



Prevention TIPS

Cybercriminals Target Online Banking Customers Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution

BACKGROUND

In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution. Close to £675,000 (about \$1,000,000 in U.S. dollars) was stolen from the bank between July 5 and Aug. 4, 2010, and approximately 3,000 customer accounts were compromised.

It appears these cybercriminals used a combination of the new Zeus v3 Trojan and exploit toolkits to successfully avoid anti-fraud systems while robbing bank accounts.

This indicates a new level of technical sophistication and signals the continuation of a cybercrime trend that has evolved. Zeus has become one of the most popular Trojans used by cybercriminals. Today, the latest iteration, Zeus v3, not only acts as a data collector -- it also performs illegal online banking transactions.

The Zeus v3, copies the passwords and usernames of customers' online details and transfers their funds to a different account. It then gives the victim of the virus a false bank balance screen so they are unaware the cash has been taken.

THE ATTACK

Multiple techniques were used to spread malicious code to as many systems as possible within the UK with the ultimate goal of targeting online customers of a specific bank. These techniques included:

- Infecting legitimate websites with malware. Consumer visits to these infected websites resulted in their own computer becoming infected.
- Creating fraudulent online advertisement websites where cybercriminals collect consumer information as they click through the site.
- Publishing malicious advertisements amongst legitimate websites where cybercriminals collect consumer information.

The cybercriminals used the Eleonore Exploit Kit and the Phoenix Exploit Kit, both of which are notorious for efficiently exploiting victim's browsers, to install Trojans onto their PCs. Once the Zeus v3 Trojan was successfully installed on victims' PCs and after the victims logged into their online bank accounts, the Trojan initiated the money transfer from their accounts, via money mules, to the cyber-thieves. So using these various techniques, the Trojan remained under the radar of common anti-fraud detection systems.

Money mule accounts are legitimate banking accounts controlled by valid bank users who transfer stolen money from one country to another to muddle the cybercrime trail. These users are typically unsuspecting middlemen, but could be a part of the scam. Money mules aren't aware that the money they deliver to cybercriminals is stolen from compromised bank accounts. Cybercriminals recruit

Continue next page



Prevention TIPS

money mules by posing as legitimate companies that hire them as employees. They ask their “employees” to transfer received money from their bank account to a different account which is related to the fraudulent company. And they do not use non-banking transactions, such as Western Union, to transfer money. To avoid warning signs by anti-fraud systems, the money mule accounts are only used a few times within a certain timeframe. Since banks monitor large transfers, the amount of money deposited in a money mule account is predefined in an effort to elude detection.

CONCLUSION

Because cybercrime is a lucrative business, illegal operations such as the one discussed are on the rise. These criminals continuously seek new, sophisticated ways to steal information and money without detection. And it's increasingly difficult for security companies to stay ahead of the proliferation of new, dynamic malware.

What can you do? All financial institutions are a target, but credit unions are especially vulnerable because of their restrained resources, and their culture to serve their members. If you are concerned that your credit union could be at risk, then Southeast Corporate's MemberGuard services can help. MemberGuard can assist you in making sure that your members' information is protected. To learn more, contact your Member Relationship Manager at (800) 342-0203.