Polish Takedown Targets 'Virut' Botnet

krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet/

Security experts in Poland on Thursday quietly seized domains used to control the **Virut botnet**, a huge army of hacked PCs that is custom-built to be rented out to cybercriminals.

NASK, the domain registrar that operates the ".pl" Polish top-level domain registry, said that on Thursday it began assuming control over 23 .pl domains that were being used to operate the Virut network. The company has redirected traffic from those domains to sinkhole.cert.pl, a domain controlled by **CERT Polska** — an incident response team run by NASK. The company says it will be working with Internet service providers and security firms to help alert and clean up affected users.

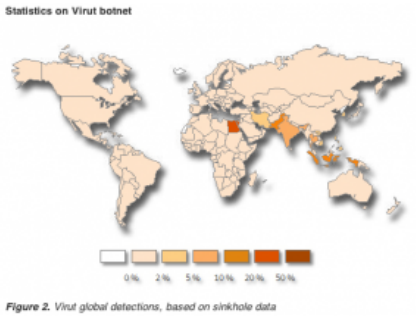


Figure 2. Virut global detections, based on sinkhole data

Source: Symantec

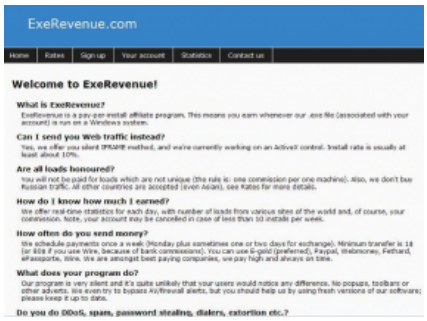
"Since 2006, Virut has been one of the most disturbing threats active on the Internet," CERT Polska wrote. "The scale of the phenomenon was massive: in 2012 for Poland alone, over 890 thousand unique IP addresses were reported to be infected by Virut."

Some of the domains identified in the takedown effort — including **ircgalaxy.pl** and **zief.pl** — have been used as controllers for nearly half a decade. During that time, Virut has emerged as one of the most common and pestilent threats. Security giant **Symantec** recently estimated Virut's size at 300,000 machines; Russian security firm **Kaspersky** said Virut was responsible for 5.5 percent of malware infections in the third quarter of 2012.

The action against Virut comes just days after Symantec warned that Virut had been used to redeploy **Waledac**, a spam botnet that was targeted in a high-profile botnet takedown by Microsoft in 2010.

SELF-PERPETUATING CRIME MACHINE

A file-infecting virus that has long been used to steal information from infected PCs, Virut is often transmitted via removable drives and file-sharing networks. But in recent years, it has become one of the most reliable engines behind massive malware deployment systems known as pay-per-install (PPI) networks. One such example was "exerevenue.com," a popular PPI network that once shared Internet resources with the aforementioned .pl domains.



PPI networks attract entrepreneurial malware distributors, hackers who are given custom "installer" programs that bundle malware and adware. In return, the distributors are paid a set amount for each 1,000 times their installer programs are run on new PCs. Access to the PPI networks is sold to miscreants in the underground, particularly spammers who are looking to increase the size of their spam botnets. Those clients submit their malware—a spambot, fake antivirus software, or password-stealing Trojan—to the PPI service, which in turn charges varying rates per thousand successful installations, depending on the requested geographic location of the desired victims.

The Exerevenue.com PPI program died off in 2010, but cached copies of the site offer a fascinating glimpse into the Virut business model. The following snippet of text was taken from Exerevenue's software end-user license agreement (EULA, and yes, this malware had a EULA). It aptly described how Virut worked: As a file-infecting virus that injected copies of itself into all .EXE and .HTML files found on victim PCs. According to the Exerevenue administrators, the program's installer relied on a trademarked "QuickBundle™" technology that bundled adware with other programs.

> "3) The software will especially target .EXE and .HTML files in the process of bundling. Other types of files may also be affected. HTML files are bundled with adware indirectly, through Internet links, and it relies upon certain features of Web browsers that are often considered undesired. Therefore, you agree you will not deliver your bundled files to anyone who can be offended by the QuickBundle technology described earlier. In order to prevent a file from being bundled with adware, you can change its name to begin with PSTO or WINC (in case of .EXE and .SCR files) or change its extension (in case of .HTM(heart), .ASP, and .PHP files), for example to .TXT. Apart from enriching your files with ad-supported content, your Windows HOSTS file will be modified to block certain domains used for adware loading automatization."

WHO IS RUNNING VIRUT?

In 2007, researchers at malware research group Team Furry published a brain dump of information that they'd collected about the individuals they believed created and ran the Virut botnet. Team Furry pointed to several subdomains of zief.pl and ircgalaxy.pl that according to archive.org hosted a somewhat active user forum frequented by hackers who used the names "XMAX" and "Adx." According to Team Furry, Adx was the hacker handle used by a computer whiz from Warsaw named Piotr Niżyński. Mr.Niżyński did not respond to multiple requests for comment.

It's not clear how the actions by NASK will impact the long-term operations of the Virut botnet. Many of Virut's control servers are located outside the reach of NASK, at Russian top-level domain name registrars (.ru). Also, Virut has a failsafe mechanism built to defeat targeted attacks on its infrastructure. In a blog post on Jan. 7, 2013, Symantec documented Virut's domain name generation algorithm (DGA); should Virut-infected PCs be unable to reach their hard-coded controllers at ircgalaxy.pl and zief.pl, the malware is configured to check one of a possible 10,000 different domain names each day, generated according to algorithm built into the malware. Armed with this backup mechanism, the miscreants responsible for Virut in theory would need simply to register one of the DGA-designated domains to be able to re-establish communications and control over the botnet.