Wiretapping Skype calls: virus eavesdrops on VoIP

September 2 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Some computer viruses have a crude but scary ability to spy on people by logging every keystroke they type. Now hackers and potentially law enforcement have another weapon: a virus that can eavesdrop on voice conversations that go over computers instead of a regular phone line.

The capability has been shown in a new "Trojan horse" virus that records Voice over Internet Protocol (VoIP) calls through the popular Skype service. Skype calls are free or low cost and can work between two computers or between one computer and a phone.

There were 480 million Skype users worldwide at the end of June, but it's unlikely many would be hit by the new virus. It's better suited for targeted espionage rather than mass infections because criminals would have to sift through an unfathomable amount of audio recordings generated by the virus.

Law enforcement in the U.S. would presumably need a court order to surveil someone's Skype calls, but the barriers to deploying the virus might be lower for intelligence agencies and authorities in other countries.

The virus, which security firm Symantec Corp. calls the first "wiretap Trojan," doesn't target a particular vulnerability in Skype. Instead, it hooks into parts of the Windows operating system that handle audio processing. Then it intercepts all audio data coming from Skype before

it's encrypted by the software, according to Symantec's analysis.

The audio gets saved as MP3 files and can be sent to computers controlled by the criminals.

"It's more interesting than dangerous," said Kevin Haley, director of Symantec Security Response. "It's an espionage tool. That's its clear purpose. It's not practical for any type of broad-based attacks."

The virus was designed and released by Ruben Unteregger, a Swiss programmer who said he started researching on his own before turning it into a project for his employer, ERA IT Solutions.

In 2006 the software company was reported by the Swiss newspaper SonntagsZeitung to have been working on a VoIP-cracking virus for the Swiss government, an account Unteregger said he couldn't confirm because of a nondisclosure agreement he signed for the project.

ERA IT Solutions says it never had an order from a government agency to develop the program, and that it stopped working on it when Unteregger left the company last year.

"This is Ruben's affair only," said company representative Riccardo Gubser.

Unteregger said in an e-mail interview with the AP that his goal in releasing the virus' programming code was to make people aware that "we are now becoming a surveillance society" and that "police Trojans are reality and questionable."