Malicious software infects computers

John Markoff

A malicious software program has infected the computers of more than 2,500 corporations around the world, according to NetWitness, a computer network security firm.

The malicious program, or botnet, can commandeer the operating systems of both residential and corporate computing systems via the Internet. Such botnets are used by computer criminals for a range of illicit activities, including sending e-mail spam and stealing digital documents and passwords from infected computers. In many cases they install so-called keystroke loggers to capture personal information.

The current infection is modest compared with some of the largest known botnets. For example, a system known as Conficker, created in late 2008, infected as many as 15 million computers at its peak and continues to contaminate more than seven million systems globally.

Botnet attacks are not unusual. Currently Shadowserver, an organization that tracks botnet activity, is monitoring 5,900 separate botnets.

Several computer security specialists also disputed the company's assertion that the botnet was a novel discovery. This type of infection is well known to the computer security research community and is routinely tracked by a monitoring system that has identified more than 1,300 botnets of this design.

NetWitness said in a release that it had discovered the program last month while the company was installing monitoring systems. The company named it the Kneber botnet based on a username that linked the infected systems. The purpose appears to be to gather login credentials to online financial systems, social networking sites and e-mail systems, and then to transmit that information to the system's controllers, the company said.

The company's investigation determined that the botnet had been able to compromise both commercial and government systems, including 68,000 corporate login credentials. It has also gained access to e-mail systems, online banking accounts, Facebook, Yahoo, Hotmail and other social network credentials, along with more than 2,000 digital security certificates and a significant cache of personal identity information.

"These large-scale compromises of enterprise networks have reached epidemic levels," said Amit Yoran, chief executive of NetWitness and former director of the National Cyber Security Division of the Department of Homeland Security. "Cyber criminal elements, like the Kneber crew, quietly and diligently target and compromise thousands of government and commercial organizations across the globe."

The company, which is based in Herndon, Va., noted that the new botnet made sophisticated use of a well-known Trojan Horse — a backdoor entryway to attack — that the computer security community had previously identified as ZeuS.

"Many security analysts tend to classify ZeuS solely as a Trojan that steals banking information," said Alex Cox, the principal analyst at NetWitness responsible for uncovering the Kneber botnet. "But that viewpoint is naïve. When we began to detect the correlation among both the methodology used by the Kneber crew to attack victim machines and the wide variety of data sets harvested, it became clear that security teams must rethink their entire perspective on advanced threats such as ZeuS."

Half of the machines infected with the Kneber botnet were also infected by an earlier botnet known as Waledec, the company noted.

The existence of the botnet was first reported by The Wall Street Journal, shortly before the company issued its news release.

Fonte: New York Times, New York, Feb. 18th 2010, Technology, online.