Home 〉 News 〉 Security News 〉

Fake antivirus scareware scams show big summer decline

Good news from the security frontline. The phenomenon of rogue antivirus ‘scareware’ really does appear to be on the wane, at least according to new figures from security company Enigma Software.

By John E Dunn | Sep 29, 2011

Share

Good news from the security frontline. The phenomenon of rogue antivirus ‘scareware’ really does appear to be on the wane, at least according to figures from security company Enigma Software.

The US-based company’s statistics culled from scans and customer support reports showed a dramatic 60 percent drop in new detections this summer, with a particularly marked fall between June and July.

Running the names of two common fake antivirus products through Google’s Trend search volume tool, Enigma researchers found that searches for ‘Vista Security 2012’ and ‘XP Security 2012’ dropped equally precipitously over the same period of time.

“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 percent decline in new fake AVs, scareware, and rogue anti-virus incidents,” the company says in a blog.

Although Enigma was not able to provide absolute numbers, the drop still chimes with that noted by McAfee in August, which said it had also seen a 60 percent drop around the same time.

The drop in scareware programs is usually and probably justifiably attributed to the FBI’s Operation Trident Tribunal summer campaign against fake AV operations across the globe that saw companies raided in Latvia, the Ukraine and half a dozen other countries.

Separately in June, the head of Russian company ChronoPay, Pavel Vrublevsky, was arrested for allegedly ordering a DDoS attack against a rival firm. His company was also believed to be a conduit for the payment processing in which fake antivirus scams depend.

Another longer-term factor could simply be the growing popularity of free antivirus programs such as Microsoft’s Security Essentials, which are now sophisticated enough to detect the biggest scam programs. If people know they can download security software without paying the attraction of buying expensive – and possibly bogus - programs declines too.

If scareware is under serious pressure that might explain a recent tendency of scareware programs to adopt a more threatening tone, sometimes using the impersonation of real organsiations.

In a recent example, infected Windows users were accused of running pirated versions of the OS, with users unwilling to pay a sum of money to a company claiming to represent Microsoft being threatened with de-activation.

In another slightly different incarnation, criminals impersonated the UK’s Metropolitan Police in an attempt to lever money from victims accused of visiting extremist and porn websites. There could be more of this to come.

Earlier this year, the first Mac fake antivirus program was discovered.

Security Apps & wearables

Share

Recommended for you

Japan foreign offices, parliament hit by virus attack

FTC compensates 320,000 victims of fake antivirus scams

Next Article

Connect

Newsletter

techworld FROM IDG

UK Tech Weekly Podcast: Soundcloud / iTunes

Explore

News
Blogs
Features
Analysis
Tutorials
Reviews

Career
Resources
Galleries
Downloads
White Papers
Techworld Authors

About

About Us
Contact Us
Advertise
T's & C's

Privacy Policy
RSS
Site Map
Cookies