Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

SECURITY THREATS LOOM OVER ONLINE BANKING

Banks and other financial institutions go online to improve their services and to reach out to their ever-growing base of Internet-savvy customers. Unfortunately, cybercriminals are also targeting this platform to further their malicious profiteering schemes. The challenge is to impose security measures that can counter evolving attacks and educate users on their responsibilities when banking online.

The banking sector is one of the industries that maximizes the use of the Internet for business. With a growing number of customers going online, banks naturally began offering services and products that appealed to their technologically savvy clientele.

One of the reasons for online banking's appeal is the convenience it offers.

Online or electronic banking poses benefits that traditional methods do not. One of the reasons for online banking's appeal is the convenience it offers. Customers also save time and effort since they can get the information they need via the Internet.

The other side of the story, however, presents serious problems to both customers and the banking industry. As expected, this emerging trend did not escape cybercriminals' prying eyes. Reports of unauthorized account transfers and stolen login credentials made the news in the past, raising serious questions about online banking's security.

Online Banking Poses Security Risks

Operating as early as 2007, the ZBOT Trojan was designed to steal online account information. It has been found to have infected around 74,000 systems worldwide.

ZBOT variants may also be downloaded by BREDOLAB malware, a simple downloading platform that creates a host of infected machines. What is interesting to note is that these botnets operate behind a complicated money-making scheme. Trend Micro senior advanced threats researcher Loucif Kharouni highlights that the botnet business model rests on each botnet's unique functionality, which in the end, benefits the creators of both variants.

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Mules are sometimes unwittingly recruited via online job postings or ads promising easy money or may be willing cybercrime accomplices themselves.

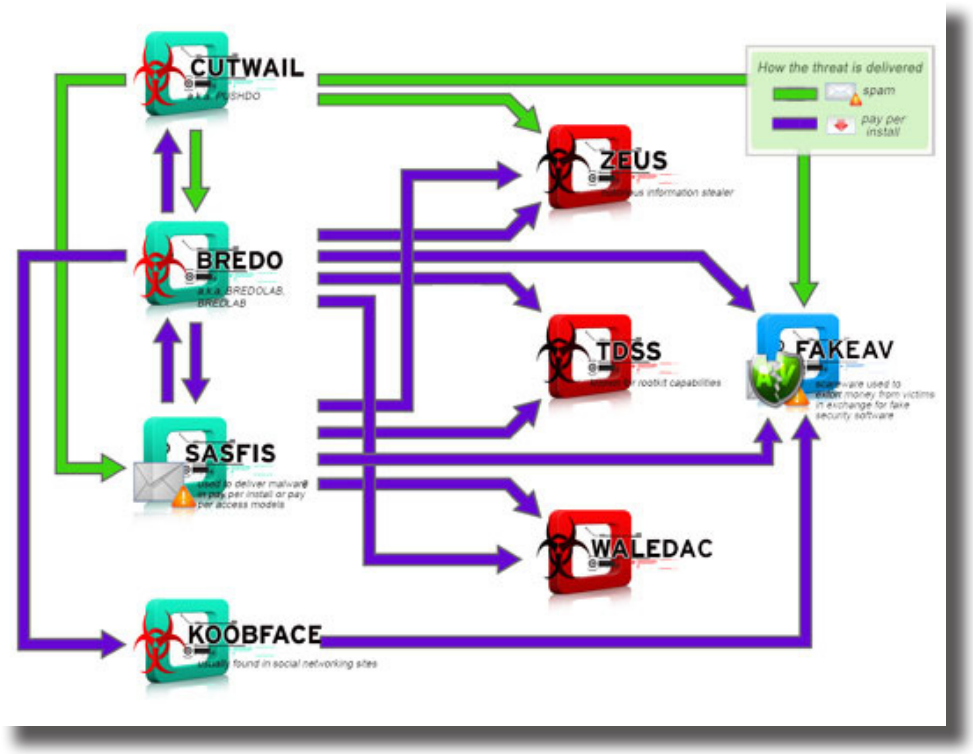

Figure 1. *The botnet business model*

After stealing crucial information from users, cybercriminals initiate small but unauthorized money transfers to spoofed accounts of transfer agents or so-called money mules. Eventually, the amounts transferred will increase. The mules are then instructed to send the funds to a foreign country via service providers like MoneyGram. Mules are sometimes unwittingly recruited via online job postings or ads promising easy money or may be willing cybercrime accomplices themselves.

TREND MICRO

Money-mule scam victims are often small businesses, as their owners usually had no clue about the threats they face or the liability they assume when conducting online banking transactions.

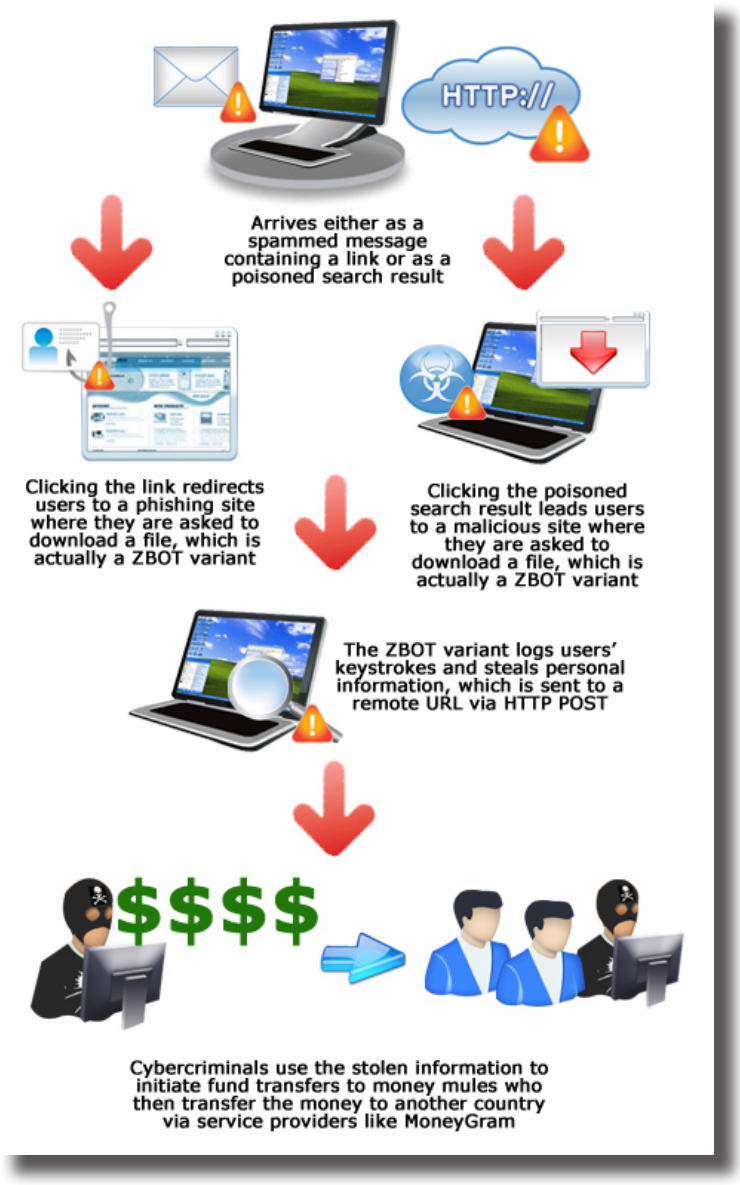

Figure 2. *Typical ZBOT infection diagram*

Security journalist Brian Krebs also reported that money-mule scam victims are often small businesses, as their owners usually had no clue about the threats they face or the liability they assume when conducting online banking transactions.

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Uncovering the Tequila Botnet

Trend Micro engineer Juan Castro recently discovered another botnet targeting Latin America, specifically Mexico. Dubbed the "Tequila botnet," this botnet steals banking-/financial-related data from people who may be tricked into clicking the phishing link. This may be particularly harmful to those in Latin America, which coincidentally boasts of a growing population of Internet users.

Based on Trend Micro senior threat researcher Ranieri Romera's analysis, the Tequila botnet infection chain starts once users click *http://www.knijo.{BLOCKED}0.net/fotografias-al-desnudo-de-la-mama-de-paulette.htm,* which supposedly contains an article on Paulette Gebara Farah's death and nude photos of her mother. When accessed, a fake dialog box pops up and requests the user to download and execute a supposed *Adobe Flash Player* installer. The users are then asked to download a malicious video file named *video-de-la-mama-de-paulette.exe* detected by Trend Micro as TSPY_MEXBANK.A.

Ranieri Romera found that the Tequila botnet:

- Has a comprehensive feature set that is comparable with more established botnet families
- Has a pharming module that lists the entities it targets, which includes *PayPal's* Mexican site and Bancomer
- Can download files from other malicious sites using either HTTP or FTP
- Has an *AdSense* module that allows a site to be repeatedly loaded along with that site's ads
- Has components that may arrive via USB devices as well as via *MSN Messenger*

Romera was able to access the Tequila botnet's command-and-control (C&C) interface to learn more about its management functions and found that:

- It has a comprehensive feature set that is comparable with more established botnet families. Each feature has its own "module," which the botnet herder can configure.
- The botnet's pharming module lists the entities it targets, which includes *PayPal's* Mexican site and Bancomer.
- It can also download files from other malicious sites using either HTTP or FTP. It also drops other notorious malware like ZBOT and FAKEAV variants.
- It has an *AdSense* module that allows a site to be repeatedly loaded along with that site's ads. Cybercriminals use this to boost traffic to their own sites, which in turn, also increases the payments made by advertising networks such as Google's *AdSense.*
- It may also arrive via USB devices as well as via *MSN Messenger.* It sends messages that either contain a file attachment or a link leading to the site where the malware can be downloaded.

Days after the botnet's proxy servers and redirected hosts were exposed, its controllers stopped all of their phishing attacks. The same people behind the attack later developed the Mariachi botnet. However, both went offline eventually after their C&C servers were taken down.

Security Challenges for a Promising Platform

Despite efforts to mitigate the problem, attacks targeting online banking remain persistent. Perpetrators cleverly employ new techniques to bypass the security measures banks impose. There have been reports of malware capable of bypassing digital tokens. It installs messaging codes onto systems that immediately send the encoded token to hackers who can use it while holding off legitimate login connections.

TREND MICRO

In this year's "RSA Conference," security experts also noted the challenges posed by ZBOT variants and other banking-related malware. *PayPal's* Michael Barrett believes that cybercriminals have a knack of making fraudulent transactions appear as if they were initiated by an end user or legitimate. Banks are also having difficulties finding the middle ground between persuading users to stay secure while enjoying the convenience online banking offers.

User Vigilance Is Part of the Equation

The battle to ensure more secure online transactions does not end with bank efforts alone. Users should also take simple but effective steps so as not to fall into cybercriminals' traps.

The battle to ensure more secure online transactions does not end with bank efforts alone. Users should also take simple but effective steps so as not to fall into cybercriminals' traps. Using a laptop exclusively for electronic banking is a good option, especially for businesses. Familiarity with a bank's official site and interface can also help consumers determine if they are really logging in to the correct site. Consumers must also avoid clicking unknown links in instant or spammed messages. If possible, coordinate with banks to customize security settings, depending on one's business needs. Installing a comprehensive security solution that blocks malicious sites and that deletes related spyware is a must to significantly decrease one's chance of being infected.

These precautions may not be new but following them can go a long way, particularly in maximizing what the promising online banking platform can offer.

References:

- Asher Hawkins. (November 16, 2009). *Forbes.com.* "Is Your Online Bank Account Safe?" http://us.trendmicro.com/us/think-again/articles/article-online-bank-account/?cm_re=LowerLinks-_-Articles-_-Is+Your+Online+Bank+Account+Safe&cm_sp=Think+Again-_-Articles-_-Is+Your+Online+Bank+Account+Safe (Retrieved June 2010).
- Brian Krebs. (March 16, 2010). *Krebs on Security.* "eBanking Victim? Take a Number." http://krebsonsecurity.com/2010/03/ebanking-victim-take-a-number/ (Retrieved June 2010).
- David Sancho. (October 2009). *TrendWatch.* "You Scratch My Back... BREDOLAB's Sudden Rise in Prominence." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/bredolab_final.pdf (Retrieved June 2010).
- *EFYTimes.com.* (2010). "Online Banking: Benefits and Safety Tips." http://www.efytimes.com/e1/creativenews.asp?edid=46080 (Retrieved June 2010).
- Elinor Mills. (February 17, 2010). *CNET News.* "ZeuS Trojan Found on 74,000 PCs in Global Botnet." http://news.cnet.com/8301-27080_3-10455525-245.html (Retrieved June 2010).
- Federal Deposit Insurance Corporation. (October 29, 2009). *FDIC.* "Fraudulent Work-at-Home Funds Transfer Agent Schemes." http://www.fdic.gov/news/news/specialalert/2009/sa09185.html (Retrieved June 2010).

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

- Finweb.com (2010). *Financial Web.* "Online Banking—Advantages and Disadvantages." http://www.finweb.com/banking-credit/online-banking-advantages-and-disadvantages.html (Retrieved June 2010).
- Linda McGlasson. (November 2, 2009). *Bank Info Security.* "Money-Mule Schemes: How to Protect Customers." http://www.bankinfosecurity.com/articles.php?art_id=1899 (Retrieved June 2010).
- Loucif Kharouni. (April 8, 2010). *TrendLabs Malware Blog.* "Spotlighting the Botnet Business Model." http://blog.trendmicro.com/spotlighting-the-botnet-business-model/ (Retrieved June 2010).
- Marcia Savage. (March 3, 2010). *SearchFinancialSecurity.com.* "RSA Panel: No Easy Solution for ZeuS Trojan, Banking Malware." http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1407907,00.html (Retrieved June 2010).
- Ranieri Romera. (June 9, 2010). *TrendLabs Malware Blog.* "Bye, Bye Tequila Botnet." http://blog.trendmicro.com/bye-bye-tequila-botnet/ (Retrieved June 2010).
- Ranieri Romera. (June 2, 2010). *TrendLabs Malware Blog.* "'Tequila Botnet' Targets Mexican Users." http://blog.trendmicro.com/tequila-botnet-targets-mexican-users/ (Retrieved June 2010).
- Sarah Radwanick. (June 17, 2010). *comScore.* "Latin America—A Story of Growth." http://blog.comscore.com/2010/06/latin_america_growth.html (Retrieved June 2010).
- Threat Research Team. (March 2010). *TrendWatch.* "ZeuS: A Persistent Criminal Enterprise." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf (Retrieved June 2010).
- Trend Micro Incorporated. (2010). *Threat Encyclopedia.* "TSPY_MEXBANK.A." http://threatinfo.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_MEXBANK.A (Retrieved June 2010).

TREND MICRO