Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

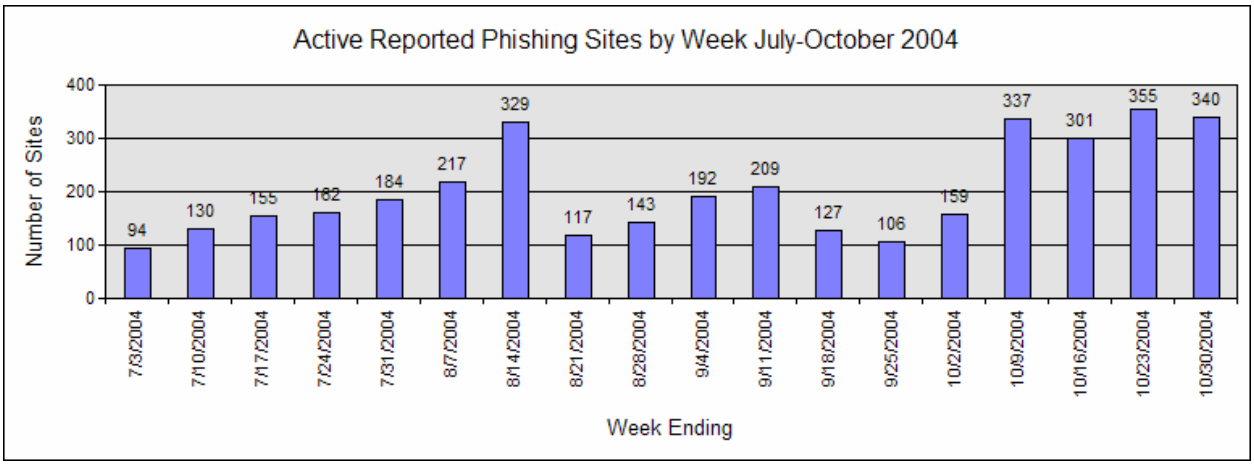
Phishing Activity Trends Report October, 2004

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 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 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 October: **1142**
- Average monthly growth rate in phishing sites July through October: **25%**
- Number of brands hijacked by phishing campaigns in October: **44**
- Number of brands comprising the top 80% of phishing campaigns in October: **6**
- Country hosting the most phishing websites in October: **United States**
- Contain some form of target name in URL **20.1 %**
- No hostname just IP address **63 %**
- Percentage of sites not using port 80 **12.2 %**
- Average time online for site **6.4 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.

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

TUMBLEWEED COMMUNICATIONS

WEBSENSE.

APWG Analysis Update

With this report for October 2004, we are introducing a new methodology which provides a measurement of phishing activity based on the number of fraudulent "baiting" websites extracted from phishing email messages, in lieu of counting the email messages themselves as presented in previous reports. Analysis of the email messages shows that a single baiting site may appear as the link in several hundred email messages with different formats and visual designs, potentially hijacking as many as six separate brands. The APWG considers this a single coordinated "attack" and a more accurate measurement of criminal phishing activity.

In order to illustrate trends, this report analyzes activity from July 1 through October 31, 2004 using this new methodology. In an additional departure from previous reports, the individual brands being hijacked are also not specifically identified. Instead, the brands are summarized by industry and more focus is placed on the baiting websites themselves.

Email Phishing Attack Trends

In October, there were 6,597 new, unique phishing email messages reported to the APWG. This was over three times the number of unique reports received in August (2,158) and represents an average monthly growth rate of 36% since July (2,625).

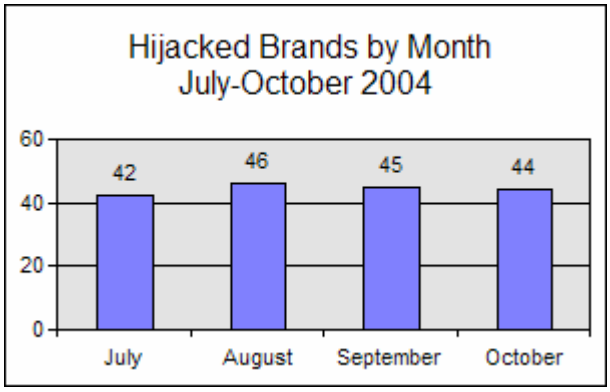
An analysis of the reported email messages reveals a similar trend in the number of unique baiting sites disguised within the messages. In October, there were 1,142 unique sites reported, corresponding to an increase of more than two times over September (543) and a month-to-month growth rate of 25% since July (584).

A wide variety of disguising techniques used by baiting sites are currently in use, above and beyond recentl attacks on browser vulnerabilities which have since been closed, including embedded images with nested MAPs, embedded forms with CSS-styled buttons disguised as links, and exploitation of "marketing partner redirect" features in the websites of the hijacked brands themselves.

What Brands Are Being Hijacked By Email Phishing Attacks?

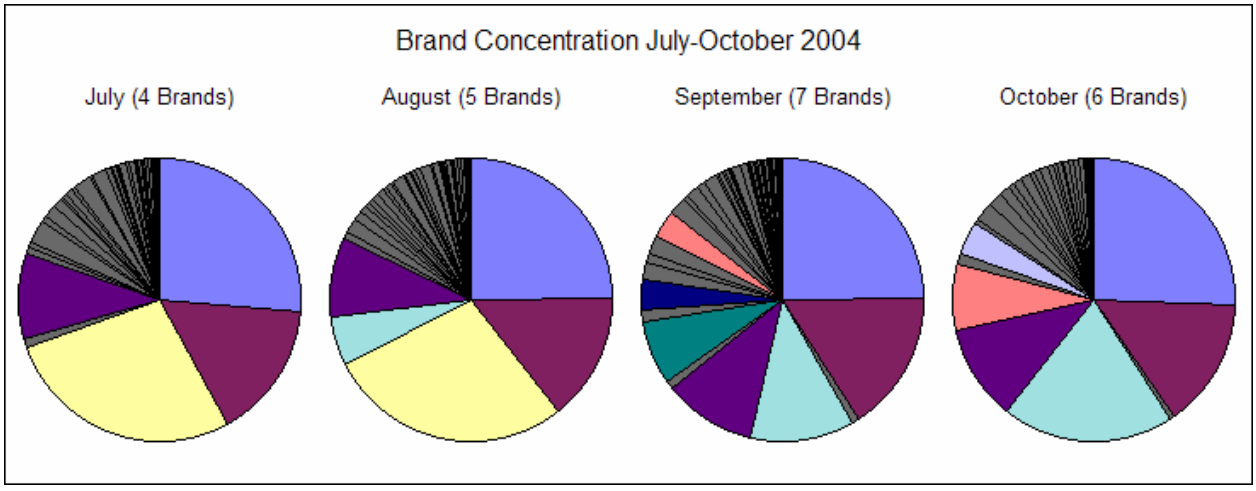
Number of Reported Brands

While nearly every measure of reported phishing activity is on the rise, one metric has remained virtually constant over the past several months: the number of reported hijacked brands. While the number of hijacked brands has ranged from 42 in July to 46 in August, there is a wide variation in the specific brands targeted in each specific month. Over the four month period, a total of 74 different brands have been targeted, and a total of 117 brands have been reportedly been hijacked since the APWG began examingphishing trends and reporting their findings in November of 2003.



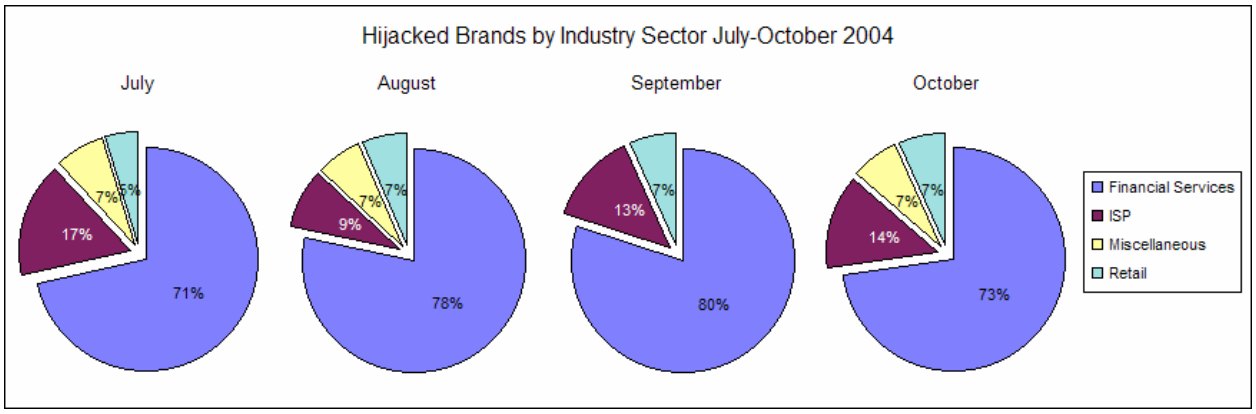
Brand Concentration

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 is on the rise slightly, ranging from four in July, to six in October. While there is still a fairly high concentration of activity involving a few well-known brands, the specific high-profile brands shift from month to month and consumers should not decrease their level of awareness based on the firms with which they specifically conduct business online.



Most-Targeted Industry Sectors

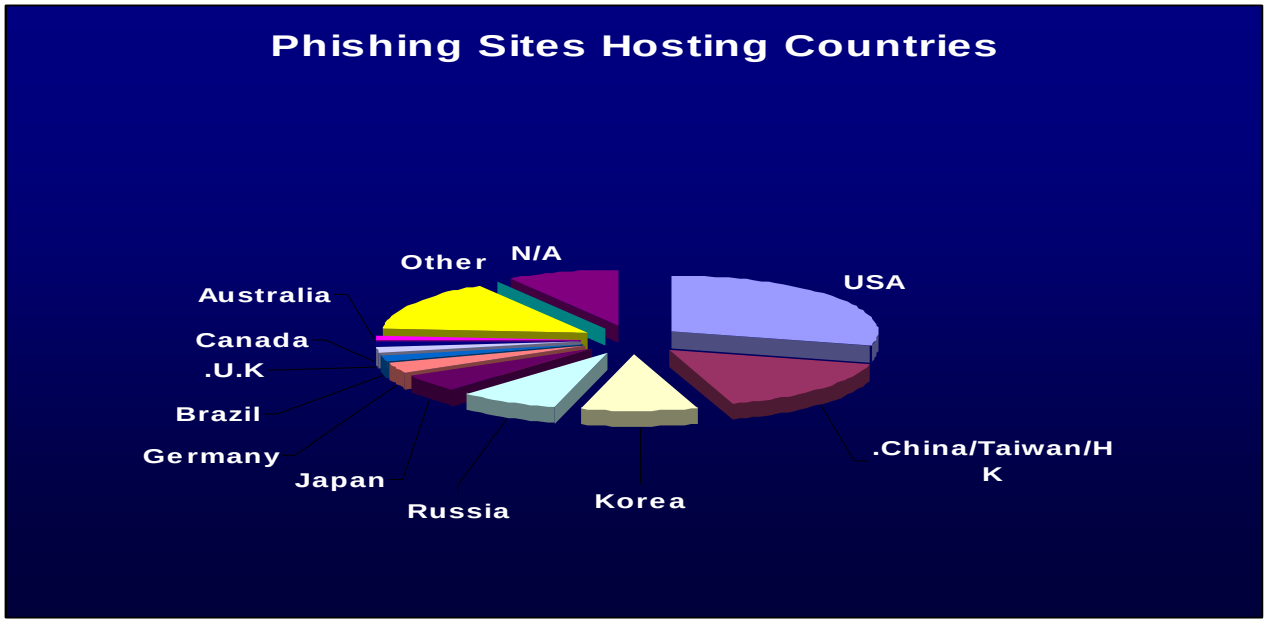
The most targeted industry sector for phishing attacks continues to be Financial Services, from the perspective of total number of unique baiting sites as well as number of companies targeted. This sector averaged 73% of all hijacked brands in October. The ISP sector now has a solid hold on second place with 14% in October, and the Retail and Miscellaneous sectors accounting for the remaining brands.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

The United States is once again the 'leader' in the number of hosted phishing sites, however, it appears to be on the decline with 29% of the total the number of sites hosted in the US decreasing during October. China, Korea, and Russia are next on the list with 16%, 9%, and 8% respectively of the total sites hosted. As reported above, the number of sites that are being hosted on what appear to be compromised broadband PC's has risen to more than 50%.



Large Increases in October

Starting on the afternoon of October 5, 2004, we started seeing a massive increase in the amount of phishing sites. Evidence indicated that the phishing exploits were not targeting one particular brand, but several targeted simultaneously. The one common theme of these phishing sites is that nearly all are being hosted on IP addresses and mostly outside of the US. It appears as though some sort of toolkit is available and/or a set of tools that are being used to produce similar exploits. The sudden large spike may, however, indicatethat some automation may be involved. We also received some feedback from a post on the incidents mailing list from individuals who have witnessed large volumes of spam increases since October 5th.

We are also seeing multiple brands being spoofed from the same machine over a few days. For example a site will be an Ebay spoof one day, and then Paypal, then Citbank, etc..The content of the attacks is quite varied. There are several versions of content that move from site to site.

The sites below have little commonality on the webserver. It appears that the "SHS" web server is popular for victimizingmachines with Trojan horse attacks, however, there appears to be a full range of Apache versions and IIS.

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(at)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(at)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 500 member organizations participating in the APWG. 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 was incorporated in June, 2004 as a non-profit association operated by its executives and steering committee.