The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Suspect in 'Blackhole' Cybercrime Case Arrested in Russia, Source Says

By The Moscow Times

October 09, 2013

Russian authorities have arrested a man believed to be responsible for distributing a notorious software kit known as "Blackhole" that is widely used by cybercriminals to infect PCs, a source familiar with the situation said.

A former Russian police detective in contact with Russia's federal government told Reuters that the suspect, who is known in hacking circles as "Paunch," had been arrested. He provided no details.

Blackhole is a piece of malicious software that hackers install on web servers that then automatically infects personal computers when users visit a tainted site.

It contains an arsenal of tools for attacking PCs, each of which leverage vulnerabilities in computers. It probes potential victims looking for a way in, then attacks when it finds a weakness.

Once they are in, cybercriminals typically install other, more specialized programs on the computers of their victims. They include tools for engaging in identity theft and selling fake anti-virus software.

Security experts say Blackhole's developers regularly update the product so that customers can exploit the newest vulnerabilities uncovered in PCs. The ones most widely exploited include Microsoft's Windows and Internet Explorer, Adobe's Reader and Flash, and Oracle's Java software.

Officials in Russia could not immediately be reached for comment on the arrest.

A spokesman for Europol in The Hague said the European crime-fighting agency "had been informed that a high-level suspected cybercriminal" was arrested in Russia. He declined to elaborate.

Russian cybercriminals who confine themselves to attacking targets in other countries are rarely arrested, so the capture of Paunch was cause for some celebration among security researchers.

Not all of those arrested are ultimately convicted, however, and even some convicted of stealing millions of dollars have been released on probation.

Russia has one of the largest pools of talented hackers and an advanced underground economy that unites customers and programmers with those who control networks of compromised computers and can install new malicious programs at will.

Original url:
https://www.themoscowtimes.com/2013/10/09/suspect-in-blackhole-cybercrime-case-arrested-in-russia-source-says-a28440