2. defaults read ~/.MacOSX/environment DYLD_INSERT_LIBRARIES

erhält man hierbei jeweils eine Fehlermeldung in folgendem Stil

Code

1. The domain/default pair of (...) does not exist

ist alles okay und man ist einem Befall noch mal entgangen. Trotzdem ist MAC OS inzwischen so weit verbreitet, dass man sich besser nicht in falscher Sicherheit wähnt doch lieber eine Antivierensoftware installiert. Kostenfreie Varianten gibt es von Sophos, Clam AV und auch FPROT einfach mal danach googeln.

Beitrag von „Forefinder“ vom 6. April 2012, 12:40

Man bekommt die Fehlermeldungen wen man NICHT befallen ist, so muss man das verstehen, oder?

Beitrag von „Griven“ vom 6. April 2012, 12:48

Genau so sieht es aus. Fehlermeldung = Rechner sauber ;O)

Beitrag von „al6042“ vom 6. April 2012, 15:48

Aber Achtung...

Solltet ihr noch weitere Browser im Einsatz haben ausser Safari, sollte ihr den beschriebenen Vorgang für diese Browser wiederholen.

z.B: Google Chrome:

Code

1. defaults read /Applications/Google\ Chrome.app/Contents/Info LSEnvironment

oder Firefox:

Code

1. defaults read /Applications/Firefox.app/Contents/Info LSEnvironment

Und ebenfalls Achtung:

Solltet ihr, wie ich, die Programme innerhalb des /Applications Ordner in diverse Unterordner verschoben haben, müsst ihr diese Unterordner in eure Abfrage einbinden, sonst ist es ja klar, dass nix gefunden wird.

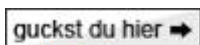
z.B:

Code

1. defaults read /Applications/Network/Google\ Chrome.app/Contents/Info LSEnvironment

Beitrag von „Frankylan“ vom 6. April 2012, 16:39

von Avira gibt es auch eine kostenlose Mac Variante ihrer Antivirensoftware





<http://www.avira.com/de/downloads>

Beitrag von „Forenfinder“ vom 6. April 2012, 17:36

Das Java für OS X 2012-002-Update 1 erhöht die Kompatibilität, Sicherheit und Verlässlichkeit durch die Aktualisierung von Java SE 6 auf 1.6.0_31. Update!