Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends Report October, 2005

Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant **crimeware** onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords.

The monthly *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. The APWG additionally measures the evolution, proliferation and propagation of **crimeware** drawing from the independent research of our member companies. In the second half of this report are tabulations of crimeware statistics and reportage on specific criminal software detected by our member researchers.

Highlights

- Number of unique phishing reports received in October: **15820**
- Number of unique phishing sites received in October: **4367**
- Number of brands hijacked by phishing campaigns in October: **96**
- 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: **56 %**
- No hostname just IP address: **32 %**
- Percentage of sites not using port 80: **5 %**
- Average time online for site: **5.5 days**
- Longest time online for site: **31 days**

Methodology

APWG is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to a specific phishing web site, (multiple campaigns may point to the same web site). **APWG** counts unique phishing report emails as those in a given month with the same subject line in the email.

APWG also tracks the number of unique phishing websites. This is now determined by unique base URLs of the phishing sites.

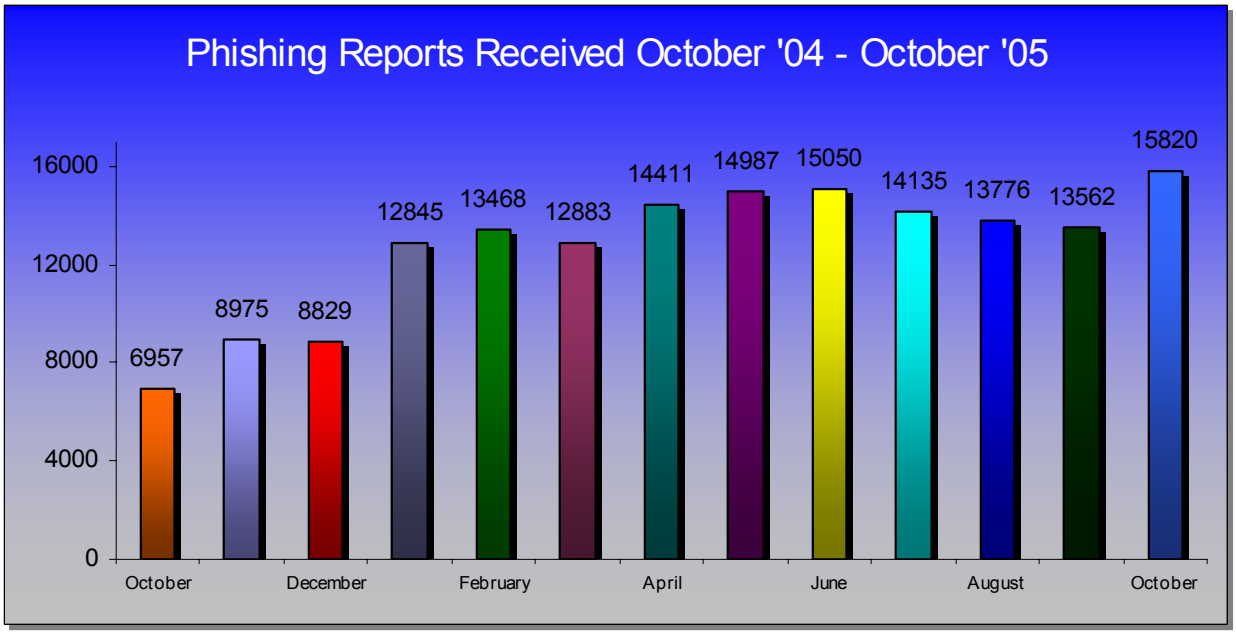
APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sties that are distributing crimeware (typically via browser drive-by exploits).

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:

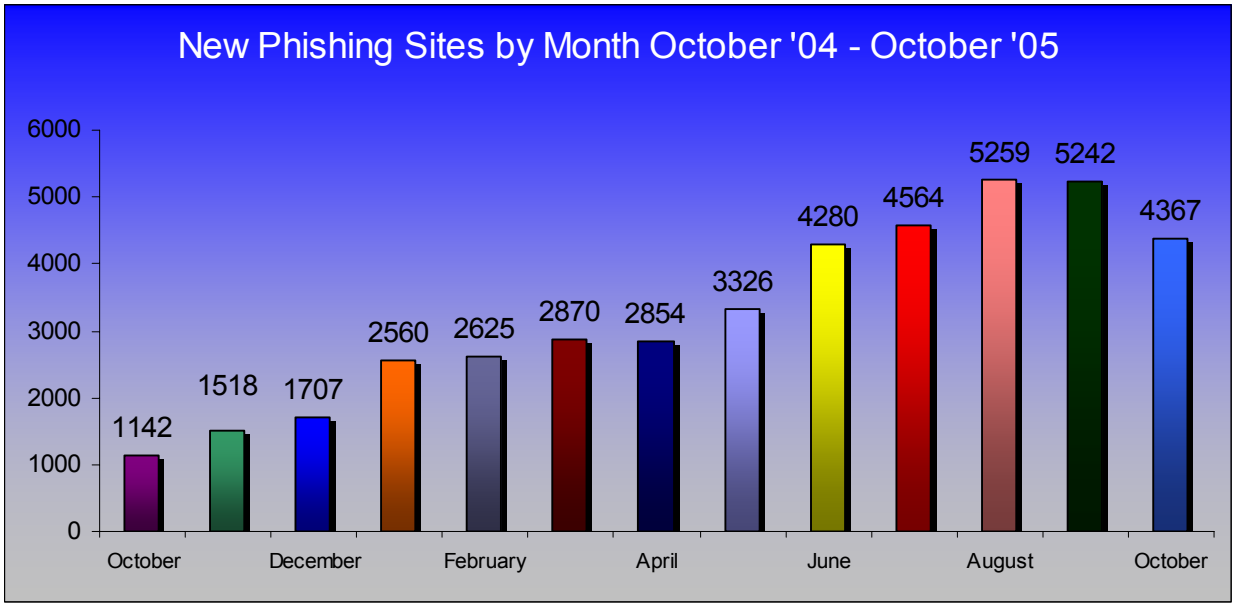
MarkMonitor panda software WEBSENSE.

Phishing Email Reports And Phishing Site Trends

The total number of *unique* phishing reports submitted to **APWG** in October 2005 was 15,820. This is a major jump of over 2,000 phishing reports from the 13,562 reported in September - this is a count of ***unique*** phishing email reports.

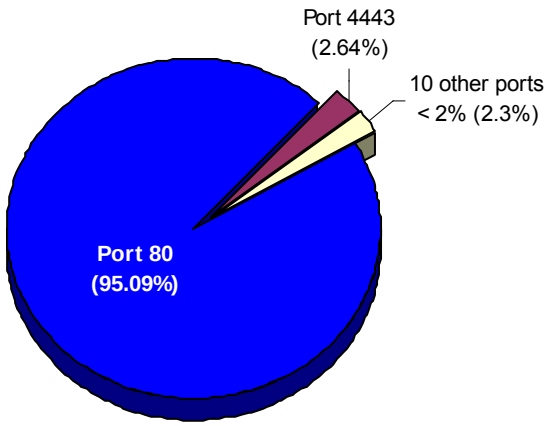


The number of *unique* phishing websites detected by **APWG** was **4210** in October 2005, a considerable drop from the previous two month highs.



Top Used Ports Hosting Phishing Data Collection Servers

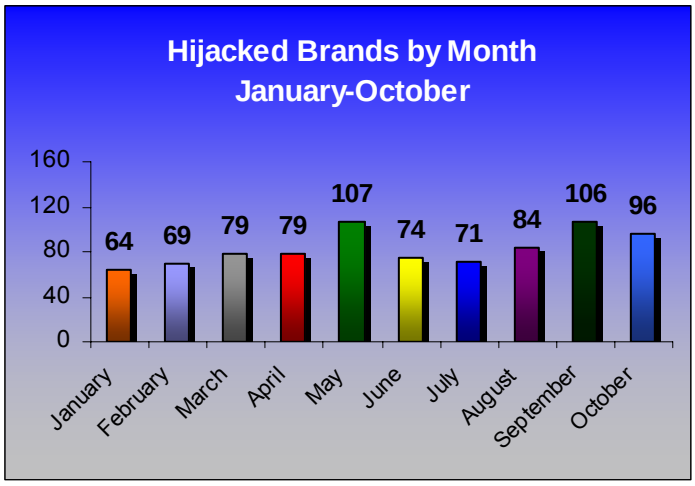
October saw a continuation of a trend of HTTP port 80 being the most popular port used at 95.09% of all phishing sites reported.



Brands and Legitimate Entities Hijacked By Email Phishing Attacks

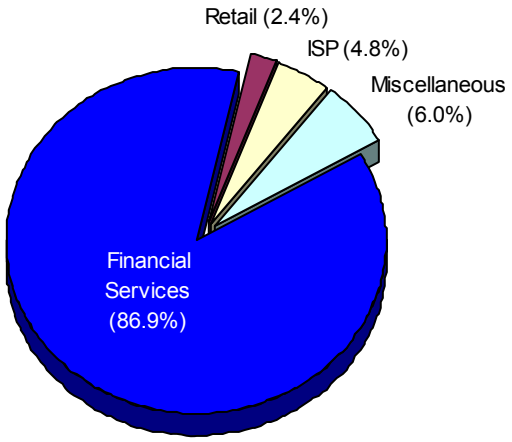
Number of Reported Brands

In October, the number of reportedly phished brands dropped to 96, down from September's 106 but still a substantial margin greater than the mean number over the past 12 months.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector growing to 86.9% of all attacks.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In October, Websense® Security Labs™ saw a continuation of the top three countries hosing phishing websites. The United States remains the on the top of the list with 28.75%, with the top 10 breakdown as follows; China 9.96%, Republic of Korea 8.4%, Germany 3.7%, Australia 3.65%, Canada 3.6%, Japan 3% United Kingdom 2.75%, Italy 2.22%, India 2.1%

PROJECT: Crimeware

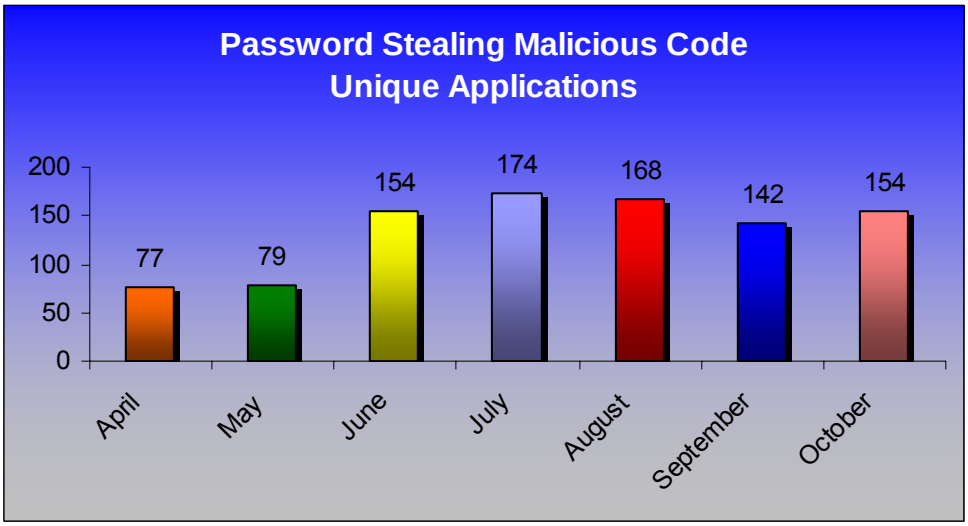
Crimeware Taxonomy & Classification Details

PROJECT: Crimeware categorizes crimeware attacks as follows, though the taxonomy will grow as variations in attack code are spawned:

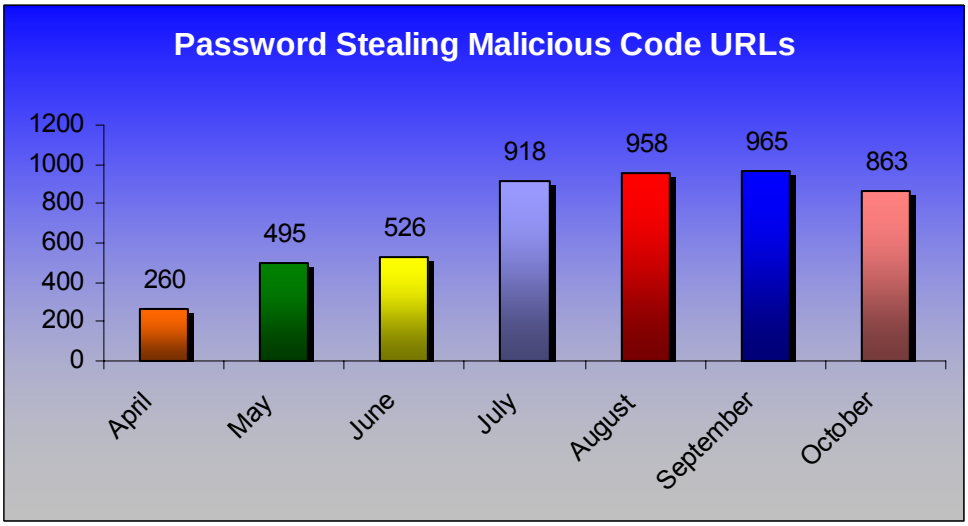
Phishing-based Trojans - Keyloggers

During the month of October, Websense Security Labs have witnessed an increase in the number of variants of keyloggers, but a large decrease of password stealing malicious code URLs.

Phishing-based Trojans – Keyloggers, Unique Variants



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers

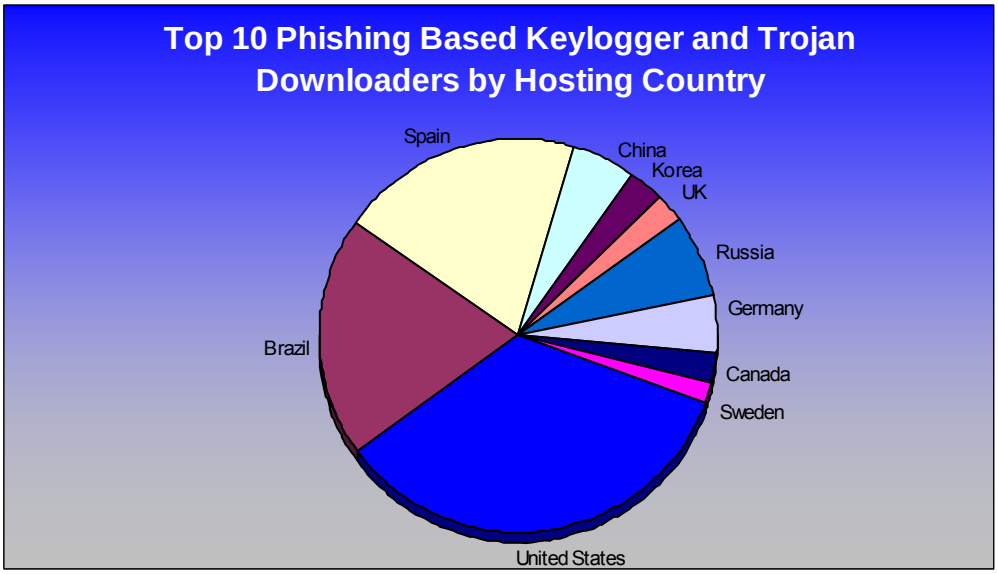


Phishing-based Trojans & Downloader's Hosting Countries (by IP address)

The chart below represents a breakdown of the websites which were classified during October as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger.

The United States is still the top geographic location with 29.9%, Spain continues to grow to 17.08%.

The rest of the breakdown was as follows; Brazil 16.89%, Spain 17.08%, Russia 5.82%, China 4.66%, Germany 4.07%, Korea 2.33%, UK 2.13%, Canada 2.13%, Sweden 1.55%



Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Research Contributors

MarkMonitor

MarkMonitor is the global leader in delivering comprehensive online corporate identity protection services, with a focus on making the Internet safe for online transactions.

PandaLabs

PandaLabs is an international network of research and technical support centers devoted to protecting users against malware.

Websense® Security Labs™

Websense Security Labs mission is to discover, investigate, and report on advanced Internet threats to protect employee computing environments.

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 more than 1300 companies and government agencies participating in the APWG and more than 2000 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.