Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends

Report for the Month of November, 2006

Summarization of November Report Findings

►The number of phishing spoof sites continues to remain high with the number of unique phishing URLs being 37,439 in November, a decrease of only five URLs from October. APWG notes that there appears to be a trend of targeting major financial institutions in waves. This is similar to the attack patterns that were happening in 2004, when banks were attacked in waves, according to vulnerabilities or cash-out opportunities for those particular accounts. ► APWG saw a total of 120 brands being hijacked in November with a mix of top US and UK banks in the top 10 targets and a number of smaller banks, though fewer credit unions were attacked during the month. Furthermore, several major online retailers had their brands spoofed in phishing attacks in November. ► More online brokerages were spoofed in November 2006 than in any previous month. This may be related to the online pump-and-dump schemes that have been using phished brokerage accounts to pump up the stock of thinly traded companies. ► APWG continued to see a steady though infrequent number of IRS government phishing attacks. ► The number of crimeware variants dropped by only seven to 230, down from last month's record of 237.

Phishing Defined and Report Scope

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, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes.

The monthly *Phishing Activity Trends Report* analyzes phishing attacks reported to the Anti-Phishing Working Group (APWG) via its member companies, Global Research Partners, the organization's website at http://www.antiphishing.org and 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.

Statistical Highlights for November 2006

- Number of unique phishing reports received in November: **25816**
- Number of unique phishing sites received in November: **37439**
- Number of brands hijacked by phishing campaigns in November: **120**
- Number of brands comprising the top 80% of phishing campaigns in November: **20**
- Country hosting the most phishing websites in November: **United States**
- Contain some form of target name in URL: **30 %**
- No hostname just IP address: **12 %**
- Percentage of sites not using port 80: **2.8 %**
- Average time online for site: **4.5 days**
- Longest time online for site: **30 days**

Methodology

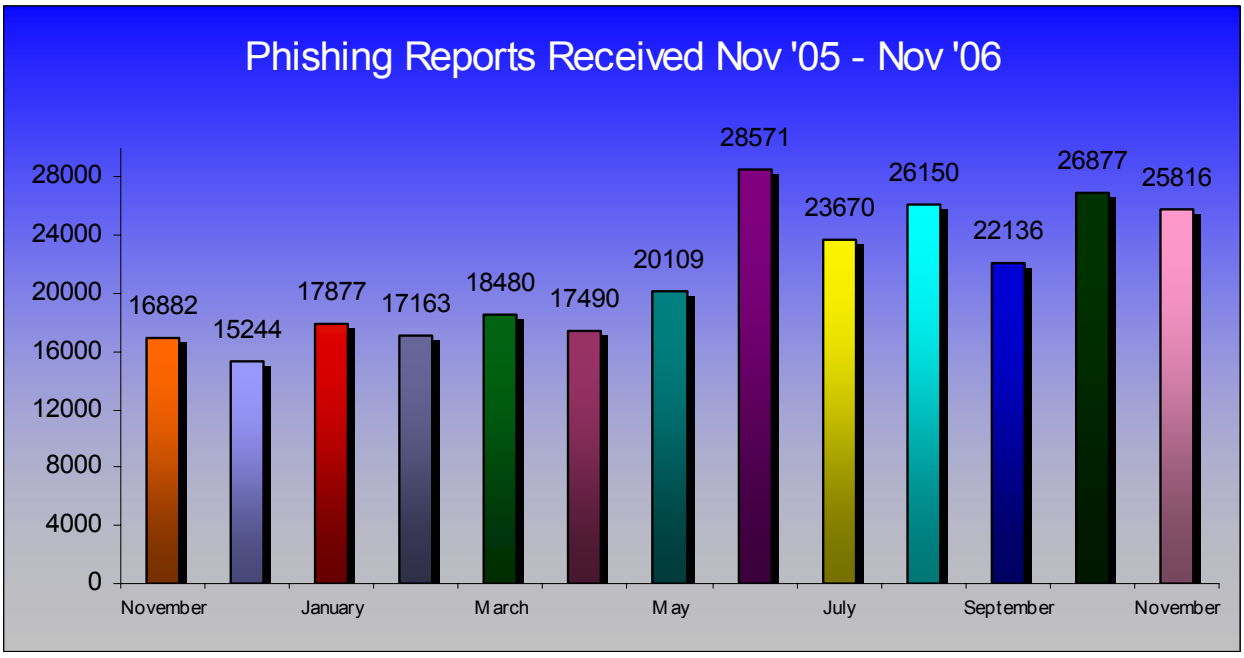
APWG is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to 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).

Phishing Email Reports and Phishing Site Trends for November 2006

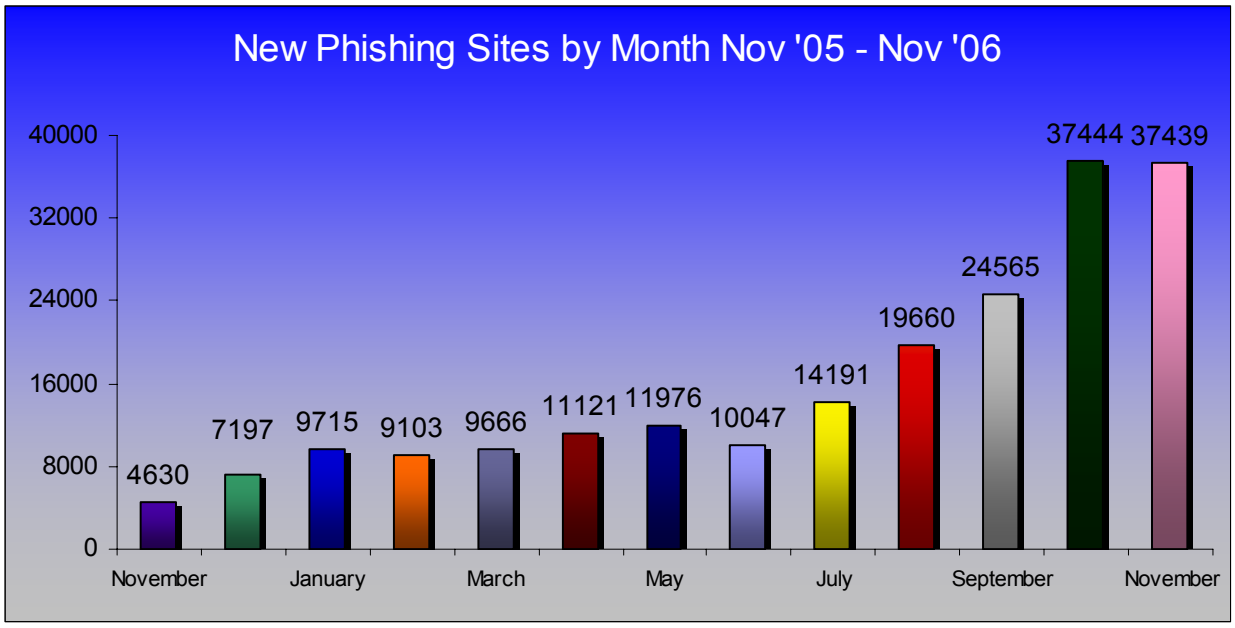
The total number of *unique* phishing reports submitted to **APWG** in November 2006 was **25,816** – an decrease of over one thousand attacks from October and the fourth highest recorded by the APWG. This is a count of ***unique*** phishing email reports received by the APWG from the public, its members and its research partners.



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:

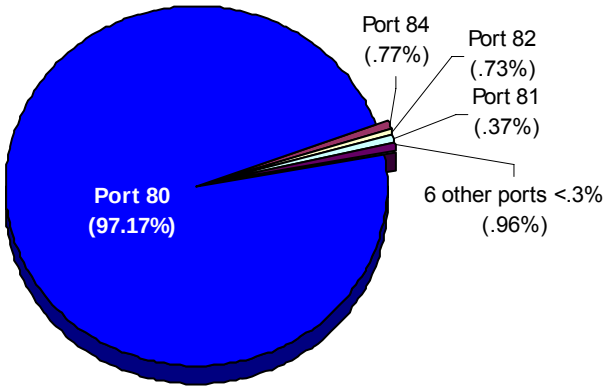
MarkMonitor panda software WEBSENSE.

The number of *unique* phishing websites detected by **APWG** was **37,439** in November 2006. Similar to October, we can see that there are far more phishing emails being sent. In particular, there are more sub-domains being used, in an attempt to thwart anti-phishing filters by rapidly introducing novel variants.



Top Used Ports Hosting Phishing Data Collection Servers in November 2006

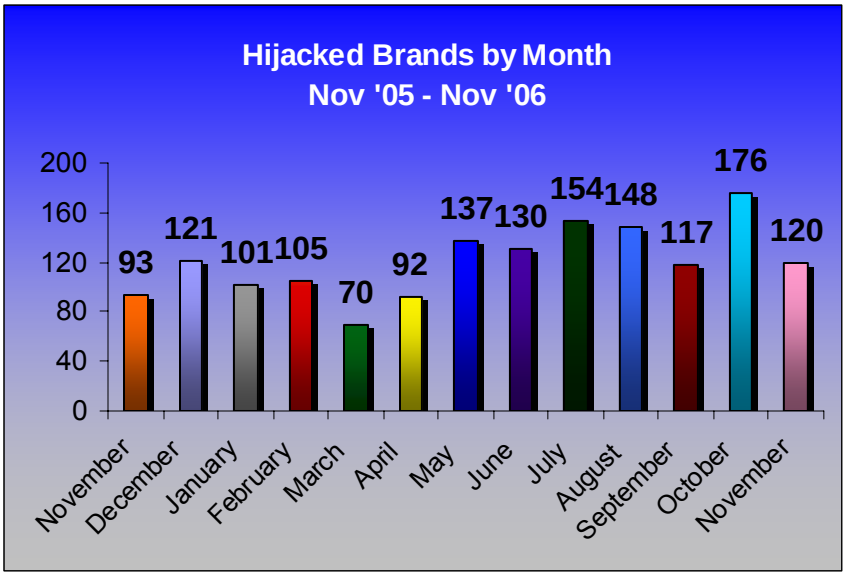
November saw a continuation of a trend of HTTP port 80 being the most popular port used at 97.17% of all phishing sites reported.



Brands & Legitimate Entities Hijacked By Email Phishing Attacks in Nov. 2006

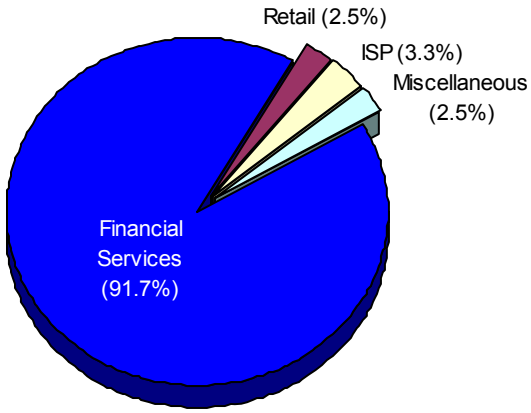
Number of Reported Brands

November 2006 showed a considerable drop in the number of hihacked brands with 120, down from the previous month's record-shattering 176. Of those brands most all were financial services firms, with a mix of top US and UK banks in the top 10 targets as well as a number of smaller banks. There were, however, fewer credit unions attacked during the month. Furthermore, several major online retailers had their brands spoofed in phishing attacks in November, opportunistically leveraging the gift-buying rush of the holidays.



Most Targeted Industry Sectors in November 2006

Financial Services continue to be the most targeted industry sector at 91.7% of all attacks in the month of November. Additionally, ISPs continue to surpass Retail as a targeted industry. More online brokerages were spoofed in November 2006 than in any previous month, accounting for two of the financial services brands attacked. The focus on brokerages may be related to some of the online pump-and-dump schemes that have been using phished brokerage accounts to pump up the stock of thinly traded companies. Scammers would pump up stocks by both sending promotional spam for sparsely traded stocks and taking over accounts to buy the stock and temporarily inflate their bourse sell prices.



Web Phishing Attack Trends in November 2006

Countries Hosting Phishing Sites

In November, 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 24.2%. The rest of the top 10 breakdown is as follows: China 15.42%, Republic of Korea 14.88%, Germany 5.27%, Romania 2.84%, Russia 2.64%, United Kingdom 2.04%, France1.83%, Venezuela 1.81%, Brazil1.43%.

PROJECT: Crimeware

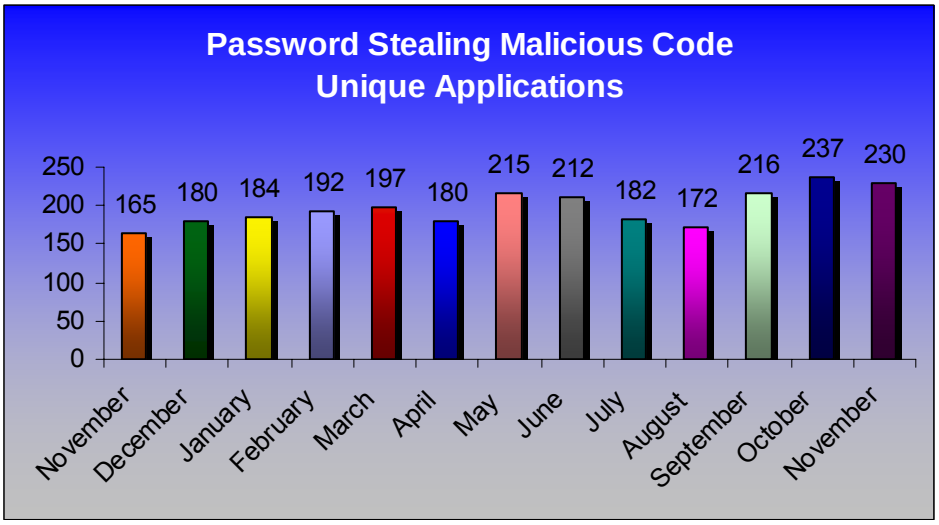
Crimeware Taxonomy & Samples According to Classification in November 2006

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

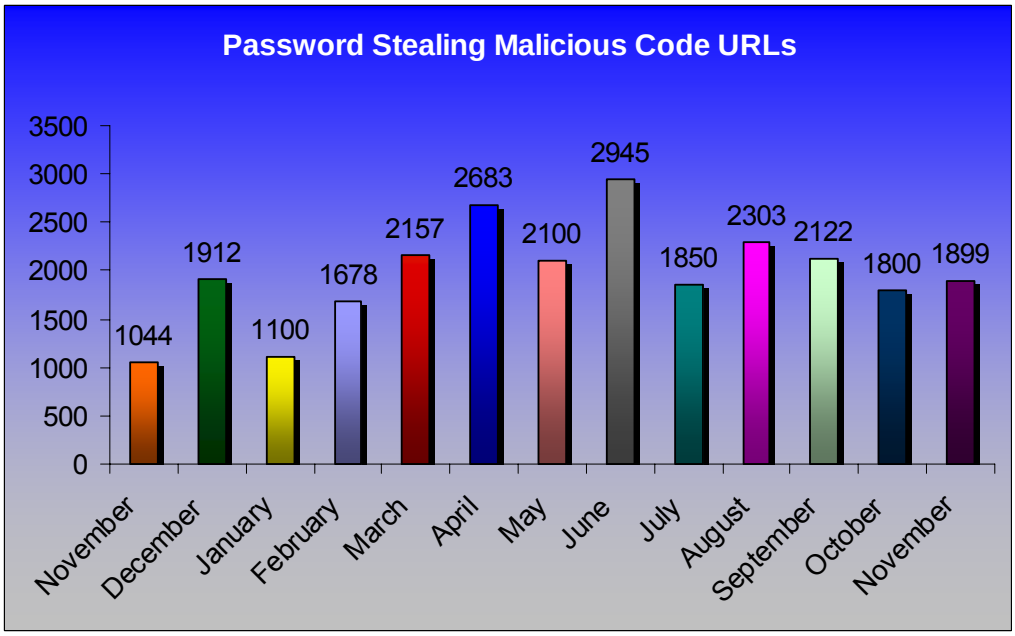
Phishing-based Trojans - Keyloggers

Definition: Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, most importantly financial institutions and online retailers and ecommerce merchants) in order to target specific information, the most common are; access to financial based websites, ecommerce sites, and web-based mail sites.

Phishing-based Trojans – Keyloggers, Unique Variants in November



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers in November



Phishing-based Trojans – Redirectors

Definition: Crimeware 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 crimeware that changes hosts files and other DNS specific information, crimeware browser-helper objects that redirect users to fraudulent sites, and crimeware that may install a network level driver or filter to redirect users 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.

Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server. The fraudulent server replies with “good”

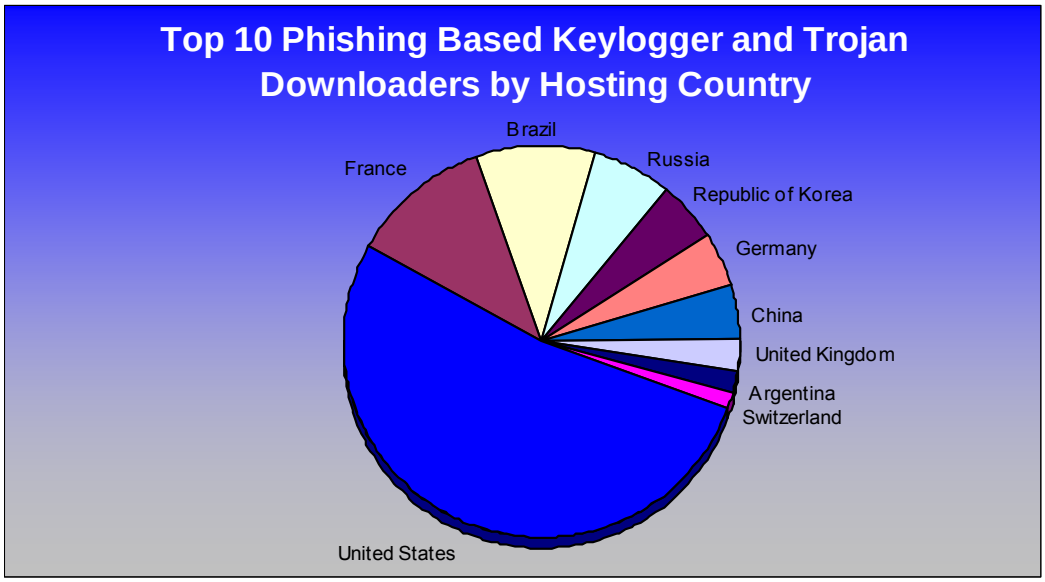
answers for most domains, however when they want to direct you to a fraudulent one, they simply modify their name server responses. This is particularly effective because the attackers can redirect any of the users requests at any time and the end-users have very little indication that this is happening as they could be typing in the address on their own and not following an email or Instant Messaging lure.

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

The chart below represents a breakdown of the websites which were classified during November 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 the top geographic location with 34.04%.

The rest of the breakdown was as follows; France 7.49%, Brazil 6.42%, Russia 4.06%, Republic of Korea 3.21%, Germany 2.99%, China 2.78%, United Kingdom 1.92%, Argentina 1.07%, Switzerland .85%.



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 1600 companies and government agencies participating in the APWG and more than 2600 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, a 501c6 tax-exempted corporation, 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.