

# Targeted Financial Attacks

By Ryan Sherstobitoff

Malware writers continue to find new and inventive ways to infiltrate computer networks and elude traditional perimeter security systems. Over the last year attention has been directed towards threats focused on specific targets. In other words, the characteristics of malware are changing from what we were familiar with to involving a more sophisticated approach that is not easily stopped.

What was once only an annoyance has morphed into a major money-making global enterprise involving hundreds of billions of dollars!

In the old days malware was designed to spread rapidly through an organization's network and with a variety of effects from damaging data to causing an internal distributed denial of service (DDoS) with multiple compromised systems (usually infected with a Trojan) being used to target a single system. All a security professional had to do was up-date patches or close specific ports related to the attack in order to prevent the further spread.

This is simply not the way malware operates anymore, which is why the epidemic seems to have disappeared altogether. That is far from the case: there is a new breed of malware designed specifically with economical and financial gain in mind. No loud, massive epidemics associated with this new type of malware – a majority of the malware infect users silently, without their knowledge.

For example there is a high volume of banker Trojans currently affecting consumers abroad using a wide range of techniques to capture confidential information such as pin numbers and other data. This information is then used illegally in several ways: credit card scams, printing fake ATM cards, purchasing goods with stolen credit cards and then reselling at discounted prices, and a host of other scams.

These Trojans are designed to work with the authentication mechanisms incorporated by the bank. For example, a number of these Trojans inject non-existent fields into the live banking session to capture additional information that the bank normally would not ask for. There are even some cases of Trojans hi-jacking transaction sessions in real-time and sending funds to accounts other than originally intended. While this all may seem like a bleak outlook in regards to the



Figure 1 – Security authentication used by banks

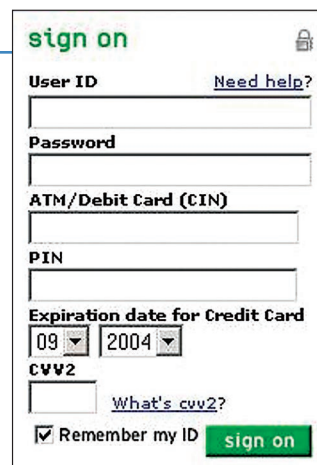


Figure 2 – Trojan injects additional fields

current state of affairs, it happens to be the reality we live in today.

So, you may be asking at this point how wide spread this problem really is. The fact is over 50% of our detections within PandaLabs are related to Trojans of some form (mostly banker Trojans) designed to steal confidential information. Furthermore, according to a research study recently conducted here at the labs, between May and July 2007 on a sample population of 1.5 million consumer PCs, it was found that out of sample set with up-to-date enabled protection, the population had a 22% infection rate of active malware currently in memory.

And the corporate side had a whopping 72% infection rate. This statistic was derived out of a population of 2000+ companies that participated in an online audit with Malware Radar.<sup>1</sup> One can conclude that computers are becoming more infected then ever with virtually undetectable malware designed with completely different motives than the days of the Melissa Virus or Code Red.

We must look at the current challenges facing security professionals today in terms of defending against this new breed. One major challenge for banking professionals is protecting consumers from on-line fraud. This is particularly difficult, especially when current tools provide only a limited insight into the new malware landscape. As it is banks usually get information regarding phishing and Trojan sites many hours after the consumers have become infected and some volume of information has been stolen. Your defenses are only as good as the knowledge you have regarding threats that affect you.

1 www.malwareradar.com

These banking Trojans have evolved well beyond simple key-logging. They are now being designed to adapt to the processes involved in providing access to the user. This is mainly performed through extremely sophisticated HTML injection techniques that intelligently inject seemingly genuine form fields into webpages during the transaction session. In January 2007 a banker Trojan known as Limbo was detected which incorporated HTML injection for specific banks. What made this particular Trojan especially malicious was the botnet capabilities it had incorporated for remotely updating the infected PCs with new information concerning injection into the online banking session. This was important in terms of effectiveness against consumers.

The banking industry is in dire need of technologies capable of detecting and preventing the fraudulent activity associated with banker Trojans without constantly investing money in developing authentication and other security mechanisms to fool the Trojans.

### **About the Author**

*Ryan Sherstobitoff is the Product Technology Officer at Panda Security USA ([www.usa.pandasecurity.com](http://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](mailto:ryans@pandasecurity.com).*