Phishing Activity Trends Report

Combined Report for September and October, 2006

Summarization of Combined September-October Report Findings

►In summer and early fall, the number of phishing spoof sites soared, driving the number of unique phishing URLs to 37,444 in October, a 757 percent increase over the 4367 reported by the APWG in October 2005 - and up some 236 percent from the 11,121 detected just six months before in April, 2006. APWG contributing analysts from MarkMonitor attributed most all of this increase to phishing campaigns employing very large numbers of sites with URLs using multiple subdomains attached to spoof domains (e.g. 123.phishsite.com, 234.phishsite.com, 345.phishsite.com.) Most of the multiple-subdomain sites were used in attacks against one frequently phished financial institution. The APWG believes the multiple subdomains ploy is used to defeat spam filters and URL-filtering systems (such as those in browser toolbars) by rapidly deploying variants that have not yet been added to blocking lists or 'black lists' of phishing URLs. ► Phishers in the month of October also broke the previous record for the number of brands attacked in a single month with 176 being subjected to spoofing, up 14 percent from the previous high of 154 in July 2006. ► For the second month running, the number of crimeware variants rose to break records - in October hitting 237, up 38 percent from August, 2006. ► **Note**: In this report, APWG restates its August, 2006 total for unique phishing sites as 19,660 (from the previously reported 10091), reflecting an augmented methodology for distinguishing and enumerating URLs used in phishing campaigns, including the subdomain variants discussed in this summary.

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 October 2006

- Number of unique phishing reports received in October: **26877**
- Number of unique phishing sites received in October: **37444**
- Number of brands hijacked by phishing campaigns in October: **176**
- Number of brands comprising the top 80% of phishing campaigns in October: **18**
- 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:   **4.9 %**
- Average time online for site: **4.5 days**
- Longest time online for site: **30 days**
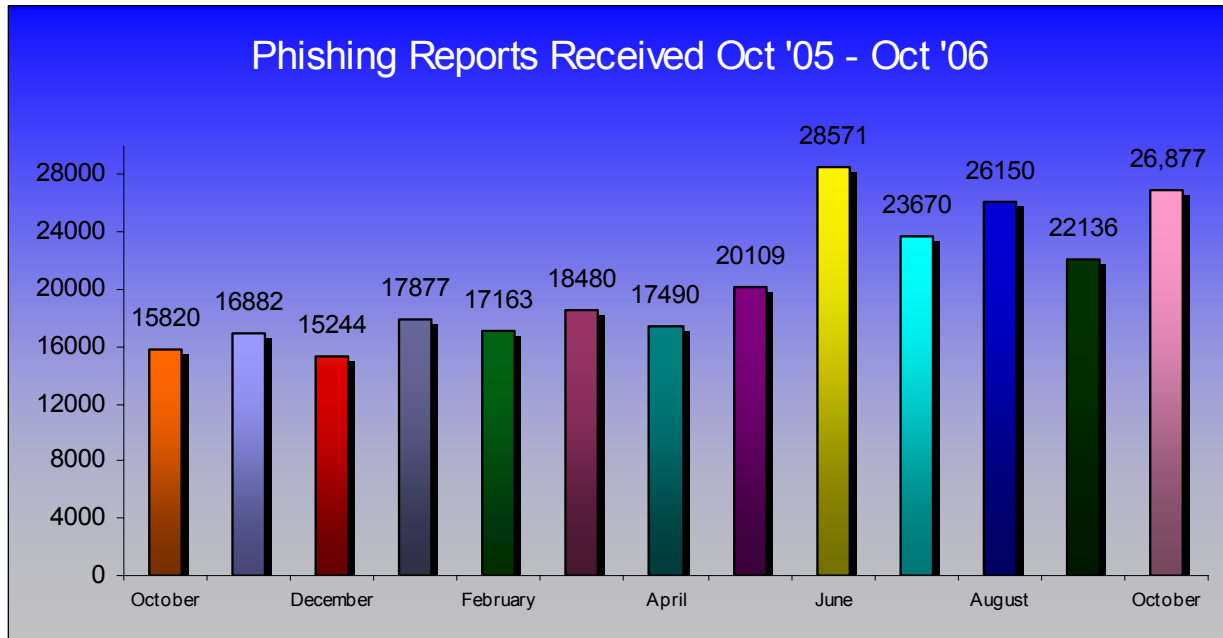
Methodology

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 October 2006

The total number of *unique* phishing reports submitted to **APWG** in October 2006 was **26,877** – an increase of over four thousand attacks from September and the second 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.

Phishing Reports Received Oct '05 - Oct '06

Month	Value
October	15820
	16882
December	15244
	17877
February	17163
	18480
April	17490
	20109
June	28571
	23670
August	26150
	22136
October	26,877

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 **37,444** in October 2006, up 52% from a month earlier. 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 fool anti-phishing filters.

New Phishing Sites by Month Oct '05 - Oct '06
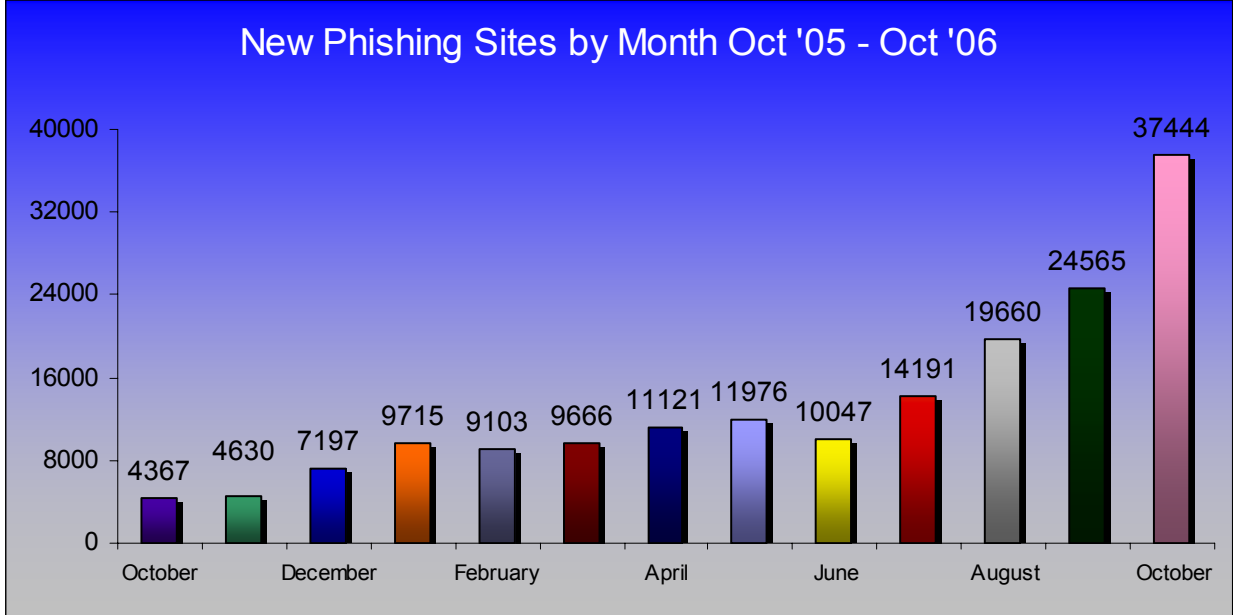
Top Used Ports Hosting Phishing Data Collection Servers in October 2006
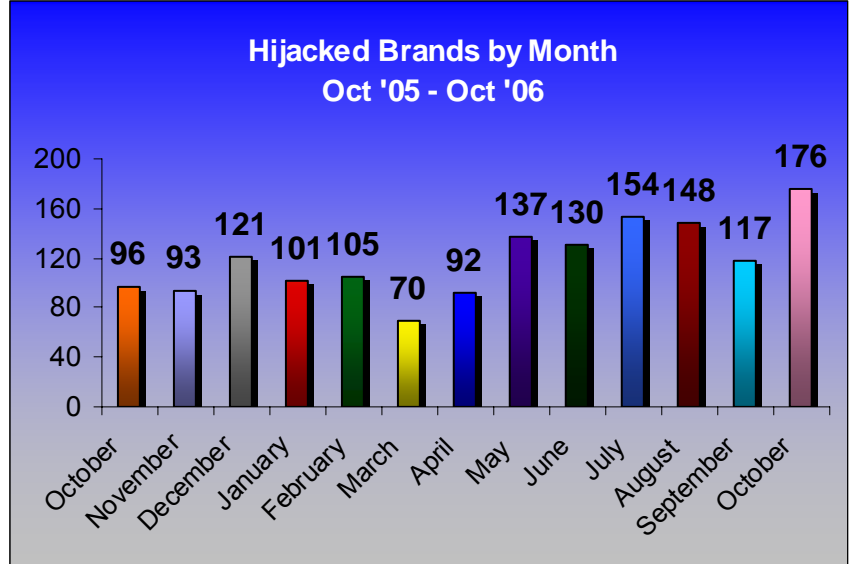
October saw a continuation of a trend of HTTP port 80 being the most popular port used at 95.09% of all phishing sites reported.
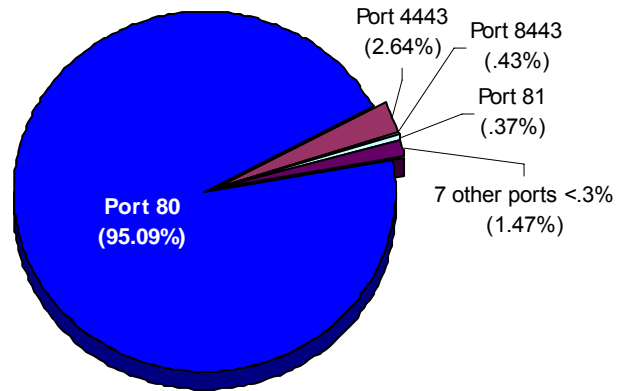
Brands & Legitimate Entities Hijacked By Email Phishing Attacks in October 2006

Number of Reported Brands

October 2006 showed the highest amount of brands being phished ever recorded by the APWG with 176. Larger numbers of smaller banks and credit unions are being spoofed and subject to phishing attacks.

Hijacked Brands by Month
Oct '05 - Oct '06

| Month	Value
October	96
November	93
December	121
January	101
February	105
March	70
April	92
May	137
June	130
July	154
August	148
September	117
October	176

Most Targeted Industry Sectors in October 2006

Financial Services continue to be the most targeted industry sector at 92.6% of all attacks in the month of October. Additionally, ISPs continue to surpass Retail as a targeted industry.

Retail (2.3%)
ISP (2.8%)
Miscellaneous (2.3%)
Financial Services (92.6%)
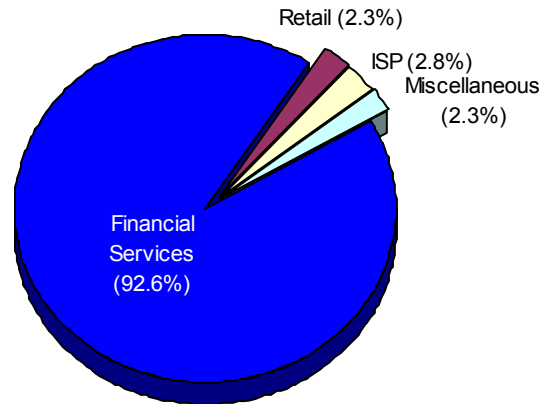
Web Phishing Attack Trends in October 2006

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 28.78%. The rest of the top 10 breakdown is as follows –China 11.96%, Republic of Korea 8.4%, Germany 3.7%, Australia 3.64%, Canada 3.6%, Japan 3.01%, United Kingdom 2.75%, Italy 2.22%, India 2.11%.

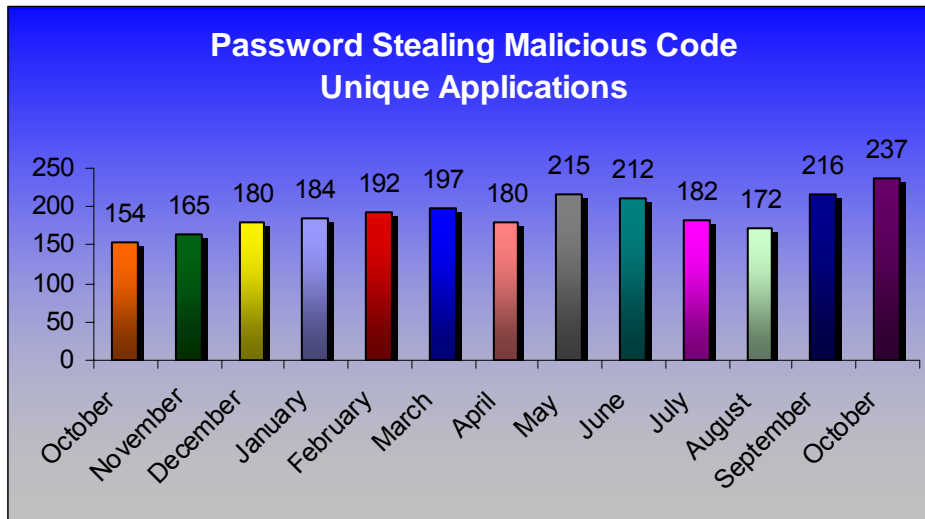**Top 10 Phishing Sites Hosting Countries**
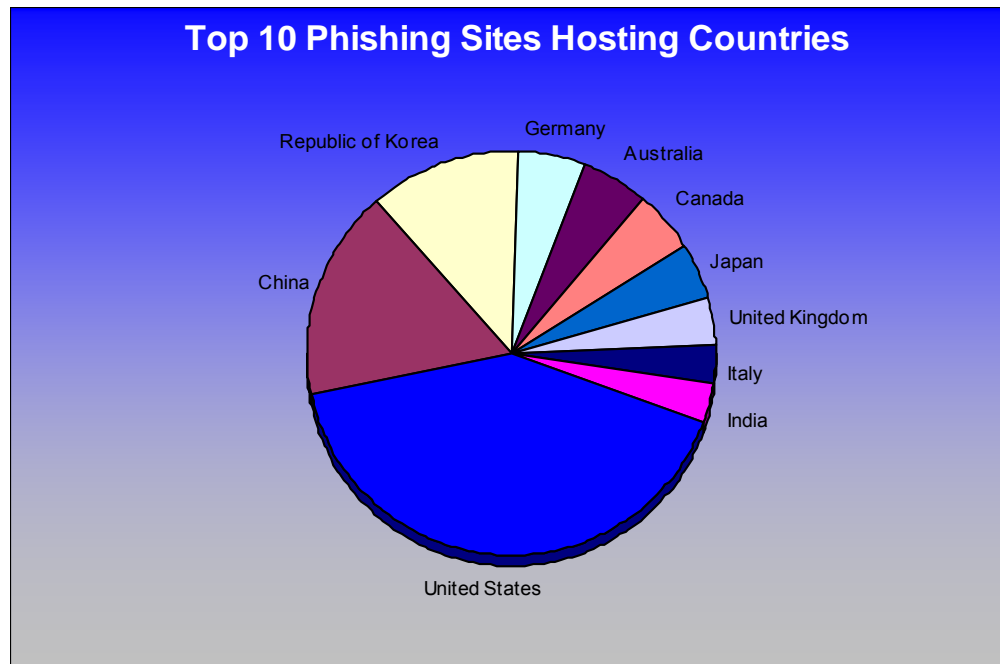
PROJECT: Crimeware

Crimeware Taxonomy & Samples According to Classification in October 2006

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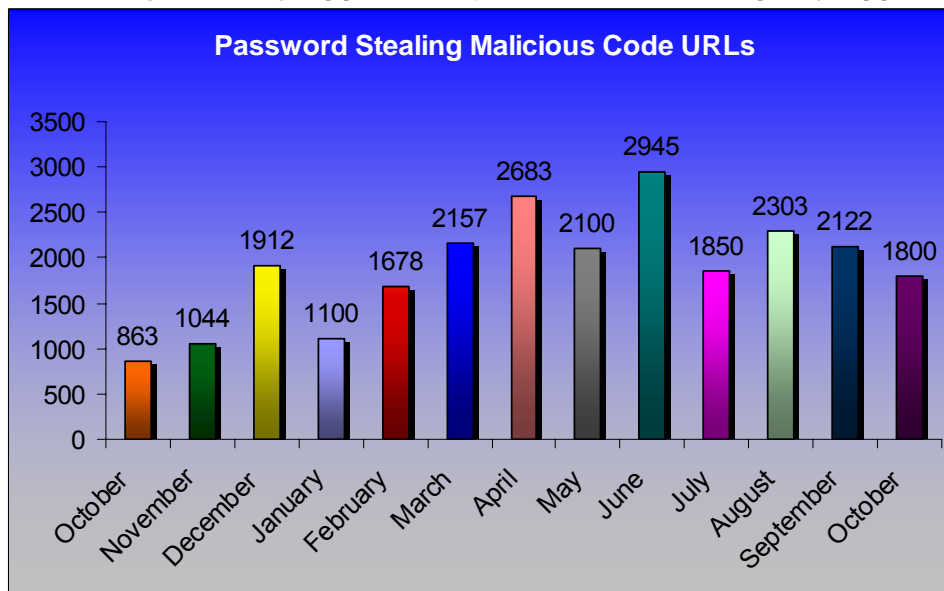
Phishing-based Trojans - Keyloggers

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 Break Record Again in October

**Password Stealing Malicious Code
Unique Applications**

Month	Value
October	154
November	165
December	180
January	184
February	192
March	197
April	180
May	215
June	212
July	182
August	172
September	216
October	237

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

Password Stealing Malicious Code URLs

Month	Value
October	863
November	1044
December	1912
January	1100
February	1678
March	2157
April	2683
May	2100
June	2945
July	1850
August	2303
September	2122
October	1800

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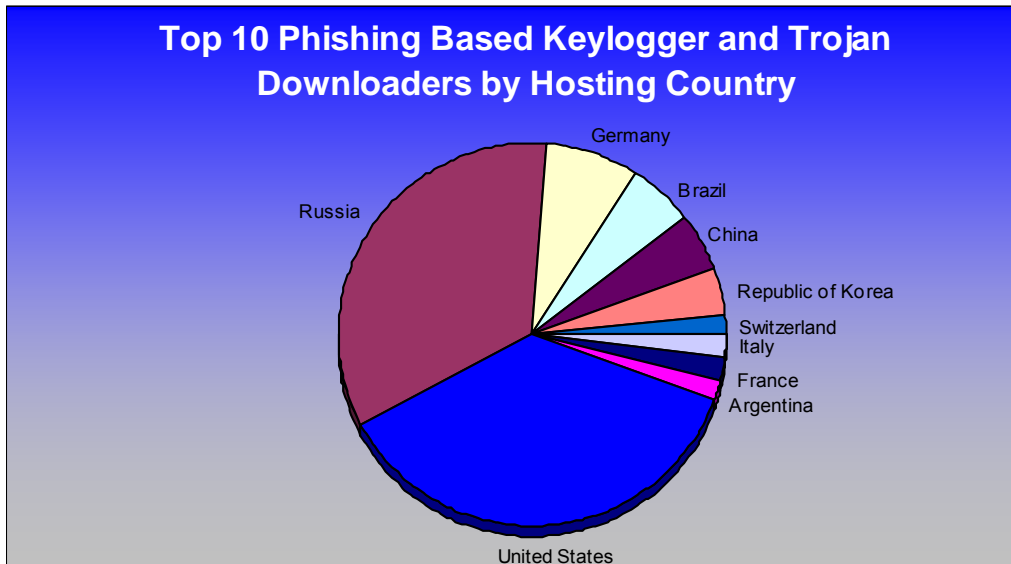
Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server.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

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 the top geographic location with 30.91%

The rest of the breakdown was as follows; Russia 28.5%, Germany 6.45%, Brazil 4.57%, China 4.22%, Republic of Korea 3.22%, Switzerland 1.61%, Italy 1.61%, France 1.61%, Argentina 1.34%.

Top 10 Phishing Based Keylogger and Trojan Downloaders by Hosting Country

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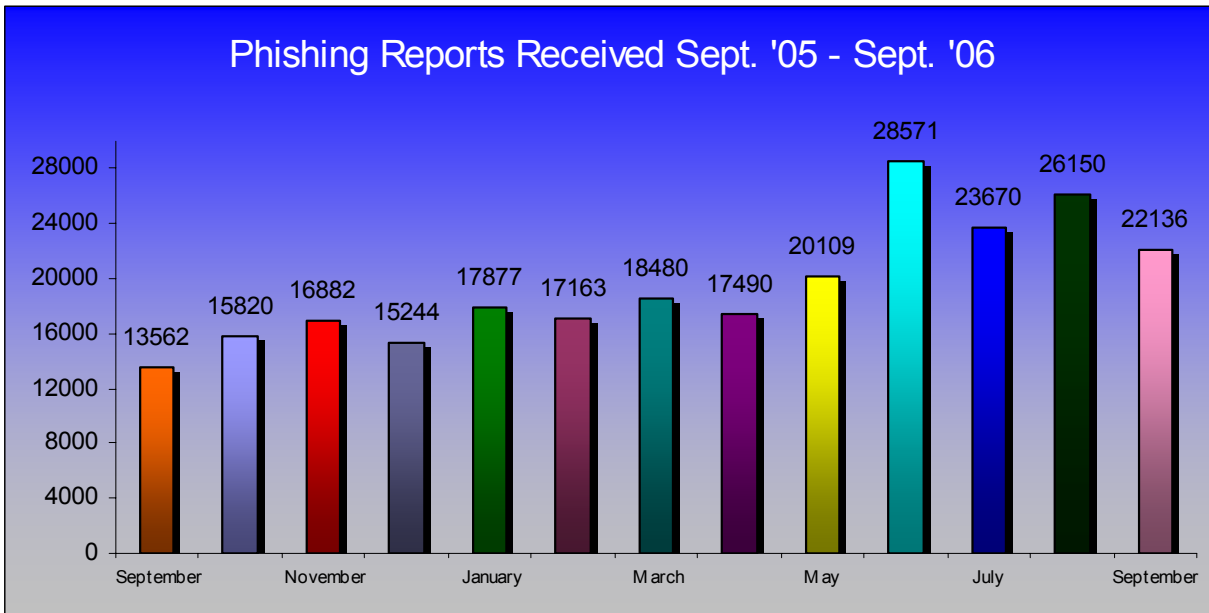Committed to wiping out Internet scams and fraud

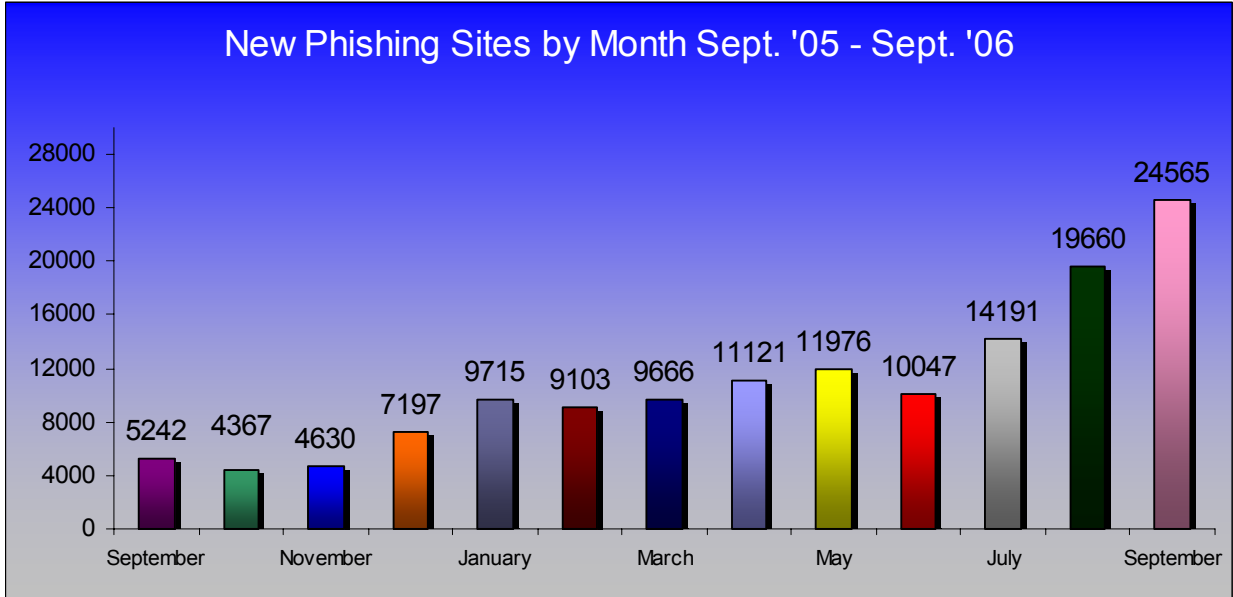## Statistical Highlights for September 2006

- Number of unique phishing reports received in September: **22136**
- Number of unique phishing sites received in September: **24565**
- Number of brands hijacked by phishing campaigns in September: **117**
- Number of brands comprising the top 80% of phishing campaigns in September: **19**
- Country hosting the most phishing websites in September: **United States**
- Contain some form of target name in URL: **49 %**
- No hostname just IP address: **34 %**
- Percentage of sites not using port 80: **2.99 %**
- Average time online for site: **4.5 days**
- Longest time online for site: **30 days**

Phishing Email Reports And Phishing Site Trends for September 2006

The total number of *unique* phishing reports submitted to **APWG** in September 2006 was **22,136** – an decrease of over four thousand attacks from August. This is a count of *unique* phishing email reports received by the APWG from the public, its members and its research partners.

Phishing Reports Received Sept. '05 - Sept. '06

Month	Reports
September	13562
October	15820
November	16882
December	15244
January	17877
February	17163
March	18480
April	17490
May	20109
June	28571
July	23670
August	26150
September	22136

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

The number of *unique* phishing websites detected by **APWG** was **24,565** in September 2006. This is a 25 percent increase over the 19660 unique phishing sites detected in August. The main reason for this increase is that there has been a rise in the number of sub-domains used for phishing, often a number of subdomains attached to a counterfeit domain being used in different phishing attack or multiple attacks against a single brandholder.

New Phishing Sites by Month Sept. '05 - Sept. '06

Month	Value
September	5242
	4367
November	4630
	7197
January	9715
	9103
March	9666
	11121
May	11976
	10047
July	14191
	19660
September	24565

Top Used Ports Hosting Phishing Data Collection Servers in September 2006

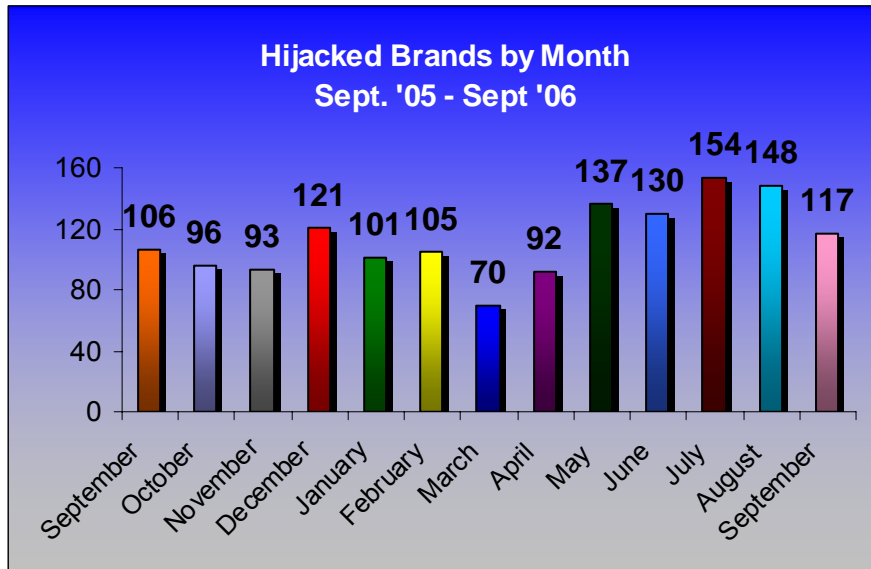September saw a continuation of a trend of HTTP port 80 being the most popular port used at 98.02% of all phishing sites reported.

Port 443
(.46%)

Port 680
(.33%)

Port 80
(98.02%)

7 other ports <.3%
(1.19%)
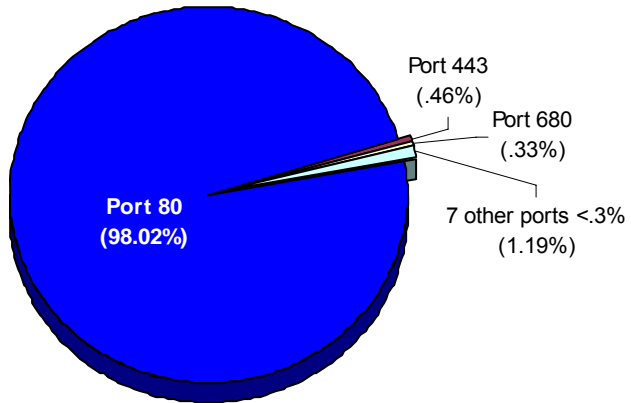
Brands & Legitimate Entities Hijacked in Email Phishing Attacks in September 2006

Number of Reported Brands

September 2006 showed a drop of over 30 brands hijacked compared to August.

Hijacked Brands by Month
Sept. '05 - Sept '06

Month	Value
September	106
October	96
November	93
December	121
January	101
February	105
March	70
April	92
May	137
June	130
July	154
August	148
September	117

## Most Targeted Industry Sectors in September 2006

Financial Services continue to be the most targeted industry sector at 91.5% of all attacks in the month of September. Additionally, ISPs have surpassed Retail as a targeted industry.

Retail (2.6%)
ISP (3.4%)
Miscellaneous (2.6%)
Financial Services (91.5%)
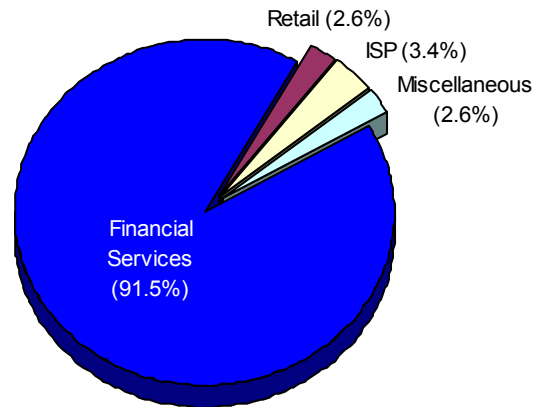
Web Phishing Attack Trends in September 2006

Countries Hosting Phishing Sites

In September, 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 31.22%. The rest of the top 10 breakdown is as follows – China 12%, Republic of Korea 8.9%, Germany 3.17%, Canada 2.97%, Japan 2.44%, France 2.31%, Poland 2.24%, Romania 1.98%, Brazil 1.98%.

Top 10 Phishing Sites Hosting Countries
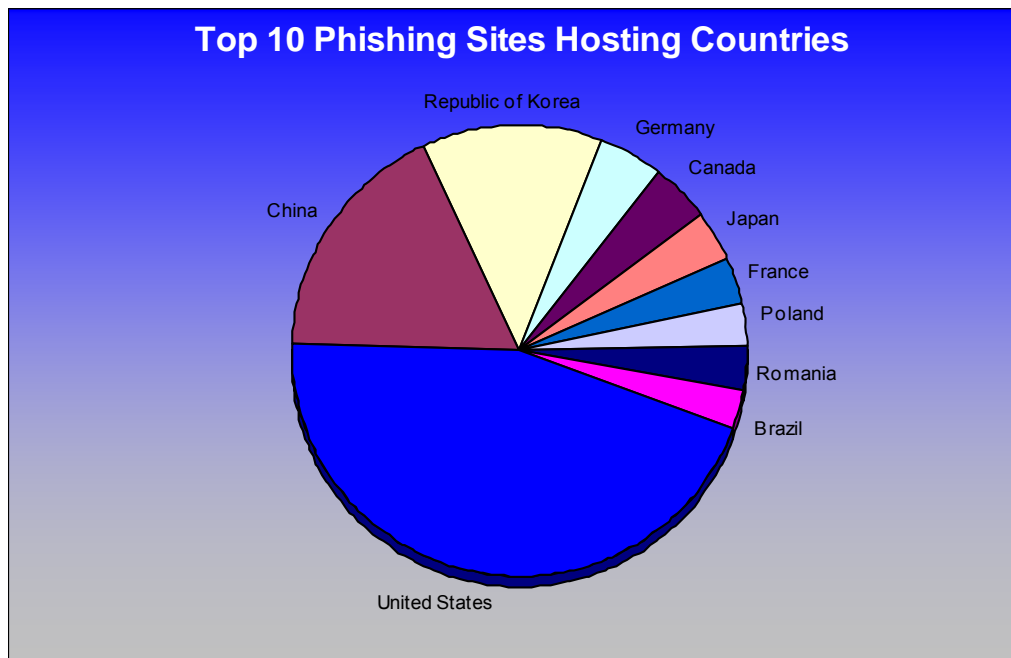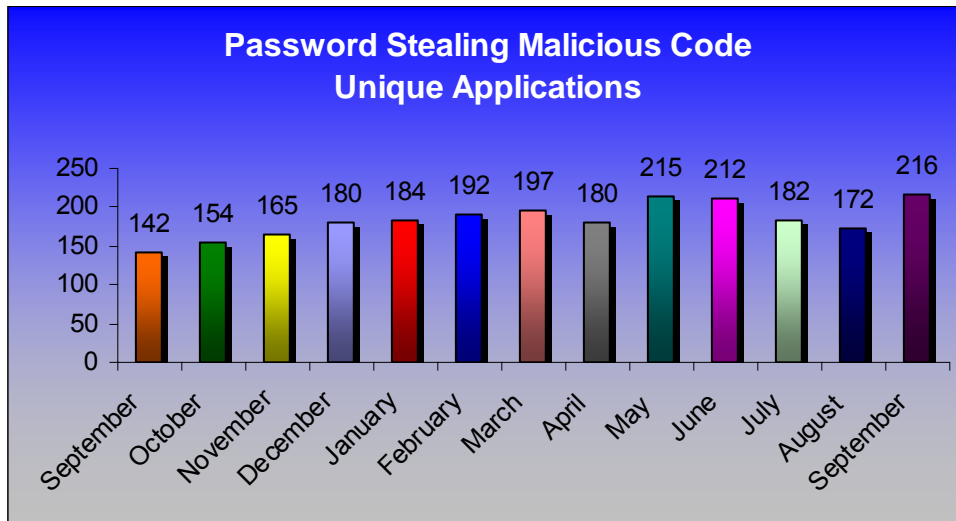
PROJECT: Crimeware

Crimeware Taxonomy & Samples According to Classification in September 2006

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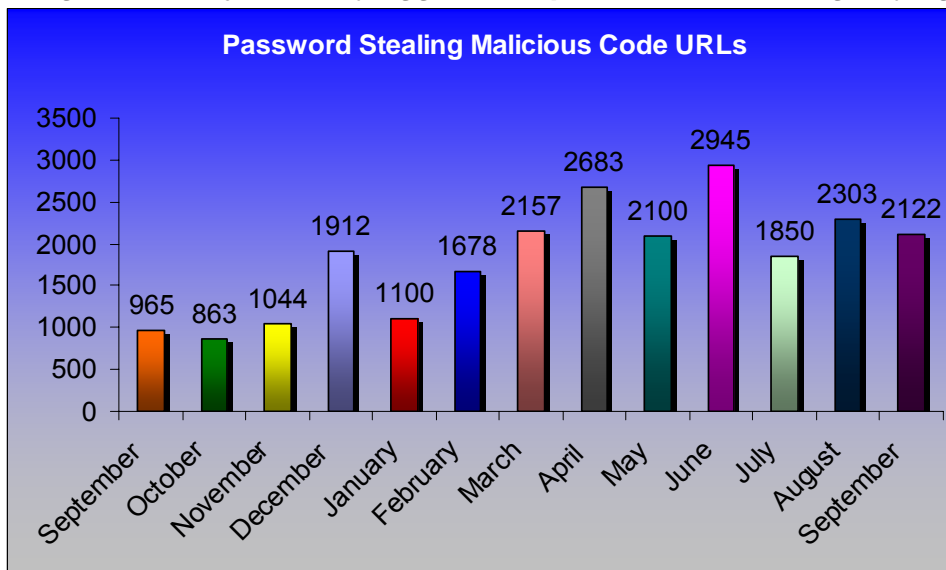
Phishing-based Trojans - Keyloggers

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 Rise to New Record in September

Password Stealing Malicious Code
Unique Applications

Month	Value
September	142
October	154
November	165
December	180
January	184
February	192
March	197
April	180
May	215
June	212
July	182
August	172
September	216

Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers

Password Stealing Malicious Code URLs

Month	Value
September	965
October	863
November	1044
December	1912
January	1100
February	1678
March	2157
April	2683
May	2100
June	2945
July	1850
August	2303
September	2122

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 September 2006

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

The United States has moved back to being the top geographic location since being surpassed by Russia in August with 33.29%.

The rest of the breakdown was as follows; Russia 25%, Brazil 5.8%, China 4.28%, Republic of Korea 3.59%, Spain 3.45%, France 2.62%, Germany 2.2%, Portugal 2.07%, Argentina 2.07%.

Top 10 Phishing Based Keylogger and Trojan Downloaders by Hosting Country
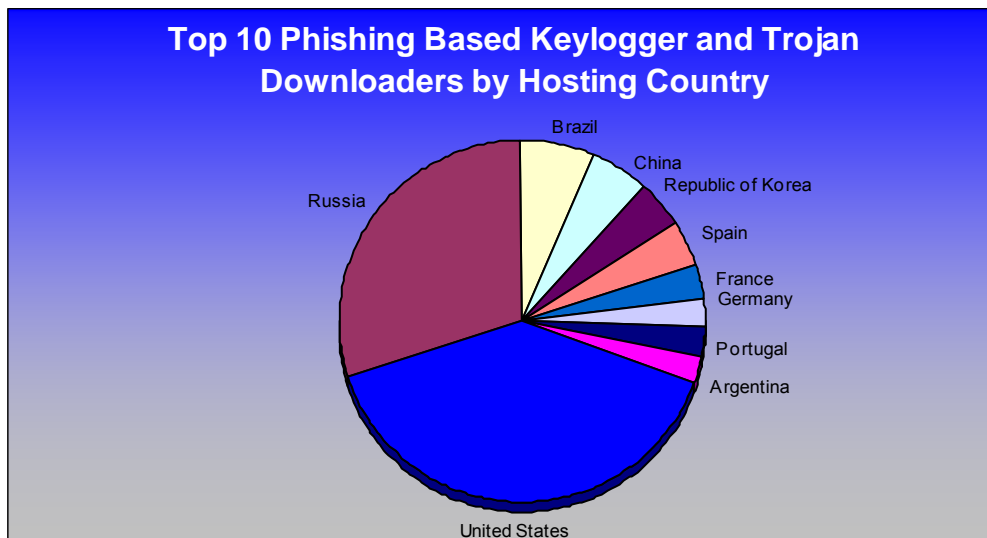
Phishing Research Contributors

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 1500 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.