Informational Articles Regarding Online Fraud

NEWS RELEASE

Trusteer Warns That Zeus Trojan Bypasses Up-to-Date Anti-Virus Systems 77 Percent of the Time Online Banking Malware Eludes Detection and Infects More than Two Thirds of Machines

NEW YORK, Sep. 16, 2009 - Trusteer, the customer protection company for online businesses, reported today that the Zeus online banking Trojan infects machines that are running up-to-date anti-virus programs up to 77 percent of the time. These findings are based on a sample of more than 10,000 users of the Rapport browser security service, whose machines were infected with the Zeus Trojan.
Zeus, which is also known as Zbot, WSNPOEM, NTOS and PRG, is the most prevalent financial malware on the Internet today. It infects consumer PCs, waits for the user to log onto a list of targeted banks and financial institutions, and then steals their credentials which are sent to a remote server in real time. It can also modify, in a user's browser, the genuine web pages from a bank's web servers to ask for personal information such as payment card number and PIN, one time passwords, etc.

The report released today by Trusteer found that the majority of Zeus infections occur on machines which have an installed and up-to-date anti-virus product. Specifically, Trusteer found that among Zeus infected machines:

- 31% had no Antivirus protection installed
- 14% had Antivirus protection installed, but signatures files were not up to date
- 55% had up-to-date Antivirus protection installed

The full report is available at http://www.trusteer.com/files/Zeus_and_Antivirus.pdf
"When we set out to measure the efficiency of antivirus products in the wild against Zeus, we had no idea what kind of results we would get," said Amit Klein, CTO of Trusteer and head of the company's research organization. "The findings, that up-to-date anti-virus programs were only effective at blocking Zeus infections 23 percent of the time, are disturbing. This is bad news for consumers and banks, since the vast majority of Zeus infections are going unnoticed."

About Rapport
Rapport from Trusteer is a lightweight browser plug-in plus security service that acts like a vault inside the browser and prevents redirection of user information to fraudulent websites. It protects personally identifiable information (PII) and Web pages from unauthorized access and theft while users are accessing sensitive Web sites. Trusteer also offers in-the-cloud reporting services where unauthorized access attempts detected by Rapport are analyzed by fraud experts who provide actionable intelligence to financial institutions.

About Trusteer
Trusteer enables online businesses to secure communications with their customers over the Internet and protect PII from a user's keyboard into the company's Web site. Trusteer's flagship product, Rapport, allows online banks, brokerages, healthcare providers, and retailers to protect their customers from identity theft and financial fraud. Unlike conventional approaches to Web security, Rapport protects users' PII even if their computer is infected with malware including Trojans and keyloggers, or is victimized by pharming or phishing attacks. Trusteer is a privately held corporation led by former executives from Cyota/RSA Security, Imperva, and NetScreen/Juniper. For more information visit www.trusteer.com.

The WSNPOEM malware – an exercise in non standard credential grabbing techniques

Recently we investigated a malware encountered in the wild. It turned out to be a recently released variant of the Banker/InfoStealer/Bancos/Zbot family (identified as PWS-Banker.gen.bw by McAfee, as Infostealer.Banker.C by Symantec, as Trojan-Spy.Win32.Bancos.aam by Kaspersky and as Mal/Zbot-A by Sophos). Initial analysis indicated that this is a descendent of the malware analyzed by SecureScience and Michael Ligh (http://ip.securescience.net/advisories/pubMalwareCaseStudy.pdf) – in fact, quite possibly a variant of the new strand identified in section 18 of that paper. The paper proved to be very useful, especially the description of how to decrypt the malware collected data.

The malware we analyzed displayed two interesting techniques for credential collection, which are not common among malwares:

- WinInet interception
- In-process key-logging

WinInet interception – as explained in the above mentioned paper, the malware makes sure it is injected into practically all user space processes. When the malware copy detects that it is injected into an Internet Explorer process, the malware appears to modify IAT entries for the HttpSendRequest family of functions within that process. As such, each time Internet Explorer requests a URL, it eventually calls HttpSendRequest, and control is transferred to the malware code. The malware collects POST request data (the POST request body, which contains credentials in case of a login submission) and periodically sends it (encrypted) via its own HTTP request to a drop site.
This is in contrast to many flavors of malware which install themselves as an Internet Explorer add-on (BHO), and intercept credential submission by subscribing to the submit/navigate event.

In-process keylogging – (this is not explicitly mentioned in the paper, and may possibly indicate that it is a later addition) it appears that the malware code inside an Internet Explorer process also patches the GetMessage/PeekMessage family of functions. This enables the malware to monitor all incoming messages into Internet Explorer. Particularly, it seems that the malware code logs keystrokes in this manner. The keystrokes are added to a 100 byte buffer. Each periodic transmission to the drop site contains the current contents of this buffer. This is in contrast to “traditional” key-logging using the GetAsyncKeyState and similar functions, and the Windows hooks methods.
The obvious question is why does this malware employ non-standard techniques? We suggest two answers:

- Enhanced stealth: by not using a BHO (which is visible through Internet Explorer’s Tools->Manage Add Ons GUI), the malware is less detectable by the user. Using a BHO also incurs having a malware DLL permanently on disk, which makes the malware more vulnerable to anti-malware products. Likewise, by using non-standard keylogging techniques, the malware can avoid detection by anti-spyware/malware products that monitor attempts to use the traditional keylogging techniques. And just like a BHO, traditional anti-keylogging techniques require a DLL (or a process) to be permanently available.
- Enhanced usability: unlike traditional key-logging techniques, an in-process (or more precisely, an in-Internet Explorer) key-logger can easily and accurately determine which keystrokes belong to the browser. It is not impossible to obtain this information in traditional key-logging methods, yet it is more complicated and less reliable than the in-process technique.

Bank Info Security

Fraud Update: The 13 Hottest Schemes You Need to Prevent

From Credit Bust-Out to In-Session Phishing, Fraudsters Are Finding New Ways to Ply Old Tricks

May 26, 2009 - Linda McGlasson, Managing Editor

The fraud fight is getting nastier by the minute, say experts familiar with the new schemes - and some old ones with new wrinkles -- being perpetrated by criminals against financial institutions and their customers. Here are 13 of the most prevalent ruses.

#1 -- Credit Bust-Out Schemes
By definition, credit bust-out schemes are a combination of a credit and fraud problem, although many organizations are not always sure where the losses sit - or who might be the party responsible. How it works: According to Michael Smith, manager of the Fraud and Market Planning division at Lexis Nexis, consumers apply for credit from lenders using similar last names, oftentimes Eastern European or Balkan, in an intentional effort to capture financial access vehicles to cause delinquency.

What makes credit bust-outs especially difficult to prevent is that many of the applications have consumers with low credit risk ratings, "so these people tend to look relatively good from the start," Smith explains. These individuals make good payments on time, ask to increase their credit line and seem legitimate, however throughout the entire process they are thinking about how much money they can get from this bank before they 'bust out' and go delinquent.

The length of the fraud usually falls between six and 18 months. "This fraud is one of the biggest reasons bank are writing off losses," Smith argues. It is the most problematic and emerging issue with fraud today -- "even more so than true-name identity fraud, and is an issue that has increasingly hampered the industry over the past few years and one that is arduous to prevent, detect, and quantify," Smith says.

#2 -- Customer Loan Account Takeover
This type of fraud occurs online, and a recent case study related by Avivah Litan, distinguished analyst at Gartner Group illustrates how customer loan account takeover happens. The case resulted in a $71,000 theft from a customer's loan account.

An online loan Web site gave a customer the ability to open demand deposit accounts (DDA), Litan explains, which were to be held as savings accounts that could only be opened and accessed via the Internet. "To open the account through the online loan application, a customer needed an existing relationship with another bank," Litan says. The customer would provide all the account information necessary for both banks to complete ACH transfers.

Prior to opening the account, the online loan application system would complete two test transactions and require the potential customer to confirm the exact dates and amounts of the transactions. "If the customer could not provide that confirmation, then it was thought to be attempted fraud, and the account relationships would be closed."

Once accounts were opened, a customer was able to transfer funds between the two accounts via ACH transfers. Fraud in this account was able to take place because, after the initial account was opened and deposits were made, the customer was allowed to change the external bank account and continue to transfer funds.

Although the online loan system could verify control of external accounts, actual account ownership could not be confirmed. "The thief took advantage of this by taking over the customer's account and changing the external account it was linked to, even though the names of the account owners at the external financial institutions were no longer the same," Litan says. The crook was able to do this by using various ploys across customer channels. The criminal also compromised other accounts at the loan company, as was later determined by examining IP addresses that were accessing various accounts.

#3 -- Corporate Account Takeovers

Corporate account takeovers are becoming more prevalent says Gartner's Litan. "Corporate banks are reporting that criminals are targeting their cash management customers and moving money out of their accounts via innocent consumer accounts," she says. The owners fall for phishing e-mails that promise lucrative commissions for participating in the schemes.

How it happens: The crook starts by stealing user IDs and passwords of cash management account owners, and by signing up random consumers via phishing attacks, asking them to accept money into their accounts and then transferring it to the criminal's offshore account while retaining a 5 percent commission. "Of course, the crooks use clever social-engineering techniques in their phishing e-mails to get consumers to sign up," Litan explains. After the groundwork has been laid, the crook simply goes into the corporate cash management account and transfers funds, using ACH fund transfer facilities, out of the corporate account to the phished consumer accounts. "The rest is history, and the victimized corporate cash management banks generally fail to recover the stolen funds," Litan notes. Strong customer authentication, fraud detection and transaction verification can significantly, if not dramatically, reduce the threat and damage caused by these crimes.

#4 - Cross-Channel Call Center/Online CD Purchase Scam
A fraudster purchases multiple CDs online from one bank, funded by ACH Transfers from multiple compromised third-party accounts at other institutions, says Ori Eisen, former worldwide fraud director for American Express. How it happens: The perpetrator contacts the Call Center within 48 hours of the CD purchases to cancel the CDs and transfers the funds to yet another institution to liquidate. "Variable email addresses are used in an effort to mask identity," Eisen says. "Current procedures and safeguards at most financial institutions may not preclude the success of this type of cross-channel attack."

To resolve this threat, Eisen advises all accounts should be monitored for unknown device access, and accounts with new or unknown device access should be isolated and assigned an elevated risk score for monitoring. "The account access by an unknown device is best discerned utilizing device intelligence technology. Risk assessment based on velocity of activity seen coming from one unique device is a key metric to monitor," he explains. Eisen advises all financial institutions search for similar activity of online CD account opening and cancellation via the call center.

#5 -- Wire Fraud Account Grooming
Financial institutions are exposed to very high levels of risk within their online wire transfer processes. "Traditional methods of detection are very labor intensive, yielding high false positive rates and low recovery of stolen funds," Eisen says.

Existing tactics and systems in place to minimize wire fraud, such as account activity restrictions and transaction anomaly systems, have begun losing their effectiveness. "Investigators are often reviewing over 800 suspicious wire transfers for every one legitimate case of fraud," Eisen says. "With an extremely low recovery rate due to the speed at which the funds transfer, banks need something to identify accounts being groomed for wire fraud long before the wires were executed."

To identify potential account grooming for wire fraud, Eisen suggests link analysis should be used to find accounts where unfamiliar devices have accessed account administration settings and made changes; such as address or phone number updates. "These suspicious accounts, once identified, should be monitored (spanning the pre-existing account activity restriction periods) for repeat account activity by unfamiliar devices," he explains. A pattern will emerge providing a highly concentrated basis of accounts, each with a strong probability of potential fraud should a wire transfer be executed.

#6 -- In-Session Phishing
A somewhat recent tactic being perpetrated by fraud rings -- "in-session Phishing" -- has emerged as one of the chief threats to the breach of secured online assets. These attacks utilize vulnerabilities in the Javascript engine found in most of the leading browsers, including Internet Explorer, Firefox and even Google's Chrome, notes Eisen.

How it happens: Utilizing a host website that has been injected with malware acting as a parasite, this parasite monitors for visitors with open online banking sessions or similar protected asset sites (such as brokerage or retirement planning sites).

Using the Javascript vulnerability, the parasite can identify from which bank the victim has a session currently open by searching for specific sites pre-programmed in the malware itself. "There are no limits to

the volumes of URLs a website hosting the parasite can test from the victim's machine. The malware asks: 'is my victim logged onto this XYZ bank website' and their browser replies either yes or no," Eisen says.

Once any site from the list is confirmed to be "in session," a pop-up claiming to be from the bank issues a warning. Most warnings appear as time-out messages stating "For security purposes your banking session has been terminated. To continue your session please re-enter your username and password here (supplied link by fraudster)."

Once an unknowing victim complies, clicks the link and enters his/her credentials, the damage has been done and the attack was successful and the game is over - right?

In most cases it would be devastating for a victim after their credentials had been breached; expecting the fraud rings to quickly begin selling off this information or pillaging through the victim's account. Since many financial institutions rely on cookies or tags to discern one device entering user credentials from another, and then count on fairly common (and easily answered by crooks) out of wallet questions - to validate a new device attempting access, this would be true.

However, simply by utilizing a robust device ID technology - which creates the equivalent of a device fingerprint for every machine attempting to log on to a banks site, coupled with historical negative lists of known bad devices, "financial institutions could render credential breaches using in-session or any other type of phishing attack useless to the fraudster," Eisen says.

The power lies in knowing what a suspicious or fraudulent attempt looks like upon log-in. "If you know a legitimate customer most always uses a device configured for local New York time and the language for this device is English, you would not provide unchallenged access to this account from a machine showing to come from China and having a default language set to Mandarin," Eisen says.

Further strengthening against future attacks, placing the device fingerprints gleaned from all known previous fraudulent attempts into a negative list effectively blocks the devices with a history of fraud from ever gaining access to another user account.

#7 -- ATM Network Compromises
The industry is seeing breaches at all stages in the payment process, including merchant terminals, the communication links between merchant acquirers, and (worst of all) core elements in ATM networks, according to Paul Kocher, Cryptography Research Institute's president and chief scientist. "Once the perpetrators have the contents of magnetic stripes and the corresponding PINs, the data is then sold to people who write the data onto counterfeit cards and drain customers' accounts," Kocher observes. Because other fraud targets are strengthening their defenses while ATM networks remain a soft target, "we're expecting ATM fraud losses to grow rapidly, and eventually financial institutions will be forced to switch the ATM infrastructure to chip cards," he predicts.

#8 -- Precision Malware Strikes
The most common defenses against malicious programs work by comparing programs against the signatures of known malware, says CRI's Kocher. As a result, attackers have learned that they can breach high-value targets' computer systems relatively easily, provided that their attack software does not spread so widely that antivirus companies get a copy and add it to their databases. "Attackers clearly have their crosshairs aimed at individuals with non-public information about publicly traded companies, sensitive government data, and systems involved in processing payment transactions," Kocher states.

#9 -- PIN-Based Attacks
For the past 10 years, Verizon Business has tracked metrics and statistics from IT investigative cases, including incident response, computer forensic and litigation support, across the globe. The Verizon Business' just-issued 2009 Data Breach Investigation Report, shows more electronic records were breached in 2008 than the previous four years combined, fueled by a targeting of the financial services industry and a strong involvement of organized crime, says Bryan Sartin, director of forensics and investigative response at Verizon Business.

Driving this explosion in compromised records are more sophisticated attacks, specifically targeting the financial sector. In fact, 2008 saw three of the world's largest known data compromises on record.

With many large individual compromises over the past two years, the value of payment card, check, and other forms of consumer data on the information black market are on rapid decline, says Sartin. "Just two

years ago, magnetic-stripe sequences sufficient for counterfeit were priced at an average of $14 per record, while today that cost has dropped to as little as 20 cents," he says. "Cybercrime, it seems, chases the almighty dollar."

Last year showed a sharp increase in attacks against counterfeit sequences plus the corresponding cardholder PIN value, leading to the direct theft of consumer assets, Sartin notes. "The lead indicators of these types of crimes were not based on the conventional analysis of signature-based counterfeit fraud patterns to find common valid transaction points within legitimate spending histories. Instead, bank customers were suddenly reporting zero balances in checking and savings accounts, alleging fraudulent ATM withdrawals." As more and more similar complaints surface, it became easier to pinpoint the likely source of compromise, whether it be a bank, data processor, or payment gateway, Sartin says.

Verizon Business tracked at least three different techniques during 2008. Until recently, many PIN-based attacks were known to be possible but no credible evidence of them being used in real-world incident has ever surfaced. That has since changed as attacks against PIN information are on the rise, setting the stage for more sophisticated forms of identity fraud.

#10 -- Account Manipulation
Aside from the five or six massive individual compromises that took place across the globe in 2008 is a vastly larger population of data breaches, also targeting financials, that garnered little public attention, Sartin notes. "Much of these involve unusually small populations of compromised records, yet massive fraud in terms of total dollar losses, resulting in significant impacts to the institutions affected. By and large, these cases appear in two forms: insider manipulation and application manipulation," he says.

Insider manipulation involves organized crime groups infiltrating a target financial entity, not through a systems-based intrusion but via its personnel, Sartin explains. "Most commonly targeted are individuals within the vendors utilized by financial entities - those entrusted with legitimate access for remote support purposes," he says. These cases do not always involve vendors, in many cases actual employees are infiltrated, often increasing the capabilities of the fraudsters.

Application manipulation is somewhat different and involves moderately sophisticated application-based attack techniques. It is common that ATM processors, credit and debit card issuers, brokerages, etc, make Web-based portals available to customers for convenience purposes. It is similarly common that PINs, usernames and passwords, and other privileged account values can me modified online through these portals by the customer, Sartin observes. For the past year, Verizon Business has tracked a rapidly escalating trend "where organized crime groups are increasingly targeting these online application interfaces in attempt to identify weaknesses in the underlying code that can be exploited for the purposes of account manipulation and fraud," he says. In most cases, these code weaknesses are vulnerabilities that are previously unknown, are unique to that individual company, and cannot be identified through common security scanning tools. The perpetrators put a considerable amount of time and effort into testing for these exposures and then exploiting them, paving the way for very similar fraud impacts to that seen in insider manipulation.

#11 -- Fraud Pattern Changes
Fraud patterns changed dramatically in 2008 as a result of both reduced percentage of successful fraudulent transactions and arrest of individuals involved in organized fraud activity, says Verizon Business' Sartin. The new fraud patterns can be divided into two categories: random fraud patterns and global ATM transactions.

Random fraud patterns used by organized fraud groups involve similar purchases as seen prior to 2008, but in a random pattern. "In 20089, the fraudsters have adapted to completely random fraudulent purchases to make pattern identification much more difficult," he notes. The fraudsters began showing up at random stores in random time patterns to make identification of a pattern difficult or impossible. "No two purchases would be made at the same merchant location in a several month period. No pattern of purchases at each exit as a group drives up a highway. The purchases were at the same chain merchant stores of the same items, but now in a random pattern," he explains.

Global ATM transactions involve hundreds or thousands of ATM transactions occurring around the world in a very short period of time, similar to what happened in the RBS ATM theft of $9 million in November 2008 (http://www.bankinfosecurity.com/articles.php?art_id=1197). In previous years, organized ATM transaction fraud was not considered a major fraud concern due to the protection of PIN in these transactions. Recent frequency of data compromises involving PINs has increased the dollar losses associated with ATM fraud dramatically, leading to an increase in high dollar, high volume ATM fraud attacks. "These attacks require a

sophisticated organized group to perform hundreds or thousands of ATM transactions simultaneously at multiple locations around the world," Sartin notes. In several instances, these high volume attacks also involve account manipulation at the same time. "In these attacks, the fraudsters have obtained hundreds of thousands or millions of dollars before the attack is recognized and preventive measures can be enacted," he says.

#12 -- Foreclosure Prevention Schemes
This doesn't hit a financial institution directly, but if an institution holds mortgages for "troubled" homeowners, this is a scheme you need to be on the lookout for, says Denise James, market planning director Lexis Nexis' Residential Mortgage Solutions. These foreclosure prevention schemes generally involve fraudsters posing as professional, knowledgeable foreclosure specialists. Homeowners facing the threat of foreclosure and nearing eviction are contacted by these "foreclosure specialists" who promise to work out their loan problems or buy their home and offer the homeowners tenancy. "Unfortunately for the homeowner, the fraudster has no intention of following through with these promises and instead will manipulate the homeowner into deeding the property to them," James says.

Once the fraudster obtains the signed documents, a false lien release is generally filed or leveraged to secure funds from a fabricated sale or refinance on the property. In many cases, the homeowner is under the belief that they will rent the property for a period of time until they are in a better position to regain ownership rights, James notes. The fraudster continues to accept payments made by the homeowner while selling the property, absconding with the funds, and eventually evicting the homeowners. "Perpetrators of this type of fraud often move from town to town, sizing up their opportunities, quickly scamming as many homeowners as possible, inflicting costly damages, and then moving on to the next location," says Jennifer Butts, director of operations at the Mortgage Asset Research Institute.

#13 -- Builder Bail-Out Fraud
This fraud involves securing funds for condominium conversion or planned community development properties that, unbeknownst to the investor (financial institution), will not be completed, says Butts of the Mortgage Asset Research Institute. The scams entail multiple purchases from would-be investors or false identities on fabricated loan transactions. "Investors are lured by photos or inspections of a few converted units used as models with promises of further rehabilitation of remaining units. Once the contracts are in place, the fraud continues as the perpetrator secures funding for the contracts," Butts explains. However, she adds, no additional work is done and the investors and lenders are left with incomplete and, in some cases, uninhabitable dilapidated buildings.

Man-in-the-middle attack

*This is an **Attack**. To view all attacks, please see the Attack Category page.*

Last revision: **4/23/2009**

Description

The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in figure 1. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.

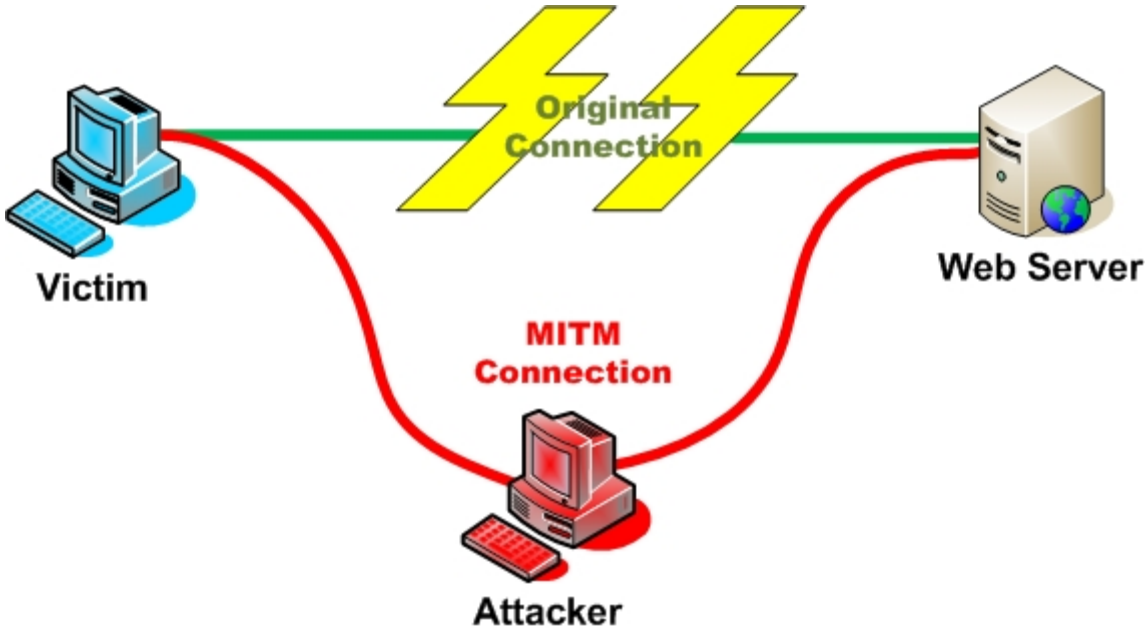


Figure 1. Illustration of man-in-the-middle attack

The MITM attack is very effective because of the nature of the http protocol and data transfer which are all ASCII based. In this way, it's possible to view and interview within the http protocol and also in the data transferred. So, for example, it's possible to capture a session cookie reading the http header, but it's also possible to change an amount of money transaction inside the application context, as shown in figure 2.

Man-in-the-browser attack

*This is an **Attack**. To view all attacks, please see the Attack Category page.*

Last revision: **4/23/2009**

Description

The Man-in-the-Browser attack is the same approach as Man-in-the-middle attack, but in this case a Trojan Horse is used to intercept and manipulate calls between the main application's executable (ex: the browser) and its security mechanisms or libraries on-the-fly.

The most common objective of this attack is to cause financial fraud by manipulating transactions of Internet Banking systems, even when other authentication factors are in use.

A previously installed Trojan horse is used to act between the browser and the browser's security mechanism, sniffing or modifying transactions as they are formed on the browser, but still displaying back the user's intended transaction. Normally, the victim must be smart in order to notice a signal of such attack while he is accessing a web application like an internet banking account, even in presence of SSL channels, because all expected controls and security mechanisms are displayed and work normally.

Operation Phish Phry Nets 100 People Including NC Suspects

The FBI arrested the largest number of people ever charged in a cyber crime case. Arrests were made in California, Nevada and North Carolina.

Los Angeles, CA -- During a multinational investigation conducted by the United States and Egypt, the FBI uncovered a sophisticated "phishing" operation. The people arrested fraudulently collected personal information from thousands of victims that was used to defraud US banks.

The FBI dubbed the investigation "Operation Phish Phry," and it was largest cyber crime investigation so far in US history. In the US, defendants were arrested in California, Nevada, and North Carolina.

On Wednesday morning, authorities arrested 33 of the 53 defendants named in the indictment by a federal grand jury in Los Angeles. In addition, authorities in Egypt charged another 47 defendants linked to the phishing scheme.

Operation Phish Phry started in 2007 when FBI agents, working with United States financial institutions, took steps to identify and disrupt sophisticated criminal enterprises targeting the financial infrastructure in the United States.

The 51-count indictment accuses all of the defendants with conspiracy to commit wire fraud and bank fraud. Various defendants are charged with bank fraud; aggravated identity theft; conspiracy to commit computer fraud, specifically unauthorized access to protected computers in connection with fraudulent bank transfers and domestic and international money laundering.

According to the indictment, Egyptian-based hackers obtained bank account numbers and related personal identification information from an unknown number of bank customers through phishing-a technique that involves sending e-mail messages that appear to be official correspondence from banks or credit card vendors. In illegal phishing schemes, bank customers are directed to fake websites purporting to be linked to financial institutions, where the customers are asked to enter their account numbers, passwords and other personal identification information. Because the websites appear to be legitimate-complete with bank logos and legal disclaimers-the customers do not realize that the websites do not belong to legitimate financial institutions.

Armed with the bank account information, members of the conspiracy hacked into accounts at two banks. Once they accessed the accounts, the individuals operating in Egypt communicated via text messages, telephone calls and Internet chat groups with co-conspirators in the United States. Through these communications, members of the criminal ring coordinated the illicit online transfer of funds from compromised accounts to newly created fraudulent accounts.

The United States part of the ring was allegedly directed by defendants Kenneth Joseph Lucas, Nichole Michelle Merzi, and Jonathan Preston Clark, all California residents, who directed trusted associates to recruit "runners," who set up bank accounts where the funds stolen from the compromised accounts could be transferred and withdrawn. A portion of the illegally obtained funds withdrawn were then transferred via wire services to the individuals operating in Egypt who had originally provided the bank account information obtained via phishing.

Each of the 53 defendants named in the indictment is charged with conspiracy to commit bank fraud and wire fraud, a charge that carries a statutory maximum penalty of 20 years in federal prison. Some of the defendants are named in additional counts that would increase their maximum possible sentences.

New Malware Re-Writes Online Bank Statements to Cover Fraud

By Kim Zetter mailto:kzetter@wired.com mailto:kzetter@wired.com

New malware being used by cybercrooks does more than let hackers loot a bank account; it hides evidence of a victim’s dwindling balance by rewriting online bank statements on the fly, according to a new report.

The sophisticated hack uses a Trojan horse program installed on the victim’s machine that alters html coding before it’s displayed in the user’s browser, to either erase evidence of a money transfer transaction entirely from a bank statement, or alter the amount of money transfers and balances.

The ruse buys the crooks time before a victim discovers the fraud, though won’t work if a victim uses an uninfected machine to check his or her bank balance.

The novel technique was employed in August by a gang who targeted customers of leading German banks and stole Euro 300,000 in three weeks, according to Yuval Ben-Itzhak, chief technology officer of computer security firm Finjan.

“The Trojan is hooked into your browser and dynamically modifies the text in the html,” Ben-Itzhak says. “It’s a very sophisticated technique.”

The information appears in a cybercrime intelligence report (.pdf) written by Finjan’s Malicious Code Research Center.

The victims’ computers are infected with the Trojan, known as URLZone, after visiting compromised legitimate web sites or rogue sites set up by the hackers.

Once a victim is infected, the malware grabs the consumer’s log in credentials to their bank account, then contacts a control center hosted on a machine in Ukraine for further instructions. The control center tells the Trojan how much money to wire transfer, and where to send it. To avoid tripping a bank’s automated anti-fraud detectors, the malware will withdraw random amounts, and check to make sure the withdrawal doesn’t exceed the victim’s balance.

The money gets transferred to the legitimate accounts of unsuspecting money mules who’ve been recruited online for work-at-home gigs, never suspecting that the money they’re allowing to flow through their account is being laundered. The mule transfers the money to the crook’s chosen account. The cyber gang Finjan tracked used each mule only twice, to avoid fraud pattern detection.

“They instruct the Trojan that the next time you log into your online banking account, they actually modify and change the statement you see there,” says Ben-Itzhak. “If you don’t know it, you won’t report it to the bank so they have more time to cash out.”

The researchers were able to capture screen shots showing the rogue bank statements in action, disguising, for example, a transfer of Euro 8,576.31 as Euro 53,94.

The researchers also found statistics in the command tool showing that out of 90,000 visitors to the gang’s rogue and compromised websites, 6,400 were infected with the URLZone trojan. Most of the attacks Finjan observed affected people using Internet Explorer browsers, but Ben-Itzhak says other browsers are vulnerable too.

Finjan provided law enforcement officials with details about the gang’s activities and says the hosting company for the Ukraine server has since suspended the domain for the command and control center. But Finjan estimates that a gang using the scheme unimpeded could rake in about $7.3 million annually.

“The example we found relates to German banks,” Ben-Itzhak says. “But we believe this will increase to other countries.”

Bankers Online Article
How to Stop Account Takeover

by Julie Conroy-McNelley

Account takeover is one of the more prevalent forms of identity theft. It occurs when a fraudster obtains an individual's personal information (account number and social security number usually suffice), and changes the official mailing address with that individual's financial institution (FI). Once accomplished, the fraudster has established a window of opportunity in which transactions are conducted without the victim's knowledge.

As detrimental as this can be to consumers, the businesses and financial institutions actually suffer the greatest loss.

- According to Meridien Research, while the victim suffers an average loss of $808, businesses and FIs absorb about $18,000 in fraudulent charges per victim.
- Celent Communications recently published statistics showing institutions average losses of about $2.7 billion per year since 1998, a figure that is expected to grow to over $8 billion by 2004.

Account takeover is becoming increasingly prominent and is a growing point of financial exposure for FIs, businesses, and consumers. Reducing exposure is best accomplished through a combined approach of Process, Consumer Education, and Technology.

- **Process:** Scrutinize internal processes surrounding customer address-change procedures. In addition to confirming identity using data points such as account number and social security

number, use an additional token, such as pet's name, or parent's anniversary-something not readily available to a fraudster.

- **Consumer Education:** Educate customers about identity theft risks. Provide verbal and written communications that explain simple steps that can be taken to minimize potential exposure such as:
    - Putting a lock on their mailbox;
    - Shredding receipts that contain account information, as well as pre-approved credit-card offers and billing statements;
    - Reviewing billing statements thoroughly for unauthorized charges; and
    - Periodically check credit bureau statements for irregularities.
- **Technology:** Unfortunately, regardless of steps taken on the Process and Education fronts, determined fraudsters still manage to find ways of perpetrating this crime. Technology is a necessity for catching account takeover before a loss is allowed to occur. An effective solution must detect unusual and unauthorized address changes, as well as suspicious characteristics or events that may be indicative of account takeover. The transaction pricing for these tools is generally low, and the offset to risk exposure considerable.

Fraudsters will exploit the easy targets. Is your institution doing all it can to minimize its exposure? The ROI will come not only in the savings reaped by lower fraud losses, but also in the minimization of reputation risk-no institution wants to appear in the headlines as the latest victim of identity theft and account takeover rings.

For over a decade, Early Warning Services, LLC (formerly Primary Payment Systems) has been an industry pioneer by facilitating cooperation and information sharing among financial services organizations as a best-practice means to help prevent fraud losses and safeguard the financial assets of those organizations and the consumers they serve. A suite of services delivers this intelligence to where it is needed most resulting in billions of dollars in loss avoidance each year. For more information, please visit www.early-warning.com.

Author:
Julie Conroy-McNelley
Primary Payments Systemsâ (PPS)
707.793.7629
jmcnelley@primarypayments.com

Facebook, Twitter users beware: Crooks are a mouse click away

STORY HIGHLIGHTS

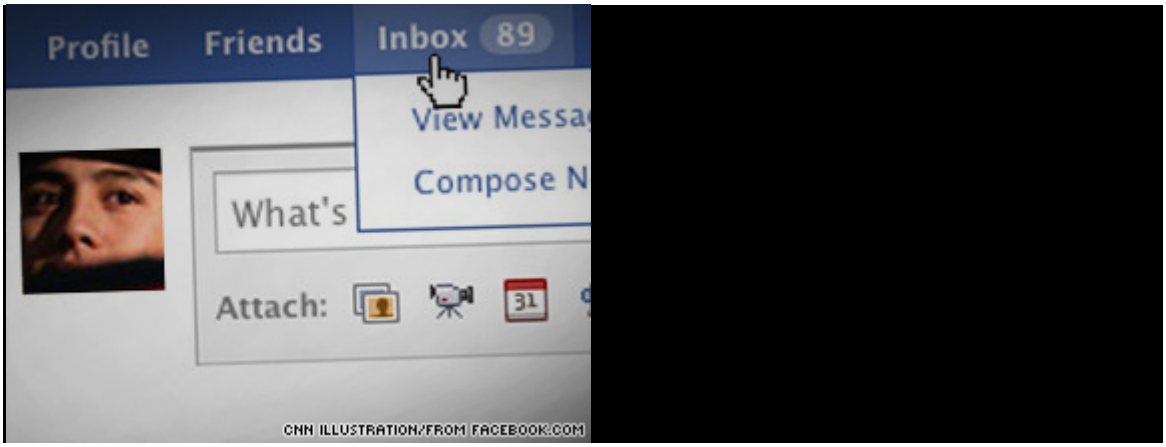
The FBI reports nearly 3,200 account hijacking cases since 2006

Online scam losses amounting to $264.6 million reported in 2008

Facebook has automated systems that detect compromised accounts

MySpace.com creates blacklists of phony accounts

(CNN) -- If you're on Facebook, Twitter or any other social networking site, you could be the next victim.



Experts say cybercrooks are lurking just a mouse click away on popular social networking sites.

That's because more cyberthieves are targeting increasingly popular social networking sites that provide a gold mine of personal information, according to the FBI. Since 2006, nearly 3,200 account hijacking cases have been reported to the Internet Crime Complaint Center, a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance.
It starts with a friend updating his or her status or sending you a message with an innocent link or video. Maybe your friend is in distress abroad and needs some help.

All you have to do is click.

When the message or link is opened, social network users are lured to fake Web sites that trick them into divulging personal details and passwords. The process, known as a phishing attack or malware, can infiltrate users' accounts without their consent. Once the account is compromised, the thieves can infiltrate the list of friends or contacts and repeat the attack on subsequent victims. Social networking sites show there is ample opportunity to find more victims; the average **Facebook** user has 120 friends on the site.
"Security is a constant arms race," said Simon Axten, an associate for privacy and public policy at Facebook. "Malicious actors are constantly attacking the site, and what you see is actually a very small percentage of what's attempted."

Social Media Crimes

How to protect yourself against scams:

- Change your passwords frequently
- Adjust Web site privacy settings
- Be selective when adding friends
- Limit access to your profile to contacts you trust
- Disable options such as photo sharing
- Be careful what you click on
- Familiarize yourself with the security and privacy settings
- Learn how to report a compromised account
- Use security software that updates automatically

(Information provided by FBI and Internet security experts)

As some social networking sites experience monstrous growth, they are becoming a new -- and extremely lucrative -- frontier for cybercrime. Facebook says it has 300 million users, nearly the size of the U.S. population, and it continues to attract users outside the college student niche. From February 2008 to February 2009, Twitter, a micro-blogging site where users post 140-character messages known as tweets, grew 1,382 percent to more than 7 million users.

"They [cybercriminals] are very adept to using social engineering," said Donald DeBold, director of threat research for CA, an Internet security company. "Your friend is in trouble traveling in another country, 'I lost my wallet. I need help.' They exploit the curiosity aspect out of human nature."

A few decades ago, malicious software and viruses were usually the result of a prank, but Internet security experts say today's attacks are profit-driven. A study from the University of Indiana in 2005 discovered that phishing attacks on social networks operated with a 70 percent success rate. These users had fallen for the scam, opened the foreign link and released personal information. Cybercriminals are employing phishing and malware attacks for a number of reasons, including trying to redirect users to sites where profit is fueled by the number of visitors. They also try to elicit private information like passwords and bank account numbers to perform scams.

Early this year, **Twitter** experienced several phishing attacks in which a Web page that looked identical to the widely recognized light blue Twitter page was a hoax. The company warned users to double-check the URL to ensure they were visiting the correct site. The Internet Crime Complaint Center received more than 72,000 complaints about Internet fraud in 2008 that were referred to law enforcement agencies for further investigation. These cases involved financial losses amounting to $264.6 million, an increase from 2007. Each person lost an average of $931. "Most of us would want to help a friend in need, but if it's an online friend, and they want you to wire money, you should double-check," FBI spokesman Jason Pack said.

Security experts said it makes sense that cybercriminals are turning to social networking sites. Personal information is abundant on sites like Facebook and **MySpace**. Each time users give out valuable information like birth dates or addresses, they could be providing hints about their password, security experts say.

The American Civil Liberties Union has expressed concern about the information visible through Facebook quizzes and applications. "They'll have access to all that information, so they can sell it, they can share it, they can do an awful lot with it," Chris Calabrese, legislative counsel for privacy-related issues with the ACLU, told CNN.com in September.

Many Internet security experts consider the first virus attack on the PC to have occurred in 1986. By the early 1990s, viruses transmitted on floppy disks became ubiquitous. When the World Wide Web became widely available that same decade, viruses, worms and malware became problems in e-mail accounts, frustrating users who clicked on messages thought to be legitimate.

In the new millennium, the most common form of malware attack has become known as drive-by downloads. While surfing on Google or Yahoo, spyware or a computer virus is automatically and invisibly downloaded on a computer, requiring no user interaction for the computer to be infected.
"We are on the verge from shifting from the Web being the No. 1 victim of infecting to social network," said Mikko H. Hypponen, chief of research technology at F-Secure Corp. His company sells anti-virus software and malware protection programs. "It's going to get a lot worse before it gets better."

Social networks are fighting the aggressive attacks from **cybercriminals**. Most sites have information pages dedicated to educating users about the risks of Internet scams. Users can become a fan of "Facebook Security" and receive updates on how to protect their accounts. One of the most common pieces of advice given by security experts is to change passwords frequently.

Facebook has also developed complex automated systems that detect compromised accounts. They spot and freeze accounts that are sending an unusually high number of messages to their friends. Company security officials said Facebook is a closed system, which can be helpful in erasing phony messages from all accounts.

At News Corporation's MySpace.com, the company creates blacklists of phony accounts to prevent people from clicking on a faulty link. Hemanshu Nigam, first chief security officer for MySpace, said the firm warns about suspicious links and educates users about the harm phishing and malware attacks can bring.

FULL NELSON: THE GROWING THREAT OF CYBERWARFARE

Many more causalities will pile up, but policy and agreements will prove meaningless against today's anonymous cyberwarrior.

By **Fritz Nelson**
InformationWeek
October 19, 2009 10:45 AM

Gladiators and jousters, Wild West gunslingers and kamikaze pilots, are long retired to history books and celluloid epics, each a reminder of war tactics from a bygone era. They're supplanted today by anonymous warriors--pseudonyms sitting in virtual garrisons, spying, probing, and launching attacks from non-descript buildings all over the world. This is not your father's war. It's not even your older brother's war. In cyberwarfare, there may be no victors, no spoils, just havoc, theft, and assault.

Those who cling mindlessly to notions of war driven by sovereignty and territorial conquest through armed forces should look no further than the specter of current events, where warlords live in caves and their henchmen strap on home-made explosives. Take shock value and terror and layer in the Internet's abstraction and suddenly those who hate or feel disenfranchised or seek wealth or yearn for sanity, or whatever else, gain instant targets and instant audience, and an almost-impossible cave to find.

New wars call for new rules and new definitions. Kris Herrin, chief security officer of Heartland Payment Systems, recently riveted banking industry veterans, as he often does when he folds his company's disastrous security breach inside out. The Russian hackers who breached Heartland and stole its data late last year outsource their malware development to India, have customer service guarantees, offer a help desk, and provide a fully automated attack platform (you can select a target and an attack method, much as you would customize a hand bag online).

It would be easy enough to label this cybercrime, but Russian civilians have engaged in cyberattacks against neighboring Georgia. During Herrin's talk, a Bank of America executive reminded the audience that the Department of Homeland Security revealed that Al-Qaeda had attacked banks worldwide to the tune of hundreds of millions of dollars to fund its operations. Cybercrime, or cyberwarfare? The Russian outfit that attacked Heartland breached 300 financial institutions. If they marched into America as armed militia, or took out electric grids with guns and tanks, would that be crime or war? The lines blur.

Fear and outrage followed North Korea's alleged infiltration of the Department of Justice and Federal Trade Commission computer systems. The U.S. reportedly hacked into Iran's systems early this decade to monitor that country's nuclear program. The New York Times reported that U.S. soldiers lured Al-Qaeda into a death trap by hacking into a computer and falsifying information. There are numerous reports on persistent probes from Chinese hackers into U.S. systems, including network operators penetrating several electric grids. Some government officials suspect China of building trapdoors (hidden code or altered physical layers) into the chips that run many of our computer systems.

Well-known security researcher Marcus Ranum argues that cyberwarfare doesn't exist, that cyberattacks only accompany a vast military invasion. Besides, what right-minded military would tolerate a weapon that could be disabled with a push of a button. And yet unmanned fighter drones capable of surveillance and strikes fly non-stop miles above Iraq and Afghanistan and regularly fall into automated holding patterns when pilots thousands of miles away lose Internet connectivity to the aircraft, cyberflanks exposed.

Each F-35 Joint Strike Fighter contains several hundred chips, many of which aren't fabricated in the United States and which, according to some theorists, could be the target of trapdoors. A Wall Street Journal article reported that the F-35 program was recently compromised by an attack using Chinese Internet host systems, and the data stolen was encrypted. An AviationWeek story later downplayed the incident. Cyberthreats.

In 2007, Israel, suspecting a nuclear installation in Syria, sent an air raid to destroy the facility, bypassing Syria's vaunted radar systems. Many speculate that the radar had been tampered with. Cyberwarfare.

Because civilians allegedly drove the Russia-Georgia battle in cyberspace, many refuse to call it war. Likewise, in Estonia, a country was disrupted, money was lost, but no sovereignty was taken, no guns, no victory or defeat. The wars of history don't allow for engines of abstraction, only those of explosives.

Mike McConnell, former director of national intelligence, recently said: "The ability to threaten the U.S. money supply is the equivalent of today's nuclear weapon."

Despite the threats, some experts, including RAND Corp., suggest a slowdown in spending on cyberwar defenses, and there already have been substantial cuts, including the Air Force cybersecurity programs. The government has been mum on developing cyberoffensive capabilities, although many arm-chair pundits have suggested we're building our own trapdoors in the hardware and software we export.
There are, however, several initiatives under way, including building a replica of the Internet to test for vulnerabilities and a DARPA-funded initiative through MIT to test our own ability to examine chips for things like trapdoors (the program is called Trust in IC). Col. Charles Williamson III, the staff judge advocate for Air Force Intelligence, argued in the Air Force Journal for creating a .mil botnet using an army of discarded or aging computers, though he stopped short of calling for civilian zombies.

And then there's policy. Certainly, the rules will need some rewriting. The Geneva and Hague Conventions make civilian involvement in war illegal, but those agreements don't account for cyberwarfare. Melissa Hathaway, former senior director for cyberspace for the National Security Council and Homeland Security Council, made the case to take the discussion international given the widespread nature of these threats. "If we can bring it into some of the policies we're looking at, the synchronization, formulation, rules of engagement, and what is ethical behavior . . . that's one way to address it."

While policy and agreements are nice in theory, they will prove meaningless against today's cyberwarrior. The anonymity of attackers and the thick dossier of attack targets mean more casualties and a call for an ever-more-vigilant defense posture. The painful part is figuring out who may attack, how it will occur, and where it will begin. Indeed, it may have already begun. After all, on the Internet, nobody knows they're in a dogfight.

BEING PROACTIVE AND COOPERATIVE STILL KEYS TO FOILING CYBER THREATS

Presenters at the annual SIFMA conference said banks and others need multi-sector cooperation to protect systems from criminals and to act more quickly.
By Maria Bruno-Britz(**More from this author*)***
June 25, 2009

The industry may be trying to face down an economic crisis, but that still doesn't mean the old specter of security isn't looming over financial services executives' heads.

According to Patrick Peck, SVP, Booz Allen Hamilton (McLean, Va.), managing cyber security and how to protect the enterprise is still front and center on the minds of his clients. During a presentation yesterday called "Cyber: Are You Ready for What's Next?," Peck told attendees of the annual SIFMA Technology Conference & Exhibit in New York that the threats still exist and they'll only worsen. Ultimately, the key to succeeding against them is to establish a three-way cooperative between industry, government and academia to intercept threats more quickly.

At one point, Peck showed a video of Michael McConnell, an SVP at Booz Allen and the former director of national intelligence under President Bush. McConnell noted that if the 9-11 terrorists had instead chosen to hack into a major bank and destroy all the data in that bank, the global damage would have far exceeded the tragedies of the World Trade Center, Pentagon and Flight 93.

"The global financial system is not based on a gold standard," McConnell noted. "It's based on confidence." Once that confidence is shaken, there is a cascading effect, as has been illustrated throughout this financial crisis.

To properly address cyber threats to the banking system and the nation's infrastructure, he said companies have to remember to look beyond technology solutions at policy, culture and the company's operating profile.

Peck followed this up with an example of a simulation Booz Allen performed that involved taking 230 leaders from industry, government and society (such as academics, the media) and watched how they reacted to the simulated cyber threat. What really struck Peck was that people couldn't clearly understand the lines of authority in an emergency. "People didn't know who to go to, where policy was coming from," he explained. "We recommend establishing a single voice around cyber education."

He noted this is what President Obama is doing with the establishment of a cyber authority within the Dept. of Homeland Security. "Cyber is too complex for one authority to handle alone," he said. There is a growing array of state and nonstate members seeking to attack American government and commercial interests—including financial institutions. "The nation must act quickly to protect our national infrastructure," Peck commented.

Co-presenter Scott Kaine, also from Booz Allen, suggested banks and others be mindful of the threats from within as well as outside of the organization, since 80 percent of risk is from insider threats. "You need the basic blocking and tackling and the key is training—from the C-level down to customer services reps," he noted.

A continuous risk process that is revisited regularly is required if a financial institution is to protect itself from cyber threats, both current and future, Kaine said. This starts with the budget process. The funding for IT and security should not be relegated to the bottom like it often is. Banks are trying to cut costs. If money is shaved off the IT security budget, how much risk is being introduced to the organization? "You have to know this," he said. "Do a risk assessment more than once a year and allocate the budget according to those risks."

Something that might encourage this practice is a bill being floated in the Senate that would require businesses to adhere to the same security standards as government agencies. "Do your IT folks know about this?" Kaine posed to attendees. "They're going to need to know the ramifications of this policy."

Regardless of whether the Cybersecurity Act of 2009 is passed, information security people at banks need to act first. They need to use the technology at their disposal to look outside the organization so that when patterns of illicit cyber activity emerge in other parts of the world, they are forewarned and better able to repel the threat once it reaches their organizations' borders. "Work with your ISP, managed security players and government," Kaine said. "Your role is to be proactive."