Bogus security software growing threat: Microsoft

April 8 2009, by Glenn Chapman

A man surfs the internet in Beijing, September 2007. Hackers are increasingly hiding viruses in bogus computer security software to trick people into installing treacherous programs on machines, Microsoft warned.

Hackers are increasingly hiding viruses in bogus computer security software to trick people into installing treacherous programs on machines, Microsoft warned on Wednesday.

The software giant said in a security intelligence report that "rogue security software" is a growing threat as hackers take advantage of people's fears of worms such as the notorious Conficker.

"Rogue security software is the number one threat worldwide," said George Stathakopoulos, general manager of the Trustworthy Computing Group at Microsoft.

"If you think about the Conficker case, how many people went looking for a security solution and downloaded rogue malware?"

Rogue security software referred to as "scareware" pretends to check computers for viruses, and then claims to find dangerous infections that the program will fix for a fee.

"The rogue software lures them into paying for protection that, unknown to them, is actually malware offering little or no real protection, and is often designed to steal personal information," Microsoft said.

Two "rogue families" of scareware were detected in 1.5 million computers, according to Microsoft. Another form of scareware was found on 4.4 million computers, a rise of 66 percent from the previous six-month period.

"That means when users downloaded the software they probably gave away credit card numbers and got infected," Stathakopoulos said. "That's a double hit."

Microsoft releases security reports twice annually. Stathakopoulos expects scareware infections to soar in the first six months of this year because of massive hype regarding Conficker.

The Conficker worm's April 1st trigger date came and went without the bedeviling computer virus causing any mischief but security specialists warn that the threat is far from over.

The virus evolved on April Fools' Day to better resist extermination and make its masters tougher to find.

A task force assembled by Microsoft has been working to stamp out Conficker, also referred to as DownAdUp, and the software colossus has

placed a bounty of 250,000 dollars on the heads of those responsible for the threat.

The worm, a self-replicating program, takes advantage of networks or computers that haven't kept up to date with security patches for Windows.

It can infect machines from the Internet or by hiding on USB memory sticks carrying data from one computer to another.

Conficker could be triggered to steal data or turn control of infected computers over to hackers amassing "zombie" machines into "botnet" armies.

Microsoft's report found that as operating system defenses have improved cybercriminals have shifted attacks to software applications people use in their online lives.

Ruses such as bogus software updates or security checks and booby-trapped Web pages or emails are among "social engineering" scams hackers use to dupe people into allowing malicious software past computer defenses.

"We see cybercriminals increasingly going after vulnerabilities in human nature rather than software," said Vinny Gullotto, general manager of the Microsoft Malware Protection Center.

Stathakopoulos urged people to keep computer applications and anti-virus software updated and to be wary of online come-ons by strangers.

"Use a little common sense," Stathakopoulos counseled.

"If you browse the Web and someone you never met before is offering

you a lot of money, it is probably not a good thing ... You wouldn't buy medicine from people you didn't know."

Despite the increasingly wily tactics employed by hackers, the primary causes of data breaches were classic real-world problems of loss or theft of computer equipment, according to Microsoft.

The report, based on data gathered from hundreds of millions of computers worldwide during the second half of 2008, said half of security breaches involved computer gear vanishing, not being hacked.

"For businesses, the security concern is the laptop you left in the cab or the CD-ROM you left in the bar," Stathakopoulos said. "Encryption is so important."

(c) 2009 AFP