Anti-Phishing Working Group
APWG
Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud

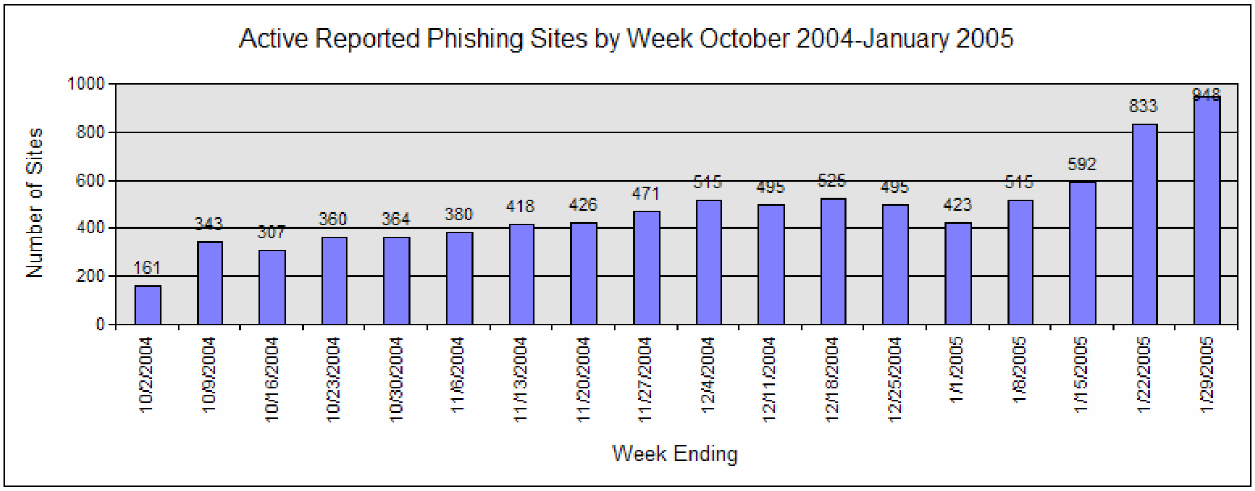
Phishing Activity Trends Report January, 2005

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent web sites 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 up to 5% of 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 web site 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 January:	**2560**
• Average monthly growth rate in phishing sites July through January:	**28%**
• Number of brands hijacked by phishing campaigns in January:	**64**
• Number of brands comprising the top 80% of phishing campaigns in January:	**7**
• Country hosting the most phishing web sites in January:	**United States**
• Contain some form of target name in URL:	**25 %**
• No hostname just IP address:	**53 %**
• Percentage of sites not using port 80:	**9.53 %**
• Average time online for site:	**5.8**
• Longest time online for site:	**31 days**



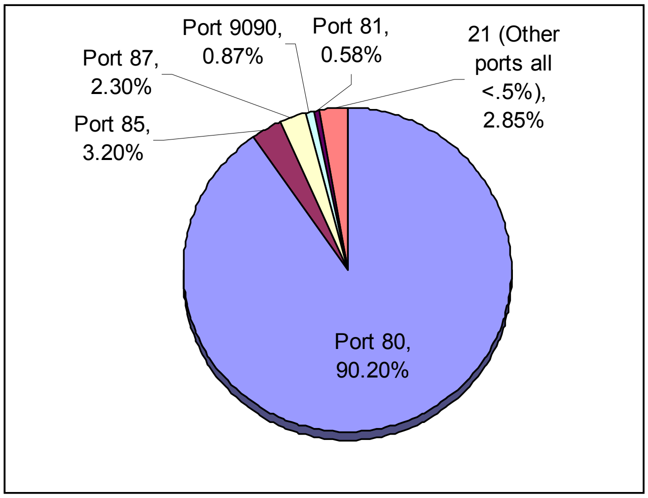
The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. For further information, please contact press@antiphishing.org, Secretary General Peter Cassidy at 617.669.1123 or 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.

Top Used Ports Hosting Phishing Data Collection Servers

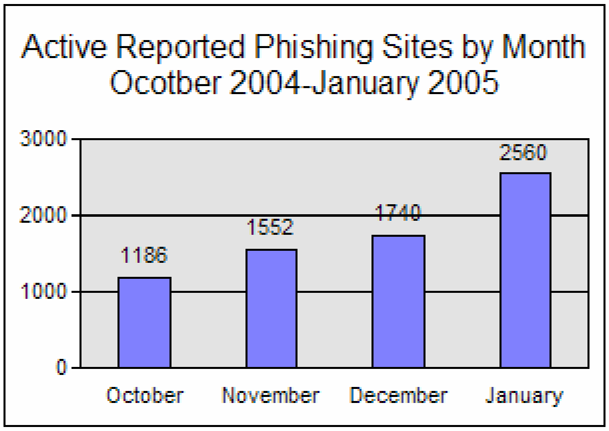
The rise in non port 80 hosted sites and the number of sites which are hosting phishing attacks continues to lead us to believe that the number of machines that are compromised and are being used to host these attacks is growing.



Email Phishing Attack Trends

In January, there were 12,845 new, unique phishing email messages reported to the APWG. This is a substantial increase of 42% over the unique reports for December, and represents an average monthly growth rate of 30% since July (2,625).

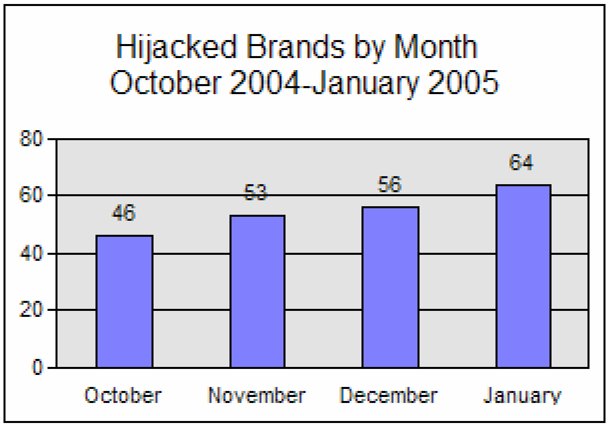
The number of phishing web sites supporting these attacks rose even more dramatically. In January, there were 2,560 unique sites reported, a jump of 47% over December (1740) and more than double the number reported just three months ago in October (1186).



What Brands Are Being Hijacked By Email Phishing Attacks?

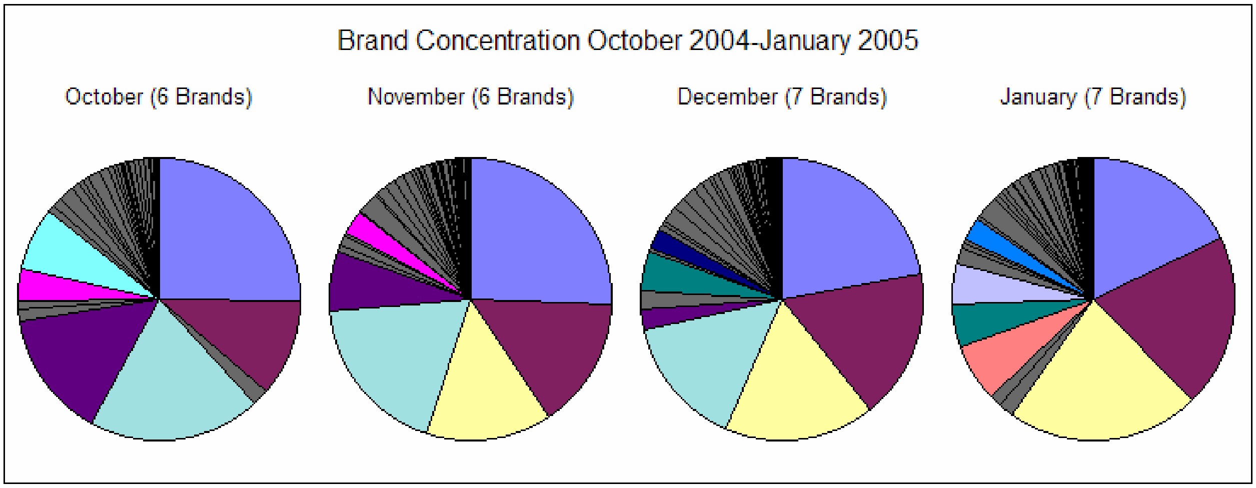
Number of Reported Brands

In January, the number of reported hijacked brands rose to 64, including nine brands first reported this month, eight of them financial institutions. This brings to 140 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.



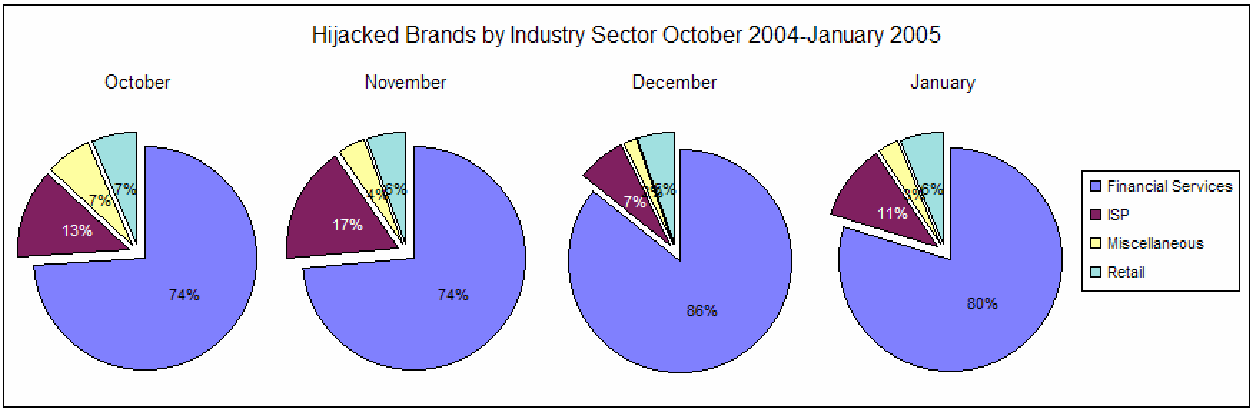
Brand Concentration

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 seven brands accounting for the bulk of phishing activity in December. Of the top seven in January, the top three were the same brands as the top three in December, and three of December's top seven are no longer in the top 80%.



Most-Targeted Industry Sectors

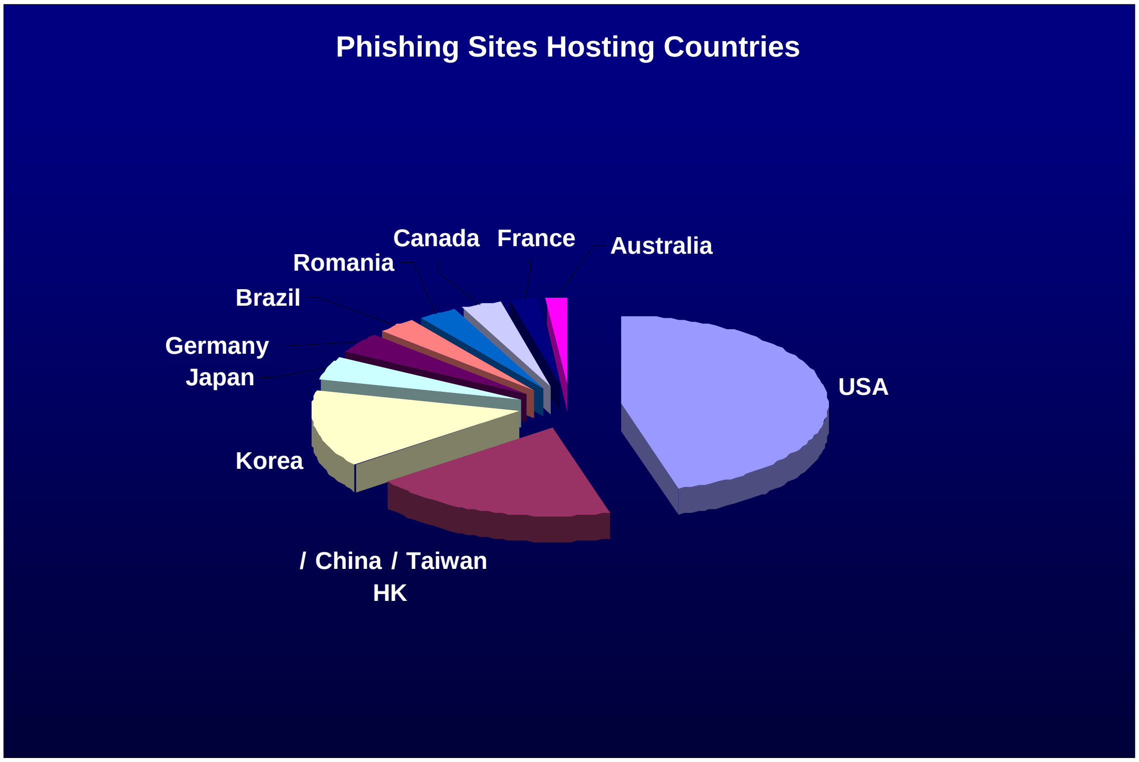
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total number of unique baiting sites as well as number of companies targeted. This sector averaged 80% of all hijacked brands in January with eight of the nine new brands reported this month falling in this category.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

United States continues to be the top geographic location for hosting Phishing sites with more than 32 %. Other top countries are: China 13%, Korea 10%, Japan 3.1%, and Germany 2.7%, Brazil 2.7%, Romania 2.2%, Canada 2.1%, France 2.7%, and Australia 2.1%.



Utilizing More Attack Vectors

Cross-Site Scripting / Redirects

During the month of January, Websense® Security Labs™ saw a number of attacks using cross-site scripting to redirect URL's from popular web sites in order to better present themselves and as a means to prevent blocking. An example of this is an attack that was discovered utilized the Lycos search engine.

By crafting a URL, the hacker can redirect any end user though Lycos directory to their fraudulent page. An example is below:

http://r.lycos.com/r/BJTWQSAUE/http://www.websensesecuritylabs.com

This link will automatically send the end user to Lycos, which in turn redirects the to the www.websensesecuritylabs.com web site.

We suspect that this type of attacks may be one of the reasons why the number of sites that have no hostname is down from 63% in December '04 to 53% in January '05.

Malicious Code Phishing

During the month of January we also witnessed some significant gains in attackers utilizing malicious code in order to gain access to end user keystrokes. Password stealing Trojans are not just coming through email; we have seen multiple attacks through Microsoft Messenger where Trojan Horses and password stealing keyloggers are run. The Bropia worm had five variants in January alone.

Malicious web sites are also rising as a vector to install password stealing keyloggers. These sites are utilizing several browser vulnerabilities, some of which are un-patched, to install and run upon simply accessing a web site.

Also common are blended attacks which use combinations of email, instant messaging, and web sites to gain access to systems.

Some examples of password stealing Trojan Horses from January include:

- Buchon.c
- Bropia Worm
- Goldun (Several Variants)
- Bankos Trojan (Several Variants)
- Banks-De (Several Variants)

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

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 706 organizations participating in the APWG and more than 1100 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.