Anti-Phishing Working Group APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

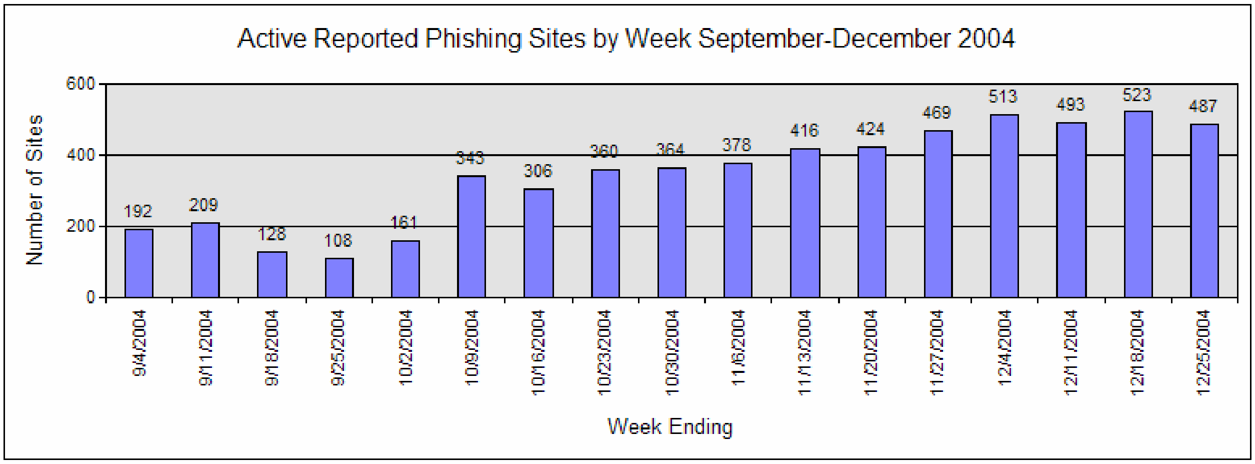
Phishing Activity Trends Report December, 2004

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 December:	**1707**
• Average monthly growth rate in phishing sites July through December:	**24%**
• Number of brands hijacked by phishing campaigns in December:	**55**
• 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:	**24%**
• No hostname just IP address:	**63%**
• Percentage of sites not using port 80:	**13.1%**
• Average time online for site:	**5.9 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 the APWG at press@antiphishing.org 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

HTTP Port(s)	Percentage
80	86%
87	3.6%
85	1.88%
5180	1.5%
2333	1%
24 other port numbers	6.02%

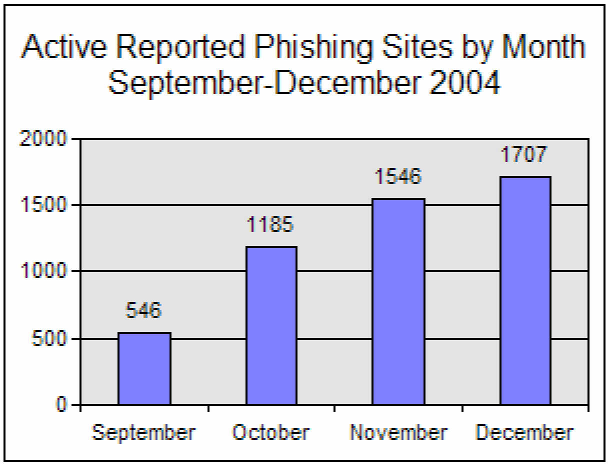
Port 80 is the most widely used for hosting phishing data collection servers. Other ports are used in an attempt to defeat web filters or to host phishing servers on compromised machines that are already hosting a legitimate web server on port 80.

Email Phishing Attack Trends

In December, there were 9,019 new, unique phishing email messages reported to the APWG. This is an increase of just over 6% of the unique reports for November, but represents an average monthly growth rate of 38% since July (2,625).

Despite relatively modest growth in the number of reports, the number of phishing websites supporting these attacks continues to rise more dramatically. In December, there were 1,707 unique sites reported, a jump of 10% over November (1546) and a month-to-month growth rate of 24% since August (731).

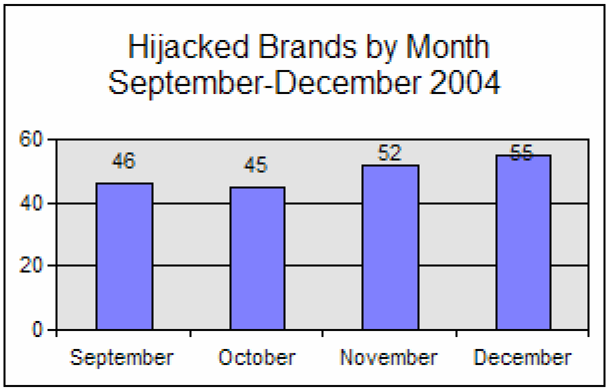
Due to the Christmas holidays, reports were somewhat diminished as businesses, consumers and phishers alike took time off during the last week of December 2004.


Active Reported Phishing Sites by Month
September-December 2004

What Brands Are Being Hijacked By Email Phishing Attacks?

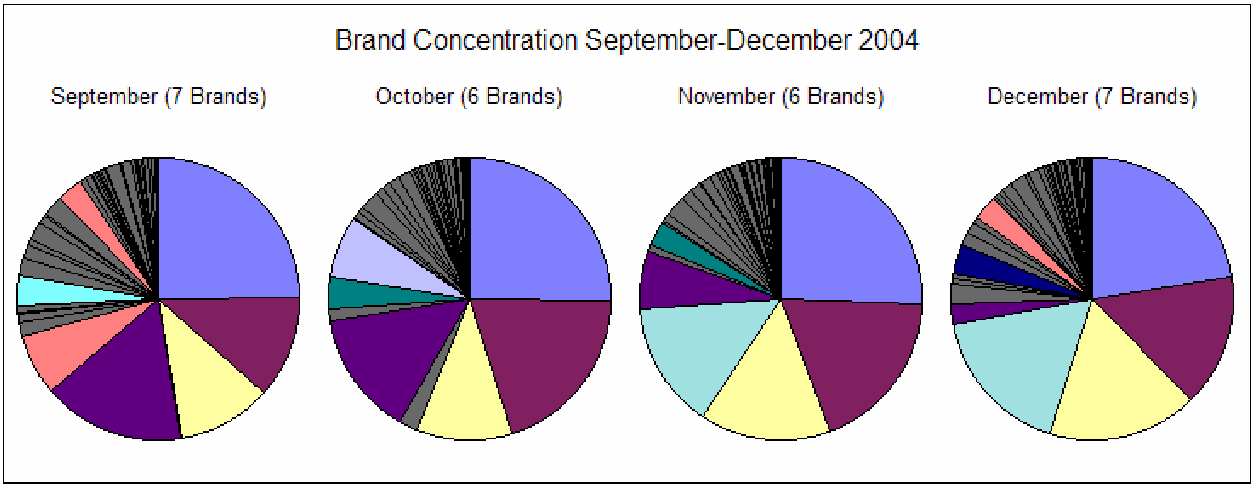
Number of Reported Brands

In December, the number of reported hijacked brands grew again to 55, including nine brands first reported this month, eight of them financial institutions. This brings the total number of brands that have reportedly been hijacked to 131 since the APWG began examining phishing trends and reporting findings in November of 2003.


Hijacked Brands by Month
September-December 2004

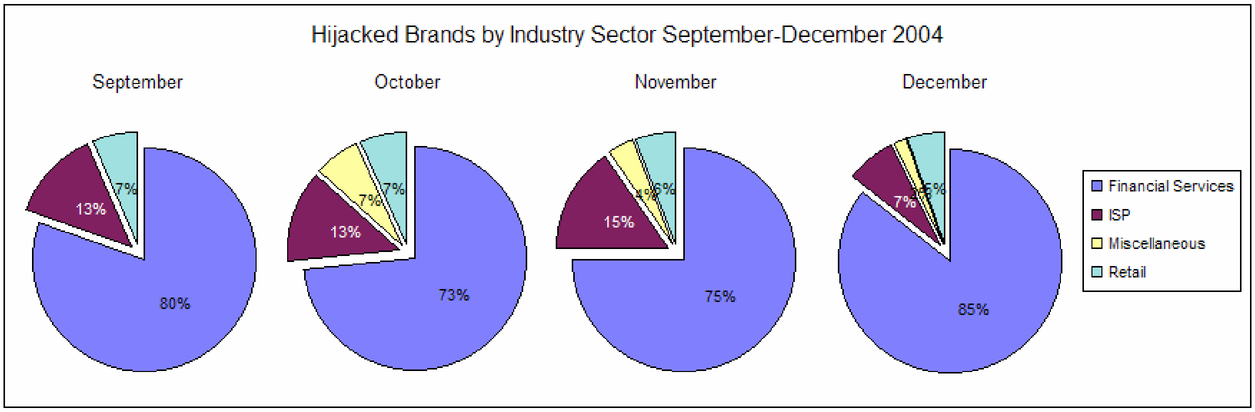
Brand Concentration

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 December, the top five were the same brands as the top five in November.



Most-Targeted Industry Sectors

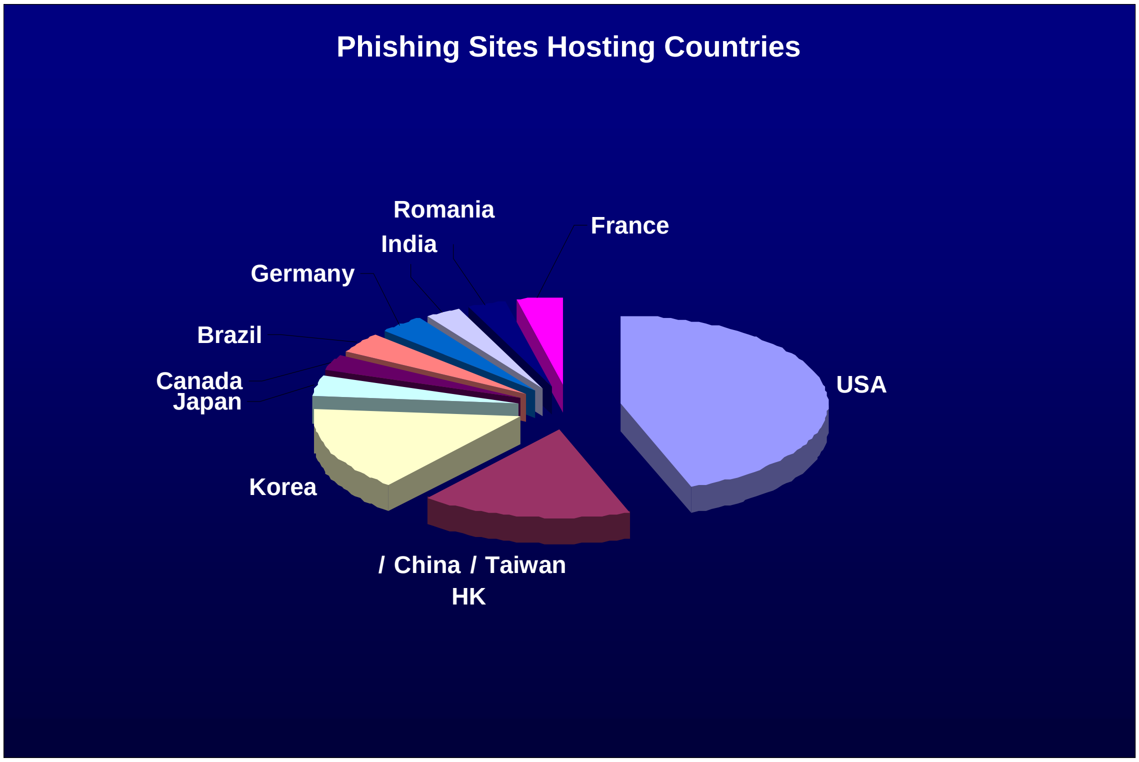
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total number of unique baiting sites as well as number of companies targeted. This sector averaged 85% of all hijacked brands in December with eight of the nine new brands reported this month falling in this category.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

United States continues to be the top location geographic location for hosting Phishing sites with more than 32%. Other top countries are, in order: China 12%, Korea 11%, Japan 2.8%, Germany 2.7%, France 2.7%, Brazil 2.7%, Romania 2.2%, Canada 2.1%, and India 2.1%.



Web Phishing Attack Example

Phishing with Malcode -> Anatomy of a Malcode Phishing Attack

The November 2004 “Phishing Trends Activity Report” outlined that internet attack methods are becoming more sophisticated with Phishing and the increased use of concealed malicious code on corrupt websites to gather information about end users without their knowledge. Below is an example of such an attack that was reported from Brazil.

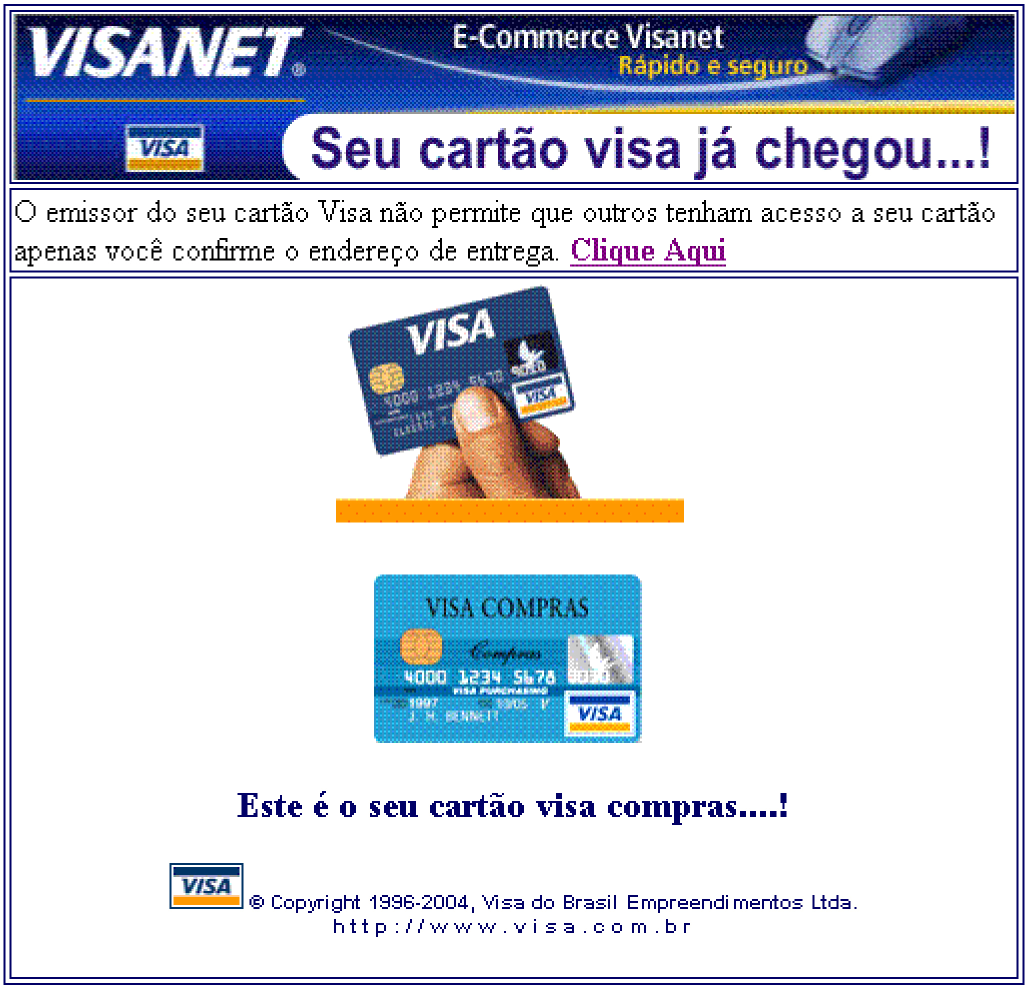
The attack vector. This example attack uses a similar technique to a common Phishing attack where users are sent what appears to be a legitimate looking email. Like other Phishing attacks, the email requests that the user access a URL of a fraudulent website in order to update their account information. However, unlike most Phishing attacks, this site was hosting a malicious application.

As the example shows, written in Portuguese, the email poses as a legitimate email from Visa Brazil and urging the customer to click on the link embedded within the HTML of the email message.

Although email is still the top vector for Phishing, there is increased use of exploiting browser vulnerabilities to gain access for running malicious applications on end-users machines.

Email:

From: Visa.com
To: removed
Sent: Wednesday, January 05, 2005 6:09 PM
Subject: visa brasil



VISANET® E-Commerce Visanet Rápido e seguro

Seu cartão visa já chegou...!

O emissor do seu cartão Visa não permite que outros tenham acesso a seu cartão apenas você confirme o endereço de entrega. Clique Aqui

Este é o seu cartão visa compras....!

© Copyright 1996-2004, Visa do Brasil Empreendimentos Ltda.
http://www.visa.com.br

Translated into English, the email reads:
Your VISA card just Arrived!
The person who sent your Visa card does not allow other people to have access to your card. Only you can confirm the address to where it should be delivered.
Click here. This is your VISA card for shopping.

The Payload: As mentioned previously, this Phishing attack is different in its collection method of user information. Most Phishing attacks send you to a website which requests that the user supply and submit information. Items such as credit card numbers, social security number, username and passwords are the most common requests. The information is stored on a fraudulent site which has been setup by the attacker, allowing information to be collected.

This attack only uses a malicious website to host an application which is then downloaded and run on the user's machine. This particular piece of malicious code was called visa.exe and was hosted on an end-users home directory on a Brazilian web hosting facilities server. Once the application is launched, it modifies system registry files, is set to start on reboot, logs keystrokes when predetermined sites are accessed, and sends information back to the attackers.

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 706 member 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 and executives.