Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

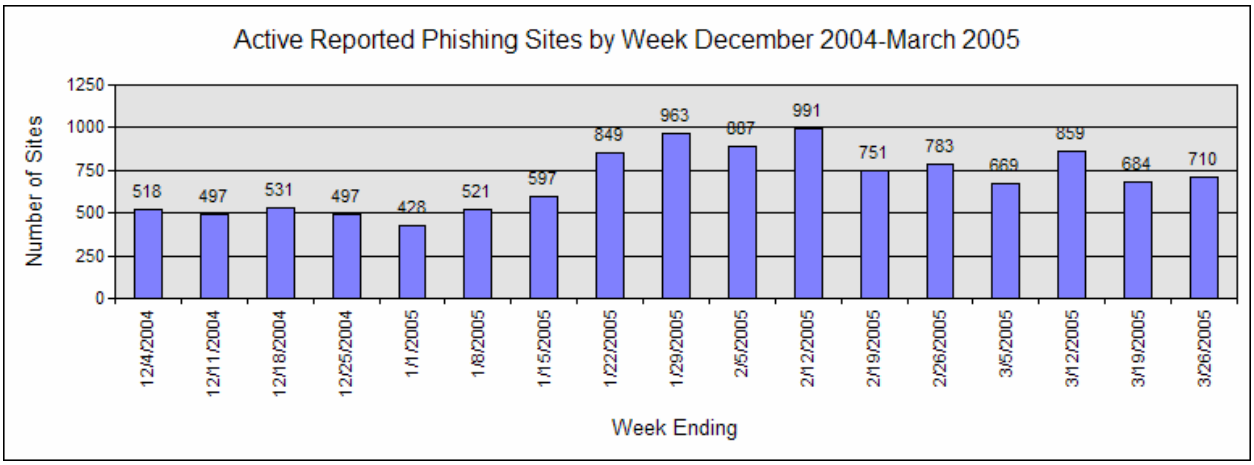
Phishing Activity Trends Report March, 2005

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, data suggests that phishers are able to convince recipients to respond to them. As a result of these scams, an increasing number of consumers are suffering credit card fraud, identity theft, and financial loss.

The 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.

Highlights

- Number of active phishing sites reported in March: **2870**
- Average monthly growth rate in phishing sites July 2004 through March 2005: **28 %**
- Number of brands hijacked by phishing campaigns in March: **78**
- Number of brands comprising the top 80% of phishing campaigns in March: **8**
- Country hosting the most phishing websites in March: **United States**
- Contain some form of target name in URL: **31 %**
- No hostname just IP address: **48 %**
- Percentage of sites not using port 80: **3.89 %**
- Average time online for site: **5.8 days**
- Longest time online for site: **31 days**



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:

TUMBLEWEED COMMUNICATIONS

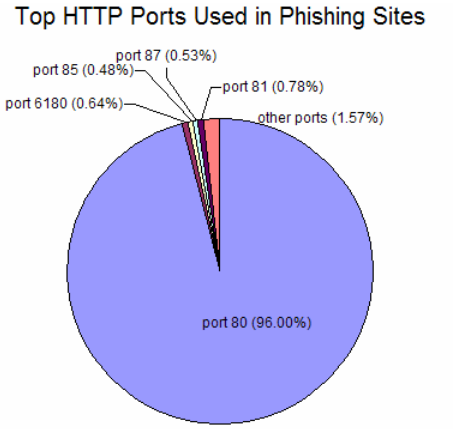
WEBSENSE.

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

APWG Trend Alert

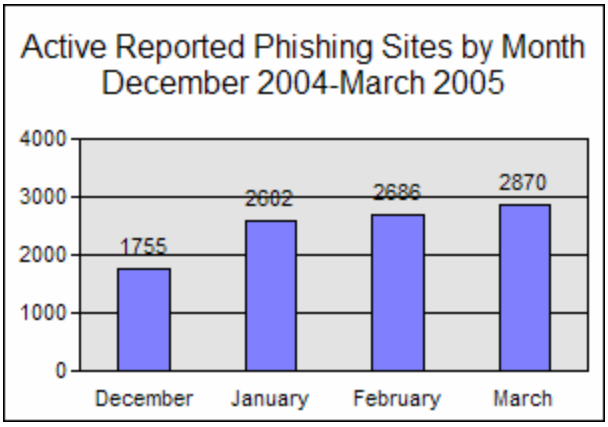
March saw a continuation of a trend of using cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use at 96% of all phishing sites reported.



Email Phishing Attack Trends

In March, there were 13,353 phishing email messages reported to the APWG. This is a slight increase of 2% over the reports for February. This is over five times the number of reports from July (2,625).

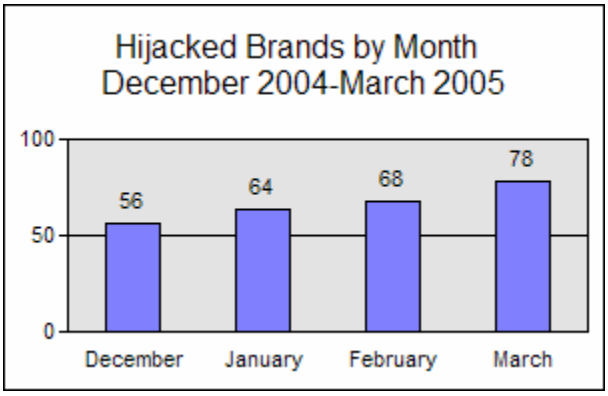
The number of phishing websites supporting these attacks grew faster, rising 6.9% from 2686 to 2870.



What Brands Are Being Hijacked By Email Phishing Attacks?

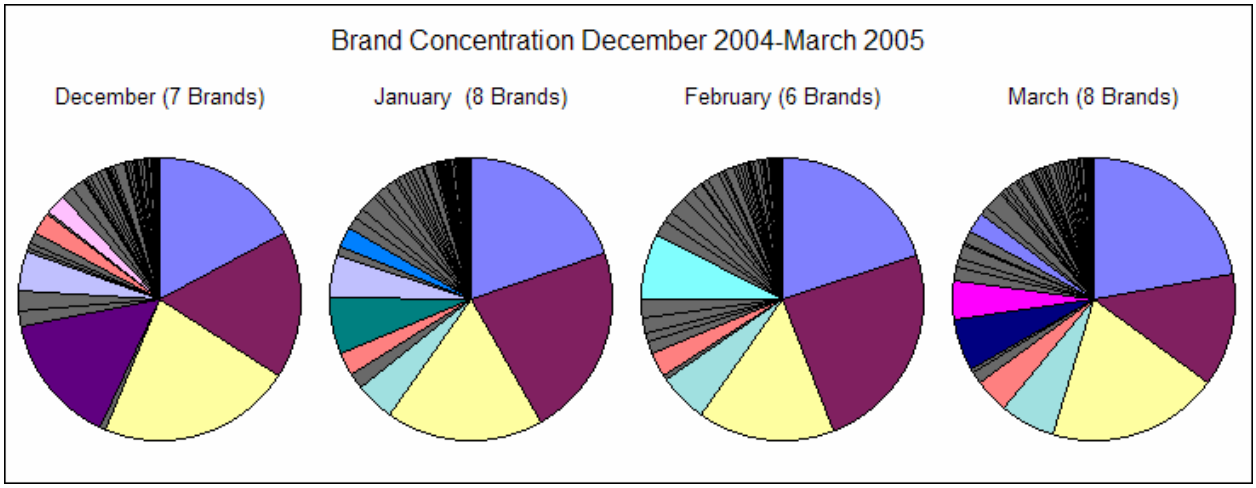
Number of Reported Brands

In March, the number of reported hijacked brands rose to 78, continuing an unbroken trend of monthly increases. Twelve new brands were first reported this month, nine of them financial institutions. This brings the total to 161 brands that have reportedly been hijacked since the APWG began examining phishing trends and reporting findings in November of 2003.



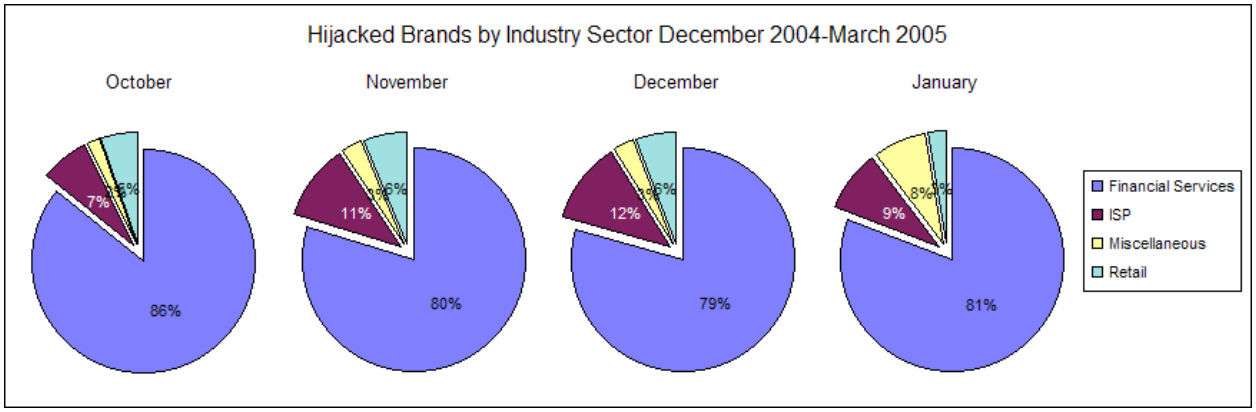
Brand Concentration

The figures below illustrate the concentration of phishing activity as reported against hijacked brands. The number of reported brands comprising the top 80% of all phishing activity has remained roughly stable in recent months, with eight brands accounting for the bulk of phishing activity in March. Of the top seven in December, only three are also in the top list for March.



Most-Targeted Industry Sectors

The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total number of unique baiting sites as well as number of companies targeted. This sector averaged 81% of all hijacked brands in March with nine of the 12 new brands reported this month falling in this category. In this category, phishing attacks have been reported against community banks and credit unions in addition to well-known institutions with global brands.

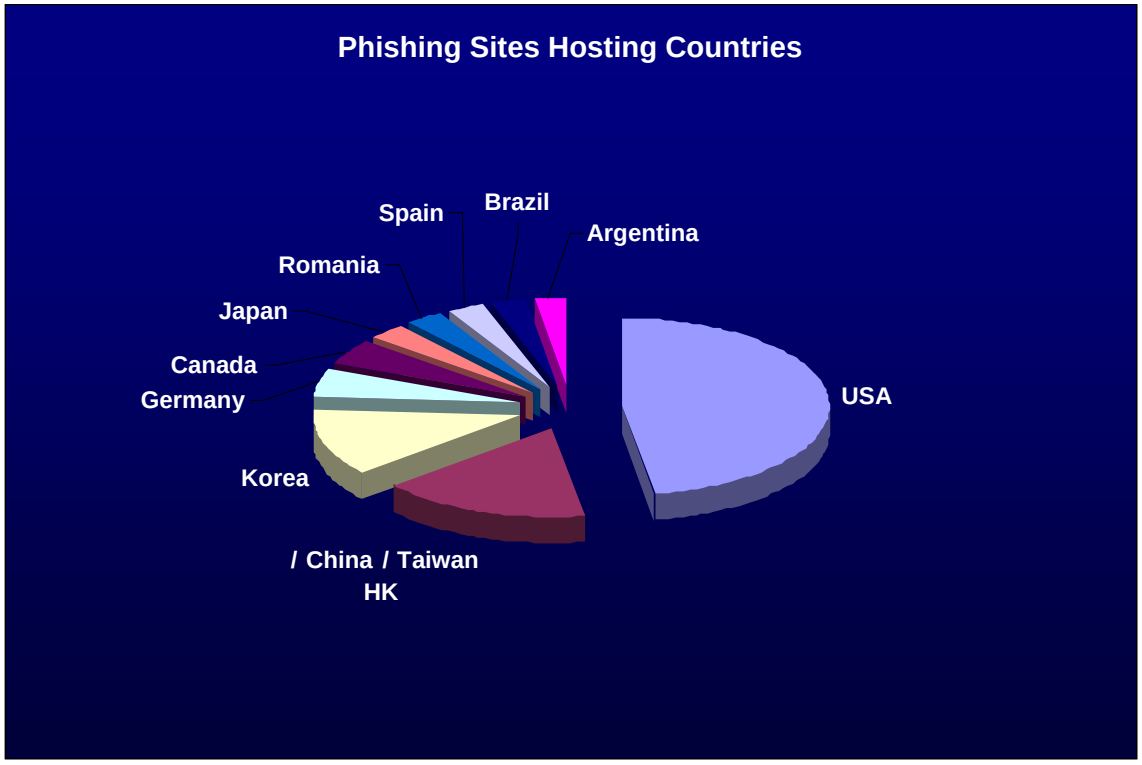


Web Phishing Attack Trends

Countries Hosting Phishing Sites

United States continues to be the top location geographic location for hosting phishing sites with more than 34%. China remains second with 12%, followed by Korea at 9%.

March had a total of 66 unique countries that were hosting phishing sites.



High Increases in Malicious Code Designed for Logging Keystrokes

Over the last two months, Websense® Security Labs™ has seen a dramatic increase in the volume of phishing-based malicious code attacks, in particular, code that targets the Portuguese language. This code is designed to run on a machine and log keystrokes when connection is made to predetermined websites. The keylogger sends that information to a remote location for the purpose of identity theft. From November 2004 through December 2004, Websense Security Labs researched and identified an average of 1-2 new phishing keylogger variants and 10-15 new malicious websites hosting this code per week. In comparison, from February 2005 through March 2005, research has identified 8-10 new keyloggers and more than 100 malicious websites, per week, which are hosting keylogger variants.

Example attack anatomies

A variety of attack vectors are delivering malicious code to end-user's machines. To date, Websense Security Labs have seen attacks from the following sources:

- Websites that host adult entertainment and shopping content which exploit Internet Explorer vulnerabilities to run code remotely without user interaction.
- Instant Messaging (IM) messages and IM worms which blast a message to users enticing them to visit a remote website and run code which is hosted on that site.
- IM messages which include attachments and entice users to run the code.
- Blasts of emails that have attachments enticing users to run the code.
- Blasts of emails that entice users to visit a remote website, and then lure users to run malicious code that is hosted on that site.
- Blasts of emails that entice users to visit a remote website, and then attempt to use an Internet Explorer vulnerability to download and run code without user interaction.

Anatomy of an attack: Specifics

Recently information was captured from a host used as part of one of these phishing attacks. There were two versions of the attack. The host had more than 100,000 email addresses that were mostly from the **.br** domain space.

Version 1: Terra Music Dedication

Selected users are emailed with a spoofed email address of **radio@terra.com.br** with the subject of "Dedicaram uma Musica Para voce". All content is in Portuguese and translates to: "We have dedicated music for you". The program uses the mail server from one of Brazil's most popular internet portals to send the emails.

English Translation: *A friend has dedicated a song to you. To listen to this song, click here: You too can dedicate a song.*

Upon clicking on the link **clique aqui**, an executable is served up from a malicious website on a machine from California that provides web hosting. If the executable is run, the malicious code installs a keylogger. The logged information is then sent to a third party to obtain identify information and access banking records.

Version 2: Symantec Bugbear Warning

Selected users are emailed with spoofed information that resembles Version 1 of the phishing example; however, users are emailed different content and receive a different variant of the keylogger.

English Translation: *We have detected that your email is sending messages contaminated by the virus* ***W32.BugBear.B@mm***
A different version of the virus W32.BugBear@mm.

The worm W32.BugBear.B@mm is:

- *A different version of* ***W32.BugBear.@mm***
- *A worm that that can be widely spread and that also spreads though network sharing*
- *Polymorphic and also infects a list of executable files*
- *Takes control of the keyboard and has backdoor abilities*
- *Tries to stop the processes of several antivirus programs and firewall*
- *Critical update*

Download now the vaccine that will eliminate this virus!
Download here!

Upon clicking on the link **Baixe Aqui!**, an executable is served up from a malicious website hosted in Brazil on a machine which appears to have been compromised. If run, the malicious code installs a keylogger, which sends logged information to a third party to obtain identify information and to access banking records.

Phishing Research Contributors

Tumbleweed Message Protection Lab

The mission of the Tumbleweed Message Protection Lab is to analyze current and emerging enterprise email threats, and design new email protection technologies.

Lead investigator:
John Thielens, johnt@tumbleweed.com

Websense Security Labs™

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

Lead investigator:
Dan Hubbard, dhubbard@websense.com

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 nearly 900 companies and government agencies participating in the APWG and nearly 1400 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.