6 DEC 2011 NEWS

Scareware is back to spook, swindle users, warns Enigma

The summer 'holiday' was the result of an international crackdown on scareware cybercrime rings carried out in June. Twelve countries collaborated in an anti-cybercrime effort to shut down two crime rings that caused more than $72 million in losses to over 900,000 people. In addition, the Russian police arrested Pavel Vrublevsky, co-founder of Chrono-Pay, the online payment processor for several large scareware scams. So the scammers were not able to process credit card transactions.

That appeared to stem the tide for the summer months, as scareware traffic plummeted, according to Enigma Software figures. But it's tough to keep a profitable criminal enterprise down for long.

"Scareware has been very active in September, and that activity increased tremendously around Thanksgiving", said Alvin Estevez with Enigma Software. "We are really seeing a lot of this rogue anti-virus program coming back stronger than ever", he told *Infosecurity*.

While malware infections are not up to pre-crackdown levels, there are some aggressive scareware campaigns underway.

The largest number of infections now is coming from System Fix, the second largest is called Cloud AV 2012, and the third is Win 7 Security 2012. These three infections are "insidious" because they lock the machine. They do not let the victim open up any programs, Estevez said.

"These are three different families; it is almost like a mafia", Estevez explained. And these families make an offer to customers that they can't refuse: "protection" against viruses.

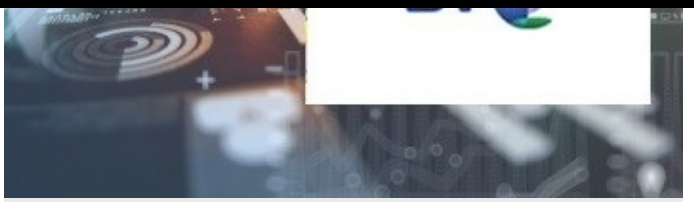
The families found a way around not having a company to process their credit card payments. "Somehow they figured out that if they go into affiliated networks, like Plimus or Clickback, and they are able to process these cards. When they made that switch, they came right back", Estevez explained.

Estevez is not confident that another law enforcement crackdown would work because many of the scareware makers are located in Russia. "The FBI would never get cooperation from the Russian authorities. They would never let the FBI arrest Russian nationals on Russian soil because the Russian government doesn't care that these guys are publishing malware", he judged.

Why Not Watch?

2 APR 2015

Browsers, Certificates and Trust: What's Changing and What You Need to Know



18 MAY 2017

How to Get Smart About Prevention

14 JAN 2016

Securing Your Windows 10 Estate

26 MAR 2015

Insights into Incident Response – A View from the Front Lines

Related to This Story

Search for patient zero: uncovering malware infection at the source

Windows Risk Minimizer intended to minimize your wallet, warns Symantec

AVG's popularity means it is being targeted by fake maintenance site scams

Does it Matter if It's Black or White(listing)?

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
2. 19 APR 2010 NEWS
   Porn sites top drive-by download list
3. 9 MAR 2018 NEWS
   Yahoo Agrees $80m Securities Class Action Settlement
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