Anti-Phishing Working Group
APWG
www.antiphishing.org

**Anti-Phishing Working Group**

Committed to wiping out Internet scams and fraud

# Phishing Activity Trends

## Report for the Month of July, 2007

## Summarization of July Report Findings

► For the first time recorded by the APWG, China has surpassed the United States as the country hosting the largest percentage of phishing websites with 23.74% of the total detected in a month's sampling period. ► The average time online for phish sites descended to 3.6 days, the shortest time-live duration yet recorded by the APWG. ► The number of unique phishing websites detected by APWG in July was 30,999, a decrease of nearly 1,000 from June. ► July saw a decrease in the number of hijacked brands to 126, a drop of 20 from June. ► The number of unique phishing reports submitted to APWG in July was 23,917, a decrease of nearly 5,000 reports from the previous month. ► Financial Services continue to be the most targeted industry sector at 94.4% of all attacks recorded in the month of July. The APWG notes that more than half of the most targeted brands belong to European financial institutions. ►The APWG continues its brand-domain pairs measurement (page 4) which combines the stats for all monthly statistics based on brands phished, unique domains, unique URLs and the new unique domain/brand pairs metric which counts the unique instances of a domain being used to target a specific brand.

## 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, brandholders, Global Research Partners, the organization's website at http://www.antiphishing.org and emailed submissions 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 July 2007

| | |
|---|---|
| • Number of unique phishing reports received in July: | **23917** |
| • Number of unique phishing sites received in July: | **30999** |
| • Number of brands hijacked by phishing campaigns in July: | **126** |
| • Number of brands comprising the top 80% of phishing campaigns in July: | **13** |
| • Country hosting the most phishing websites in July: | **United States** |
| • Contain some form of target name in URL: | **20.1 %** |
| • No hostname; just IP address: | **13 %** |
| • Percentage of sites not using port 80: | **.6 %** |
| • Average time online for site: | **3.6 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).

## Phishing Email Reports and Phishing Site Trends for July 2007

The total number of *unique* phishing reports submitted to APWG in July 2007 was 23,917, a decrease of nearly 5,000 reports from the previous month. This is a count of *unique* phishing email reports received by the APWG from the public, its members and its research partners.

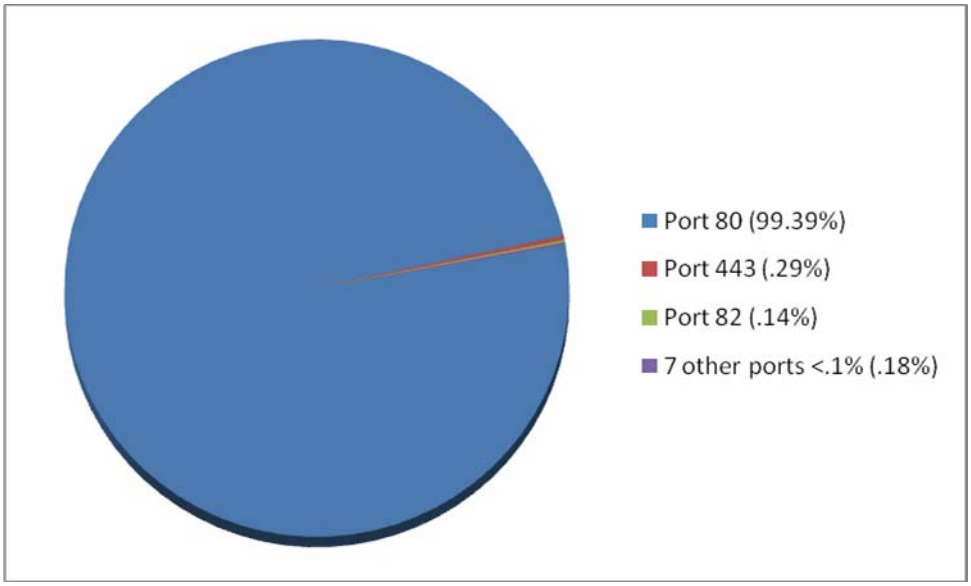

The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry and law enforcement association focused on eliminating the identity theft and fraud that result from the growing problem of phishing, crimeware and email spoofing. For further information, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282. Data and analyses 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 **30,999** in July 2007, a decrease of less than 1,000 from the month of June.


## Top Used Ports Hosting Phishing Data Collection Servers in July 2007

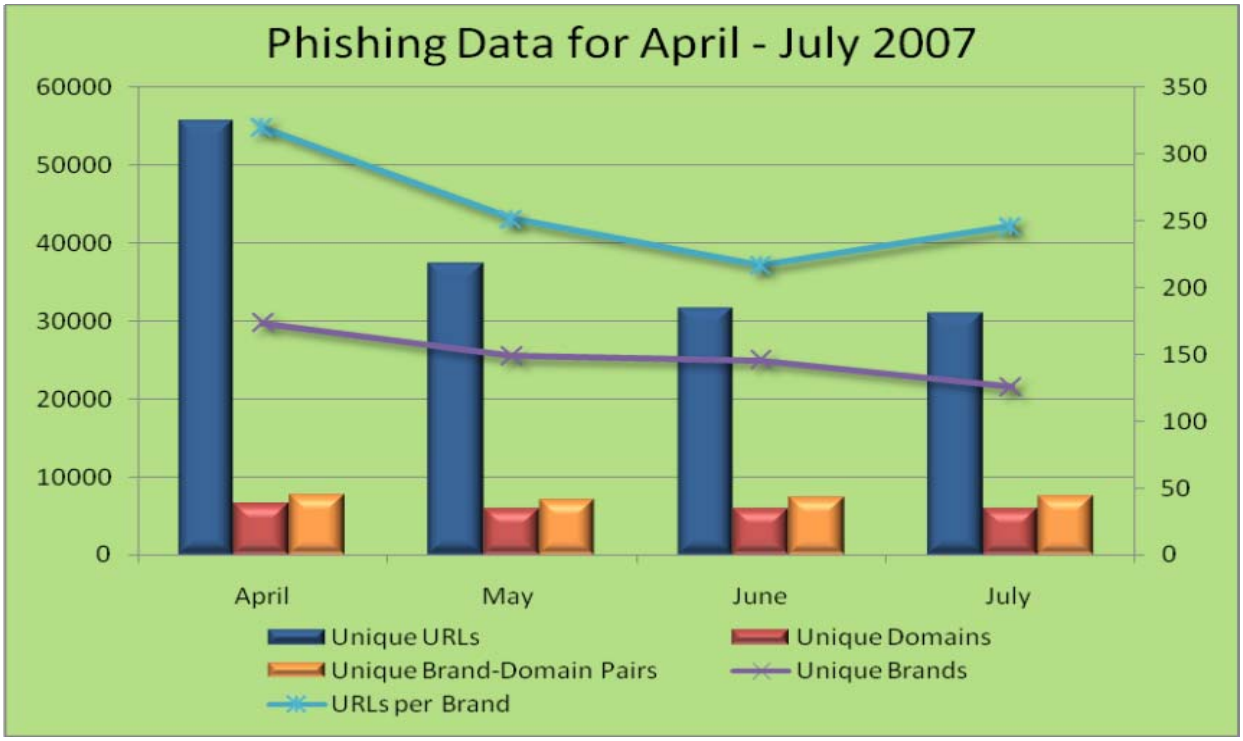
July saw a continuation of HTTP port 80 being the most popular port used at 99.39% of all phishing sites reported.



## April - July 2007 Brand-Domain Pairs Measurement

The following chart combines statistics for the last four months based on brands phished, unique domains, unique domain/brand pairs and unique URLs. Brand/domain pairs count the unique instances of a domain being used to target a specific brand. *Example*: if several URLs targeting a brand - but are hosted on the same domain - this brand/domain pair would be counted as one instead of several. *Forensic utility*: If the number of unique URLs is greater than the number of brand/domain pairs, it indicates many URLs are being hosted on the same domain to target the same brand. Knowing how many URLs occur with each domain indicates the approximate number of attacking domains a brandholding victim needs to locate and neutralize. Since Phishing-prevention technologies (like browser and email blocking) require the full URL, it is useful to understand the general number of unique URLs that occur per domain.

"As we continue to see the phishers use more technical rock phish-like tactics, it is becoming increasingly important for registrars and registries to take action against them," said Laura Mather, PhD, Senior Scientist at MarkMonitor. "The difference between an ISP shutting down a phish site and a registrar or registry suspending the phishing domain is substantial. When an ISP shuts down the phish site, the phisher can use another ISP to host their domain. When a registrar or registry suspends a domain, the phisher must start over with a new domain. Action by the registrar or registry is the one way to guarantee that the phish site is truly eradicated from the internet."

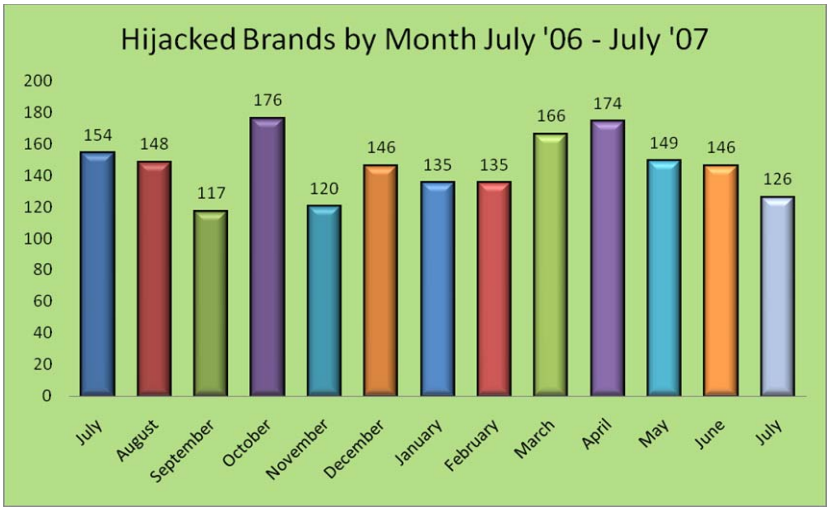



| | April | May | June | July |
|---|---|---|---|---|
| Unique URLs | 55643 | 37438 | 31709 | 30999 |
| Unique Domains | 6637 | 5967 | 6006 | 6005 |
| Unique Brand-Domain Pairs | 7622 | 7092 | 7359 | 7538 |
| Unique Brands | 174 | 149 | 146 | 126 |
| URLs per Brand | 319.79 | 251.26 | 217.18 | 246.02 |

## Brands & Legitimate Entities Hijacked By Email Phishing Attacks in July 2007

### Number of Reported Brands

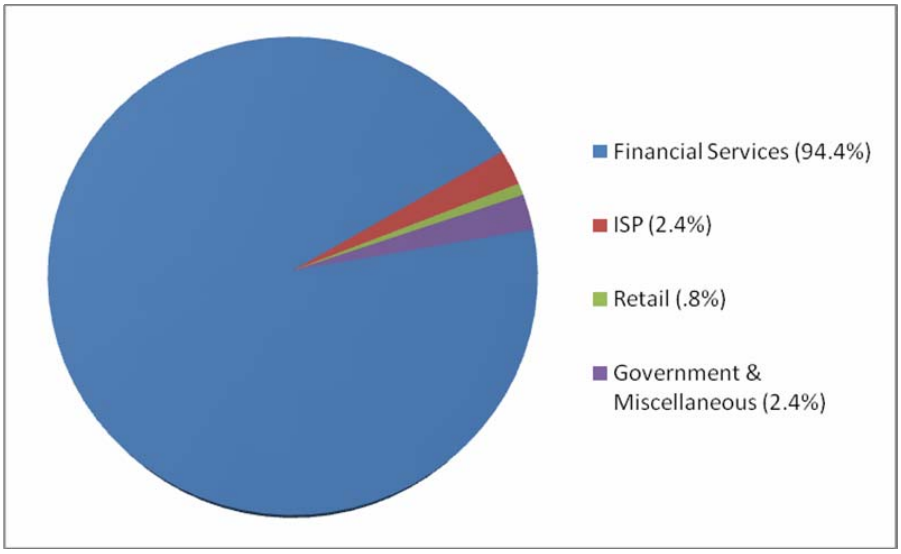
July 2007 saw a decrease in hijacked brands to 126.




## Most Targeted Industry Sectors in July 2007

Financial Services continue to be the most targeted industry sector at 94.4% of all attacks in the month of July.

"In July 2007, there was lot of focus on the top banking targets. About half of the major targets are European financial institutions," said Dave Jevans, Chairman, APWG. "We continue to see the IRS and UK tax authorities being used as phishing lures. There appears to be an increase in reports of international phishing in Europe and Japan. There are continued low-level attacks against a great many US credit unions and smaller banks."



# Web Phishing Attack Trends in July 2007

## Countries Hosting Phishing Sites

In July, Websense Security Labs saw China over take the United States as the top of the list for countries hosting phishing websites with 23.74%. This is first time that China has surpassed the United States as the top country hosting phishing websites. The rest of the top 10 breakdown is as follows: United States 22.93%, Japan 6.24%, Thailand 4.44%, Venezuela 4.37%, Brazil 3.74%, Russia 3.42%, France 3.25%, United Kingdom 2.68% and Germany with 2.38%.


# PROJECT: Crimeware

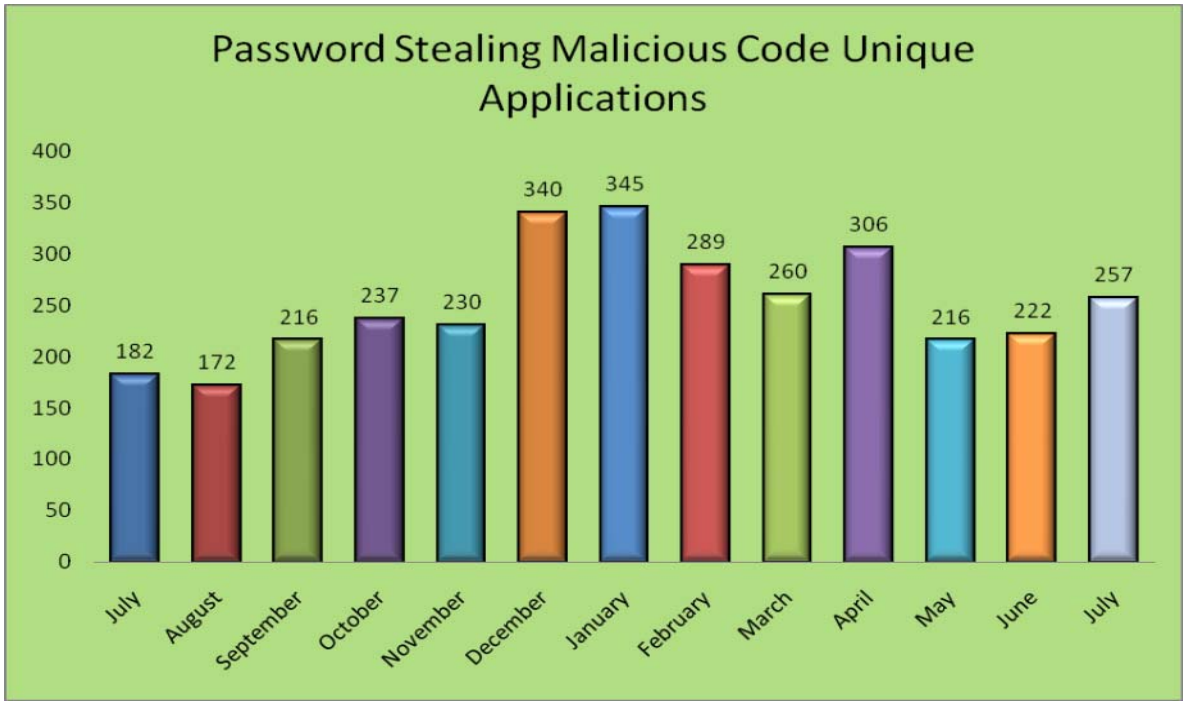
## Crimeware Taxonomy & Samples According to Classification in July 2007

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

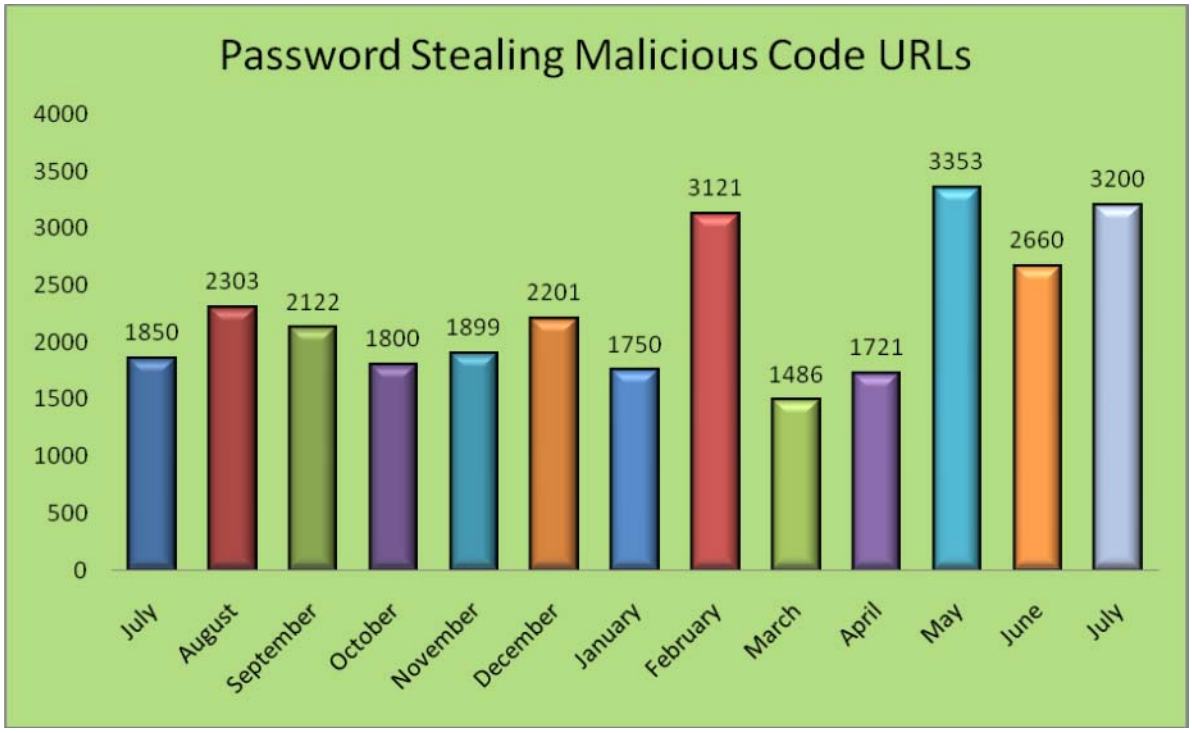
### *Phishing-based Trojans - Keyloggers*

**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 July***




***Phishing-based Trojans – Keyloggers, Unique Websites Hosting Keyloggers in July***



## *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.

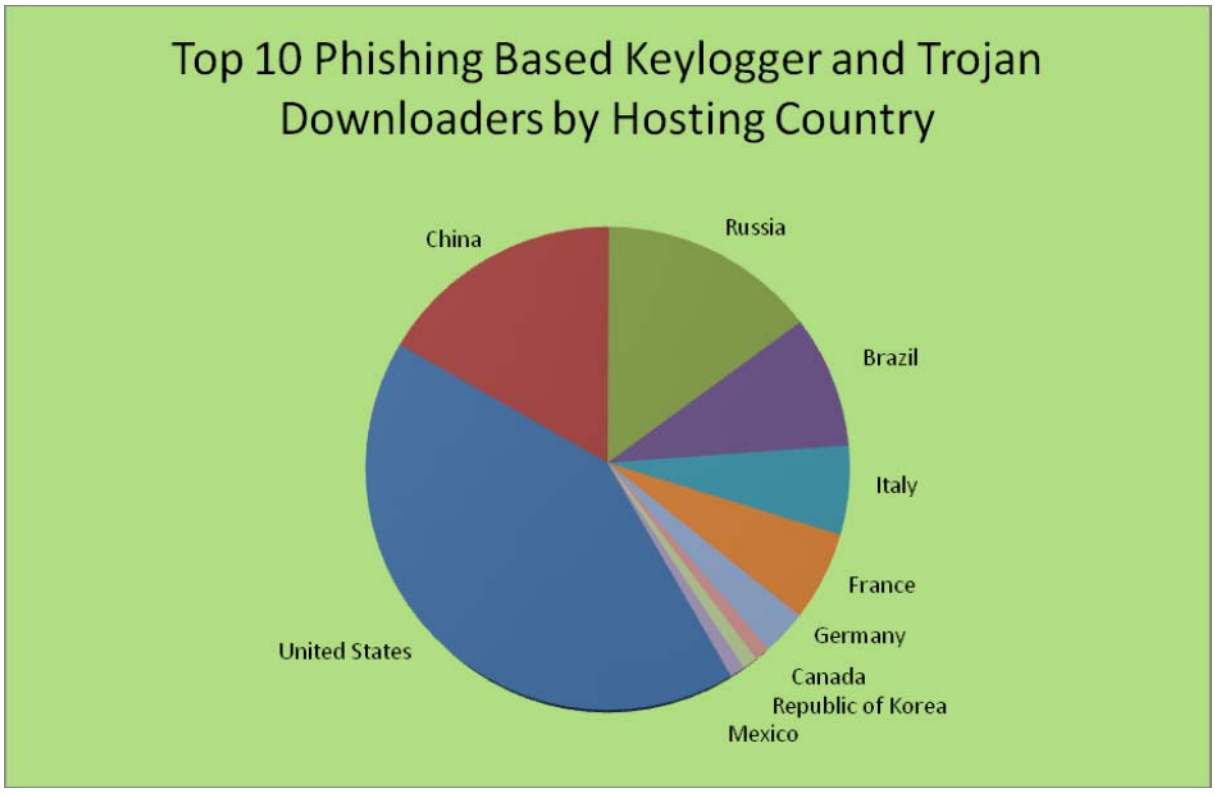
Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server.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

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

The United States continues to be the top crimeware hosting country with 42% of the total crimeware-spreading websites detected during the month of July.

The rest of the breakdown in July was as follows; China 17%, Russia 15%, Brazil 9%, Italy 6%, France 6%, Germany 3%, Canada 1%, Korea 1% and Mexico with 1%.



# 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 Peter Cassidy, APWG Secretary General at 617.669.1123 or pcassidy@antiphishing.org; Cas Purdy at 858.320.9493 or cpurdy@websense.com; and Te Smith at 831.818.1267 or Te.Smith@markmonitor.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 consequences, 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 1700 companies and government agencies participating in the APWG and more than 2900 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 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 of directors and its executives.