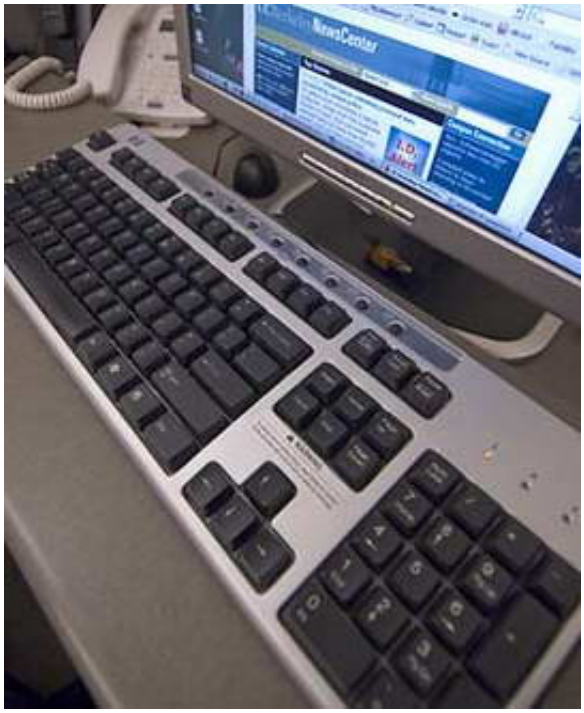
Bitdefender researchers find evidence of viruses infecting worms creating new form of malware

27 January 2012, by Bob Yirka



(PhysOrg.com) -- Romania based antivirus software company Softwin, makers of Bitdefender, have announced that they have found multiple instances of computers being infected with worms that have been infected by viruses, creating what they describe as a new Frankenstein piece of malware that should have users all over the world concerned as the new resultant mutant offspring may be more destructive than either alone and more difficult to detect by traditional software programs.

The problem they say, occurs when a computer becomes infected by a virus that has already been infected by a worm. Because worms tend to exist as executable (.exe) files and viruses tend to infect executable files, it's only a matter of time before a preexisting worm becomes infected with a virus that manages to make its way onto the computer as well. And while the idea of a mutant bit of malware on a computer seems much worse than the traditional fare, thus far, the research team at Bitdefender doesn't seem to have any evidence backing up its claim that the new double-whammy worm/virus combo is actually any more destructive than either would be alone if both existed as separate entities on the same computer. Although it does seem plausible that such a type of coexistence could allow viruses to spread much more easily through a network than it could were it to go it alone, as worms are generally much better at doing so.

In their announcement, the research team says it found 40,000 instances of the mutated malware out of a sample of ten million files; a hit rate of 0.4 percent. One such instance was the Virtob virus infecting worms such as the Rimecud, a potentially potent combination as Rimecud was designed to steal information such as passwords, and Virtob to create a hacker-controlled back door. Thus the two combined could find private information and then allow a hacker to sneak in and use that information to access private accounts such as for banks or credit cards.

One issue not addressed in the announcement however was the degree of damage to the worm caused by the virus upon attack, the purpose of most viruses after all, is to wreak havoc. If extensive enough, damage to a worm could kill it or make it unable to do its job which would mean no viable mutant malware would result.

Thus far the researchers say, they don't believe the virus attacks on worms were intentional or planned by makers of either, but it's clearly not

beyond the realm of possibility now that the option has been raised, and if that does occur, it most certainly could pose a very serious threat to computers and networks the world over.

More information:
via Malware City

APA citation: Bitdefender researchers find evidence of viruses infecting worms creating new form of malware (2012, January 27) retrieved 7 December 2021 from https://phys.org/news/2012-01-bitdefender-evidence-viruses-infecting-worms.html