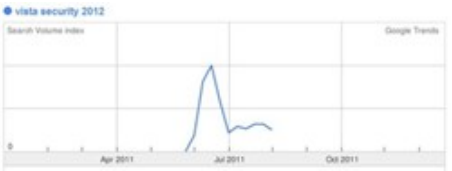
12 OCT 2011 OPINION

Comment: Cyber-gang Crackdown Cripples Malware Traffic...for Now

Estevez says the scareware industry is like a multi-headed hydra: by the time you cut off the remaining heads, double the number have grown back

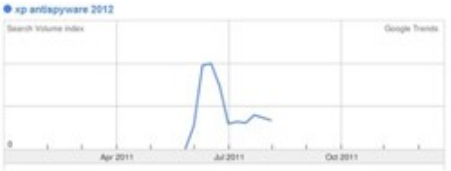
Operation Trident Tribunal, involving the cooperation of authorities in more than 10 countries, targeted specific sophisticated business enterprises found to be associated with criminal gangs responsible for selling $72 million in fake anti-virus programs to over 960,000 computer users. What made this crackdown even more effective was the arrest by Russian police of Pavel Vrublevsky, co-founder of Chrono¬Pay, Russia's biggest processor of online payments and a lead player in several fake anti-virus scams.

By also cutting off the ability for scareware makers and distributors to get paid, the impact of these two events combined has ushered in 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 equating to a 60% decline in new fake AVs, scareware, and rogue anti-virus incidents.



Google Trends searches for "Vista Security 2012"

Security company McAfee has also experienced a drastic drop in the number of customers reporting fake anti-virus detections. Another indicator of the state of things is to check the search volume of popular rogue anti-spyware programs in Google Trends. Please see the two figures showing how often people have searched for "Vista Security 2012" and "XP Antispyware 2012" – these are the names of what used to be very widespread fake security programs.



Google Trends searches for "XP Antispyware 2012"

However, while the dramatic drop off in late June makes clear the impact of removing one of the key players in the scareware industry, I fear that this will be temporary.

Even if the FBI and other investigating authorities were able to identify and take out the source of the other 40% of the scareware industry, it would not solve the problem. The fact is that the scareware and malware industry is like a multi-headed hydra: by the time you have cut off the remaining heads, double the number has grown back in their place.

What's likely to endure until the next coordinated crackdown is a continuation of our existing malware digital arms race. Every time malware makers come up with a new, sophisticated way to infect computers with their scareware, we'll come up with a way to remove it.

The question we really need to pose more often in this industry is not just how we are going to neutralize the threat once it emerges, but how to stem the conditions that give the threat life, and make it so profitable in the first place.

The bottom line is if people knew that a 2010 Google study found 11,000 domains hosting fake anti-virus software, and that 50% of all malware is delivered by internet advertising, then they might be more vigilant about the links they clicked through. Perhaps it behooves Google to take the lead here, and not only invest more in closing their own security holes, but also consider using their home page search box to alert users to the latest threats, or search topics –such as breaking news stories – that have been poisoned.

What is equally more important is the cooperation of the credit card processors. This is the conclusion of a research paper on spam, published earlier this year by researchers at the University of California. What they concluded – and we can infer is likely to be true for the malware and scareware industry – is that tough legislation that cuts off the transaction cycle may be the only effective public policy intervention by Western countries.

Given the impact blacklisting certain types of transaction would potentially have on the real anti-malware industry, the best option is for acquirers to terminate offending merchant accounts. While this may be seem difficult, given that criminal gangs tend to use banking facilities in countries with more relaxed regulations, there is nothing to stop Visa and MasterCard from forcing member banks to stop processing payments by implementing much lower thresholds for investigating potentially fraudulent activity, for example.

As former *Washington Post* writer Brian Krebs has shown, metrics such as the volume of transactions and/or the number of 'chargebacks' – refunds forcibly issued by banks after the transaction has been cleared – can be used to detect and shut down online criminal activity.

Sadly, it's likely this past summer's crackdown will give legislators, who already have so many other pressing issues to consider, more cause to think enough is already being done. In the meantime, we must continue to raise awareness of the wider cooperation required, while continuing to outsmart the next head the hydra grows.

Alvin Estevez is the president and managing member at Enigma Software Group

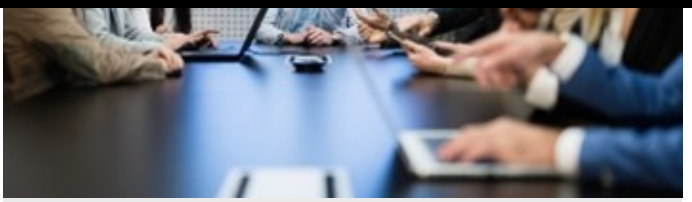
Why Not Watch?

25 MAY 2017

From Targeted to Distributed - Raise your Defenses Against Ransomware and Modern Malware

9 APR 2015

Crunch Time for Securing Big Data



25 MAY 2017

Be the Champion of Security in a DevOps World

8 DEC 2016

How to Keep on Top of Security Hygiene Without Sacrificing Speed and Efficiency

Related to This Story

Windows Risk Minimizer intended to minimize your wallet, warns Symantec

Symantec says internet users plagued by fake anti-virus software

Microsoft Security Essentials registers 1.5 million hits in first week

IEEE Launches Two Anti-malware Services

Windows 8 security useless against 15% of malware

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1

6 SEP 2016 NEWS

Brazzers Porn Site Users Caught Out in Data Breach

19 APR 2010 NEWS

Porn sites top drive-by download list

4 9 MAR 2018 NEWS
RedisWannaMine Uses NSA Exploit to Up the Crypto-Jacking Game

5 9 MAR 2018 NEWS
China Backdated Bug Disclosures to Hide State Hacking: Report

6 9 MAR 2018 NEWS
Slingshot APT Actor Shoots onto the Scene