New bank theft software hits three continents: researchers

Joseph Menn, Reuters

(Reuters) - A new wave of automated hacking of online bank accounts might have stolen $78 million in the past year from customers in Europe, Latin America and the United States, according to researchers who peered into the computers of the hacking gangs.

The groups used recent improvements to two families of existing malicious software, known as Zeus and SpyEye, which lodged on the computers of clients at 60 banks.

While previous versions of the software have proved adept at stealing logon information, the latest variants automate the subsequent transfer of funds to accounts controlled by accomplices.

The findings, to be released on Tuesday by security firms McAfee and Guardian Analytics, confirmed and expanded on research from Japan-based Trend Micro Inc that was first reported last week by Reuters.

"This looks like the beginning of a new technique," said Guardian's Vice President Craig Priess, whose firm specializes in protecting banks.

The software is sophisticated enough to defeat "chip and PIN" and other two-factor authentication and to avoid transferring the entire contents of an account at one time, which can trigger review, according to the study.

Trend Micro said it had seen the automated versions in action in Germany, the United Kingdom and Italy.

Guardian and Intel Corp-owned McAfee said the same technology, while still emerging, had been used by a dozen gangs against consumers and business clients of financial institutions in those countries and Colombia, the Netherlands, and the United States.

"Someone designing this system has insider knowledge as to what the banks are looking for," said Dave Marcus, research director at Mcafee Labs.

Server logs viewed by the researchers saw commands from the fraud rings to transfer a total of $78 million, including $130,000 from one account. The banks may have been able to block some of those transactions, the researchers acknowledged.

MONEY MULES

Though written and controlled by different groups, SpyEye and Zeus share the ability to be installed on computers that visit malicious websites or legitimate pages that have been compromised by hackers, as well as through tainted links in emails.

The programs already have used a technique called "web injection" to generate new entry fields when victims log on to any number of banks or other sensitive websites. Instead of seeing a bank ask for an account number and password, for example, a victimized user sees requests for both of those and an ATM card number. All that information is sent to the hacker, who signs in and transfers money to an accomplice's account.

Those transfers can be time-consuming, and the hacker has to consider how much can be sent at once without drawing attention. Multiple, smaller transfers are preferable but take more time.

For the past year or more, some variants have also captured one-time passwords, such as those sent from the banks by text messages to client cell phones as an added security measure. But a hacker had to be online within 30 or 60 seconds in order to use the one-time password.

The new software allows the criminal to siphon money out at all hours, potentially increasing the number of hacked accounts and the speed with which they are drained.

Brett Stone-Gross, a senior security researcher with Dell Inc unit Dell SecureWorks, said previously that the main limiting factor for crime groups is the number of accomplices, known as money mules, that they can hire to accept transfers from victim accounts. Automation will not lessen the need for mules, Stone-Gross said.

Trend Micro spoke online with sellers of the automated transfer modules who were based in Russia, Ukraine and Romania, where arrests and prosecutions are rare. It said the new software costs between $300 and $4,000.

Banks generally compensate individuals in full for such losses if they are detected quickly. But recent versions of SpyEye and Zeus can present fake account balances to individual bank customers, so they might not realize their savings are being drained until too late.