The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Top Hacker 'Retires,' Experts Brace for His Return

October 31, 2010

ZeuS debuted in 2007 as spyware that hides in users' computers and logs keystrokes to steal their passwords. **Sergei Porter**

WASHINGTON — The Russian-based programmer who wrote ZeuS — malicious software used to steal an estimated $100 million so far this year from U.S. towns, companies and individuals — says he is retiring.

But security experts believe that there is a good chance he will soon emerge with even more powerful ways to steal, a pattern of behavior seen after previous retirements in 2007 and 2008.

ZeuS' unidentified programmer, who lives in Russia and seems to like nice cars and powerful trucks, first introduced ZeuS in 2007 as spyware that would hide in users' computers and log keystrokes to steal passwords, said Don Jackson, director of threat intelligence at the security firm SecureWorks.

The programmer, rather than doing the stealing himself, used a middleman to sell the

spyware software to criminal gangs. A basic version would run as low as $1,000 but could be customized for an extra fee. He would also offer round-the-clock support.

Thieves who use ZeuS tend to avoid big companies and banks with top-line security, preferring instead smaller companies, townships and even churches. In a recent case, however, they breached and emptied brokerage accounts at E*Trade Financial Corp. and TD Ameritrade Inc., according to a criminal complaint filed in New York in September.

"We have seen banks in almost every major country targeted by these [ZeuS] tool kits," said Dmitri Alperovitch, a vice president at security software company McAfee.

But there has been pressure on the ZeuS gangs. About a month ago, authorities in the United States, Britain and Ukraine arrested dozens of people suspected of involvement in a global cybercrime scheme that used a version of the ZeuS Trojan to steal $70 million from U.S. bank accounts, the FBI said.

In October, the ZeuS author announced through his main reseller that he had had enough, said SecureWorks' Jackson.

Jackson, a ZeuS expert, said the Trojan program's author spread the word that he was handing his source code to the author of Spy Eye, an up-and-coming Trojan and a ZeuS competitor. In fact, when the Spy Eye Trojan infected a computer it would clear out ZeuS.

Jackson said he believed that the retirement announcement was a ruse. "He probably has a private client set up. They had already made the decision to merge, or to pretend to merge with Spy Eye," he said.

What little is known about the ZeuS author has been gleaned from online chat rooms where he sometimes uses names based on expensive vehicles.

Some security experts believe that there is a possibility the ZeuS programmer is really headed for retirement.

"One can only imagine that he's made enough money to take a vacation for a long period of time," said Elias Levy, senior technical director at Symantec Security Response.

He has probably made at least a million and perhaps multiple millions of dollars, said Bill Conner, president and chief executive of computer security firm Entrust.

Gangs who used ZeuS software stole $100 million in 2010 in the United States, said Jackson.

In 2007, the ZeuS author, who goes by the handle Monstr, among others, in online forums, started to feel that he was gaining too much notoriety and said at that time that he was stepping aside, but instead went underground to work more discreetly, Jackson said.

In late 2007, security experts started finding a souped-up version of ZeuS doing automated bank frauds. The cycle repeated itself in 2008.

"Once he attracts a lot of attention, he goes underground. Says, 'I'm going to hand it over to some guy and get them to deal with it.' Tries to push the high-maintenance, second-tier

customers onto someone else," Jackson said.

Last year, ZeuS became so deft that it can now read text messages sent by banks to customers' phones to inform them of fraudulent transfers. ZeuS intervenes, and prompts the customers to enter codes to confirm the fraudulent transfers.

One of the latest versions of ZeuS allows the Trojan to hide in an executable program, like a word processor. That way, if the ZeuS Trojan is cleared out, it can reinstall itself the next time the word processor is used, Levy said.

Security experts said they planned to monitor ZeuS and Spy Eye for new developments.

“Up until now, they were two completely different Trojans,” said McAfee’s Alperovitch, who said it was possible that the ZeuS author was retiring. “If we start seeing capabilities evolving rapidly in Spy Eye that borrow from the ZeuS functionality then we’ll know that, yes indeed, he [the Spy Eye author] has access to the ZeuS source code.”

Original url:
https://www.themoscowtimes.com/2010/10/31/top-hacker-retires-experts-brace-for-his-return-a2617