Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Phishing Activity Trends Report July, 2006

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 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 July: **23670**
- Number of unique phishing sites received in July: **14191**
- Number of brands hijacked by phishing campaigns in July: **154**
- Number of brands comprising the top 80% of phishing campaigns in July: **15**
- Country hosting the most phishing websites in July: **United States**
- Contain some form of target name in URL: **46 %**
- No hostname just IP address: **42 %**
- Percentage of sites not using port 80: **8.9 %**
- Average time online for site: **4.8 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.

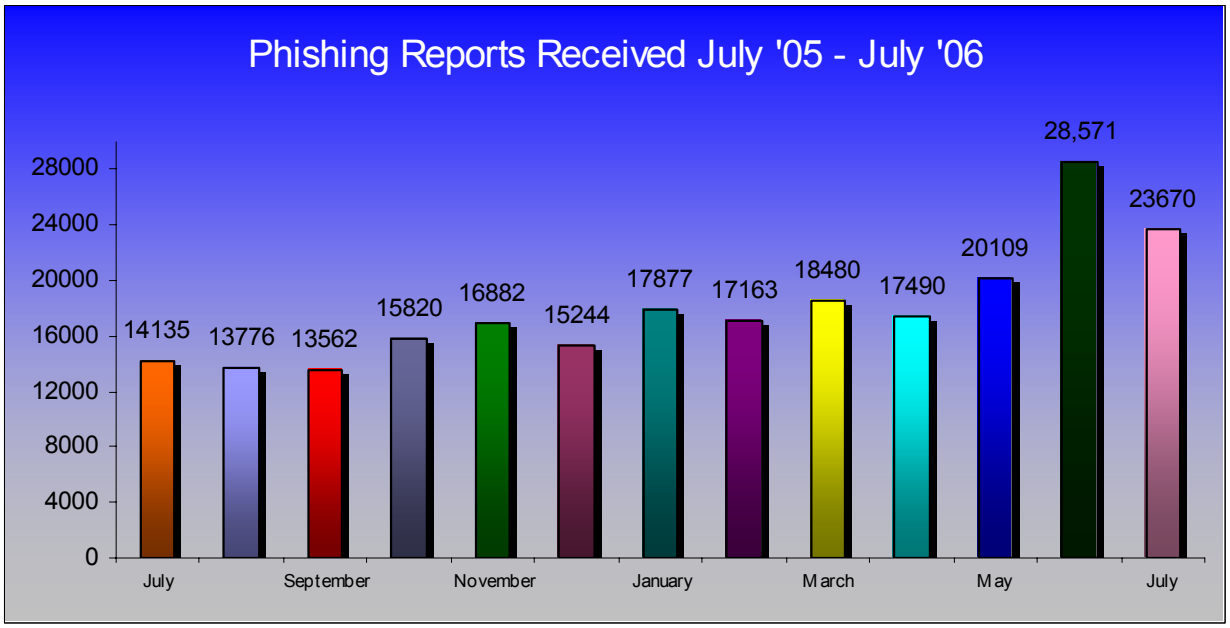
APWG is also tracking crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sties that are distributing crimeware (typically via browser drive-by exploits).

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:

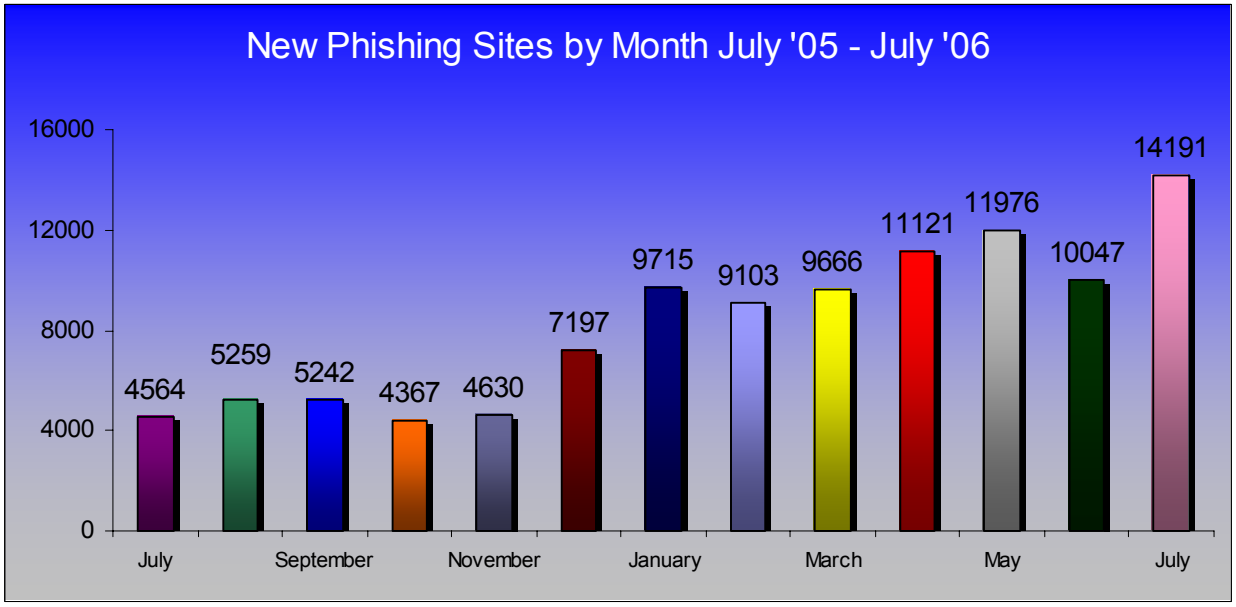
MarkMonitor panda software WEBSENSE.

Phishing Email Reports And Phishing Site Trends

The total number of *unique* phishing reports submitted to **APWG** in July 2006 was **23,670** – a decrease of nearly five thousand attack reports from June and is the second highest number ever recorded by the APWG. This is a count of ***unique*** phishing email reports received by the APWG from the public and its research partners.

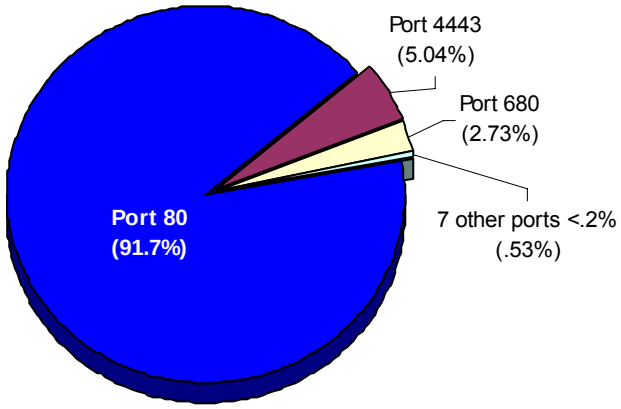


The number of *unique* phishing websites detected by **APWG** was **14,191** in July 2006, an increase in unique phishing sites from June and the highest ever recorded by the APWG.



Top Used Ports Hosting Phishing Data Collection Servers

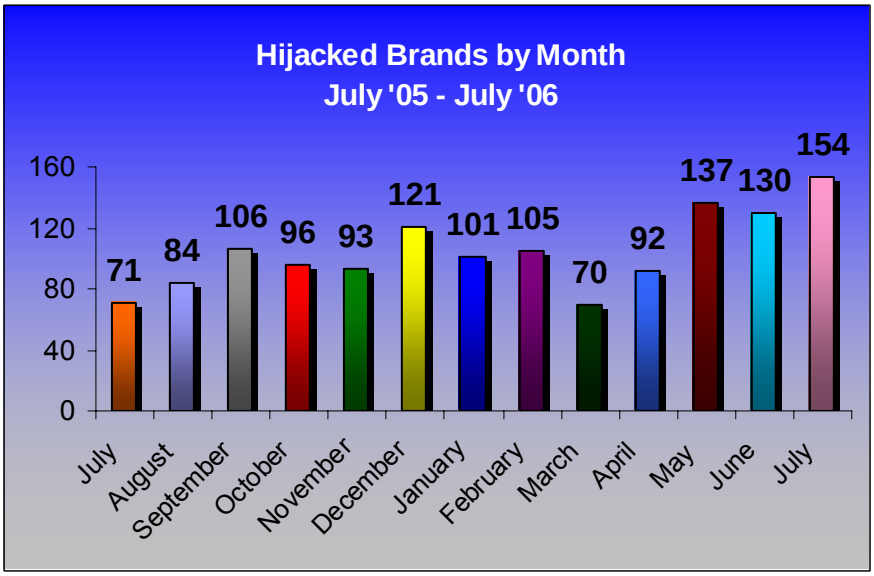
July saw a continuation of a trend of HTTP port 80 being the most popular port used at 91.7% of all phishing sites reported.



Brands and Legitimate Entities Hijacked By Email Phishing Attacks

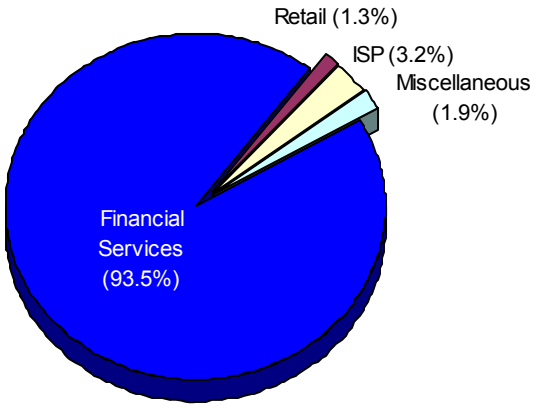
Number of Reported Brands

July 2006 showed the highest number of brands subjected to phishing attacks recorded by the APWG to date.



Most Targeted Industry Sectors

Financial Services continue to be the most targeted industry sector, growing to 93.5% of all attacks in the month of July.



Web Phishing Attack Trends

Countries Hosting Phishing Sites

In July, 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 29.85%. The rest of the top 10 breakdown is as follows – Republic of Korea 13.34%, China 12%, France 5.87%, Australia 4.56%, Germany 3.32%, Japan 3.04%, Canada 1.78%, Thailand 1.59%, and Italy 1.52%.

PROJECT: Crimeware

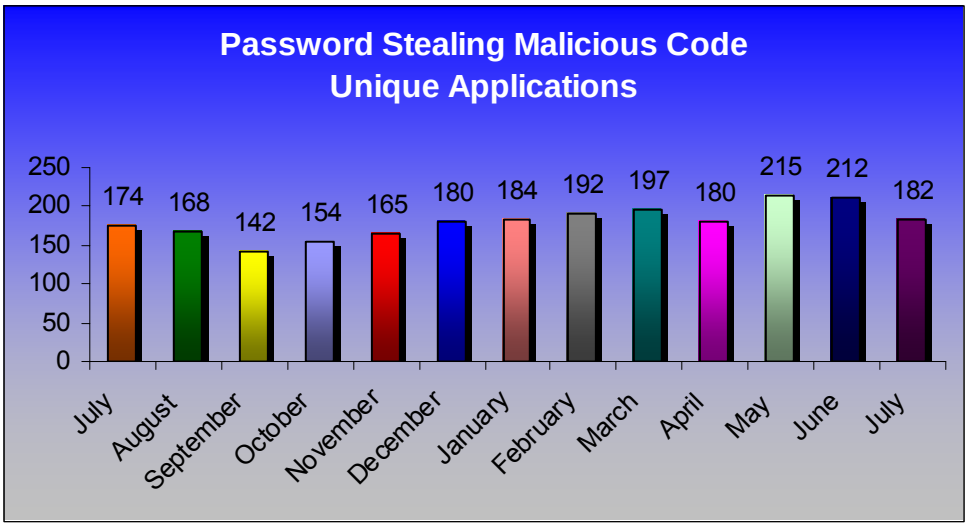
Crimeware Taxonomy & Samples According to Classification in July 2006

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

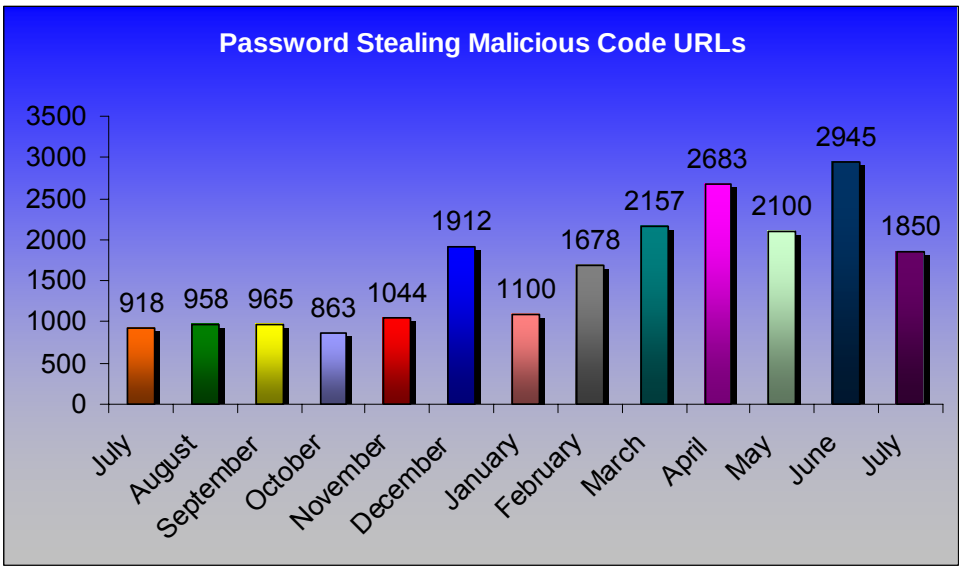
Phishing-based Trojans - Keyloggers

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



Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers



In July, Websense® Security Labs discovered a new malicious website, which distributed malicious code that installs a Trojan Horse on end-users' machines. This potentially occurs without user interaction.

The site appeared to be mirroring a World Cup 2006 Soccer website with the exception that they have a lead story regarding the now infamous, Zinedine Zidane head butt incident from the World Cup final against Italy.

Upon visiting any of the pages on the site, end-users were potentially infected with a Trojan Horse downloader. This Trojan Horse downloads additional payload code from the site. The site was using the underground "Web Attacker" toolkit (discussed in an earlier alert http://www.websense.com/securitylabs/alerts/alert.php?AlertID=472).

The Web Attacker toolkit is sold on a Russian website and costs anywhere from $20 to $300. This toolkit allows users to install code that exploits users based on their browser types. The installed code includes one of five different variants, including exploits for old and new vulnerabilities.

This site was hosted in the United States.

Site screenshot:


FIFA WORLD CUP
GERMANY 2006
BERNAMA WORLD CUP 2006 SPECIAL PAGE
Main
News List
Match Schedule
Results
World Cup 2006 Top Story
What did Materazzi say to Zidane?
PARIS - The Zinedine Zidane mystery is not quite solved yet.
In his first, highly awaited comments since the World Cup final, the French soccer star only partly explained what caused him to react in fury and head-butt an Italian opponent: repeated harsh insults about his mother and sister.
But Zidane didn't go into specifics about what Marco Materazzi said. Materazzi swears he never insulted Zidane's mother. And FIFA is still investigating.
Materazzi 'wished death on Zidane's family'
FIFA World Cup 2006 Champion
Italy
Second Place
France
Third Place
Germany
Fourth Place
Portugal
Teams that did not qualify
Brazil
England
Ukraine
Argentina
Spain
Ghana
Switzerland
Australia
Netherlands
Ecuador
Mexico
Sweden
Poland
Costa Rica
Paraguay
Trinidad & Tobago
Ivory Coast

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.

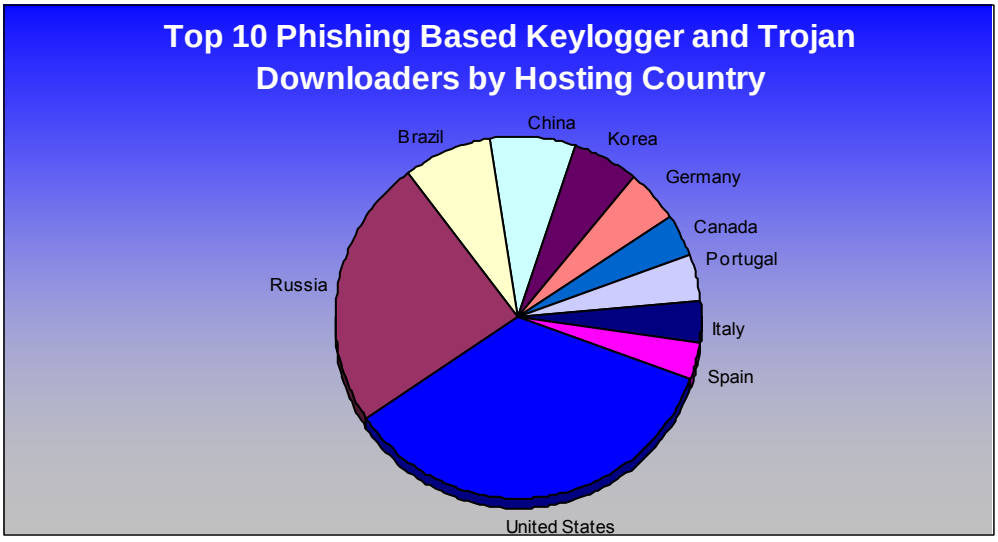
Along with phishing-based keyloggers we are seeing large increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server.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

The chart below represents a breakdown of the websites which were classified during April 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 27.77%.

The rest of the breakdown was as follows; Russia 19.17%, Brazil 6.1%, China 5.98%, Korea 4.6%, Germany 3.74%, Canada 3.24%, Portugal 3.11%, Italy 2.86%, Spain 2.74%.



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 1500 companies and government agencies participating in the APWG and more than 2400 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.