Nefarious Conficker worm racks up $9.1 billion bill

Contributed by Aharon Etengoff
Tuesday, April 21, 2009 12:46

Researchers at the Cyber Secure Institute estimate that the nefarious Conficker worm has racked up a staggering $9.1 billion bill.

Chicago (IL) - Researchers at the Cyber Secure Institute estimate that the nefarious Conficker worm has racked up a staggering $9.1 billion bill.

The Institute also warned against "downplaying" the worm's significance.

"Because there was no major Conficker-created problems on April 1st when hijacked computers went online and began communicating with controller domains, numerous commentators are now downplaying the significance of the Conficker problem. This conclusion is wildly off base and patently flawed," explained Rob Housman, executive director of the Cyber Secure Institute. "In short, just because the other guy in a fight doesn't pull the trigger when he's got the gun to your head, doesn't mean you won the fight. It is important to look at the totality of the Conficker problem. Whether or not Conficker ultimately turns out to be a sales tool for bogus Ukrainian security software or something much more destructive, the simple fact is that the Conficker worm has infected vast numbers of computers around the world."

According to Housman, any analysis of the Conficker worm's impact should factor in "wasted time, resources, and energies of the cyber-community, governments, companies and individuals."

In addition, Housman noted that while Conficker has yet to play out a doomsday scenario, there was a "strong possibility" that future worms would be much less benign. As such, the executive director recommended deploying secure technologies, including the Integrity Global Security operating platform and the Tenix Interactive Link Device. Both have reportedly been certified by the National Information Assurance Partnership and NSA against sophisticated cyber threats.

As TG Daily previously reported , Conficker, like many other worms, is a blended threat relying on many different attack methods - ranging from password-guessing and brute force techniques to infection via flash drives in effort to replicate and then spread over a network.

The most recent versions of the code were responsible for the infection of many networks through peer-to-peer communication. The worm had protective measures which enabled it to duck detection and removal through the disabling of Windows Automatic Updates and Windows Security Center. The virus also blocked access to the web sites of numerous security vendors -- rendering many anti-virus programs which had an effective removal protocol ineffective.

Conficker is expected to stop functioning on May 3, 2009.