Worms infesting computers worldwide: Microsoft

November 2 2009, by Glenn Chapman

The logo for Microsoft at their office in Herndon, Virginia. A Microsoft security report released Monday warns that cyber crooks are digging into computers for weak spots to penetrate with worms -- malicious software that steals control or data.

A Microsoft security report released Monday warns that cyber crooks are digging into computers for weak spots to penetrate with worms -- malicious software that steals control or data.

Rogue security software remained the top hacker threat to computers during the first half of this year, but the number of infections was dropping while penetrations by worms doubled, according to the Security Intelligence Report.

"We still see rogue security software in high volume but not on the rise,"

Microsoft Malware Protection Center principal architect Jeff Williams told AFP. "What is on the rise is resurgence of worm activity, particularly Conficker and Taterf."

Worms are programmed to replicate themselves, wriggling from machine to machine by hiding in legitimate applications or piggy-backing on USB drives or other portable data storage devices.

Rogue security software, or "scareware," typically spreads by tricking people with pop-up boxes bearing bogus alerts that their machines are infected.

Spooked computer users are then enticed to pay for applications to fix the supposed computer problems. People that fall for the scam wind up paying hackers; providing them credit card information, and installing malware.

Automated scareware blocking in Web browsers and efforts by law enforcement agencies to crack down on companies peddling rogue security software has helped curb the threat.

"When selecting an anti-virus product, do it from a proven provider, not someone you never heard of who just pops up on your screen," Williams said.

Improving defenses of computers was seen as a reason hackers are reverting to worms, which were a top bane about a decade ago.

"We see a rise again in worms as profit-motivated criminals are digging deeper, finding more arcane vulnerabilities to execute remotely," Williams said.

A Conficker worm that plagued the Internet at the start of the year was

so pernicious that a task force to combat it was formed by computer software and security firms.

Conficker and Taterf worms have reportedly wriggled into millions of machines.

One of the troublesome ways both worms spread is by stowing away on thumb drives, which are becoming increasingly popular vehicles for people to move music, videos, games, files or other data between computers.

"Think about how and where people play online games," Williams said. "What you tend to see is people remove a drive from home or an Internet kiosk and take it back into the enterprise (workplace)."

A memory stick carried in by a worker tends to bypass computer security systems designed to guard against hackers breaking in from outside the walls of a business, according to Williams.

Businesses should establish security protocols for removable media drives, and have new arrivals automatically scanned for malware, Microsoft recommends.

"The criminals out there are becoming more overt, more malicious and more direct in their attacks," Williams said.

"That emphasizes the need for multi-layer protections. It is great we have anti-virus software to remove the threats, but clearly it is better to prevent the threat from getting in."

Cyber criminals are moving with increasing speed when it comes to reverse engineering patches released to fix vulnerabilities in software programs or operating systems, according to Microsoft.

Hackers dissect patches to identify weakness being repaired, then craft malicious code to take advantage of flaws in machines with software that isn't kept up-to-date.

"A patch is released and that is what starts these days of risk" Williams said.

"There is a window of vulnerability, so we need to close that window more quickly" he said. "Making sure you are up-to-date on security updates is one strong method of protecting yourself against attack."

Microsoft's security report is based on data from "billions of scans a day" in more than 200 regions of the world.

(c) 2009 AFP