Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

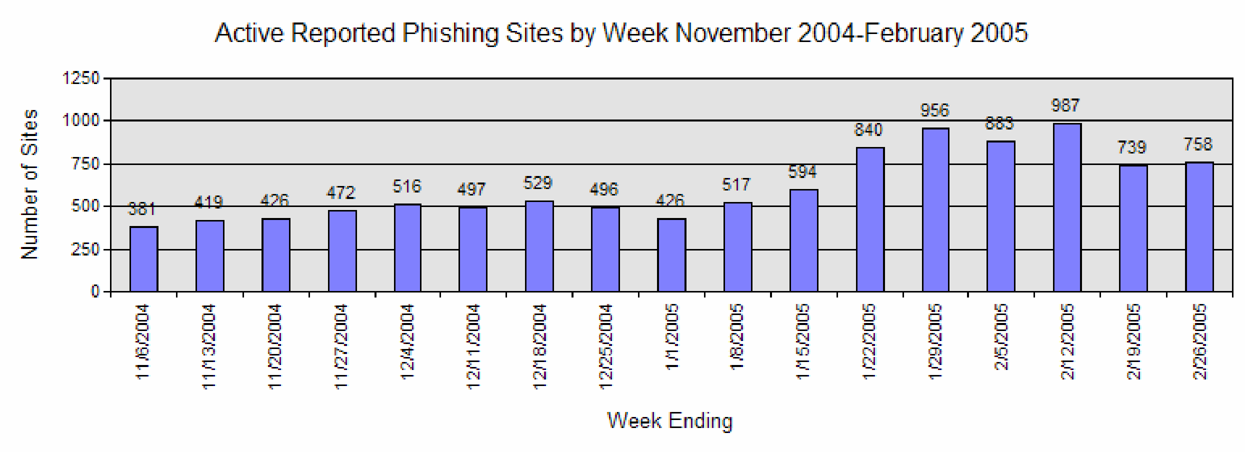
Phishing Activity Trends Report February, 2005

Phishing is a form of online identity theft that uses spoofed emails, fraudulent websites, and crimeware of various types to trick consumers 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, 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 February:	**2625**
• Average monthly growth rate in phishing sites July through February:	**26%**
• Number of brands hijacked by phishing campaigns in February:	**64**
• Number of brands comprising the top 80% of phishing campaigns in February:	**6**
• Country hosting the most phishing websites in February:	**United States**
• Contain some form of target name in URL:	**26%**
• No hostname just IP address:	**48%**
• Percentage of sites not using port 80:	**8.85%**
• Average time online for site:	**5.7 days**
• Longest time online for site:	**30 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.

Analysis for the **Phishing Attack Trends Report** has been donated by the following companies:

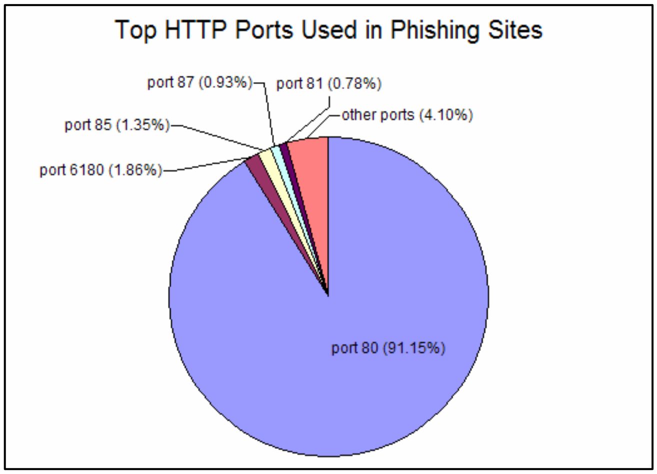
TUMBLEWEED COMMUNICATIONS WEBSENSE.

APWG - Anti-Phishing Working Group

Digitally signed by APWG - Anti-Phishing Working Group
DN: CN = APWG - Anti-Phishing Working Group, C = US, L = Cambridge, S = MA, O = Anti-Phishing Working Group
Reason: I am the author of this document
Location: Cambridge, MA
Date: 2005.04.28 15:16:04 -04'00'

APWG Trend Alert

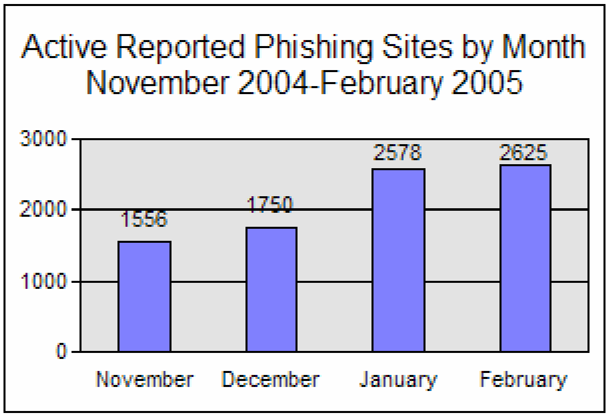
This month saw a trend back to using cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use at over 90% of all phishing sites reported.



Email Phishing Attack Trends

In February 2005, there were 13,141 new, unique phishing email messages reported to the APWG. This is an increase of 2% over the number of unique reports for January, despite February being a shorter month. The average monthly growth rate since July 2004 (2,625) is 26%.

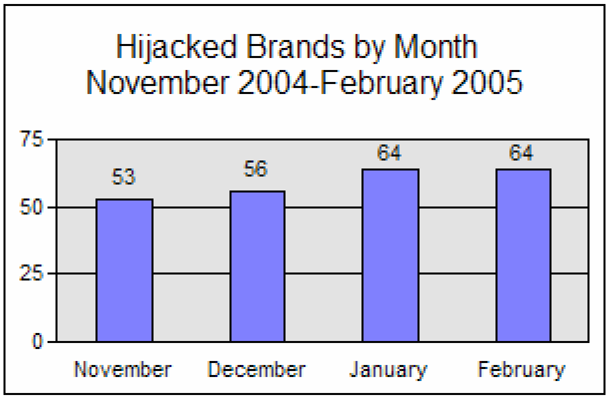
The number of phishing web sites supporting these attacks also held steady, rising 1.8% from 2578 to 2625 in the month of February.



What Brands Are Being Hijacked By Email Phishing Attacks?

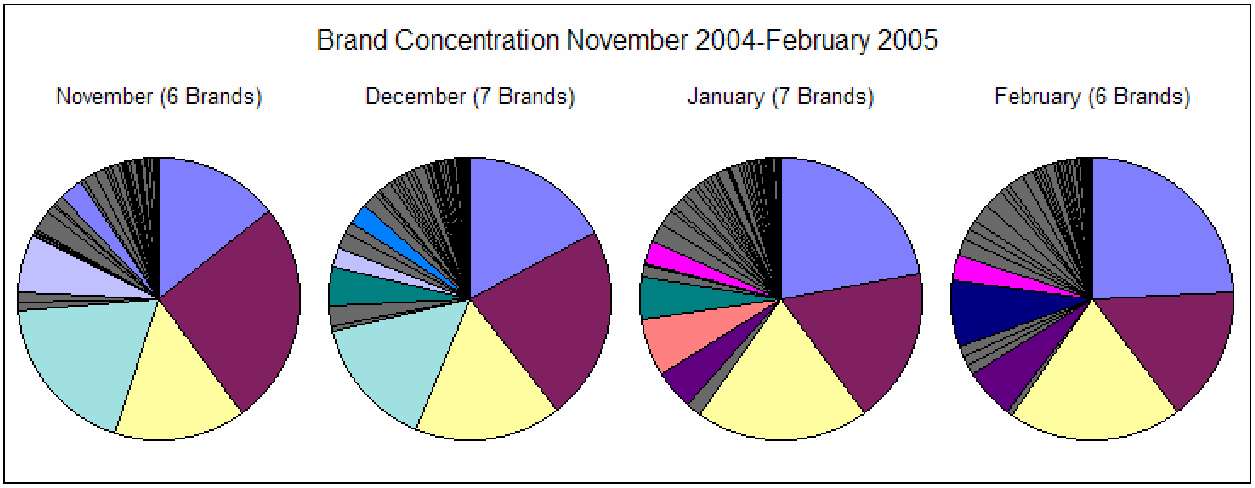
Number of Reported Brands

In January, the number of reported hijacked brands remained at 64. As in January, nine new brands were first reported this month, eight of them financial institutions. This brings to 149 the total number of brands that have reportedly been hijacked since the APWG began examining phishing trends and reporting their findings in November of 2003.



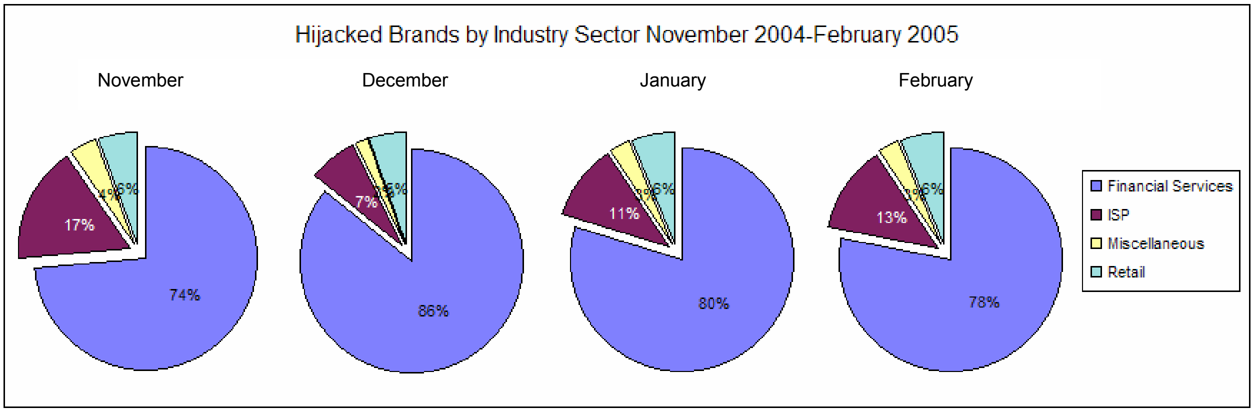
Brand Concentration

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 six brands accounting for the bulk of phishing activity in February. Of the six in February, only three are also in the top list for November.



Most-Targeted Industry Sectors

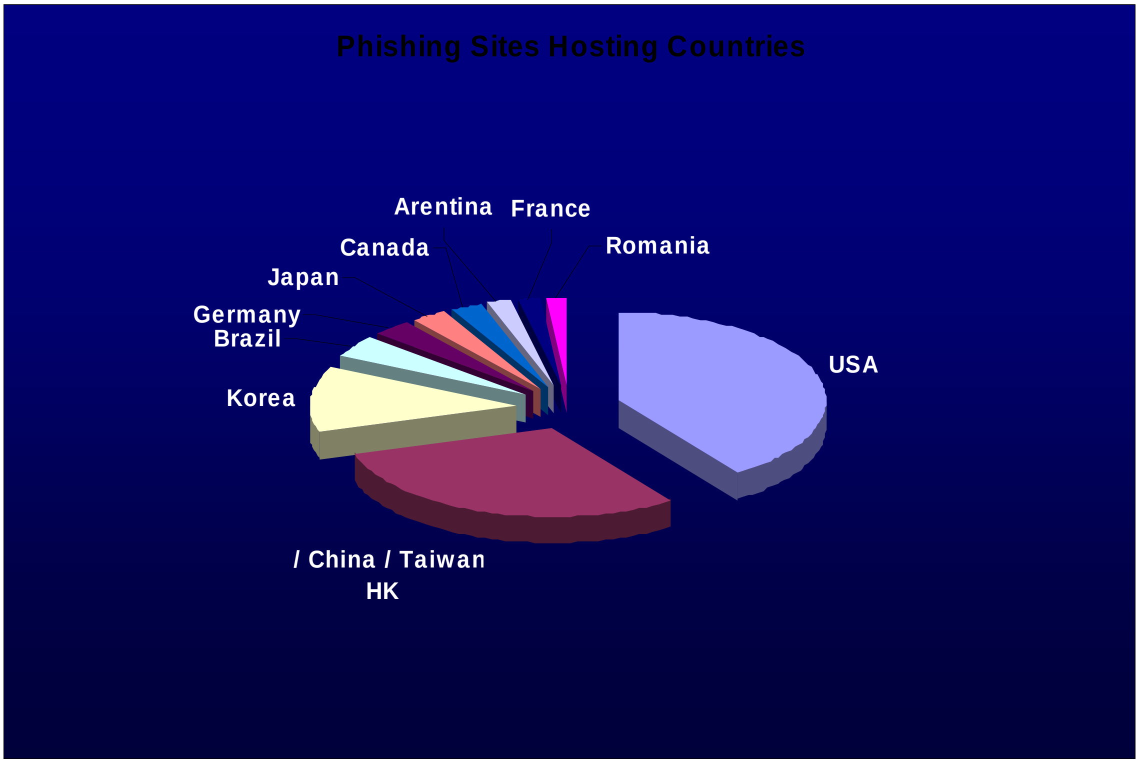
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total number of unique baiting sites as well as number of companies targeted. This sector averaged 78% of all hijacked brands in February with eight of the nine new brands reported this month falling in this category.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

The United States continues to be the top location geographic location for hosting phishing sites with more than 37%. This was almost a 6% increase from last month. Also, China was up more than 10% to 28%. Other top countries are: Korea 11%, Brazil 3.97%, Germany 2.95%, Japan 2.46%, Canada 2.28%, Argentina 1.78%, France 1.74%, and Romania 1.45%.



Traditional Phishing Is Changing – Pharming, IM and Crimeware

As reported in December and January, the phishers are using alternative methods to “Phish” for end-user information. Previous phishing attacks were based around luring a user to perform an action through social engineering, primarily through spoofed email and websites. The use of Instant Messaging (IM) to spoof companies and phish for information is becoming more frequent.

Phishing without a lure is now becoming more prevalent among attack styles. The most common is malicious code which either modifies your hosts file to point commonly accessed sites to the fraudulent site (so-called “Pharming”) and malicious code that logs your keystrokes based upon a set of predetermined URLs that are accessed (“keylogging”). DNS cache poisoning is also an alternative means that can be used to resolve information to non-legitimate pharming web sites. This will be the subject of a forthcoming special APWG crimeware report.

During February there were also several reports of vulnerabilities within internet browsers handling of International Domain Name parsing (IDN). However, we did not see many phishing attacks utilizing this technique during the month.

Lastly, Websense Security Labs has seen a large number of small ecommerce sites and regional banks becoming victims of phishing attacks.

Phishing Research Contributors

TUMBLEWEED COMMUNICATIONS

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(at)tumbleweed.com

WEBSENSE.

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(at)websense.com

Anti-Phishing Working Group
APWG
www.antiphishing.org

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 currently over 800 organizations participating in the APWG and more than 1200 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 Web site 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 Web site 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.