Koobface computer virus gang unmasked

January 17 2012

Online security researchers claimed to have identified the members of a Russian gang of cyber criminals behind the Koobface computer virus which has attacked Facebook and other sites. Facebook said that its security team had helped knock out a computer server which controlled a Koobface "botnet" of malware-infected personal computers.

Online security researchers claimed Tuesday to have identified the members of a Russian gang of cyber criminals behind the Koobface computer virus which has attacked Facebook and other sites.

Facebook said meanwhile that its security team had helped knock out a computer server which controlled a Koobface "botnet" of malware-infected personal computers.

According to Jan Droemer, an independent computer security researcher, and Dirk Kollberg of security firm SophosLabs, the five members of the Koobface gang live in St. Petersburg, Russia.

In a blog post, Sophos said evidence and the identities of the five Koobface suspects has been handed over to law enforcement.

The Koobface virus first emerged in 2008, spreading in the form of messages with subject lines such as "You look just awesome in this new movie."

Users who clicked on the message were informed their Flash player was out of date and were prompted to download Flash software, exposing their computer to Koobface malware.

Koobface tricked some owners of infected personal computers into buying anti-virus software and enlisted their machines into a botnet made up of hundreds of thousands of infected computers.

"Koobface was able to perform these actions by communicating with a central 'Command & Control' server, which directed the compromised computers to do the gang's bidding," Facebook said.

"This remained the case until last March, when Facebook Security was able to perform a technical takedown of this 'Command & Control' Mothership," it said.

"Since then we have had no new sightings of Koobface for over nine months and our teams are working hard to keep it that way," Facebook said.

"While we have been able to keep Koobface off Facebook, we won't declare victory against the virus until its authors are brought to justice," it said.

"To this end, we will be sharing our intelligence with the rest of the online security community in the coming weeks in an effort to rid the

Web of this virus forever," Facebook said.

(c) 2012 AFP