Huge 'botnet' amputated, but criminals reconnect

March 11 2010, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- The sudden takedown of an Internet provider thought to be helping spread one of the most promiscuous pieces of malicious software out there appears to have cut off criminals from potentially millions of personal computers under their control.

But the victory was short-lived. Less than a day after a service known as "AS Troyak" was unplugged from the Internet, security researchers said Wednesday it apparently had found a way to get back online, and criminals were reconnecting with their unmoored machines.

The drama initially raised hopes of a sharp drop-off in fraud, because criminals could no longer communicate with many computers infected with a type of malware known as "ZeuS," which is mostly used to steal online banking usernames and passwords. Hundreds of criminal operations around the world use the malware.

It's unknown how many computers are infected with ZeuS, but it's estimated to be in the millions. Cisco Systems Inc. said as many as 25 percent of the world's ZeuS-infected machines were unplugged from the massive "botnet" overnight with the takedown of AS Troyak.

Botnets are networks of infected PCs that behave like criminals' remote-control robots. They steal identities en masse and are used to attack Web sites.

But instead of a slam-dunk victory, the incident wound up highlighting

the whiplash pace at which criminals can resurrect their illicit businesses after what should have been a devastating setback.

RSA, the security division of EMC Corp., said dozens of malicious servers that criminals used to spread ZeuS were connected to the Internet by AS Troyak. The service inexplicably went dark Tuesday, severing the ties between criminals and ZeuS-infected machines under their control.

It's not publicly known who pulled the plug. It could have been law enforcement, security researchers, or even the criminals themselves if they decided to move their operations to other servers.

Shutting down malware operations is a constant cat-and-mouse game.

Some services exist solely to host malicious content, and when their connections to the Internet are severed, it's often relatively easy to find another provider willing to sell them a new connection.

RSA researchers wrote in a note to clients that their experience shows that "these kinds of drastic changes are usually short-lived, as in the long run, criminals tend to restructure their criminal activity and relaunch their online attacks."

That apparently happened - and quickly. By Wednesday, researchers said the servers appeared to be back online, through a new Internet provider.

Cisco researchers said a total of 68 command-and-control servers were brought down, but that it's unknown how many infected computers were connected to each of those.

But they added that the criminals may have known the servers were going to be brought down, because traffic to those servers spiked over the weekend, suggesting they were directing infected computers to point

to new servers.

One of the most high-profile takedowns of a malicious Web site hosting service involved a company called McColo Corp. whose Internet service was severed in the winter of 2008 after researchers amassed evidence of the company's wrongdoing.

Worldwide spam volumes almost instantly dropped by half, but within days started climbing again.