Hiding the honeypots: Is it possible to hide honeypot traps from Botnet drones

February 26 2010

Armies of networked computers that have been compromised by malicious software are commonly known as Botnets. Such Botnets are usually used to carry out fraudulent and criminal activity on the Internet. Now, writing in the *International Journal of Information and Computer Security*, US computer scientists reveal that the honeypot trap designed to protect computers from Botnets are now vulnerable to attack because of advances in Botnet malware.

In the 1990s and early 2000s, viruses and worms were the main problems facing computer security experts, with the likes of Melissa, Love Letter, W32/Sircam, MyDoom, Netsky and Bagle familiar to anyone reading the computer press during that period. There has not been a major outbreak of a conventional computer virus or worm on the internet since the Sassar worm of May 2004. That is not because improvements in computer security have outstripped the skills of the virus writers but simply because the focus has shifted to taking control of computers invisibly. Instead of erasing information from hard drives or causing other mischief, compromised computers are recruited into Botnets that track keystrokes and steal usernames, passwords, and credit card details with criminal intent.

Cliff Zou and colleagues of the University of Central Florida in Orlando, explain that Botnets have become one of the major attacks on the internet today, allowing those that control them to take control of tens of thousands of computers and websites, steal credit card and banking information, send millions of spam emails, and infect other computers, all for illicit financial gain. Moreover, those in control of the most powerful Botnets even hire out computer time on these illegal systems to other criminals.

The self-propagating nature of a Botnet means that the underlying software is always attempting to infect new computers. This has allowed security experts to create "honeypot" traps - unprotected computers with hidden monitoring software installed - that attract Botnets and then extract data about the Botnet and the compromised computers it controls. Honeypots set up by security defenders thus become spies in exposing botnet membership and revealing Botnet attack behavior and methodology allowing security experts to find ways to block Botnet activity.

Zou and his team have now discovered that Botnet software could be developed to detect honeypots. Given that security defenders have an obligation to dis-arm their own honeypot computers so that they do not become active components of the Botnet, the malicious software could, they explain, simply detect such a honeypot during initial activity as it will not send back appropriate information. The Botnet would then either disable the honeypot computer or else simply ignore its existence and move on to the next target.

By revealing this vulnerability to the computer security industry and presenting possible guidelines for creating honeypots that might be undetectable, the team hopes to pioneer a way to trap and block Botnet software before the Botnet controllers are able to exploit this technical loophole in legitimate computer systems employing honeypots.

"Honeypot research and deployment still has significant value for the security community, but we hope this paper will remind honeypot researchers of the importance of studying ways to build covert honeypots, and the limitation in deploying honeypots in security defense," Zou says, "but all that effort will be for naught if honeypots remain as easily detectible as they are presently."

More information: "Honeypot detection in advanced botnet attacks" in Int. J. Information and Computer Security, 2010, 4, 30-51

Provided by Inderscience Publishers

Citation: Hiding the honeypots: Is it possible to hide honeypot traps from Botnet drones (2010, February 26) retrieved 7 May 2024 from https://phys.org/news/2010-02-honeypots-honeypot-botnet-drones.html