Anti-Phishing Working Group
APWG

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

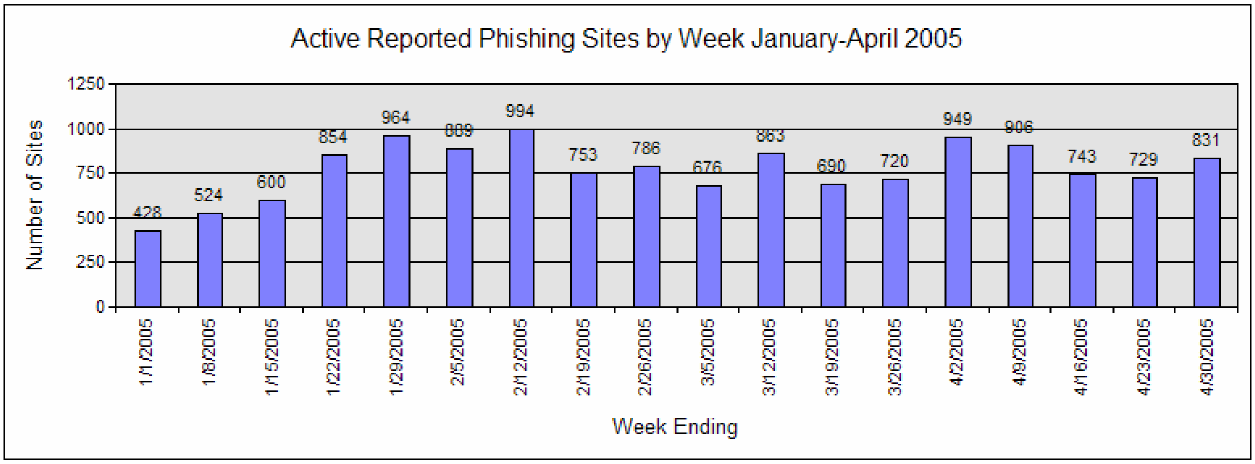
Phishing Activity Trends Report April, 2005

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 April:	**2854**
• Average monthly growth rate in phishing sites July 2004 through April 2005:	**15%**
• Number of brands hijacked by phishing campaigns in April:	**79**
• Number of brands comprising the top 80% of phishing campaigns in April:	**7**
• Country hosting the most phishing websites in April:	**United States**
• Contain some form of target name in URL:	**33 %**
• No hostname just IP address:	**37 %**
• Percentage of sites not using port 80:	**5.5 %**
• Average time online for site:	**5.8 days**
• Longest time online for site:	**30 days**



Phishing domains trends

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.

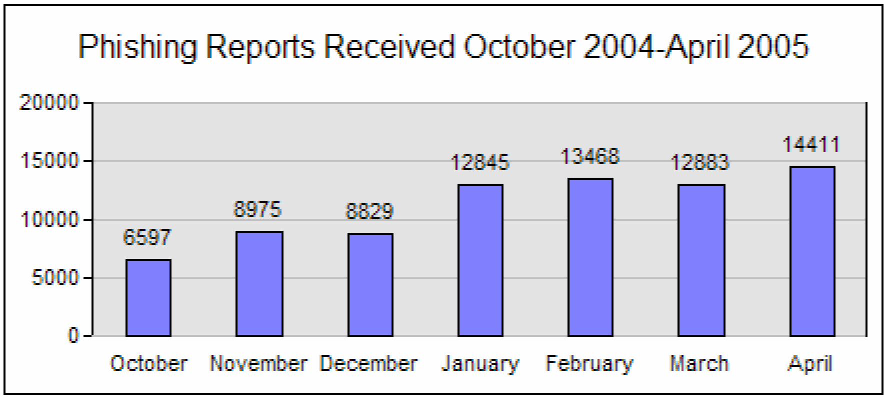
While the number of reported phishing domains has slightly dropped in April compared to March, there was a very significant (the third largest on record) spike in the first week of April.

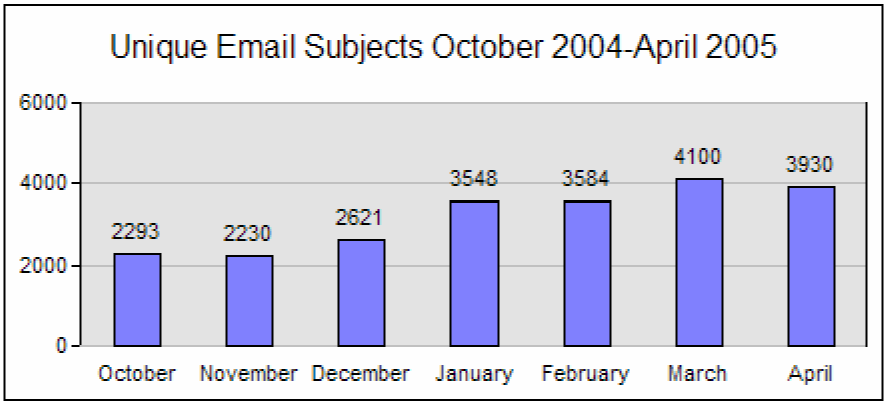
Another notable trend is the decrease in the 'just an IP address domains' percentage. It has been falling for the past 3 months, and the strongest decrease was in April (11%). This trend shows the growing skill of phishers in disguising their scam attempts – a lot of the recent phish sites use 'hijacked' servers – i.e. the scam is located on the domain of a legitimate enterprise, that the phisher has a remote access to – by hacking, installing malware, etc. This tactic gives the scammers the advantage of having a link that leads to a legitimate domain that can not be blacklisted. In fact, it is likely that such a phish message would get through a spam filter that uses 'whitelisting'.

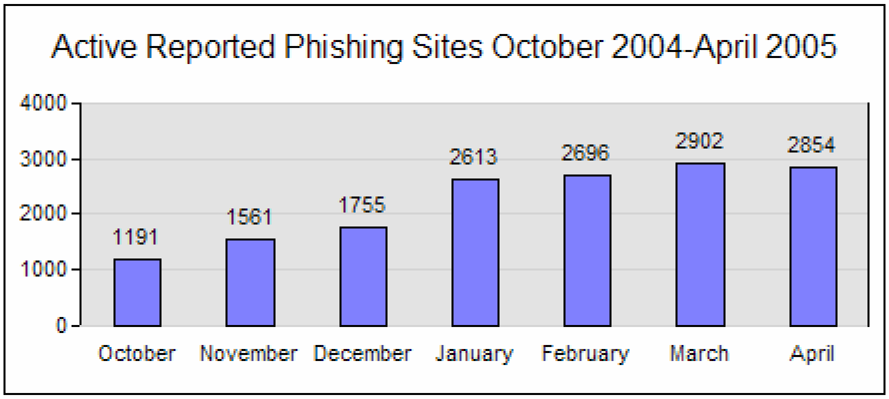
Email Phishing Attack Trends

The number of reports received in April rebounded to 14,411, continuing a trend of slight growth during 2005. (Note that reports received in April may describe phishing messages pertaining to prior months).

The number of "unique" email messages (based on subject) pertaining to phishing attacks launched in April decreased slightly. In conjunction with a similar drop in the number of sites reported active in April, this indicates a slight lessening of email-based phishing in the month.

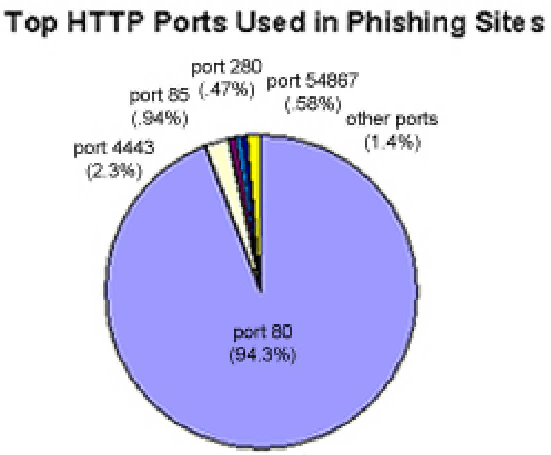

Phishing Reports Received October 2004-April 2005


Unique Email Subjects October 2004-April 2005


Active Reported Phishing Sites October 2004-April 2005

Top Used Ports Hosting Phishing Data Collection Servers

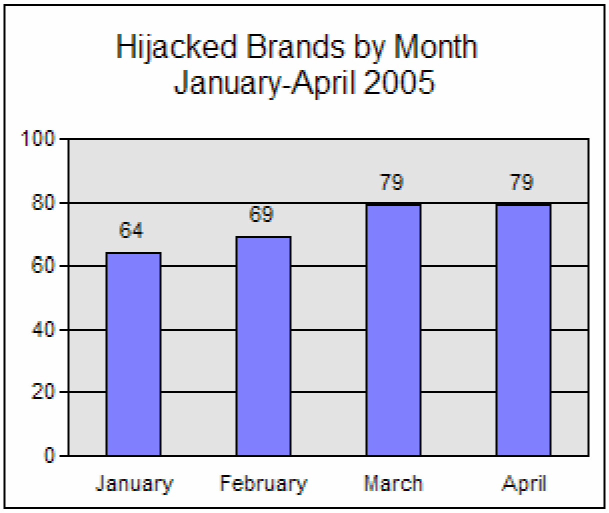
April saw a continuation of a trend of using cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use at 94.3% of all phishing sites reported.



Brands and Legitimate Entities Hijacked By Email Phishing Attacks

Number of Reported Brands

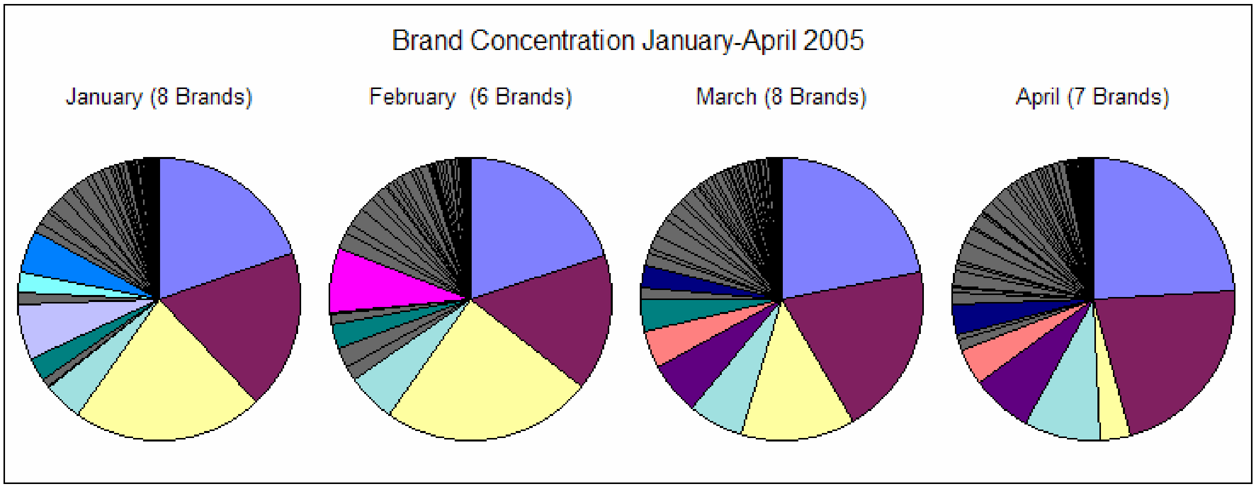
In April, the number of reportedly phished brands stayed the same as in March. This is coincidential, since the brand list saw some movement – eleven newly targetted brands replaced the same number falling off the list. The visible trend is that there is a consistent set of "favorite" brands targetted by phishers combined with an ever-changing "tail" of brands in the broader market. Brands in the "favorites" list tend to remain for a long time—most of the big names are here—and the ones in the "tail" frequently change. This separation has its logic: while some of the scammers count on the popularity of some brands to generate more hits to the phishing site (the ones in the "favorites" list), others try to scam the customers of enterprises that had not experienced the phenomenon so far, and are presumably less experienced in exposing phishing.



What Brands Are Being Hijacked By Email Phishing Attacks?

Brand Concentration

The top 7 brands comprised over 80% of the attack sites in April. Each of these brands also appeared in the top 80% list of 8 in March. The list of targets continues to grow, however, even while the favorite targets remain. In April, eleven new brands appeared in the reports—ten financial institutions and one ISP.

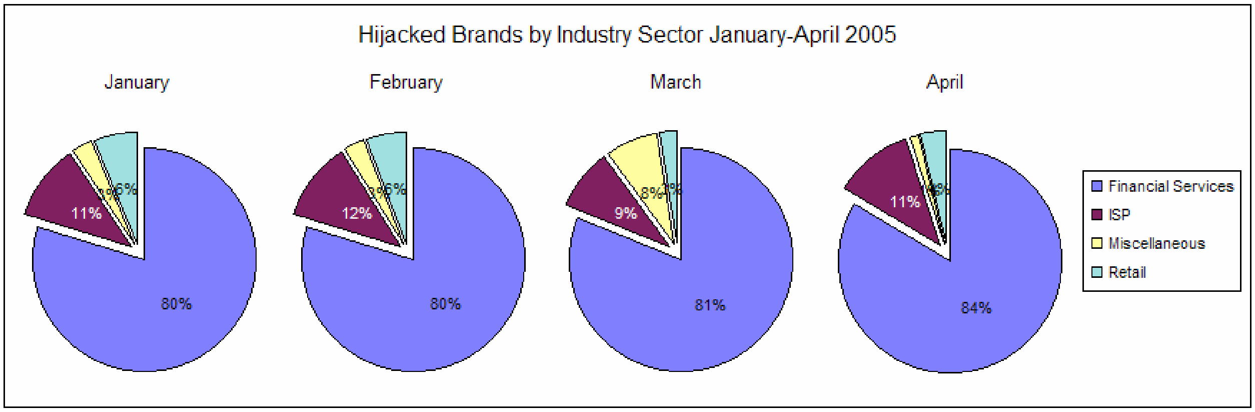


Most Targeted Industry Sectors

The logical consequence of the “favorites” list consisting of predominantly financial companies is that the financial sector is the most frequent phishing target:

The sector distribution is a function of the brand distribution, thus there is a large, stable share (the financial sector) and a small, fluid share (everything else).

Compared to March, the ISP sector has an increased share – this is due to a number of seemingly coordinated attacks against ISPs in the middle of April.

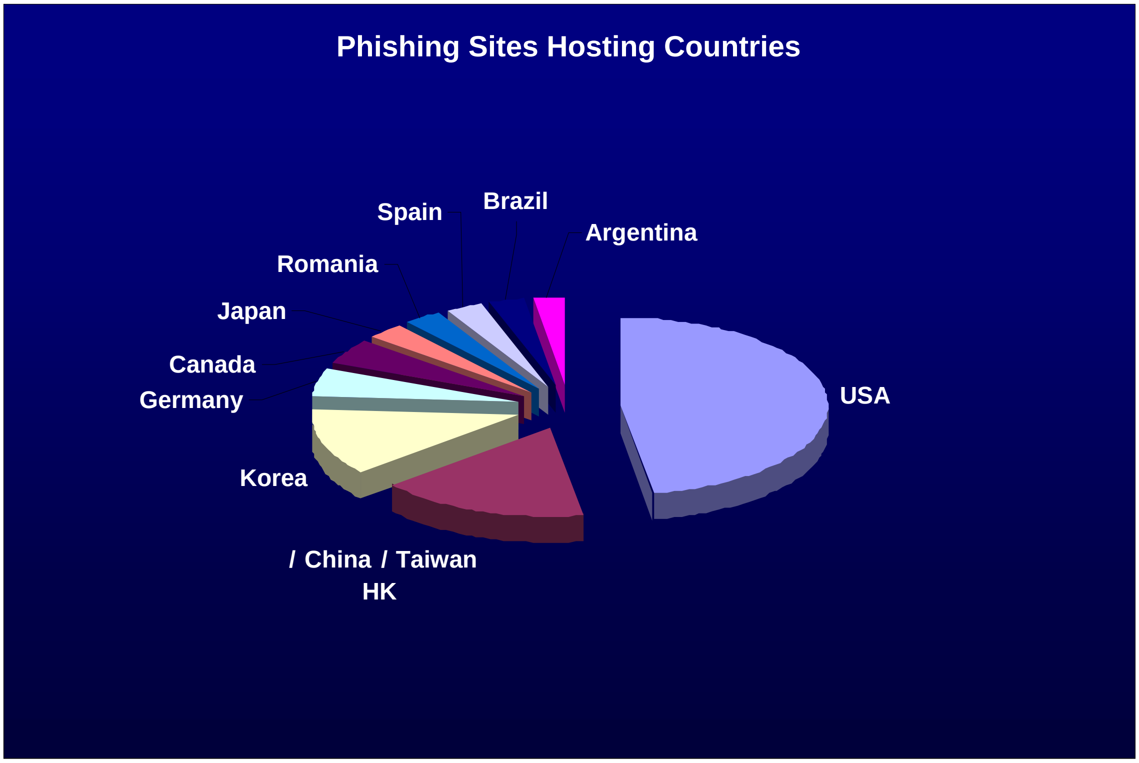


Web Phishing Attack Trends

Countries Hosting Phishing Sites

As the number of broadband users in China grows it appears as though so does the number of phishing sites hosted in China. They have almost passed the USA as the number one country hosting phishing sites. USA 26.3%, China 22 %, Korea 10%, Japan 2.87%, Germany 2.71 %, France 2.1%, Canada 1.94%, India 1.70%, Netherlands 1.50%, Italy 1.30%.

This month had a total of 68 unique countries that were hosting phishing sites.



Changing Targets

Increase in Credit Unions being targeted

Websense® Security Labs™ has seen a large increase in the number of credit unions that have been targeted in phishing scams in April. These range from regionally focused credit unions to niche credit unions that target particular employee sets.   Hackers are modifying their attack methods by shifting away from attacking popular or large institutions.

Attack Method Update

The evolution of phishing attacks continue in April. Malicious code in the form of Trojan Horses, Keyloggers, and Proxy servers, are being used increasingly. The vectors as to how the malicious code is being downloaded and run are also changing. Websense Security Labs has seen several emerging forms of payload and vectors. The following are some examples:

Emerging Payloads

- *Phishing-based Trojans – Keyloggers*

  This is malicious code which is designed with the intent of collecting information on the end-user in order to steal the users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions in order to target particular information, the most common are; access to financial based websites, ecommerce sites, and web-based email sites.

- *Phishing-based Trojans – Redirectors*

  This is malicious 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 malcode that changes hosts files and other DNS specific information, malcode browser-helper-objects that redirect information to fraudulent sites, and malcode that may install a network level driver or filter to redirect 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.

- *Pharming Attacks*

  This is an attack that intercepts information in between two parties' communications in order to redirect users to a fraudulent location. The most popular form of Pharming is currently DNS cache poisoning.

Emerging Vectors

- *Typo-Attacks*

  These are attacks that direct you to a website which is hosting malicious code by making a typo when typing in the URL for a domain. For example, the attacker will substitute the letter 'L' in a URL with the letter 'K' which resides next to the 'L' on the keyboard. If the end-user were to mistakenly type the wrong letter in that exact location within the URL, they will be taken to a fraudulent website.

- *Search Engine Poisoning*

  These are attacks that direct you to a website by showing up in early in search engine results. This could be for commonly used terms, could be used in combination with typo's in search terms, and/or with social engineering.

Dominating and Emerging Attack Techniques

- *New legitimate redirects exploitation*

  Phishers continue to find more open redirects on legitimate sites and use them to form seemingly legal links.

- *A rise in the 'main-in-the-middle' phishing attacks*

  This type of attack is reported increasingly often. It uses some knowledge on the way a given legitimate site processes logins. Given such knowledge, a scammer can build a site that acts as a 'front end' mask for the legitimate login site – it would return an error message when incorrect login data is passed, for example.

  These attacks are harder to spot and are growing very dangerous.

- *A new phish email spread pattern*

  A new pattern in emerging phish scams was noticed – there were multiple occasions of different scheme attacks occurring against the same target at once. This points to a common root, or - at least - some interconnection and organization among phishers.

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.