Technical Trends in Phishing Attacks

Jason Milletary
CERT Coordination Center[1]

1 Abstract

The convenience of online commerce has been embraced by consumers and criminals alike. Phishing, the act of stealing personal information via the internet for the purpose of committing financial fraud, has become a significant criminal activity on the internet. There has been good progress in identifying the threat, educating businesses and customers, and identifying countermeasures. However, there has also been an increase in attack diversity and technical sophistication by the people conducting phishing and online financial fraud. Phishing has a negative impact on the economy through financial losses experienced by businesses and consumers, along with the adverse effect of decreasing consumer confidence in online commerce.

Phishing scams have flourished in recent years due to favorable economic and technological conditions. The technical resources needed to execute phishing attacks can be readily acquired through public and private sources. Some technical resources have been streamlined and automated, allowing use by non-technical criminals. This makes phishing both economically and technically viable for a larger population of less sophisticated criminals.

In this paper, we will identify several of the technical capabilities that are used to conduct phishing scams, review the trends in these capabilities over the past two years, and discuss currently deployed countermeasures.

2 Background

The act of tricking individuals into divulging their sensitive information and using it for malicious purposes is not new. Social engineering attacks have occurred on the internet throughout its existence. Before widespread use of the internet, criminals used the telephone to pose as a trusted agent to acquire information. The term “phishing” has origins in the mid-1990s, when it was used to describe the acquisition of internet service provider (ISP) account information. However, today the term has evolved to encompass a variety of attacks that target personal information. For this paper, we will focus on crimes targeting personal information used for financial fraud and identity theft.

Criminals targeting user information are able to profit from the increased adoption of online services for many day-to-day activities, including banking, shopping, and leisure activities. Users of these services provide a target of opportunity in that they possess information of value. Along with an increase in the number of potential targets, there are three major factors that criminals have been able to take advantage of:

[1]CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Unawareness of threat - If users are unaware that their personal information is actively being targeted by criminals, they may lack the perspective needed to identify phishing threats and may not take the proper precautions when conducting online activities.

Unawareness of policy - Phishing scams often rely on a victim's unawareness of organizational policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation. Customers unaware of the policies of an online merchant are likely to be more susceptible to the social engineering aspect of a phishing scam, regardless of technical sophistication.

Criminals' technical sophistication - Criminals conducting phishing scams are leveraging technology that has been successfully used for activities such as spam, distributed denial of service (DDoS), and electronic surveillance. Even as customers are becoming aware of phishing, criminals have responded with technical tricks to make phishing scams more deceptive and effective.

2.1 Phishing Today

Originally, phishing was identified as the use of electronic mail messages, designed to look like messages from a trusted agent, such as a bank, auction site, or online commerce site. These messages usually implore the user to take some form of action, such as validating their account information. These messages often use a sense of urgency (such as the threat of account suspension) to motivate the user to take action. Recently, there have been several new social engineering approaches to deceive unsuspecting users. These include the offer to fill out a survey for an online banking site with a monetary reward if the user includes account information, and email messages claiming to be from hotel reward clubs, asking users to verify credit card information that a customer may store on the legitimate site for reservation purposes. Included in the message is a URL for the victim to use, which then directs the user to a site to enter their personal information. This site is crafted to closely mimic the look and feel of the legitimate site. The information is then collected and used by the criminals. Over time, these fake emails and web sites have evolved to become more technically deceiving to casual investigation.

Recently the definition of phishing has grown to encompass a wider variety of electronic financial crimes. In addition to the widespread use of these fake email messages and web sites to lure users into divulging their personal information, we have also observed an increase in the amount of malicious code that specifically targets user account information. Once installed on a victim's computer, these programs use a variety of techniques to spy on communications with web sites and collect account information. This method differs from the technical subterfuge generally associated with phishing scams and can be included within the definition of spyware as well. It is important to include them in a discussion on phishing trends for the following reasons:

Social component – Criminals often use social engineering along with vulnerabilities in applications such as web browsers or email clients to trick users into installing malicious code on their computer.

Common infrastructure – We have observed the use of common tools and techniques for delivering phishing emails and distributing malware. These include the use of botnets, open mail relays, and compromised web sites to host phishing sites and malware.

The big picture - As countermeasures are implemented to thwart one method of stealing information, criminals still have additional opportunities available to them. It is important to understand the technical capabilities available to these criminals so that more effective measures for protecting customer information can be developed and law enforcement personnel tasked with tracking down and prosecuting criminals conducting phishing scams can be more effective.

3 Tackle Box

Just as with real fishermen, phishers today have a large tackle box of tools available to them. These tools serve a variety of functions, including email delivery, phishing site hosting, and specialized malware.

- Bots/Botnets
- Phishing Kits
- Technical Deceit
- Session Hijacking
- Abuse of Domain Name Service (DNS)
- Specialized Malware

3.1 Bots/Botnets

"Bots" refer to programs that reside on a computer and provide remote command and control access via a variety of protocols, including IRC, HTTP, instant messaging, and peer-to-peer protocols. When several of these bots are under common control, it is commonly referred to as a botnet. Bots provide the controller with features that can be used to support illicit activity, including

- Relays for sending spam and phishing emails
- Web servers or redirectors for spam/phishing sites or malware distribution
- Updates for existing malware
- Installation of additional malware
- Distributed denial of service (DDoS)
- Proxy services
- Pay-for-click services
- Vulnerability scanning and exploitation
- Surveillance

In addition to the ability of most bots to infect new hosts through built-in scanning and exploitation of vulnerabilities, bots can also be deployed through social engineering techniques. These include mass mailing, file-sharing programs, and instant messaging networks.

3.2 Phishing Kits

Over the past two years, the criminals performing phishing attacks have become more organized. One indication of increased organization is the development of ready-to-use phishing kits containing items such as pre-generated HTML pages and emails for popular banks and online commerce sites, scripts for processing user input, email and proxy server lists, and even hosting services for phishing sites. These hosting services usually advertise themselves as being impossible to shut down, or "bulletproof" [Roberts 2004] and have been used by spammers for years [McWilliams 2003]. Traditionally these kits are bought and sold by criminals within the underground economy; however, versions of these kits have been found available for anyone to download at no cost [Sophos 2004]. Phishing kits provide a lower barrier to entry into the marketplace for criminals, reducing the amount of technical knowledge required to conduct a phishing scam.

3.3 Technical Deceit

As users have become more aware of phishing and better educated about the signs for detecting fake emails and web sites, criminals are developing techniques to counter this awareness. These techniques include URL obfuscation to make phishing emails and web sites appear more legitimate, and exploitation of vulnerabilities in web browsers that allow the download and execution of malicious code from a hostile web site.

3.3.1 Basic URL Obfuscation

URL obfuscation misleads the victims into thinking that a link and/or web site displayed in their web browser or HTML-capable email client is that of a trusted site. These methods tend to be technically simple yet highly effective, and are still used to some extent in phishing emails today.

Simple HTML redirection

One of the simplest techniques for obscuring the actual destination of a hyperlink is to use a legitimate URL within an anchor element but have its href attribute point to a malicious site.[2] Thus clicking on a legitimate-looking URL actually sends the user to a phishing site. This deception can be detected because web browsers display the actual destination of a hyperlink when a user moves the mouse pointer over the link; this information is typically displayed in the web browser's status bar.

Use of JPEG images

Electronic mail rendered in HTML format is becoming more prevalent. Phishers are taking advantage of this by constructing phishing emails that contain a single image in JPEG format. When displayed, this image appears to be legitimate email from an online bank or merchant site. The image often includes official logos and text to add to the deception. However, when users click on this image, they are directed to a phishing site. As with the previous example, phishing emails using this technique can often be detected by observing the actual destination URL when mousing over the image.

[2] See http://www.w3.org/TR/html401/struct/links.html#h-12.1 for an overview of anchors and links in HTML.

Use of alternate encoding schemes

Hostnames and IP addresses can be represented in alternate formats that are less likely to be recognizable to most people. Alphanumeric characters can be changed to their hexadecimal representations as follows:

Hexadecimal	`%68%74%74%70%3a%2f%2f%77%77%77%2e%65%78%61%6d%70%6c%65%2e%63%6f%6d`
ASCII Text	`http://www.example.com`

Also, IP addresses can be specified as a hexadecimal number:

Dotted Quad Notation	`192.168.1.1`
Hexadecimal Format	`0xc0a80101`

Web browsers will properly interpret both of these representations. These alternate encoding formats are most often observed in cross-site scripting attacks to obfuscate the malicious URL.

Registration of similar domain names

At initial glance, users may attempt to verify that the address displayed in the address or status bar of their web browser is the one for a legitimate site. Phishers often register domain names that contain the name of their target institution to trick customers who are satisfied by just seeing a legitimate name appear in a URL. An example is hosting a phishing site at http://www.<bankname>-online.biz, where <bankname> would be replaced by the name of the target bank. A widely implemented version of this attack uses parts of a legitimate URL to form a new domain name as demonstrated below:

```
Legitimate URL          http://login.example.com
Malicious URL           http://login-example.com
```

3.3.2 Web Browser Spoofing Vulnerabilities

Over the past two years, several vulnerabilities in web browsers have provided phishers with the ability to obfuscate URLs and/or install malware on victim machines. Below are two examples of recent web browser vulnerabilities that could be used in phishing scams. All the vulnerabilities listed currently have fixes available from their associated vendors. However, these vulnerabilities can still be exploited on computers that are not up to date with security patches.

VU#490708 - Microsoft Internet Explorer window.createPopup() method creates chromeless windows

Exploitation of this vulnerability could allow an attacker to include code in a phishing site that would create a borderless pop-up window that would overlay the address bar. This window could contain an image of a legitimate URL that would obscure the illegitimate URL of the phishing site. We have observed this vulnerability included in pre-generated web pages in phishing kits for popular banks.

VU#356600 - Microsoft Internet Explorer DHTML Editing ActiveX control contains a cross-domain vulnerability

Exploitation of this vulnerability could allow an attacker to use the DHTML Edit ActiveX control loaded from the malicious web site to alter content in a browser window in a different domain. A phisher can take advantage of this by tricking a user into clicking on a malicious URL that loads the DHTML Edit control, opens a new browser window for the trusted site, and then uses the vulnerable control to replace content within the browser window containing the trusted site. All other attributes of the browser window (SSL certificate information, page properties) would be for the legitimate web site. Proof-of-concept attacks for this vulnerability have been demonstrated, but its use in actual phishing attacks has not been confirmed.

3.3.3 International Domain Names (IDN) Abuse

International Domain Names in Applications (IDNA) is a mechanism by which domain names with Unicode characters can be supported in the ASCII format used by the existing DNS infrastructure. IDNA uses an encoding syntax called Punycode [RFC3492] to represent Unicode characters in ASCII format. A web browser that supports IDNA would interpret this syntax to display the Unicode characters when appropriate. Users of web browsers that support IDNA could be susceptible to phishing via homograph attacks [Gabrilovich 2002], where an attacker could register a domain that contains a Unicode character that appears identical to an ASCII character in a legitimate site (for example, a site containing the word “bank” that uses the Cyrillic character “a” instead of the ASCII “a”). While a proof-of-concept of this type of attack was made public, there has not been any publicly reported IDNA abuse within a phishing scam.

3.3.4 Web Browser Cross-Zone Vulnerabilities

Most web browsers implement the concept of security zones, where the security settings of a web browser can vary based on the location of the web page being viewed. We have observed phishing emails that attempt to lure users to a web site attempting to install spyware and/or malware onto the victim’s computer. These web sites usually rely on vulnerabilities in web browsers to install and execute programs on a victim’s computer, even when these sites are located in a security zone that is not trusted and normally would not allow those actions.

VU#323070 – Outlook Express MHTML protocol handler does not properly validate location of alternate data

This is a cross-domain vulnerability where a specifically formatted URL invoking the InfoTech Storage (ITS)[3] format protocol handlers could cause Internet Explorer to load an HTML document located within a Microsoft HTML Help (CHM) file. This HTML document would then be rendered in the Local Machine Zone.

This HTML document could contain a script, ActiveX object, or IFRAME element to download and execute malicious code. We have observed this vulnerability used extensively in attempts to install malware.

VU#973309 – Mozilla may execute JavaScript with elevated privileges when defined in site icon tag

This cross-domain vulnerability in the Mozilla suite of web browsers allows scripts within the LINK tag to run unprompted with the privilege of the user running the web browser. We have observed this vulnerability used in an attempt to install malware.

3.4 Session Hijacking

Most phishing scams rely on deceiving a user into visiting a malicious web site. However, there is the threat of a user being redirected into a phishing site even if they correctly try to access a legitimate site.

3.4.1 Domain Name Resolving Attacks

Navigation of the internet by humans heavily relies on the process of mapping easy-to-remember domain names to IP addresses. There are techniques for subverting this process to forcefully redirect users to a malicious site. One technique compromises the information used by the Domain Name System (DNS) through injection of malicious information into authoritative DNS query responses, a technique called DNS cache poisoning. The term “pharming” was recently created to describe this particular attack being used to perpetrate phishing scams. Another technique is to add malicious entries to a computer’s *hosts* file, which on some operating systems will be checked by the local domain name resolver before making a request to a DNS server. There have been many instances of malware adding bogus entries to a computer’s *hosts* file.

3.4.2 Cross-Site Scripting Attacks

Cross-site scripting (XSS) attacks can occur in programs on web sites that accept user input. If the program does not properly sanitize the input data, the vulnerable program may process input or even execute code that the original program was not intended to do. For example, a phisher could construct a URL that uses a vulnerable program on a legitimate commerce site. This URL would also contain (probably obfuscated) code, such as JavaScript, that could target account credentials. There have been reports that this type of attack was used in a phishing scam against a bank.

[3] The ITS format is used by Compiled HTML (CHM) files.

A more common XSS attack that has been used in phishing involves the exploitation of vulnerable URL redirector programs. URL redirectors are often used by web sites to perform custom processing based on attributes such as web browser or authentication status or even just to display a message when clicking on a link to an external site. There have been multiple incidents of commerce sites using URL redirectors that allowed a user to input any external URL they wanted to. Thus phishers were able to send phishing emails with URLs that used the vulnerable redirectors on the legitimate sites to trick people into visiting phishing sites.

3.4.3 Domain Name Typos

A recent attack trend has been the registration of domain names that closely resemble the domain name of a legitimate high-traffic site. The domain names are sometimes used to host sites aiming to install spyware or malware on the computer of a victim who mistypes the intended domain name. It would also be possible to register domain names that could be common typographical variants of online commerce sites.

3.4.4 Man-in-the-Middle Attacks

Man-in-the-middle attacks define a broad class of potential attacks in which an attacker is able to intercept, read, and modify communications between two other parties without their knowledge. As related to phishing, a man-in-the-middle attack involves an attacker serving as a proxy between a user and an online commerce site. The attacker potentially has access to all authentication and account information, including an opportunity to hijack credentials used in two-factor authentication.

3.5 Abuse of Domain Name Service

Criminals often take advantage of dynamic DNS providers, which are often used for providing a static domain name mapping to a dynamic IP address. This service can be useful to phishers by providing them with the ability to easily redirect traffic from one phishing site to another if the initial site is shut down. With ISPs and law enforcement becoming more proactive in shutting down phishing sites, the use of dynamic DNS and registration of multiple IP addresses for a single fully qualified domain name (FQDN) is becoming more prevalent to increase the resilience of phishing sites.

3.6 Specialized Malware

Over the past two years, there has been an emergence of malware being used for criminal activity against users of online banking and commerce sites. This type of specialized malware (which can be considered a class of spyware) greatly increases the potential return on investment for criminals, providing them with the ability to target information for as many or as few sites as they wish. One benefit for criminals is that most malware can easily be reconfigured to change targeted sites and add new ones. Malware also provides several mechanisms for stealing data that improve the potential for successfully compromising sensitive information.

3.6.1 Electronic Surveillance

Software that can capture and record a user's keystrokes and mouse clicks has existed for years. These programs are now being customized to specifically target information about online sites of interest by looking at keystrokes typed in web browsers. Malware can also capture network packets or protocol information of interest (for example, HTTP post data sent to a targeted banking URL). While HTTPS (HTTP over SSL) is used for most online commerce web sites, malware can easily access sensitive data before it is encrypted for transit over the network. We have also observed malware that takes screenshots when it detects that a web browser is visiting a site of interest. This could potentially allow the capture of sensitive information, including bank account numbers and account balances.

3.6.2 Password Harvesters

Several classes of malware are able to search a computer for account and password information. On Microsoft Windows platforms, this includes searching the registry and Protected Store. The Protected Store is a facility provided by the Microsoft CryptoAPI and is used to store sensitive data, including Internet Explorer AutoComplete fields, passwords, and digital certificates.

3.6.3 Self-Contained Scam Pages and Dialog Boxes

Several samples of malware that target banking information have been observed to use techniques similar to phishing sites. These programs monitor for connections to specific banking URLs and either display a pop-up window or dialog box, or attempt to overlay the existing web page with a fake one. These forged screens usually prompt the user to reenter all their account information, often using the same techniques seen in phishing emails (such as a warning about fraud activity that requests the user to verify their account information).

Malware with this capability appears to be targeted against sites where sensitive information may not be easily recovered from the data submitted to the server during authentication. An example would be the obfuscation of this sensitive information on the client-side before transmission to the server, such as asking the user to enter the individual digits of their PIN in random order. Interception of this data would reveal the correct digits, but not in their correct order. Malware attempting to counter this protection would wait for a successful login to a targeted site, then display a dialog box or overlaid web page asking the user to confirm their sensitive information, which would include the PIN number in correct order.

3.6.4 Account Siphoners

Almost all phishing malware functions by attempting to steal account authentication information and exfiltrate that information to a location where it can be used later. However, there is at least one example of malware that actively steals money from a financial services site by automating a monetary transfer from the victim's account.

3.6.5 Phishing-Related Malware Examples

The following are examples of malware used to conduct phishing scams. This is by no means an exhaustive list, but it is a fair representation of the different techniques and capabilities of most malware currently used in phishing attacks.

Bancos

Originally identified in July 2003, Bancos (also identified as Banker by some anti-virus companies) is one of the oldest and largest categories of phishing malware. Bancos originally targeted Brazilian banks. The arrests of a phishing crime ring lead by Vladir Paulo de Almeida in March 2005 [Leyden 2005] demonstrates the impact a trojan like Bancos could have in Brazil. Bancos monitors Internet Explorer for specific bank URLs and attempts to capture account information. Bancos can overlay certain banking web pages with a fake one that captures the information directly from a user.

This includes the graphical touchpad that some banks are using on their websites for users to enter in their account numbers and PINs to counter against keystroke loggers.

Bankash

Bankash originally made news in February 2005 as the first known malicious program that attempted to disable the Microsoft anti-spyware program [Broersma 2005]. Bankash is implemented as an Internet Explorer Browser Helper Object (BHO) and targets online banking information. BHOs are "components—specifically, in-process Component Object Model (COM)[4] components—that Internet Explorer loads each time it starts up. Such objects run in the same memory context as the browser and can perform any action on the available windows and modules" [Esposito 1999].

Once Bankash is installed, it monitors Internet Explorer activity for URLs of targeted banks. It uses the COM interfaces for Internet Explorer to harvest information from web pages and to display custom scam pages for banks of interest. These scam pages, which appear to be legitimate bank pages, ask the users to verify their account information. All the information available to users to verify the legitimacy of the web site (address bar, SSL certificate, and title bar) indicates the original bank. Bankash also targets TANs (transaction numbers) used by many banks in Germany to authorize individual transactions.

In addition, Bankash targets any information submitted via HTTPS. A blacklist is used to avoid logging information captured during SSL connections to sites that may be considered less valuable. This list is continually updated as new variants are released. Finally, Bankash scans the computer for email addresses and the Microsoft Protected Store for stored passwords.

[4] See http://msdn.microsoft.com/library/default.asp?url=/archive/en-us/dnarguion/html/msdn_drguion020298.asp for an overview of Microsoft COM.

W32/Grams

W32/Grams is an account siphoner that uses COM automation to directly steal money from a victim's account on an online financial site. Since this malware does not target account credentials, current authentication countermeasures such as two-factor authentication do not mitigate this threat.

CoreFloo

CoreFloo (also known as AFCore) is a bot that gains remote command and control of an infected computer. Among many capabilities it provides is the ability to monitor for HTTP traffic to specified URLs. We have received reports of this malware being used to specifically target banking sites.

4 Phishing Countermeasures

Various solutions have been developed in response to phishing. These solutions target both technical and non-technical problem areas.

4.1 Widely Implemented Countermeasures

Although there are multiple recommendations for countering phishing, the following list contains the ones most commonly implemented today to either combat phishing directly or to mitigate phishing-capable threats such as malware.

4.1.1 Awareness and Education

Originally, the primary advantage for criminals conducting phishing-related fraud was the lack of education and awareness of a) the existence of financial crimes targeting internet users, and b) the policies and procedures of online sites for contacting their customers regarding account information and maintenance issues. Both of these issues are being addressed by the online commerce sites and the information security community though various awareness mechanisms:

- General information on phishing distributed in company email or on a company's web site
- Alerts sent to customers about phishing scams directly targeting a specific company
- Reminders to customers of corporate policies on contacting customers regarding their account
- Papers and talks from the security community targeted to users and businesses

When companies choose to implement a customer phishing awareness program, it is important that they educate employees as well. In particular, the employees who interact with customers should be knowledgeable about phishing so they can answer customers' questions.

Note that we have observed the criminals attempting to take advantage of increasing awareness by phrasing their phishing emails accordingly; for example, a phishing email might state that the customer's account information may have been compromised due to a phishing scam.

Finally, a significant portion of phishing awareness efforts have focused on the threats posed by phishing emails and web sites. However, there is a significant threat from malware that people need to be made aware of as well. When a phishing email or web site is properly identified by a consumer, he or she can easily correlate it with the action of trying to steal account information. However, if malware is detected on a user's computer, the common response is to follow instructions on isolating and removing the threat. The user may not be aware of the functionality of the malware and thus the correlation to the action of trying to steal account information may not be clear.

4.1.2 Targeting Hosting Sites

One advantage to those who seek to shut down phishing sites is that there is little stealth in the sending of phishing emails. Since phishing emails use the same mass-mailing infrastructure as spam, affected institutions, ISPs, and law enforcement can be made aware of a site hosting a phishing scam and take efforts to get that site shut down. Affected companies have implemented methods for customers to submit phishing emails they have received. These emails, along with monitoring of web access logs for suspicious activity, can help indicate the existence of a new phishing site. Data from the Anti-Phishing Working Group's trends reports show an approximate decrease of 10% in the average time online for a phishing site from October 2004 to April 2005 (6.4 days to 5.8 days) [APWG].

Phishers have taken steps to make phishing sites hosting scam pages and the drop sites for compromised data more survivable. This includes the use of dynamic DNS entries and/or port-level redirectors to make networks of phishing sites more resistant to failure of any individual node. If a site that was pointed to by a hostname is taken down, it is possible for a phisher who is using dynamic DNS or a hosting service that provides DNS management to change the hostname to resolve to another compromised machine to serve as a phishing site. Shutting down a redirector shuts down a pathway to a phishing site, but not the site itself. Also, a FQDN resolving to multiple IP addresses makes the phishing site harder to shut down unless the FQDN itself is revoked.

Another form of redirection is the use of a 3rd party to collect information before transmission to its final destination. This could be the use of a 3rd party forms provider used to collect data as part of an e-mail based phishing attack or a script at a drop site for phishing malware that transports the data to a different host. In either case, take down of the publicly-visible site may stop the phishing attack, but not provide access to the cache of stolen information.

4.1.3 Web Browser Toolbars

One of the efforts to protect customers from phishing scams is the development of toolbars for web browsers that can help identify that a customer is viewing a possible phishing site. Primarily, these toolbars function by referencing a database of known FQDNs and IP addresses that have been reported as hosting phishing sites. This requires the phishing site to have been observed and reported in the database.

Some toolbar solutions also offer detection of potential phishing sites by checking for certain heuristics that usually indicate that a site is not a legitimate commerce site (for example, the server IP address belongs to a network associated with a broadband service provider in a different country than the user).

4.1.4 Strong Authentication and Authorization

Two-factor authentication is a mechanism requiring two or more authenticators, usually consisting of something you know (such as a password or PIN) and something you have (such as a credit card or hardware token). For online commerce, two-factor authentication is being implemented by providing the customer with a hardware token for generating a continually changing component for their authentication credentials. The goal is to protect the users if their authentication credentials have been captured by an attacker via electronic surveillance. The timeliness of the ever-changing component limits the attacker's ability to use the credentials in the future. However, with the W32/Grams trojan, we have already seen that it is theoretically possible for malware to automate a web browser to initiate a funds transfer from an already authenticated session.

Another countermeasure being implemented by certain banks is the use of transaction numbers (TANs) for authorizing individual transactions. Customers are sent a list of TANs with their monthly statement, and they enter the next unused TAN when authorizing a transaction online. There are also implementations in which users receive a request for their TAN via an out-of-band mechanism, such as an SMS message on their cell phone. As noted previously, at least one trojan (Bankash) attempts to trick customers of specific banks into divulging their next TAN. The criminal then has a limited but significant time window in which to use that TAN before the customer attempts another transaction.

4.1.5 Virus, Spyware, and Spam Prevention

Solutions designed to protect users from viruses, trojans, spyware, and spam play a role in protecting users from phishing scams. With the marked increase in phishing malware, products that detect and prevent the installation and execution of malicious code are an essential part of an environment for secure home computing. These products must be enabled and, in the case of anti-virus and anti-spyware products, must have up-to-date signatures. A large portion of recent malware attempts to disable anti-virus and anti-spyware software before a detection signature is able to detect and neutralize the malware.

Spam prevention has also contributed to the fight against phishing. Phishing emails use the same distribution mechanism as spam and usually have many of the same characteristics. Email filtering based on content blacklisting, Bayesian filtering, blocking mail from known spamming/phishing relays, anti-forgery solutions such as Sender Policy Framework (SPF) and Sender ID, and other heuristics specific to phishing can help prevent a great many phishing emails from ever reaching potential victims in the first place. However, spammers are continually evolving their tricks for bypassing filters [Schmidt] and the phishers can leverage this.

4.2 Recommendations

Though there has been an increase in the general public's awareness of phishing and has been success in reactive solutions to prevent phishing scams, countermeasures need to be designed with the big picture in mind. Based on the trends in the technical capabilities of phishing, the following recommendations provide high-level guidance for businesses, customers, and law enforcement to help them deal with the increasing technical capabilities of criminals conducting phishing scams.

4.2.1 Awareness

Phishing awareness must continue to evolve to address the growing capabilities available to phishers. This awareness should be promoted not just to customers, but also to employees of targeted businesses and law enforcement personnel who are responsible for investigating electronic financial crimes. Customers need to be aware of the increasing sophistication and use of technical deceit in phishing emails and web sites that make them more difficult to detect. They must also be aware of the potential financial impact to them from the installation of malicious code on their computers. Businesses need to be aware of the ever-changing capabilities of phishing attacks in order to design more secure online applications and to more rapidly recognize scams targeting them.

Individuals in law enforcement and support roles need to understand the tools used in phishing attacks and how they work in order to increase the chances of attack attribution.

4.2.2 Vigilance

Part of the strategy to curtail phishing is to decrease the return on investment of the activity to the criminal community. By continuing to develop and enforce existing countermeasures to phishing, the resources used for phishing (compromised computers, effective malware, etc.) become more scarce and expensive, making phishing less profitable. Thus it is important to aggressively target and shut down phishing sites. Since many phishing emails contain direct links to graphic elements stored on the site being spoofed, some online sites have begun to monitor their web access logs looking for suspicious patterns that may indicate a phishing site in use. Also, commerce site administrators must be aware of attack vectors such as IDN and similar domain name abuse that phishers may use and take steps to stop the abuse of these domain names.

Secure home computing is another important element in combating phishing attacks. Key steps in achieving this goal are having secure configurations, keeping up to date with operating system and program patches, and mitigating against malware (anti-virus, anti-spyware, and not using accounts with administrator privileges to browse the web and read email) protects computers from malware targeting their sensitive information directly and from bots that turn their computers into resources to commit phishing scams and other crimes.

4.2.3 Foresight

When designing and implementing online commerce sites, companies should be aware of when sensitive information is at risk. Traditionally, the concern was interception of data from the customer's computer to the online commerce site.

However, as we have seen with phishing malware, the web browser is a target of opportunity for criminals to intercept sensitive information before it leaves the customer's computer. Also, it is important to realize the importance of authorization of transactions. Most phishing attacks target authentication information because it is still relatively simple and the economic reward is large. However, as protections such as two-factor authentication are more widely implemented, attacks can evolve to target weaknesses in transaction authorization, as demonstrated by W32/Grams and Bankash.

While businesses are making customers aware of the threat of phishing and their policies and practices for contacting users, there should also be consideration for providing the customer with the ability to verify the authenticity of electronic communications.

5 Conclusion

Phishing is a highly profitable activity for criminals. Over the past two years, there has been an increase in the technology, diversity, and sophistication of these attacks in response to increased user awareness and countermeasures, in order to maintain profitability.

Users have become more aware of phishing crimes and how to identify unsophisticated phishing sites. In response, criminals are using web browser vulnerabilities and obfuscation techniques to create phishing scam pages that are more difficult to differentiate from legitimate sites; thus users can become victims even if they are aware of phishing scams.

In reaction to increasing response from service providers and law enforcement, criminals are using increasing technical sophistication to establish more survivable infrastructures that support phishing activities. The key building blocks for these infrastructures are the botnets that are used to send phishing emails and host phishing sites.

We have also observed specialized malware that can be used to target sensitive information, with an increased potential to cause damage. Malware is providing the means for criminals to create more effective phishing attacks that can target multiple businesses at a time. Malware is also evolving to acquire particular sensitive information (e.g., TAN numbers) that was created especially for authorizing online commerce transactions.

These trends are important to understand as they show the ability of criminals to recognize and adapt to increasing awareness of and response to phishing. By properly understanding the continual evolution of technical capabilities used by those who commit phishing and online financial fraud in general, more effective countermeasures and more secure online commerce systems can be developed.

References

[APWG] Anti-Phishing Working Group. *Phishing Activity Trends Report, October, 2004.* http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf

[APWG] Anti-Phishing Working Group. *Phishing Activity Trends Report, April 2005.* http://antiphishing.org/APWG_Phishing_Activity_Report_April_2005.pdf

[Broersma 2005] Broersma, Matthew. "Trojan Targets Microsoft's AntiSpyware Beta." http://www.eweek.com/article2/0,1759,1763560,00.asp (February 10, 2005).

[Esposito 1999] Esposito, Dino. "Browser Helper Objects: The Browser the Way You Want It." http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp (January 1999).

[Gabrilovich 2002] Gabrilovich, Evgeniy & Gontmakher, Alex. "The Homograph Attack." *Communications of the ACM*, 45(2):128, February 2002. http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf

[Leydon 2005] Leydon, John. "Brazilian cops net 'phishing kingpin'." http://www.channelregister.co.uk/2005/03/21/brazil_phishing_arrest/ (March 21, 2005).

[McWilliams 2003] McWilliams, Brian. "Cloaking Device Made for Spammers." http://www.wired.com/news/business/0,1367,60747,00.html (October 9, 2003).

[RFC3492] Costello, A. "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)." http://www.ietf.org/rfc/rfc3492.txt (March 2003).

[Roberts 2004] Roberts, Paul. "More Scam Artists Go Phishing." http://www.pcworld.com/news/article/0,aid,116330,00.asp (May 31, 2004).

[Schmidt] Schmidt, Tom. "How Filtering Screens Out Spam." http://www.itstrategycenter.com/itworld/Threat/viruses/how_filtering_screens/

[Sophos 2004] "Do-it-yourself phishing kits found on the internet, reveals Sophos," http://www.sophos.com/spaminfo/articles/diyphishing.html (August 19, 2004).

[Stewart 2004] Stewart, Joe. "Win32.Grams E-Gold Account Siphoner Analysis." http://www.lurhq.com/grams.html (November 4, 2004).

[VU#273262] Dormann, Will. "Multiple web browsers vulnerable to spoofing via Internationalized Domain Name support." http://www.kb.cert.org/vuls/id/273262 (March 22, 2005).

[VU#323070] Manion, Art. "Outlook Express MHTML protocol handler does not properly validate source of alternate content." http://www.kb.cert.org/vuls/id/323070 (April 5, 2005).

[VU#356600] Dormann, Will. “Microsoft Internet Explorer DHTML Editing ActiveX control contains a cross-domain vulnerability.” http://www.kb.cert.org/vuls/id/356600 (January 5, 2005).

[VU#490708] Dormann, Will & Manion, Art. “Microsoft Internet Explorer window.createPopup() method creates chromeless windows.” http://www.kb.cert.org/vuls/id/490708 (September 10, 2004).

[VU#973309] Dormann, Will. “Mozilla may execute JavaScript with elevated privileges when defined in site icon tag.” http://www.kb.cert.org/vuls/id/973309 (April 19, 2005).

Copyright 2005 Carnegie Mellon University.