Cybercriminals use Trojans and Money Mules to Loot Online Bank Accounts

In its latest Cybercrime Intelligence Report, Finjan shows how cybercrooks used a combination of Trojans and money mules to successfully avoid anti-fraud systems to steal Euro 300,000 in 22 days

San Jose, CA, USA, September 30, 2009 – Finjan Inc., a leader in secure web gateway products and the provider of a unified web security solution for the enterprise market, today unveiled new research from its Malicious Code Research Center (MCRC), which uncovered new techniques used by cybercriminals to rob online bank accounts.

Finjan sees the techniques described in this report as the start of a new trend that is expected to grow. These techniques add functionality aimed to minimize detection by traditional anti-fraud technologies in use by banks. More than a year ago Finjan identified the Zeus bank Trojan which today has become one of the most popular Trojans used by cybercriminals to steal money from banks' customers worldwide.

In its Cybercrime Intelligence Report, Finjan's Malicious Code Research Center (MCRC) shows how a cybergang used a combination of Trojans and money mules to rake in hundreds of thousands of Euros and to minimize detection by the anti-fraud systems used by banks.

The cybercriminals used compromised legitimate websites as well as fake websites, utilizing the crimeware toolkit LuckySpoilt to infect visitors. After infection a bank Trojan was installed on the victims' machines and started communication with its Command & Control (C&C) server for instructions. These instructions included the amount to be stolen from specific bank accounts and to which money mule accounts the stolen money should be transferred. Furthermore, the Trojan forged onscreen bank statements concealing the true transaction amount to dupe the account holders and their banks.

The cybercrime intelligence report covers the following:

· Cybercriminals use sophisticated crimeware tools to steal money online and avoid detection
· They use compromised legitimate websites as well as fake ones to infect visitors with their crime toolkit
· Once infected, the Trojans get instructions from its Command &Control center to rob bank accounts
· Instructions include criteria for the amount that should be stolen from an individual account
· This method is a highly-effective, "Anti anti-fraud" system detection tool
· Once the money is stolen, the Trojan creates a forged bank statement to hide the theft
· The stolen money is transferred to a money mule account and then forwarded to the cybercrooks to prevent any direct money trail
· The cybergang was able to steal Euro 300,000 in 22 days

"As reported previously by Finjan, cybercriminals continue to follow the money, with bank accounts steadily remaining a favourite among their targets. To avoid detection, cybercriminals continue to improve their methodologies for stealing money and going under

the radar from the victims and banks alike. With the combination of using sophisticated Trojans for the theft and money mules to transfer stolen money to their accounts, they minimize their chances of being detected," said Yuval Ben-Itzhak, CTO of Finjan. "In this case, the specific criteria that the Trojan received from its Command & Control center mark a whole new level of cybercrime sophistication in the techniques used by cybercriminals. Using these methods they successfully evade anti-fraud systems that banks deploy – we dubbed it the **Anti** anti-fraud."

The report shows in detail how this cybergang worked and provides recommendations how individuals and banks can protect themselves.

To download the report, please go to www.finjan.com/cybercrime_intelligence

Money mule accounts are legitimate bank accounts owned by legitimate bank users. Cybercriminals hire 'mules' by falsely telling them they are working for a legitimate business. These bank account owners or "mules" are normally unaware that they are "muling" stolen money, but think that they are being paid for "working from home" and other moneymaking schemes. To avoid warning signs by anti-fraud systems at the bank, the money mule accounts are only used for a limited number of times within a certain timeframe. Since banks monitor large bank transfers, the amount of money deposited in a money mule account is predefined in order to stay under the radar.

About MCRC

Finjan MCRC specializes in the detection, analysis and research of web threats, including Crimeware, Web 2.0 attacks, Trojans and other forms of malware. Our goal is to be steps ahead of hackers and cybercriminals, who are attempting to exploit flaws in computer platforms and applications for their profit. In order to protect our customers from the next Crimeware wave and emerging malware and attack vectors, Finjan MCRC is a driving force behind the development of Finjan's next generation of security technologies used in our unified **Secure Web Gateway** solutions. For more information please also visit our **info center** and **blog**.

About Finjan

Secure Gateway provides organizations with a unified web security solution combining productivity, liability and bandwidth control via URL categorization, content caching and applications control technologies. Crimeware, malware and data leakage are proactively prevented via patented active real-time content inspection technologies and optional anti-virus modules. Powerful central management enables intuitive task-based policy management, excellent drill-down reporting capabilities and easy directory integration for all network implementation options. By integrating several security engines in a single dedicated appliance, Finjan's comprehensive and integrated web security solution enables quick deployment, simplified management and reduction of costs. Business benefits include real-time web security (no patches or updates needed), lower total cost of ownership (TCO), cost savings in administration efforts, lower maintenance costs, and reduction in loss of productivity. Finjan's security solutions have received industry awards and recognition from leading analyst houses and publications, including Gartner, IDC, Butler Group, SC Magazine, eWEEK, CRN, ITPro, PCPro, ITWeek, Network Computing, and Information Security. With Finjan's award-winning and widely used solutions, businesses can focus on implementing web strategies to realize their full organizational and commercial potential. For more information about Finjan, please visit: www.finjan.com.