InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Online Criminal Gangs Battle With Botnets

Criminal cyber gangs are trying to steal zombie computers from rival botnets so they can boost their own numbers and raise the price they get from spammers.

By Sharon Gaudin, InformationWeek
May 18, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=199601992

Two or three online criminal gangs are waging an all-out battle for control of the largest botnets, sending out waves of malware aimed at stealing zombie computers from rival gangs to build up their own army.

Each online gang is trying to build up the biggest botnet because the bigger the army of infected computers they control, the more money spammers and hackers will pay to use them, explains Shane Coursen, a senior technical consultant for Kaspersky Lab. Since the gangs have their own botnets already built up, they're all trying to pilfer victimized computers from their rivals, to diminish their competitor's botnets while they build up their own.

"It's an ongoing war," said Coursen in an interview with *InformationWeek*. "The Internet is flooded with machines that already are compromised. What better way to take ownership of a machine than to get into one that is already owned. They can take advantage of it. It's like an open door to these guys."

Coursen said the author of the well-known Storm Worm, also known as Zhelatin, is going head to head with the author or authors of the Warezov and Bagle worms. It's unclear whether one group is responsible for both the Warezov worm and the Bagle worm or if different groups are behind each one, he said. Regardless, they're both working to steal zombies from the Storm Worm authors.

The Kaspersky consultant said each malware gang began coming out with a lot of variants at the beginning of the year; there have been upwards of 20 new variants a day between the three of them. The number of variants coming out daily has dipped since then, but there's still a steady assault of them.

"They probably built their botnets with those first 200 to 300 variants. Now they're using those compromised machines and installing new Trojans on them," said Coursen. "Malware writers go after low-hanging fruit. Machines that are already compromised are very easy to own again. It would make sense that one group would go after another group's machines to add to their own botnet. If they know how it's already been compromised, it's easy to take control of that machine."

Coursen explained that the malware writers can run a port scan on a block of IP addresses. If a computer comes back with a reply, then a port is open and there's a good chance the machine has been compromised. The expert malware writers have familiarized themselves with other viruses and Trojans, so they know what virus is involved by what port it's using. Once they know what virus is involved, they simply do some research into how it works and probably can even find a remote administration tool for it on underground hacker sites.

Then the hacker sends commands to the victimized machine, causing it to go to a malicious Web site where it downloads a new Trojan, which removes the original piece of malware from the machine and installs new malicious code in its place.

At that point, the hacker has taken control of the machine from the rival gang, and can add it to his own botnet.

"This is escalating," said Coursen. "Instead of just one group that was kind of active, now we're looking at two definite

groups and possibly three groups. The activities have increased very significantly over the last six months. We see a huge increase in the amount of spam, and it's largely because of this war."