Trojan tricked money on Mac belongs to Russian people?

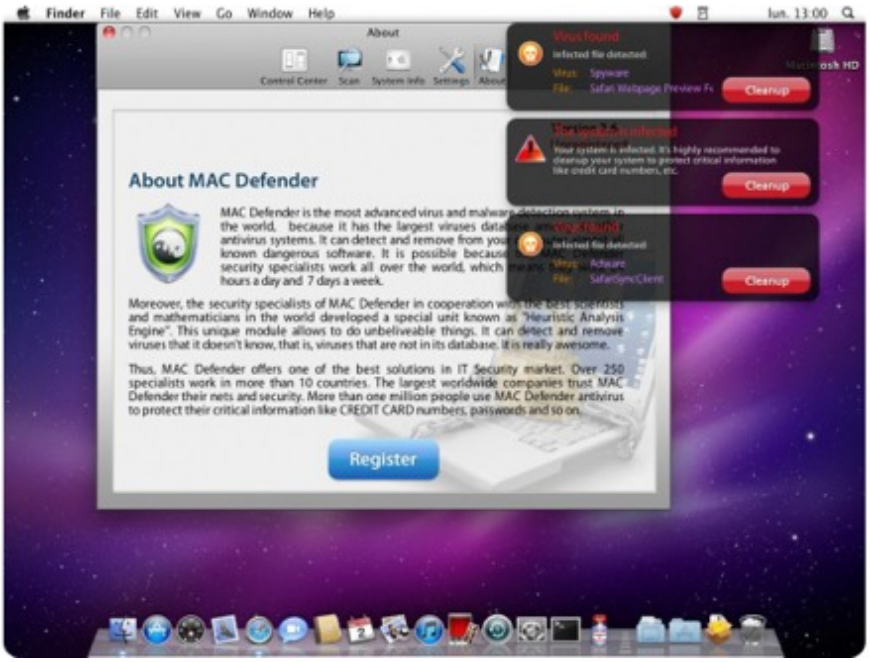
Security expert Brian Krebs accused Russia's ChronoPay company of using Mac Defender fake antivirus software. ChronoPay denied this and threatened to sue.

Security expert Brian Krebs accused Russia's ChronoPay company of using Mac Defender fake antivirus software. ChronoPay denied this and threatened to sue.

In hackers' attacks against the recent Mac user community, the Russian-made ChronoPay Company is said to be involved. A former journalist who is now a famous information security expert, Brian Krebs, announced on his blog about the incident. Since early May 2011, thousands of Mac computer users have become victims of fake **Mac Defender** antivirus software. This software has the main task of taking money from credit cards and generally has no effect against malicious software.

Mac Defender (as well as MacProtector or MacSecurity) works as follows. Users who visit a website infected with malware (via Google's image search engine) will receive a warning that their computer has a virus. And if the Safari browser setting allows automatic downloading of audio files, the victim's computer immediately appears and opens an installation package. Users only need to agree to install without entering the admin password.

After setting up the program, on the computer screen continue to appear warnings about new viruses and to be more convincing, Safari will open up the black web by accident. Finally, users are recommended to purchase a full version of the antivirus program because the free version does not kill the virus. In fact, Mac Defender is a virus that does not kill any virus but only steals money.



Mac Defender makes a lot of noise and now it is related to Russians .

According to ZDNet, after 25 days, Apple's user support service received between 60,000 and 125,000 complaints regarding the infection of fake antivirus software, and on the first day, more than half of the calls were called. This service relates to Mac Defender software. However, Apple did not support immediately. At first, according to the rules, Apple employees are strictly prohibited from giving possible alternatives to clean up malware.

To issue Mac Defender removal instructions, it takes up to 3 weeks for the provider. Currently, the tutorial is for users who require **anti-Mac Defender** technical support provided on Apple's support page.

Recently, Brian Krebs wrote that fake antivirus software offered to pay money through the domain name *mac-defence.com* . In other cases, the address noted is *macbookprotection.com* . When reviewing the registration data using these domain names (via Whois service), experts see them registered from the email box *fc@mail-eye.com* . This is the address contained in ChronoPay's internal documents since last year and leaked on the Internet.

In the documents specified, the *mail-eye.com* domain belongs to ChronoPay and that the Company pays to deploy in Germany a virtual server for this address. The records also indicate that the mailbox *fc@mail-eye.com* belongs to ChronoPay's CFO Alexandra Volkova. According to Krebs's data from an Internet service provider, the address has recently been used to register two new domain names but which ones are not disclosed by the provider. Krebs thinks that these are the intended addresses for making payments to Mac Defender.

Meanwhile, Chief Executive Officer ChronoPay Pavel Vrublevsky told Cnews.ru that *"Krebs for the second time in a year published negative articles on ChronoPay based on the documents he received from the enemies of ChronoPay* ". Vrublevsky denies the domain names belong to ChronoPay and says the company has not registered them.

On ChronoPay's official website, there was a press release, in which ChronoPay announced that they had nothing to do with Mac Defender. The Company's representative emphasized that ChronoPay is a widely recognized well-known brand (in Russia, the company owns 45% of the e-commerce market share) and defame their reputation as meaningless work. . ChronoPay warned that they were willing to perform *"appropriate legal*

actions " against those who broke the news.

You finished reading the article "**Trojan tricked money on Mac belongs to Russian people?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.