

Ryan Sherstobitoff takes us into the AV lab at Panda Security USA

The Silent Epidemic

By Ryan Sherstobitoff

Over the last year, the trend of malware appearing on the Internet has changed dramatically. While hackers used to be driven by fame and notoriety, they now are highly sophisticated members of organized crime organizations infiltrating systems for financial gain.

This year, during a pilot for a new anti-fraud service, we detected what seemed to be “just another trojan” that affected banks. However, it turned out to be one of the largest examples of crimeware detected to date, capturing the banking details of over 40,000 infected users.

Limbo, as the trojan is called, was designed to “inject” code from infected PCs into popular banking websites in order to steal credentials. The trojan injected a field into the bank authentication page so that when the user entered his username and password, the information was stolen. The stolen information was sent to a PC or ISP that had been compromised to act as a drop box. Utilizing stealth technology, the hacker was then able to access the stolen data that was stored on the drop box.

Each bank incorporates its own validation method on its authentication page. Therefore, an individual malicious code injection script is required for each bank. Limbo contained the code injection script for most major banks. However, sometimes those banks update or modify authentication methods. Thus, the hacker needed the ability to modify the injection code as time went on. This was done using an ASP control panel that allowed the hacker to remotely update infected PCs with new or updated code injection scripts.

Cybercrime for sale

The Limbo trojan was particularly interesting because it was being sold as made-to-order, including technical support and customization. Interpol was alerted while investigations continued into the hacking forums where Limbo and other made-to-order trojans, exploits, DDoS services and bot-net rental services are being sold.

For example, you can buy Limbo for \$600, and that includes customization and tech support. Renting DDoS attacks to crash a targeted server costs \$10 to \$20 for a one hour attack, \$20 to \$40 for two hours, and \$100 for an entire day. A 10-minute free evaluation attack prior to purchase is offered. This makes it easy for any person with moderate computer skills to engage in computer fraud.

Overwhelming volume

In order for hackers to maintain a strategic advantage over AV labs, the “business model” they employ is to generate such a high volume of new and unique malware samples that it overwhelms the labs.

In fact, we received 60,000 new and unique samples in May alone. This is a staggering number for any lab to manually process. In 2006, the lab saw more malware samples than in the previous 15 years combined.

The Limbo trojan was particularly interesting because it was being sold as made-to-order, including technical support and customization for \$600.

The steps an AV lab has to take to process samples of code received are as follow: First, reverse engineer and study the sample to determine if it is goodware or badware. Then, once it is determined that the sample is badware, it is necessary to create the disinfection routine and publish it to a signature file. This process can take anywhere from two to eight hours per sample, depending on complexity of the sample.

Obviously the manpower requirements to process 1500 to 2000 samples a day are enormous. Due to this, traditional AV labs are only able to handle a percent of the samples they receive each day and a large volume of code is left with no signature files.

Automation of collection and analysis of malware samples can reduce manual tasks by 95 percent resulting in a signature file data base of over a million samples of malware while traditional labs using manual methods are only able to capture an average range of 250,000 to 500,000 samples. The trend of the future will be for more automation if AV labs are to keep up with the current threat levels.

About the Author

Ryan Sherstobitoff is the Product Technology Officer at Panda Security USA (www.usa.pandasecurity.com). Ryan lectures across the USA on cybercrime trends as well as corporate risk assessments. He can be reached at ryans@pandasecurity.com.