Who killed the fake-antivirus business?

The fake-antivirus business was a big money-maker in the first half of this year. Then, at the end of June, fake-AV products practically disappeared from the web. Was it technology, or does traditional law enforcement deserve the credit?

By Ed Bott for The Ed Bott Report | August 29, 2011 -- 20:29 GMT (21:29 BST) | Topic: Windows

0

The fake-antivirus business went from boom to bust in record time.

Early this year, the bad guys were making money hand over fist with scareware and rogue security products. Then, suddenly, the business dried up.

The event that caused the sudden plunge? A high-profile bust by Russian authorities. On June 23, a network of web sites that were distributing fake antivirus software for Windows PCs and Macs suddenly went offline when the head of the company that processed payments for the group was busted.

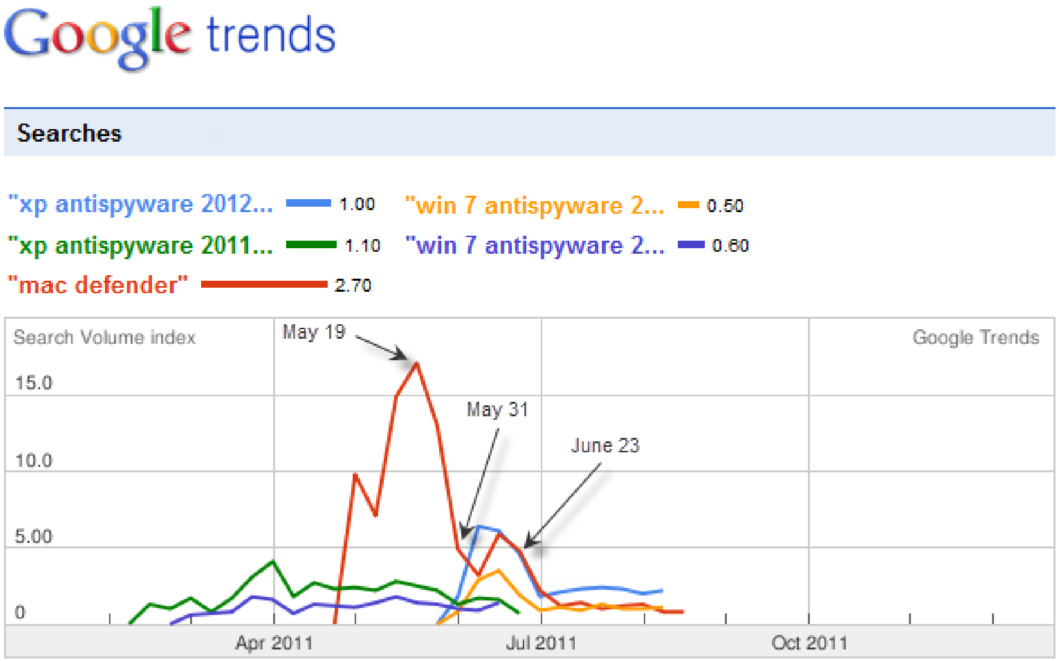
The effect on the fake-AV industry was dramatic, according to Enigma Software Group:

> Aside from the FBI cracking down on international “scareware” rings in 12 countries, Russian police arrested Pavel Vrublevsky, co-founder of ChronoPay, Russia’s biggest processor of online payments and a lead player in several fake AV scams. The combination of these two events [led] to a dramatic decline in fake anti-spyware and anti-virus software. On our end, we’ve seen a drastic drop in scan logs from new users, support logs, detections, and support tickets from new customers. Basically, we’ve witnessed a 60% decline in new fake AVs, scareware, and rogue anti-virus incidents.

Independent security researcher Brian Krebs also noted a "huge decline" in the fake-AV racket. According to Krebs, McAfee reported "a dramatic drop in the number of customers reporting scareware detections in recent weeks… McAfee has tracked more than a 60 percent decrease in the number of customers dealing with fake AV since late May."

The Enigma Software report included a fascinating set of graphics that used data from Google Trends to monitor consumer searches for known fake-AV products. In theory, those searches represent interest by victims in how to remove the threats they've encountered. A spike in searches means more infections in the wild; a drop means the malware distributors are seeing less success.

I decided to use the same methodology to track the progress of this underground market from a slightly different angle. Starting with a similar set of Google Trends data, I came up with this chart, which tracks fake AV products for Windows XP and Windows 7 and adds Mac Defender to the mix:



That picture shows the ebbs and flows of an entire underground market. The green and purple lines on the left represent a pair of fake Windows AV products (XP Antispyware 2011 and Win 7 Antispyware 2011) that emerged in February and peaked at the beginning of April. They were replaced with 2012 versions (light blue and yellow) at the beginning of June, giving the market a new jolt of activity.

I've annotated that chart with a few key dates:

- May 19: Mac Defender search activity peaks. That's the date a leaked Apple document emerges, in which the company orders support professionals not to acknowledge infections or attempt to remove them.
- May 31: A month after the Mac Defender attack began, Apple finally releases a security update that downloads antivirus definitions daily. By that time, though, the threat had nearly run its course. Apple's response really was late.
- June 23: An international law enforcement effort shuts down the payment infrastructure for the Mac and Windows fake-AV industry. The effect is dramatic: business drops precipitously and has remained down since them.

The moral of the story is clear: technological solutions have some effect, but nothing gets rid of a gang of criminals like a series of well-coordinated worldwide police raids.

Sadly, this break in the action is probably nothing more than a brief interruption. Sooner or later—probably sooner—a new gang will be along to start up where the previous one left off. But for now, at least, the quiet is welcome.

Related posts:

- Trojans, viruses, worms: How does malware get on PCs and Macs?
- Stay safe online: 5 secrets every PC (and Mac) owner should know
- Why Windows users should care about malware on Macs
- Do you really need antivirus software?
- Why do people fall for Trojans?

RELATED TOPICS: APPLE MICROSOFT ENTERPRISE SOFTWARE WINDOWS 10 PCS REVIEWS

0

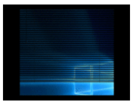
LOG IN TO COMMENT | Community Guidelines

Join Discussion

RELATED STORIES

Enterprise Software
JavaScript rules but Microsoft programming languages are on the rise

Security
Windows security: Microsoft fights massive cryptocoin miner malware outbreak



Windows 10
Microsoft tweaks Windows 10 privacy settings in Insider test

Enterprise Software
Windows 10 bug: Microsoft fixes issue that broke USB, built-in cameras, keyboards

© 2018 CBS Interactive. All rights reserved. Privacy Policy | Cookies | Ad Choice | Advertise | Terms of Use | Mobile User Agreement

Visit other CBS Interactive sites:

Select Site ▾

TOPICS

ALL AUTHORS

GALLERIES

VIDEOS

SPONSORED NARRATIVES

MEMBERSHIP

NEWSLETTERS

SITE ASSISTANCE

ZDNET ACADEMY