c|net NEWS.COM http://www.news.com/

Online threats outpacing law crackdowns

By Joris Evers
http://news.com.com/Online+threats+outpacing+law+crackdowns/2100-7349_3-6084317.html

Story last modified Thu Jun 15 13:37:28 PDT 2006

SCOTTSDALE, Ariz.--Authorities are cracking down on phishing and botnets, but the threats are advancing instead of diminishing, two law enforcement officials said.

Cybercrooks are organizing better and moving to more sophisticated tactics to get their hands on confidential data and turn PCs of unwitting users into bots, representatives from the U.S. Department of Justice and the U.S. Air Force Office of Special Investigations said in separate presentations here at the Computer Security Institute's NetSec event this week.

Law enforcement has had increased successes in catching, prosecuting and convicting phishers and bot herders over the past couple of years. However, catching the bad guys is getting tougher as the criminals become more professional, the representatives said.

"We're seeing increasingly sophisticated groups online that are more indicative of crime groups," Jonathan Rusch, special counsel for fraud prevention at the Justice Department, said in a presentation. The criminals who have been caught range from teenagers to retirees, he said.

Rusch spoke about phishing, a prevalent type of online attack that combines e-mail spam and fraudulent Web sites made to look like trusted sites, which are aimed at tricking a user into giving up sensitive information such as a credit card or Social Security number. Almost 17,500 phishing Web sites were reported to the Anti-Phishing Working Group in April.

A top phishing concern is the increased use of malicious software, Rusch said. Increasingly, phishers use Trojan horses that pack backdoors, screen grabbers or keystroke loggers to capture log-in names, passwords and other information, he said. In April, there were 180 unique examples of such malicious code, he said.

Backdoor software gives attackers remote access to an infected PC, which could let them piggyback onto a user's Internet connection and conduct online transactions from the victim's PC while masquerading as the person, Rusch said.

Screen grabbers and keystroke loggers can be programmed to capture very specific information and are even designed to wait until a user logs on to a certain banking Web site and send that information to the attacker.

"Botnets are one of the greatest facilitators of

Malicious software is where phishers intersect with bot herders, those who run networks of compromised machines, called a bot net. Computers typically

become compromised and turned into a bot, also popularly called a zombie, after visiting a malicious Web site or opening an infected e-mail message or attachment. The bot software often nestles itself on a PC unbeknownst to the user by exploiting an unpatched security flaw on the system.

Law enforcement has been catching up to bot herders, and there have been some high-profile convictions. But here, too, the battle is getting harder, Wendi Whitmore, a special agent with the Air Force Office of Special Investigations, said in a presentation on botnets.

"Botnets are one of the greatest facilitators of cybercrime these days. Really the cybercrime arena is wrapped around botnets," she said.

cybercrime these days. Really the cybercrime arena is wrapped around botnets."
--Wendi Whitmore, special agent, Air Force Office of Special Investigations

With ubiquitous broadband connections and exploits for security flaws in software out before patches, the Internet environment is ideal for bots or zombies to proliferate, she said. That assertion is backed by a recent analysis by Microsoft. The software maker found that bots were the most common Windows threat, with more than 60 percent of compromised computers running bot code.

A zombie PC can be used by miscreants to store illegal content, such as child pornography, or in a botnet to relay spam and launch cyberattacks. Additionally, hackers often steal the victim's data and install spyware and adware on PCs, to earn a kickback from the spyware or adware maker.

Practice makes perfect

Meanwhile, bot masters are getting smarter about hiding. Today, most botnets are controlled using Internet Relay Chat, or IRC, servers and channels. Soon that could become instant messaging, peer-to-peer technology or protocols used by Internet phone services such as Skype or Vonage, Whitmore said.

"That is something that we're worried about because those protocols are proprietary," she said. "They don't publish routing protocols; it would be very difficult to catch that kind of crime."

Also, Whitmore expects cybercrooks to maintain smaller botnets with the hope of staying under the radar. People being caught today operate networks of as many as 1 million PCs. "There is a greater chance that you're going to get caught, if you do that much activity and command and control that many computers," she said.

Cybercriminals are often after data they can turn into cash, such as credit card numbers or even trade secrets. "If you have a smaller botnet and you combine that with targeted, really sophisticated social engineering tactics, you're going to be potentially a lot more successful," Whitmore said.

The military has seen a rise in such attacks over the last couple of years, Whitmore said. The attackers know what organizations work together, which generals would be involved and what issues they would talk about, she said. It's "incredibly disturbing, because those are the kinds of things that should be kept somewhat secret," she said.

Law enforcement alone cannot solve the phishing and botnet problems, Rusch and Whitmore said. The technology industry and consumers have key parts to play, they said.

"Part of the problem is the way we design the online environment for users," Rusch said. It should be

easier for people to see whether a site can be trusted or not, he said. Some of that is happening today with increased security coming in new Web browsers, for example.

A stronger effort to take down phishing Web sites is also welcome, he said. The average phishing Web site was up for five days in April, and that's too long, Rusch said.

In fighting bots, Whitmore sees benefits in Internet service providers delivering security software to their users. "The long-term benefit of ISPs becoming more involved would be an overall reduction of malicious code on the Internet, and most of us believe that's a good thing," she said.