Cyber Fraud Trends and Mitigation

Richard Howard, Ralph Thomas, Jeff Burstein, and Roxanna Bradescu

Abstract— **Phishing Trojan horse programs are not traditional bots, but sophisticated and original pieces of malicious code. Since iDefense began tracking this technique in May 2006, attackers have quietly seeded dozens of variants into the wild to target at least 30 specific banking institutions. These attackers had intimate knowledge of each targeted bank's Web infrastructure and built a sophisticated command-and-control system that completely automated the attacks. The authors believe that criminal organizations are using these phishing Trojans to compromise millions of bank accounts across the globe. These Phishing Trojan attacks can defeat sophisticated authentication schemes that security experts previously thought rock solid.**

This document discusses mitigation techniques that work and fail in light of these new malicious code attacks. The audience will be given an overview on malicious code attacks against the financial infrastructure and an introduction to banking authentication schemes. The document also includes cyber fraud detection and mitigation strategies.

Index Terms— **Authentication, Online Fraud, Information Security, Malicious Code, Phishing**

I. Executive Summary

PHISHING Trojan horse programs like MetaFisher are not traditional bots, but sophisticated and original pieces of malicious code. Since iDefense began tracking the MetaFisher issue in May 2006 (iDefense, "MetaFisher: A Sophisticated Bot Attack," May 26, 2006), the attackers behind MetaFisher have quietly seeded dozens of variants into the wild to target at least 30 specific banks. These attackers had intimate knowledge of each targeted bank's Web infrastructure and built a sophisticated command-and-control (C&C) system that completely automated the attacks. iDefense believes that criminal organizations are using these phishing Trojans to compromise millions of bank accounts across the globe.

These Phishing Trojan attacks can defeat sophisticated authentication schemes that security experts previously thought to be rock solid. The only mitigation scheme that has yet proven impervious to this Phishing Trojan technique is the Indexed Out-of-Band One-Time-Password authentication scheme; however, no single tool will likely be enough to defeat future attacks. iDefense recommends that the affected banking institutions consider a "Defense in Depth" approach to cyber fraud prevention. Banks should consider client anti-virus solutions, fraud detection services and some form of robust authentication as possible tools to mitigate the threat posed by MetaFisher-type attacks.

Manuscript received July 25, 2007.

Richard Howard is with VeriSign's iDefense Security Intelligence Service, Dulles, VA 20166 USA (rhoward@idefense.com).

Ralph Thomas is with iDefense's Malicious Code Operations group, Dulles, VA 20166 USA (phone: 703-948-4169; fax: 571-434-6006; e-mail: rthomas@idefense.com).

II. Introduction

Cyber fraud is the act of stealing money from unsuspecting users via the Internet. Since May 2006, iDefense has tracked the rapid evolution of sophisticated cyber fraud techniques used by organized crime groups.

iDefense research revealed a new kind of phishing attack, one that did not redirect the victim to complex mock-ups of commercial banking websites like the majority of phishing schemes to date. Instead, this new technique allowed the attacker to inject HTML directly into the user's browser via a kind of phishing Trojan horse. These attackers targeted the users of specific European banks, crafted Web pages designed to look exactly like a legitimate bank's website and injected HTML code, designed to steal logon credentials, directly into the victim's browser. Once successful, the attacker logged onto the victim's legitimate banking site using the stolen credential information and transferred money out of the account and into other third-party banking accounts. Later, unknowing accomplice "money mules" withdrew the cash for delivery presumably to the cyber criminals who initiated the attacks.

The MetaFisher cyber fraud attacks comprise several unique components never before seen by iDefense, including:

- Sophisticated software development process indicators
- Local HTML injection techniques instead of fraudulent external websites
- Ability to defeat complex one-time-pad (OTP) authentication schemes
- Botnet control of "phished" computers

In its analysis of MetaFisher, iDefense predicted that it would only be a matter of time before the attackers migrated to US banking systems and were able to defeat standard two-factor authentication schemes, but that prediction came true much sooner than expected. In summer 2006, press sources reported that at least one client from CitiBank, using a token-based two-factor authentication scheme, had fallen victim to a

phishing attack[1].

Even with an attack this sophisticated, not all experts agree that cyber fraud is a significant problem. At the iDefense Customer Council held in Texas in the summer of 2006, banking customers unanimously agreed that cyber fraud does not financially impact their institutions to any great degree. The conclusion was that simple fraud, the way it has been done for years, costs banks more money than cyber fraud. Banks simply were not very worried about cyber fraud.

These banks do, however, worry about how their customers, and potential customers, perceive them. If customers choose one bank over another because of that bank's reputation for security, or lack thereof, it could impact the bottom line. Banks must make its customers feel safe and keep its name out of the press if it hopes to be competitive. At the same time, banks must minimize the cost to implement necessary security and ensure that such measures are not so intrusive that they scare the customer away. For any organization, this is a tall order.

The keys are authentication and detection. How does the online banking system authenticate a user with any degree of confidence or detect malicious behavior to lower the risk of cyber fraud to acceptable levels? Fortunately, the solution set is a spectrum of choices that range from the very complex and completely secure to simpler solutions that are not as secure, but may be secure enough.

According to an iDefense Weekly Threat Report, the industry is also concerned about compliance. The Federal Financial Institutions Examination Council (FFIEC) guidelines mandated the validation of identities for online users by Dec. 31, 2006. The FFIEC released the regulations, which are not mandatory, in the autumn of 2005. The regulations do not specify what forms of authentication should be used, nor do they require banks to comply, but the FFIEC will begin auditing banks in 2007. Since the FFIEC does not stipulate how to accomplish these tasks, the banks are left to themselves to determine the appropriate solution.

This report discusses how the phishing Trojan technique works, how it defeats some authentication schemes and how some banks and security firms are mitigating the threat with more complex authentication and fraud detection schemes. Finally, this report will examine a list of possible mitigation techniques.

III. Phishing Trojan Overview

Techniques for establishing a phishing Trojan on a victim's computer vary, but typically consist of three components: the initial exploit, communication with the command-and-control website, and communication to the FTP drop server to hold the information the attacker wants to steal. This process is illustrated in Fig. 1.

A. 3.1 Initial Compromise

When iDefense first discovered the MetaFisher Trojan in the spring of 2006, attackers used the Microsoft Windows Metafile Format (WMF) vulnerability to establish the initial foothold (Step 1 above). Even though large corporations patched this vulnerability as far back as January 2006, iDefense assumes that many home users have not. Indeed, in the original report, iDefense documented close to 30,000 hosts that made up the MetaFisher botnet. Exploitation of the WMF vulnerability is not necessary, however; any exploit that

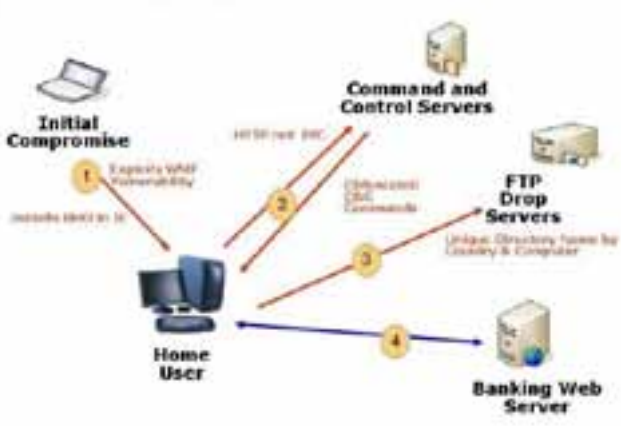

Fig. 1. Cyber-Fraud Overview: Remote resources participating in cyber attacks.

allows an attacker to take control of the host will suffice for this first step.

Once the attackers "own" the victim computer, they establish communication between the compromised host and the command-and-control servers. Attackers accomplish this by installing a Browser Help Object (BHO) on the home user system that only runs when the victim is using Internet Explorer (IE).

According to Wikipedia[2], a BHO is "a DLL module designed as a plugin for the Microsoft Internet Explorer Web browser to provide added functionality. BHOs were introduced in October 1997 with the release of version 4 of Internet Explorer." BHOs gave third-party vendors the ability to extend the capability of IE and Windows File Explorer by providing access to the Document Object Model (DOM), a fairly powerful capability. Common examples that use this capability are the IE Google Tool Bar and the IE Adobe Acrobat Viewer.

Unfortunately, there is no proactive way to prevent installation of malicious BHOs; the user must be savvy enough to know to check. If banking customers are running Windows XP with SP2, they can launch Microsoft's tool for

[1] Brian Krebs: Citibank Phish Spoofs 2-Factor Authentication. Security Fix Blog, Washington Post. July 10, 2006. http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

[2] Wikipedia: Browser Helper Object. http://en.wikipedia.org/wiki/Browser_Helper_Object

managing BHOs by opening Windows File Manager, selecting "Tools" and "Manage Add-Ons." Once there, users can disable unrecognized BHOs. However, this is cumbersome at best for the experienced computer user and not doable at all for the average home user.

Please check with your editor on whether to submit your manuscript as hard copy or electronically for review. If hard copy, submit photocopies such that only one column appears per page. This will give your referees plenty of room to write comments. Send the number of copies specified by your editor (typically four). If submitted electronically, find out if your editor prefers submissions on disk or as e-mail attachments.

B. Command-and-Control Servers

Communication between the BHO and the command-and-control (C&C) server is accomplished via the Hypertext Transfer Protocol (HTTP) instead of the aforementioned typical bot Internet Relay Chat (IRC) protocol (Step 2). Corporate and home security policies are much less likely to block this kind of traffic by default at the perimeter because it looks like regular Web traffic.

In the MetaFisher scheme, attackers obfuscated all commands between the C&C server and the compromised system through a homegrown encryption mechanism. The attackers used the compromised hostname as the key. The iDefense Malicious Code Team (Malcode) broke this encryption scheme earlier in the year in an effort to understand the impact of the phishing Trojan [MetaFisher: A Sophisticated Bot Attack//May 26, 2006].

The use of this C&C scheme is fairly typical for botnets in general, but what made the MetaFisher Trojan botnet unique was the sophistication of the C&C user interface that the attackers built to automate their activity. The key components of the software include:

- Apache website running PHP as a C&C server
- Indicators of disciplined software development techniques
- Interface that can handle multiple exploits, not just WMF
- Interface that can easily handle more than one user
- Interface that easily handles multiple FTP sites
- Interface that provides meaningful statistics to users of the software

The attackers configure the C&C servers to communicate targets, exploits and custom injection HTML to other members of the botnet.

C. FTP Drop Servers

Next, the BHO establishes communication with the FTP drop site (Step 3). It creates a unique name on the FTP server that corresponds to the newly compromised computer's country of origin and name. The FTP drop server and the C&C server can be the same computer or different computers. iDefense has seen both examples in the wild.

iDefense has uncovered evidence that Russian organized

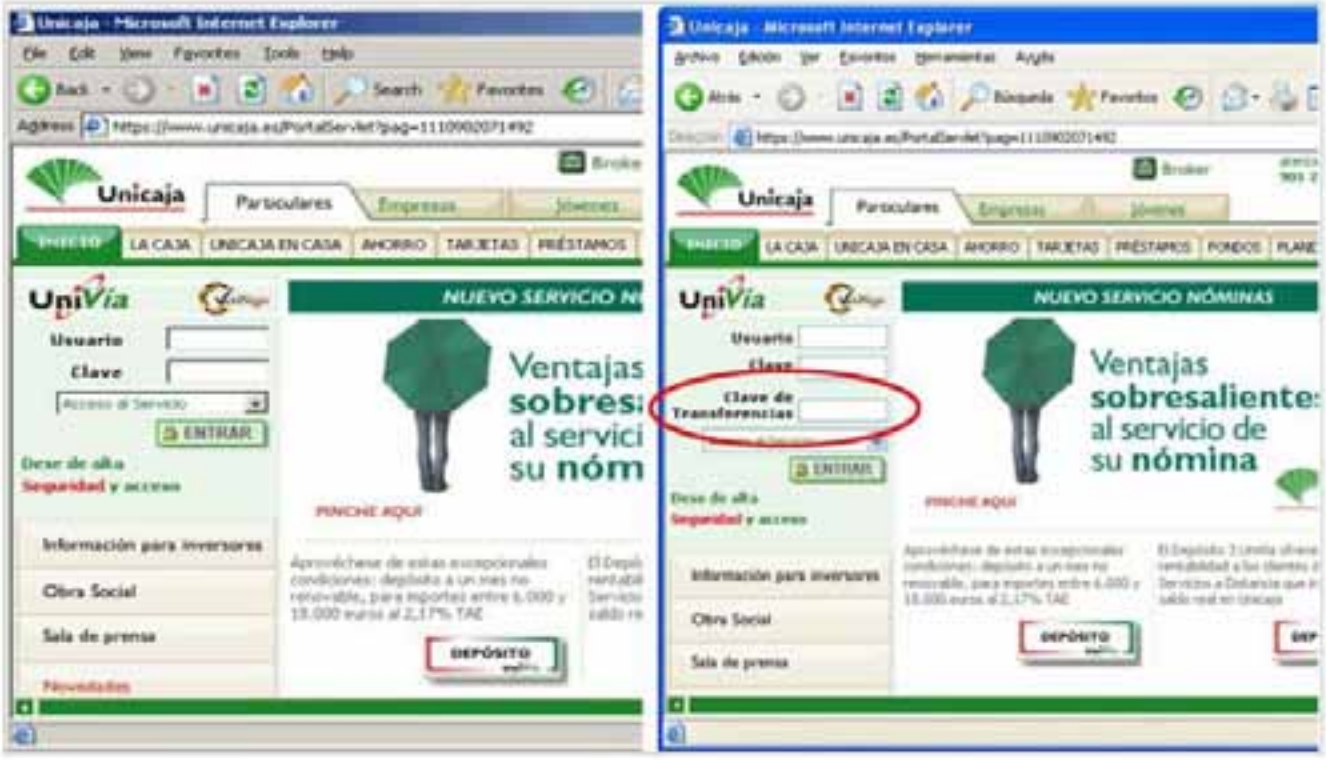

Fig. 2. MetaFisher Targeting a Spanish Banking Site: Via HTML injection an additional field is added to the banking site, asking consumers for sensitive information.

crime is behind the attacks. The C&C and FTP drop servers had multiple configurations over the past few months. Just recently, both servers were located on the same computer hosted by a Russian ISP and run by a hacker going by the handle, "Godfather." This hacker is notorious for supplying network domains to host illicit computer activity in Russia. iDefense has communicated regularly with Russian law enforcement personnel who claim to be powerless to stop the attacks. Unless the crimes occur on Russian soil (which they are not), and unless some foreign entity requests help, Russian law enforcement is largely impotent to stop this kind of activity.

D. Banking Web Server

After the attackers exploit the host computer and establish communication with the C&C server and the FTP drop server, they wait for the user to connect to the targeted bank's Web server. When the client attempts to make an online banking transaction, the BHO injects HTML code in an effort to steal the user's login credentials from the client while the client is logged onto the banking Web application (Step 4 above). Similar to traditional remote phishing schemes, the BHO attempts to trick users into entering user names and passwords in a classic man-in-the-middle attack. The difference is that the attackers launch the man-in-the-middle attack locally on the host instead of remotely on an external Web server. Fig. 2 shows the real website and the spoofed site with injected content.

On the left, users must enter a user ID and a password just to gain access to the site. If users want to make a financial transaction, though, they must enter a third password (indicated by the red circle on the right) to authenticate and authorize the transaction.

The HTML shown on the right is injected into the client's browser from the BHO. IE never actually connects to the banking website at all. The BHO collects the user name, password and transaction password and sends it to the FTP drop server for later use. The BHO then presents users with some form of error message indicating that they should enter these credentials again. This time the BHO allows the transaction to go through to the banking web site and users are unaware that anything has transpired.

Later, the attacker can log onto the website using the stolen credentials and transfer money from the compromised account to some other online banking institution. To complete the cyber fraud, the attackers hire "money mules," or unsuspecting accomplices, to withdraw the money and deliver it to the attackers.

IV. Techniques and Malicious Code Evolution

VeriSign iDefense classifies malicious code targeting financial institutions in several different categories. Although malicious code authors design specific Trojan horses to target financial institutions with login systems with more advanced designs than standard username and passwords, less advanced pieces of malicious code such as generic keystroke-logging Trojans and generic form-grabbing Trojans cause financial burdens on institutions as well.

A. Keystroke Logging

Keystroke-logging software, or keyloggers, is the simplest form of information stealing software. Keystroke logging records each key typed on the victim's keyboard. Keystroke logging produces large amounts of data that include spaces, line breaks and backspace keys. Authors have incorporated keystroke logging in Trojan and Remote Administration Tools (RAT) toolkits since the late the 1990's. Keystroke logging became widespread with early Trojans such as BackOrifice, Netbus and SubSeven. Today, keystroke loggers are features found in many RATs such as Nuclear Rat, ProRAT and Bifrost. Many other types of Trojans have generic keyloggers that gather large amounts of stolen data, even if the attacker is not targeting specific sites. In addition to RATs, generic keyloggers are often present in online game credential-stealing Trojans and various IRC bot families. Keystroke logging is not capable of grabbing forms. As a result, an attacker who searches keystroke logs to isolate recorded keystrokes relevant to a financial institution might retrieve the following results:

www.mybank.com[CRLF]myonlineidmypassword

The user, in the example above, visited the website of "MyBank" from their home computer. The attacker is unable to capture the state of the user's account. The site presented the user with the login page and they subsequently entered their password. The attacker is unable to retrieve enough information to log in from a computer not already registered to that user. If the user were not at their home location, the attacker would receive additional fields of text, but would not be able to determine the state or what questions the answers corresponded to, as the victim never enters this information using the keyboard.

B. Form Grabbing

Keystroke logging reveals all text typed by a user. Obvious disadvantages include unmanageable amounts of data and inability to capture important pieces of data such as dropdown boxes, check boxes and fields entered without a keyboard.

Form grabbing is a generic term given to the ability to capture all fields sent via POST and GET requests by intercepting the form before the data reaches the server. Attackers have two primary options to achieve this feat. Attackers can sniff GET and POST requests directly from traffic on the system using sniffing tools. Attackers can also inject DLLs into browsers to intercept requests before the browser sends them to the server. Attackers most commonly achieve this by using a Browser Helper Object (BHO) with Internet Explorer. More recently, attackers started targeting Firefox with similar pieces of software. This method also has the added advantage of being able to capture requests before encryption and retrieve responses after decryption. Because

most sites that require authentication use SSL, browser-based form grabbing is the only technique that will work.

C. Screen-shots and Mouse Event Capturing

Trojan authors added the ability to take screen-shots and capture mouse events around the same time they added the ability to log keystrokes. Despite this, many information stealing Trojan's that simply copied the techniques of common RATs, did not add this ability until banks started using virtual keyboards to enter credentials. Virtual keyboards for some banks use Java and result in specially encrypted or encoded strings. Other banks submit the form data without any additional encryption other than SSL, meaning that generic form grabbers can still steal the data from the virtual keyboard.

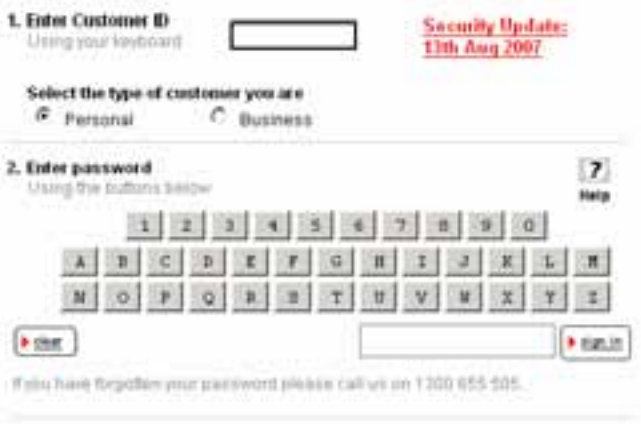

Fig. 3 Virtual Keyboard Login.

D. Phishing and Pharming Trojans

Phishing and pharming Trojans are nearly identical. The basic goal behind them is to display an alternative Web page when users visit a website. The confusion mainly stems from the definition of pharming and whether redirecting a user to a specific URL is phishing or pharming, as many security company's definitions of pharming would only count redirection of the entire domain to a separate IP, which then must be able to accept the entire host. The argument is not important, because both techniques work essentially the same, resulting in redirection to a set of templates. The most advanced application of this type of Trojan involves connecting to the real site so that the real SSL exchange happens and the URL bar remains intact, while simultaneously overlaying a phishing page.

E. HTML Injection

HTML Injection is a way for attackers to carry out an "on-the-fly" phishing attack. Victims visit their real banking website, and the Trojan injects additional HTML code into the page during, or after the page loads. This allows attackers to capture fields that are not part of standard forms, but provide useful information (see Fig. 2). Attackers also use HTML injection to create pop-ups with virtual keyboards and fields to attempt to capture entire TAN sheets.

F. Protected Storage Retrieval and Saved Password Retrieval

Windows 2000, XP and Server 2003 all provide a Protected Storage system that stores passwords to applications including Internet Explorer, Outlook Express and MSN. Users that use the "remember my password" feature of Internet Explorer have all of their passwords stored in this area. Firefox and Opera also come with similar features to remember form data such as passwords. Protected storage retrieval is standard in many Trojans and extremely effective against sites that use standard username and password authentication. Attackers target Firefox's and Opera's password managers less often, but as Firefox's market share continues to increase, so will the likelihood of being targeted. Opera's password manager poses an even greater threat, as websites cannot direct it to turn off, as they can do by using "autocomplete=off" attributes that Internet Explorer and Firefox follow.

G. Certificate Stealing

As many financial institutions are requiring digital certificates for various account types, Trojan authors logically took the next step and added certificate stealing functionality to their toolkits. Although exact formats vary by Trojan, it is common to have the ability to export certificates, steal CA certificates, MY A certificates, ROOT certificates, SPC certificates, PFX certificates and potentially others. VeriSign iDefense encounters many drop sites with stolen certificates. Although it is unclear how many attackers actually use the certificates they steal, this functionality poses a threat to institutions that rely upon this technique.

V. Banking Authentication Schemes

Since the advent of online banking, financial institutions have tried a number of different methods to protect customers' online transactions. In the second example above, the Spanish bank Unicaja added a second password in an effort to provide stronger authentication to its clients than the traditional user name and password. Unfortunately, as described in that section, the MetaFisher attackers had no trouble defeating this scheme. Other, stronger authentication schemes do exist, however.

A. Authentication Schemes

According to the CISSP Exam Guide, Third Edition (All-in-One) by Shon Harris, identification is the process of verifying the identity of the user attempting to connect to the secure server. Subsequently, authentication is the act of determining the access privileges of that identified user.

The security community generally agrees that the process of validating the user's identification and authentication consists of the user supplying credential information to the system. Credentials can come from three areas: something the user

owns (like a hardware token), something the user knows (like a password) or some physical characteristic (like a fingerprint). For most systems, any two of these combined is enough to guarantee the access rights of a user; this is called two-factor authentication. For example, a user might own a token that holds a private key and know a 4-digit PIN to access a banking site; the user must have both to conduct banking transactions on a web site.

Unfortunately, some two-factor authentication schemes break down under the nuances of the phishing Trojan attack.

One-Time Pads (OTPs)

Some European banks have implemented a program that uses Transaction Authentication Numbers (or TANs). These banks hand out books of 50 TANs to users. Every time the user makes a financial transaction, he must use one of the TANs in the booklet. Once used, the TAN is never used again. TANs are essentially one-time pads for passwords. The banking TANs booklet fits within the two-factor authentication definition, as something the user owns (a TANs booklet) and something the user knows (a password).

Unfortunately, the phishing Trojan man-in-the-middle attack has no trouble defeating this authentication scheme. The attack works the same way that it did for the Spanish bank in the earlier example. Instead of stealing the second password though, the attacker steals the entered TAN. The BHO injects an error statement saying that the TAN is invalid and to please enter another. The user is unaware of a problem and gladly enters another TAN. Since the bank has never seen the first TAN, the attacker can log into the website and conduct one transaction for each stolen TAN.

To combat this weakness, some European banks have instituted more complex versions of the TAN system: timed OTPs, indexed OTPs and indexed out-of-band OTPs.

Timed OTPs

This is essentially the same as the OTP method, but with a twist. The banking application has a time limit associated with each TAN that is entered into the system (usually a minute or so). When users enter a TAN, they have only so long to complete the transaction before the TAN expires. This does not completely eliminate the possibility of a man-in-the-middle attack, but such a limitation definitely makes such an attack more difficult to implement.

Timed OTPs are essentially a simpler version of hardware-based two-factor authentication methods. Such a method would easily thwart the attack described earlier in its current form; however, as seen in the Citibank attack described below, attackers have already launched successful attacks against this kind of authentication scheme. iDefense believes that timed OTPs are a solid general authentication system that will defeat the general hacker, but it will fail against the onslaught of a more determined and skilled attacker.

Indexed OTPs

Indexed OTPs add one more step to the TANs process. Instead of the user keeping track of the used TANs from previous transactions, the bank asks the user for a specific TAN number from the booklet. For example, the banking web site may ask the user to enter TAN # 36 for a given transaction. As long as the bank randomizes which TAN it asks for, and never uses that TAN again, this marks an improvement over that standard TAN system. It prevents the phishing Trojan scheme from being successful. The attackers can ask victims to enter specific TANs, but they will not be able to guess which TAN the bank will ask for.

Although indexed OTPs prevent the standard man-in-the-middle phishing Trojan attack scenario, such indexed methods may be susceptible to others, such as brute-force attacks. For every host in the targeted botnet, the attacker steals the indexed TAN and tries to login and conduct transactions. It is therefore reasonable to assume that a bank Web application will allow the user two to three mistakes in entering a TAN into the system before it locks that user out. A TAN booklet consisting of 50 numbers gives the attackers a three in 50 (six percent) chance of guessing correctly for each account. In the original MetaFisher report, iDefense reported that the Trojan's botnet consisted of around 30,000 hosts. iDefense assumes that at least 10 percent of this botnet's hosts regularly log into the targeted banking website. If this is indeed the case, the attacker is given around 3,000 attempts to guess correctly, with a six percent chance of guessing correctly. Granted, these are not great odds, but the attacker is given a large number of tries to guess right.

Also, depending on the rigor of the randomness in producing the TAN booklets, and the randomness with which the banking application asks for the TAN during the transaction, the attacker may be able to predict the next TAN with better accuracy.

Indexed Out-of-Band OTPs

Indexed Out-of-Band OTPs are more complicated, as they take the indexed OTP method one step further. With this method, the bank uses a different channel to transmit and receive the TAN than it does for allowing its customers to navigate the web site. For instance, once the user makes a request for a transaction via the Web, the bank may send a text message to the user’s phone with the correct TAN. The user then responds with the correct one-time TAN via another cellular phone text message and the bank authorizes the Web transaction.

This authentication scheme soundly defeats the phishing Trojan attack scenario presented in this report. It is highly unlikely that attackers will find a way to defeat this authentication scheme in the near future; but there is no real need to do so. There are so many more opportunities to perpetuate cyber fraud requiring less effort and technical expertise. In addition, online banking users have not adopted this technology in volume yet. iDefense predicts that, as users adopt this method over the next three to five years, hackers will turn their attention to defeating this scheme.

B. Token-Based Two Factor Authentication

Some banks have recently adopted token-based authentication methods to secure their banking clients' transactions. The Channel Register reported in the summer of 2006 that, "banks in the Netherlands and Scandinavia have used two-factor authentication for years and the technology is widely credited with helping to make account fraud more difficult"[3]. In July 2006, however, the mainstream press reported that hackers had defeated the two-factor authentication scheme in place at Citibank[4].

The Citibank's website states that "a security token is a small handheld device that dynamically generates and displays a password. When signing onto CitiBusiness® Online, users simply push a button on the token to display a password. This token password is entered along with the User ID and static password. The use of this token serves as the second level of security in our two-factor authentication process."

According to Brian Krebs of the Washington Post, the Citibank tokens provide passwords that are good for about a minute.

To be clear, the Citibank attack is a traditional phishing attack and not the phishing Trojan attack presented in this paper. According to Krebs, "the scam e-mail says someone has tried to log into your account and that you need to confirm your account info. When you click the link, you get a very convincing site that looks identical to the Citibusiness login page, complete with a longish Web address that at first glance appears to end in Citibank.com, but in fact ends at a Web site in Russia called Tufel-Club.ru."

In this scam, the victim visited the fraudulent website and input their user ID, password and token password. In this traditional man-in-the-middle phishing attack, the attacker captured this information and, while the victim was still logged in, had to log into the site again with the stolen credentials and withdraw money from the account before the token password expired.

Even though the Citibank event was a traditional phishing attack, the Citibank two-factor authentication scheme is also susceptible to the phishing Trojan attack described in this paper. Because the authentication scheme relies upon the user reading the token password and then entering it into the website, the authentication scheme falls prey to the same weaknesses described in the standard OTP authentication scheme described earlier. To exploit this method, the hackers would have to modify the current phishing Trojan attack to immediately log into the victim's account while the password was still valid. The hackers have already demonstrated that this is possible with the traditional phishing attack. iDefense believes this would be a trivial modification to the current code set for the phishing Trojan described earlier.

As far back as March 2005, security experts predicted that two-factor authentication would not work for Web authentication. According to Bruce Schneier, CTO of Counterpane, "[Two-Factor Authentication] won't work for remote authentication over the Internet. I predict that banks and other financial institutions will spend millions outfitting their users with two-factor authentication tokens. Early adopters of this technology may very well experience a significant drop in fraud for a while as attackers move to easier targets, but in the end there will be a negligible drop in the amount of fraud and identity theft."[5].

Clearly, two-factor authentication does not protect its users from traditional phishing attacks or the phishing Trojan attack described in this report. The token suffers from the same weakness as the standard OTP authentication method described earlier

Stronger authentication schemes, like Public Key Infrastructure (PKI), may provide more protection but are expensive and more difficult to implement.

C. Authentication Certificates and Public Key Infrastructure (PKI)

According to Wikipedia, PKI is "an arrangement that provides for trusted third-party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried out by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates"[6]. X.509 is the standard for PKI certificates and specifies standard formats[7].

The Internet Engineering Task Force (IETF) defines PKI as "The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Public Key Certificates based on public- key cryptography"[8].

According to the DCOCE, PKI uses asymmetric encryption. Information is encrypted by using one key of a pair, the public key, and can only be decrypted using the other key, which is kept secret. No user can de-crypt a message using the same public key and only the private key can be used to decrypt the message.

For example, if a user wants to validate that they are a legitimate user at Bank A, they could encrypt their password with the public key of that bank. Once it receives the validation request, Bank A decrypts the user's password using its secret key. Mathematically, no other user in the world would be able to decrypt the password, only Bank A.

Enterprise's could use PKI in several different ways to protect banking transactions. Some are more secure than

[3] John Leyden: Phishers rip into two-factor authentication. 13 Jul 2006. http://www.channelregister.co.uk/2006/07/13/2-factor_phishing_attack/

[4] Brian Krebs: Citibank Phish Spoofs 2-Factor Authentication. July 10, 2006. http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

[5] Bruce Schneier: The Failure of Two-Factor Authentication. March 15, 2005. http://www.schneier.com/crypto-gram-0503.html#2

[6] Wikipedia: Public key infrastructure. http://en.wikipedia.org/wiki/Public_key_infrastructure

[7] Wikipedia: X.509. http://en.wikipedia.org/wiki/X.509

[8] Digital Certificate Operation in a Complex Environment (DCOCE), http://www.dcoce.ox.ac.uk/background/index.xml.ID=pki

others. Attackers also have several attack vectors they can use against PKI.

Scenario 1: No Client Certificate – Standard Bank SSL Certificate

This is the most common scenario today. Customers connect to the bank's website over a Secure Sockets Layer (SSL)-protected connection and enter their password. Attackers can use three different vectors against this scenario: malicious code, man-in-the-middle and phishing.

The trouble with SSL certificates is the emergence of a relatively new certificate type, the Domain Authenticated SSL Certificate. This sort of certificate goes through almost no authentication before issuance. In effect, anyone can get one. In the past, online banking customers had some sense of security if they saw a high-security (organizationally authenticated) SSL certificate on a website. Now that virtually anyone can obtain a Domain Authenticated SSL Certificate for their site, users can not use the presence of a SSL certificate to guarantee the safety of the site, as low-security certificates (domain-authenticated) look exactly like the high-security certificates (organizationally authenticated). This situation allows standard phishing sites and the aforementioned phishing Trojan to be successful.

Scenario 2: No Client Certificate – High Assurance Bank Certificate

This functionality is available with Internet Explorer (IE) 7 and Firefox. An end user connects to the bank website and provides his password as in the aforementioned scenario. The difference is that the end user will see additional visual confirmation that the website is authentic.

According to Tim Callan's SSL blog, "That's where High-Assurance SSL Certificates come in. These certificates will look different to the browsers, and the browsers will be able to display them differently as a result"[9].

According to Callan, "Internet Explorer will show an old-fashioned SSL Certificate in much the same way it does today. But a High Assurance certificate will get very different treatment. In this case, the browser will actually turn the address bar green, a very clear indication that this is a different kind of site you're attached to right now. Also, the name of the organization running this site and the name of the CA (Certificate Authority) who issued the certificate will appear in the address bar adjacent to the actual domain you've visited. These cues will make it easy for any site visitor using this browser to tell the difference between High Assurance and traditional SSL Certificates."

These visual clues will help the regular user identify standard phishing sites and the techniques used by the phishing Trojan discussed in this report.

Scenario 3: X.509 Certificates for both Client and Bank

PKI-based solutions, where sites and clients mutually authenticate using X.509 certificates, suffer from the same Trojan phishing attack weaknesses described in this report. The customer has some type of device (second factor authentication) that contains a client certificate and private keys. The bank authenticates the customer with that device. The problem occurs if the attacker has already exploited the computer through some other means and installs the phishing Trojan. The Phishing Trojan could easily wait for the client to connect to the bank using the X.509 algorithms and then siphon money out of the account while the user is conducting normal business.

At this time, iDefense knows of no banks that have deployed this technology. The issue with mutually authenticated PKI is that it requires banks to issue certificates to end-user consumers. Most banks do not consider this solution viable due to the complexity and expense involved in implementation.

Although X.509 certificates do not stop a well-crafted phishing Trojan, they do defeat the traditional man-in-the-middle phishing attack.

VI. Fraud Detection

Some strong authentication schemes for banking applications may reduce the risk of cyber fraud, but they are not the only mitigation technique to consider. Some security firms like RSA and VeriSign (of which iDefense is a part) provide fraud protection services for the banking applications themselves. Fraud detection services are essentially intrusion detection systems (IDS) or Intrusion Prevention Systems (IPS) for cyber fraud. They are a collection of signatures and anomaly detection algorithms that may indicate a cyber fraud attack in progress. Instead of relying upon the client authentication scheme only, some banking institutions use these fraud detection services to look for fraudulent behavior on the banking website.

Most commercial fraud detection systems include a rules engine that allows the customer to specify patterns characteristic to their environment. The Rules Engine examines each banking transaction to see if it matches any pre-determined pattern for fraudulent or high-risk transactions.

Some commercial systems also include an anomaly-detection capability. Rather than having to wait for a new attack to be detected and for a new rule to be written by an expert, these systems automatically and immediately detect unusual behavior for each user or group. Behavioral systems are inherently "future proof"—they can spot new types of attacks the first time that criminals execute them.

Signature-based detection and anomaly-based detection concentrate on key components of the banking transaction, including:

[9] Tim Callan: A new kind of SSL Certificate is on the way. March 28, 2006. http://blogs.verisign.com/ssl-blog/2006/03/a_new_kind_of_ssl_certificate_1.html

- *Computer*: Operating system, language, browser, etc.
- *Transaction Timing*: Hour of the day, day of the week, frequency of login, etc.
- *Network Information*: IP address, Geo-location, Connection Speed, Proxy types, etc.
- *Transaction Type*: Login, balance transfer, payment, etc.
- *User Type*: Student, high-net-worth individual, retiree, etc.

Fraud detection is generally cheaper and easier to deploy then the authentication techniques mentioned in this report. This is because the bank does not have to deploy anything to its customer base; fraudulent detection systems operate within the banking system proper. They watch banking transactions as they occur within the bank's server system and do not make their existence known to customers.

VII. Fraud Mitigation

Thus far, this report has discussed mitigation strategies to handle the phishing Trojan issue. iDefense does not recommend that banks implement every solution outlined here, as not all of them are sound solutions. In much the same way as perimeter defense is a matter of "Defense in Depth," cyber fraud is also a matter of "Defense in Depth." There is no single tool to prevent cyber fraud, but a series of defenses arrayed in depth will certainly lower the risk sufficiently to allow banking customers to operate safely.

A. Standard Security Best Practices

Best practices do not protect the banking customer. IDS signatures, blocking FTP outbound traffic and blocking access to C&C servers at the enterprise level will protect the bank's employees but not the customers that sit on the outside of the perimeter. Other mitigation strategies are necessary.

B. BHO Management

Banking customers have no automated method of discovering malicious BHOs today. The process is entirely manual and the investigator must be fairly technical. Still, it may be possible to craft a script that utilizes Microsoft's BHO Management Tool to discover BHOs that should not be running. More research is required.

C. Customer Anti-Virus

Providing anti-virus protection for all online banking customers via the America Online (AOL) model might be worth consideration. If the bank can declare that a current anti-virus signature list is a prerequisite for any bank transaction, then the bank has raised the protection bar to a degree. iDefense has noted that popular anti-virus products are about two weeks behind the current MetaFisher version, however. Therefore, such products will not protect against the newest immediate threat. This reduces the window of opportunity that hackers have to make a successful attack.

D. One-Time Passwords

Consider implementing some version of the OTP solutions. So far, the indexed out-of-band OTP authentication system is the most complete mitigation solution for the current problem set. As mentioned earlier, iDefense does not expect the hacker community to attempt to exploit this authentication scheme for some time. This technology is not widely deployed yet, and there are still easier means to conduct cyber fraud to bother with this issue. Other OTP solutions are worthy of consideration, too. Timed OTPs, although not completely secure, might represent a good middle ground. Such a method thwarts many of the known authentication exploitation methods, and is not as complicated for customers to use as other solutions.

E. High Assurance Certificates

These certificates will not be available until Microsoft releases IE 7 and Vista. iDefense and Verisign highly recommend that banks encourage their customers to use Web browsers that can distinguish between high-assurance certificates and low-security certificates.

F. X.509 Certificates

Deployment of X.509 certificates can greatly enhance identification and authentication services in most security situations. In fact, X.509 services will defeat the traditional man-in-the-middle phishing attack. Unfortunately, because of the way the phishing Trojan works, it is possible for a hacker to craft an attack that defeats the X.509 scheme. iDefense has seen no evidence of this kind of attack in the wild yet since no banks have deployed the X.509 solution to their customer base. iDefense does believe that hackers could engineer this attack with very little variation to the current phishing Trojan scheme currently in the wild.

G. Fraud Detection Services

Banking organizations should consider implementing anti-fraud services, as described earlier, in their respective banking websites. It is unclear whether the FFIEC will accept this mitigation measure as a way to validate identities, but since the group has not given any specific guidance as to how to accomplish its mandates, iDefense believes that this kind of service is a reasonable approach and that a bank could easily make such a case.

VIII. Conclusion

The tactics and techniques of the latest trend in online fraud, the phishing Trojan horse, could defeat some authentication schemes that were previously considered strong, such as hardware-based multi-factor authentication and OTPs. There are, however, some mitigation techniques that banks should consider including in their arsenals against such cyber fraud.

The key point to remember in this discussion is that enterprises have a range of options to choose from when

determining the appropriate program to combat cyber fraud. Decision makers must consider the right mix of security, complexity and cost suited to their customers and government regulations. Ultimately, there is no single perfect solution. "Defense in Depth" applies to cyber fraud as much as it applies to perimeter defense.

Cyber fraud happens every day, and the criminals implementing it are getting more sophisticated in their ability to automate the process. Government regulators are starting to mandate that banks increase their security postures in the wake of high-profile fraud cases. The good news is that enterprises have an array of solutions available to them that will reduce the risk of this particular threat to acceptable levels.

GLOSSARY OF TERMS

Authentication: The process of attempting to verify the digital identity of the sender of a communication such as a request to log in.

Anti-Virus: Software that attempts to identify, thwart and eliminate computer viruses and other malicious code.

Botnet: Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. While the term "botnet" can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.

Browser Helper Object (BHO): A Distributed Link Library (DLL) module designed as a plugin for Microsoft's Internet Explorer web browser to provide added functionality.

Cyber-Fraud: The act of using a computer to commit fraud (A deception deliberately practiced in order to secure unfair or unlawful gain.).

Distributed Link Library (DLL): Microsoft's implementation of the shared library concept in the Microsoft Windows operating system.

Document Object Model (DOM): A description of how an HTML or XML document is represented in a tree structure. DOM provides an object oriented application programming interface that allows parsing HTML or XML into a well defined tree structure and operating on its contents.

File Transfer Protocol (FTP): A commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet).

Hypertext Markup Language (HTML): A markup language designed for the creation of web pages with hypertext and other information to be displayed in a web browser.

Hypertext Transfer Protocol (HTTP): A method used to transfer or convey information on the World Wide Web. It is a patented open internet protocol whose original purpose was to provide a way to publish and receive HTML pages.

Identification: A process through which a system ascertains the digital identity of another entity.

Internet Explorer (IE): Microsoft's Web Browser.

Internet Relay Chat (IRC): A form of instant communication over the Internet. It is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication.

Intrusion Detection Systems (IDS): Detects unwanted manipulations to systems such as all types of malicious network traffic and computer usage: network attacks against vulnerable services, data driven attacks on applications, host-based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malicious code (viruses, Trojan horses and worms).

International Telecommunication Union (ITU): An international organization established to standardize and regulate international radio and telecommunications.

Man-in-the-Middle Attack: An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

Money Mule: Persons hired in cyber fraud schemes to withdraw money from bank accounts and deliver it to some unknown person. The person has no knowledge of the cyber fraud scheme that put the money in the bank in the first place.

One-time Pads (OTPs): An encryption algorithm where the plaintext is combined with a random key that is as long as the plaintext and used only once. If the key is truly random, never reused, and (of course) kept secret, the one-time pad can be proven to be unbreakable.

Phishing: A form of criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.

PHP: A recursive acronym that describes a general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

Secure Sockets Layer (SSL): Cryptographic protocol which provides secure communications on the Internet for such things as e-mail, Internet faxing, and other data transfers.

Trojan horse: A malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

Two-Factor authentication: Any authentication protocol that requires two independent ways to establish identity and privileges. This contrasts with traditional password authentication, which requires only one factor (knowledge of a password) in order to gain access to a system.

Windows File Explorer: Microsoft program that allows the user to view the contents of the hard drive.

Windows Metafile Format (WMF): A graphics file format on Microsoft Windows systems that hackers exploited as a zero-day exploit over a four week period at the end of December 2005 and the beginning of January 2006.

X.509: The standard for public key infrastructure (PKI),

X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm.

Note: Glossary of terms is taken and edited from entries found in Wikipedia. http://en.wikipedia.org/wiki/Main_Page

REFERENCES

[1] Shon Harris: CISSP Certification All-in-One Exam Guide, Second Edition, 2003.

[2] Brian Krebs: Citibank Phish Spoofs 2-Factor Authentication. Security Fix Blog, Washington Post. July 10, 2006. http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

[3] Wikipedia: Browser Helper Object. http://en.wikipedia.org/wiki/Browser_Helper_Object

[4] iDefense: MetaFisher: A Sophisticated Bot Attack. May 26, 2006

[5] John Leyden: Phishers rip into two-factor authentication. 13 Jul 2006. http://www.channelregister.co.uk/2006/07/13/2-factor_phishing_attack/

[6] Bruce Schneier: The Failure of Two-Factor Authentication. March 15, 2005. http://www.schneier.com/crypto-gram-0503.html#2

[7] Wikipedia: Public key infrastructure. http://en.wikipedia.org/wiki/Public_key_infrastructure

[8] Wikipedia: X.509. http://en.wikipedia.org/wiki/X.509

[9] Digital Certificate Operation in a Complex Environment (DCOCE), http://www.dcoce.ox.ac.uk/background/index.xml.ID=pki

[10] Tim Callan: A new kind of SSL Certificate is on the way. March 28, 2006. http://blogs.verisign.com/ssl-blog/2006/03/a_new_kind_of_ssl_certificate_1.html

Rick Howard (rhoward@verisign.com), Director – iDefense Security Intelligence, is responsible for the day-to-day intelligence gathering and distribution efforts at iDefense and is charged with developing strategic and tactical plans for the department. He is an experienced computer security professional with proven success in the utilization of network intelligence for network defense.

Prior to joining iDefense, Mr. Howard lead the intelligence gathering activities at Counterpane Internet Security and ran Counterpane's global network of Security Operations Centers (SOCs). Mr. Howard served in the US Army for 23 years in various command and staff positions involving information technology and security and retired as a Lieutenant Colonel in 2004. He spent the last two years of his career as the US Army's Computer Emergency Response Team Chief (ACERT) where he coordinated Network Defense, Network Intelligence and Network Attack operations for the Army's global network.

Mr. Howard holds a Masters of Science degree in Computer Science from the Naval Postgraduate School and an Engineering degree from the United States Military Academy where he also taught computer science later in his military career.

Ralph Thomas (rthomas@verisign.com), Manager – iDefense Malicious Code Operations, heads the iDefense Malicious Code Operations Group. This group is responsible for the active collection of open-source intelligence, and for the reporting and analysis of public reports and outbreaks of malicious code. Mr. Thomas also directs the malicious code research lab in iDefense, which is tasked with the development of tools for discovery and analysis of malicious code and related threats.

Before joining iDefense, Mr. Thomas worked as Principal Computer Forensics Consultant in several data acquisition and litigation support projects and served as expert witness in federal court. Early in his career Mr. Thomas designed hardware and real-time software in the controls and digital television sectors before turning his attention to enterprise software. A Certified Lotus Specialist, he has expertise in e-mail archiving, document imaging, Siebel, SAP, and Oracle Applications.

Mr. Thomas holds a Masters of Science degree in Electrical Engineering from the University Dortmund, Germany.

Jeff Burstein (jburstein@verisign.com), Product Manager - VeriSign Authentication Services, has been involved in almost every one of VeriSign's security offerings, from PKI and secure messaging to managed security services and consumer authentication. As a member of the VeriSign Identity Protection team, he has worked closely with leaders in authentication technology in designing the next generation of consumer authentication services.
Jeff holds Bachelor and Master degrees in Computer Science from the Massachusetts Institute of Technology.

Roxana Bradescu (rbradescu@verisign.com), Senior Manager - VeriSign Innovations, defines new VeriSign Identity Protection (VIP) services.

Prior to VeriSign, Roxana provided product marketing consulting to a number of startups developing security and networking products, and was an Entrepreneur in Residence at Foundation Capital. Roxana has held numerous senior management positions including Excite@Home, Sun Microsystems, Navio/Liberate, and AT&T Bell Labs focusing on new product and emerging business opportunities.