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 June, 2007

## Summarization of June Report Findings

► In the June 2007 report the APWG introduces a brand-domain pairs measurement (page 4) which combines the stats for all of Q2 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. ► The number of unique phishing websites detected by APWG was June was 31,709 in June 2007, a drop of nearly 6,000 from May. ► June saw a decrease in the number of hijacked brands to 146, a slight drop from May. The APWG also noted during this reporting period increasing numbers of online brokerages being phished, a cohort that includes both equities trading websites and full-service mutual fund companies. ► The number of unique phishing reports submitted to APWG in June was 28,888, an increase of over 5,000 reports from May. ► Financial Services continue to be the most targeted industry sector at 95.2% of all attacks in the month of June. The APWG notes that more government agencies, such as US and UK tax authorities, are being phished along with more social networking websites.

## 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 June 2007

| | |
|---|---|
| • Number of unique phishing reports received in June: | **28888** |
| • Number of unique phishing sites received in June: | **31709** |
| • Number of brands hijacked by phishing campaigns in June: | **146** |
| • Number of brands comprising the top 80% of phishing campaigns in June: | **14** |
| • Country hosting the most phishing websites in June: | **United States** |
| • Contain some form of target name in URL: | **16.1 %** |
| • No hostname; just IP address: | **6 %** |
| • Percentage of sites not using port 80: | **1 %** |
| • Average time online for site: | **3.8 days** |
| • Longest time online for site: | **30 days** |

## Methodology

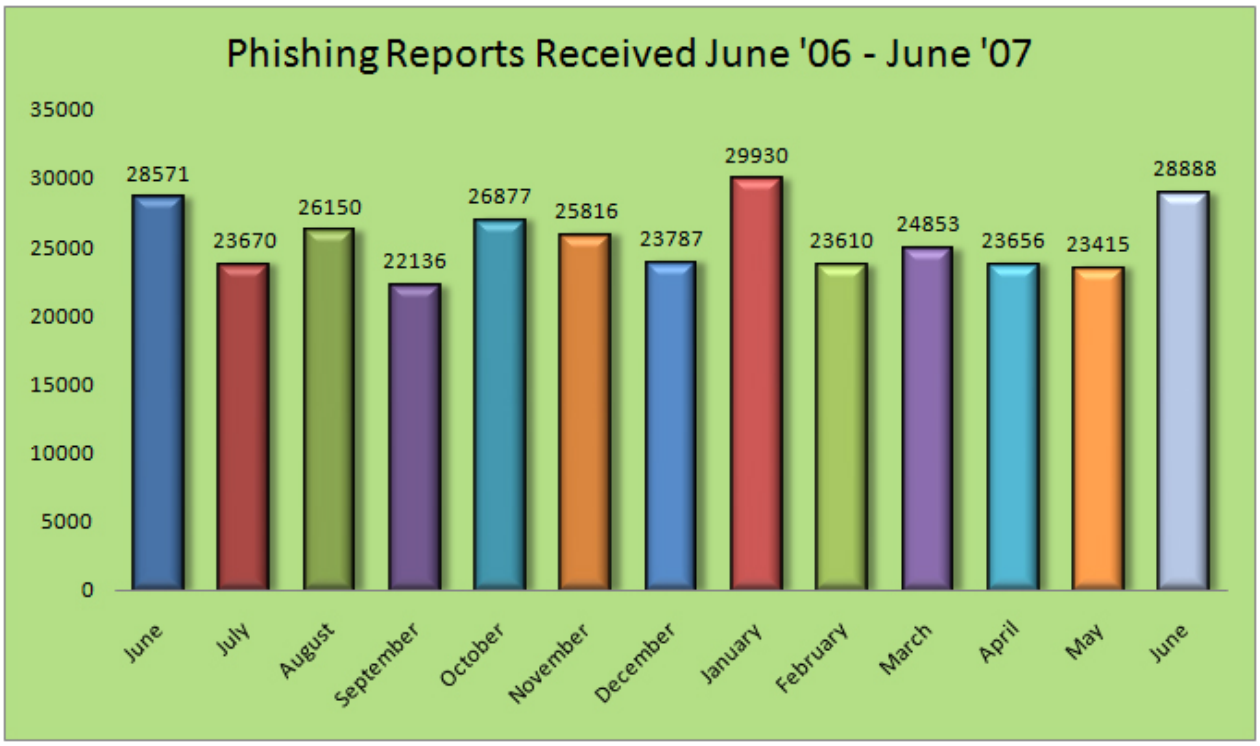
**APWG** is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them 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 June 2007

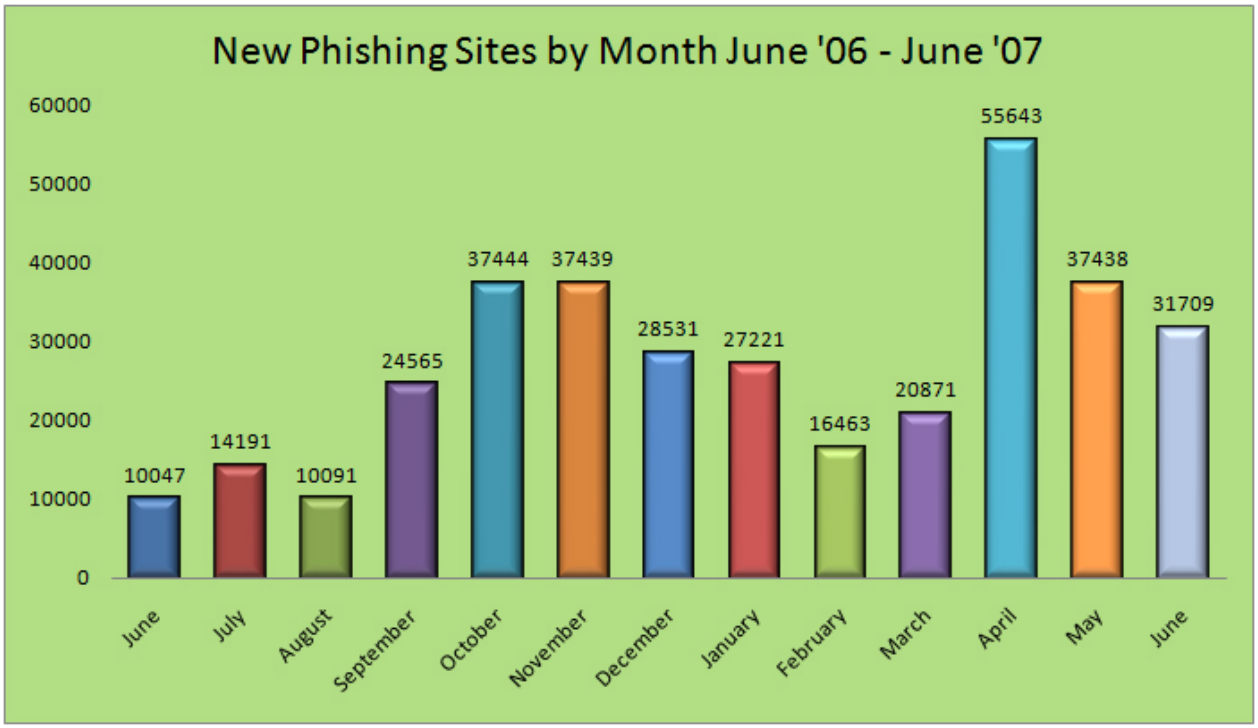
The total number of *unique* phishing reports submitted to **APWG** in June 2007 was **28,888**, an increase of over 5,000 reports from the previous month. This is a count of ***unique*** phishing email reports received by the APWG from the public, its members and its research partners.




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:

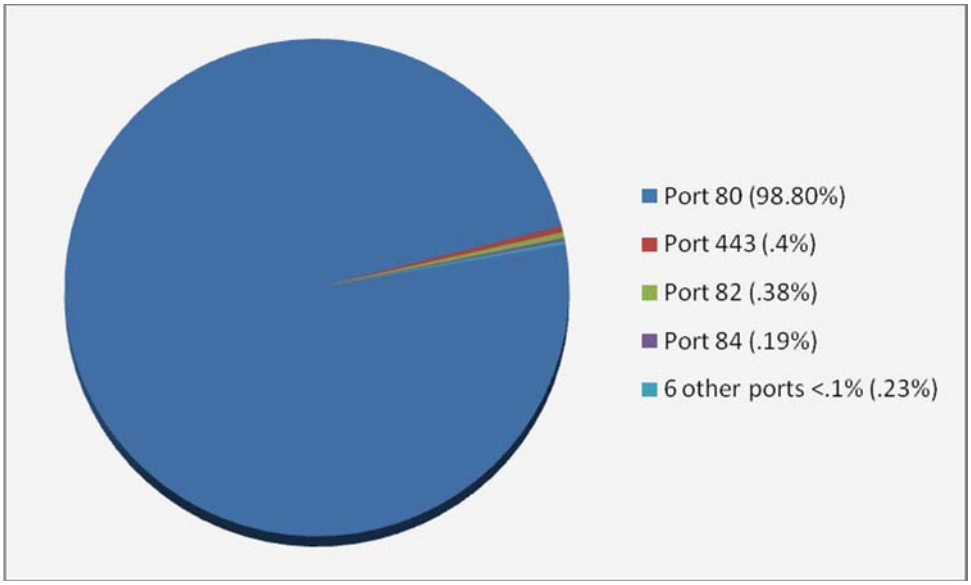
MarkMonitor panda software WEBSENSE.

The number of *unique* phishing websites detected by **APWG** was **31,709** in June 2007, a decrease of nearly 6,000 from the month of May




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

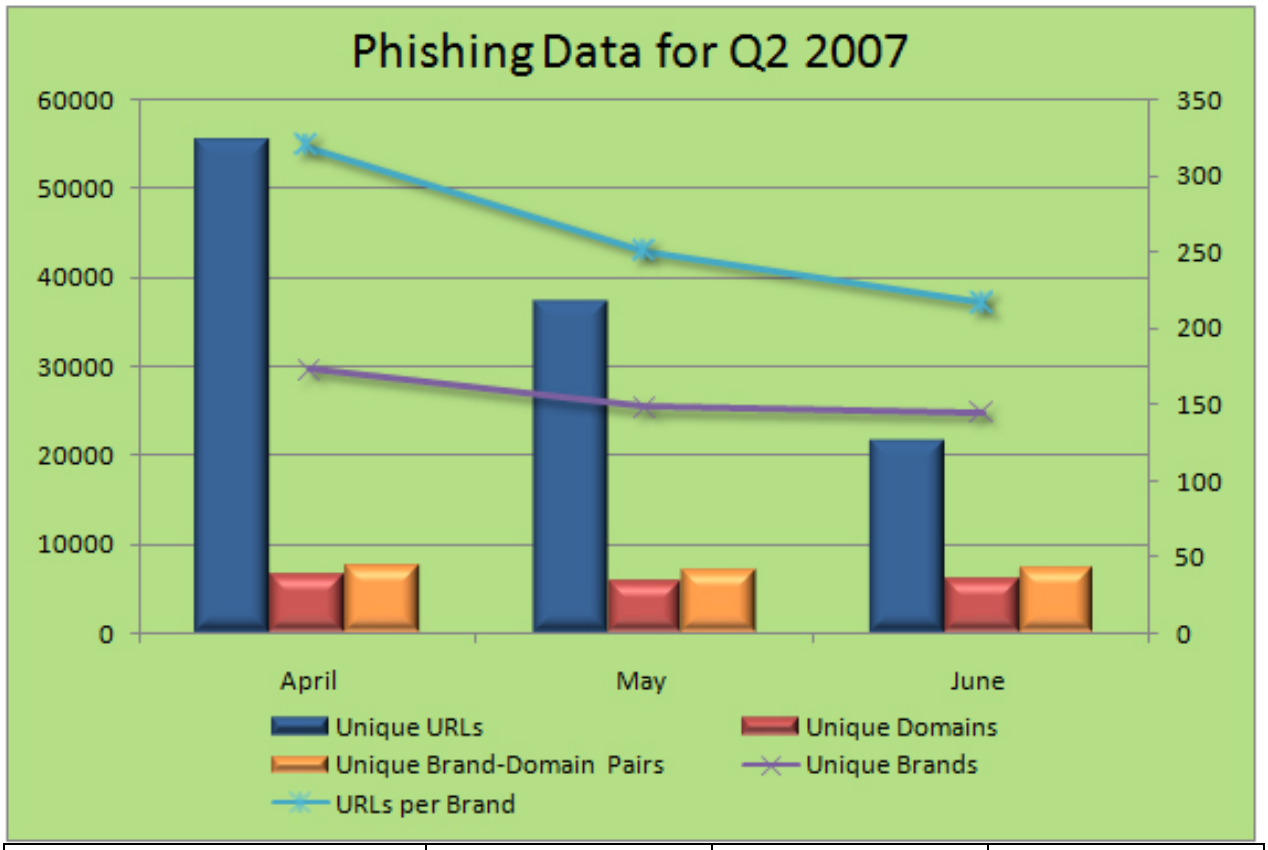
June saw a continuation of HTTP port 80 being the most popular port used at 98.80% of all phishing sites reported.



## 2nd Quarter 2007 Brand-Domain Pairs Measurement

The following chart combines statistics for all of Q2 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.

"In June, we saw a 15% decrease in the number of unique URLs hosting phishing sites. Because it is important to report on the full aspect of the phishing phenomenon, we are now including three additional metrics in our reports: the number of brands phished, the number of domains used in the unique phishing URLs, and the number of brand-domain pairs," said Laura Mather, Ph.D., senior scientist at MarkMonitor and APWG Managing Director of Operational Policy. "Comparing June's data with May's shows that there were both fewer brands phished in June and fewer URLs used for phishing. Since April we have seen a continued decrease in the average number of URLs used to target each brand. The number of URLs per brand is still high compared to this time last year, though, indicating that technologies like browser blocking and blocking phishing emails at the inbox continue to be successful."



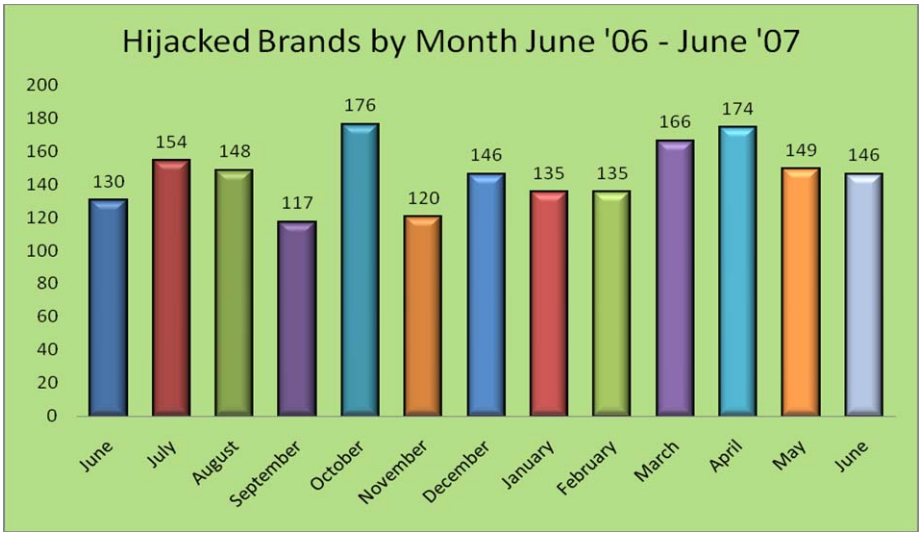

| | April | May | June |
|---|---|---|---|
| Unique URLs | 55643 | 37438 | 21709 |
| Unique Domains | 6637 | 5967 | 6006 |
| Unique Brand-Domain Pairs | 7622 | 7092 | 7359 |
| Unique Brands | 174 | 149 | 146 |
| URLs per Brand | 319.79 | 251.26 | 217.18 |

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

### Number of Reported Brands

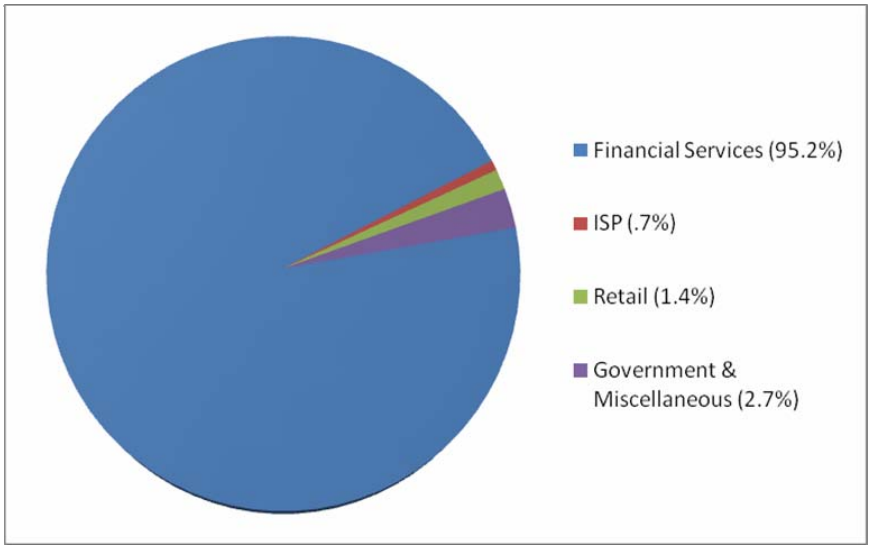
June 2007 saw a drop in hijacked brands to 146.

The APWG notes that there is a continuing trend for banks and credit unions to be targets and that they are seeing more brokerages being phished.




## Most Targeted Industry Sectors in June 2007

Financial Services continue to be the most targeted industry sector at 95.2% of all attacks in the month of June. APWG notes that more US and UK tax authorities are being phished along with more social networking websites.



## Web Phishing Attack Trends in June 2007

### Countries Hosting Phishing Sites

In June, Websense® Security Labs™ saw the United States remain on the top of the list for countries hosting phishing websites with 31.95%. The rest of the top 10 breakdown is as follows: Republic of Korea 10%, Poland 6.88%, Russia 6.55%, Bangladesh 4.03%, India 2.84%, Japan 2.58%, Germany 2.56%, France 2.057%, Romania 1.75%.


## PROJECT: Crimeware

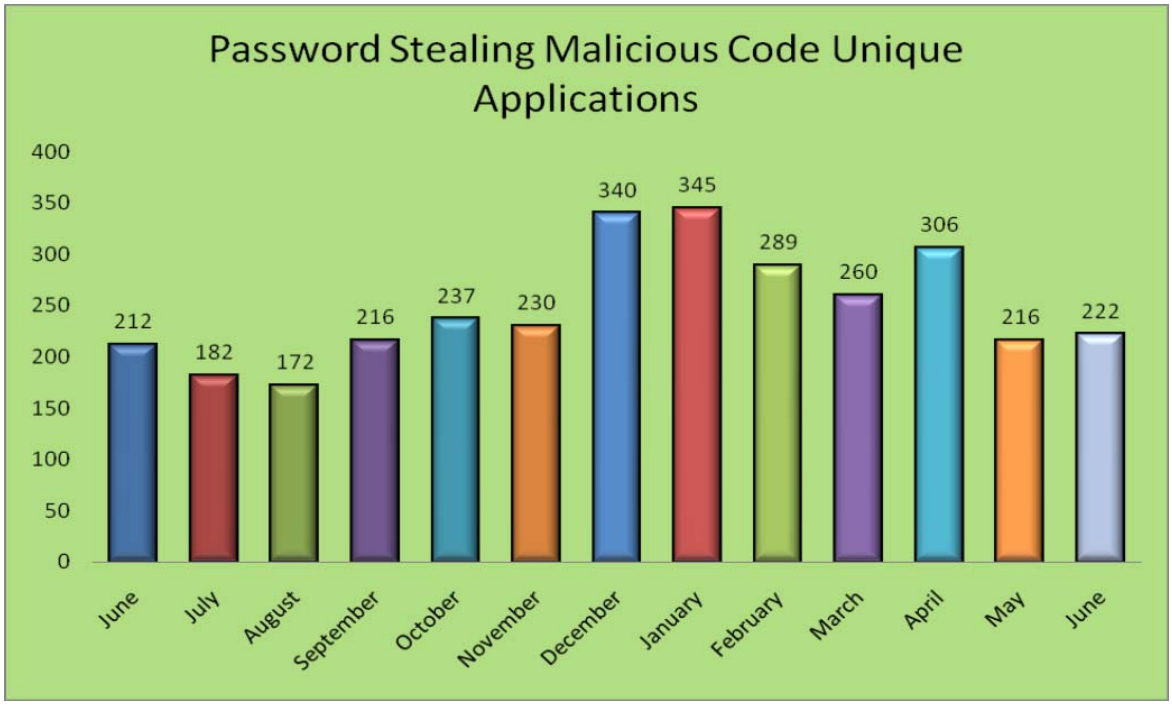
### Crimeware Taxonomy & Samples According to Classification in June 2007

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

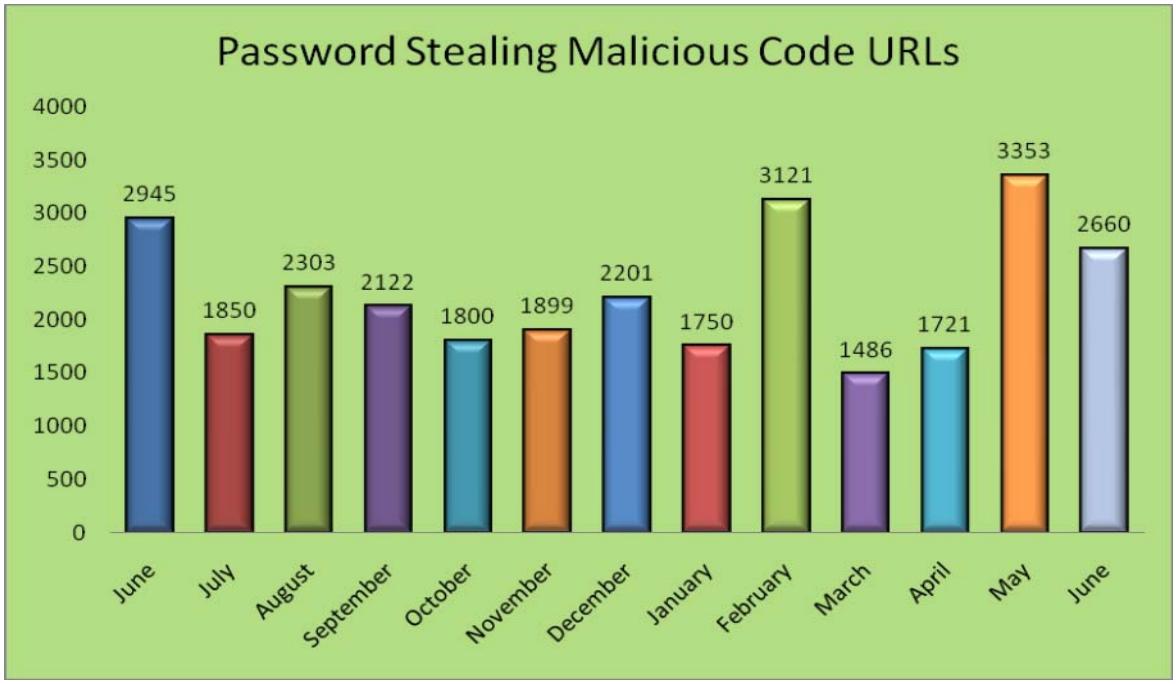
### *Phishing-based Trojans - Keyloggers*

**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 June***




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



## *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.

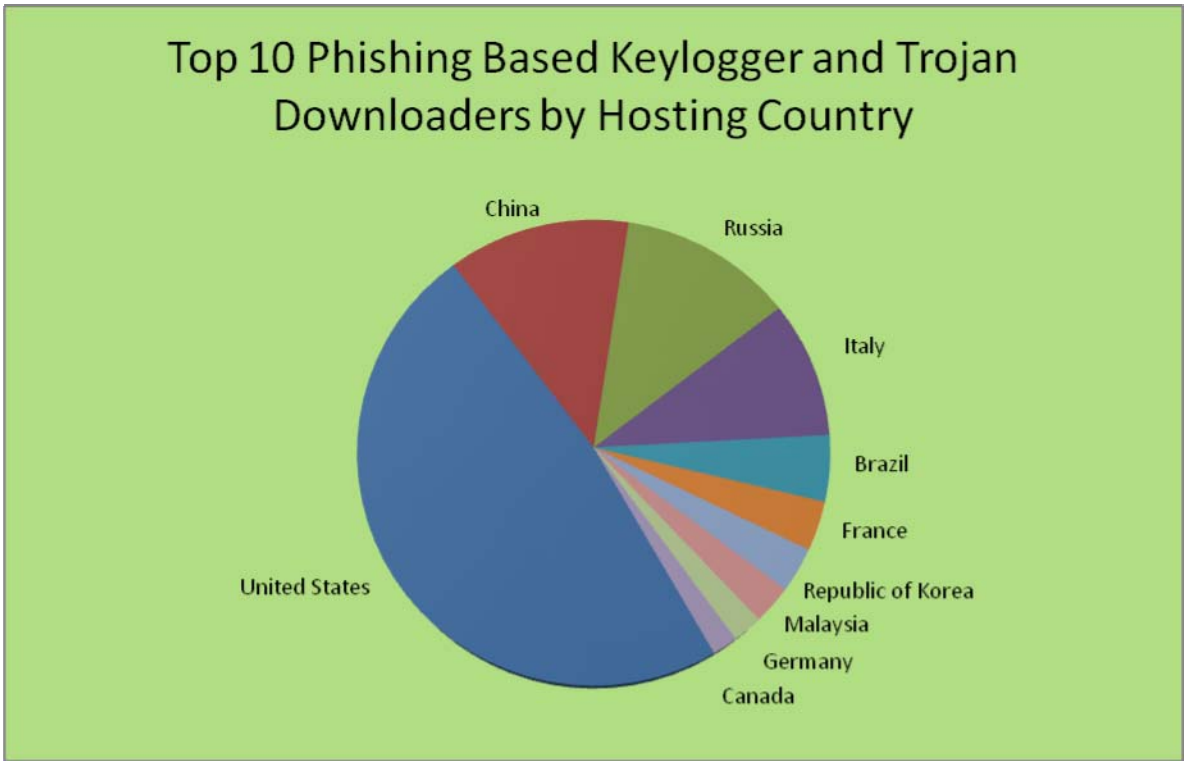
Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server.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

The chart below represents a breakdown of the websites which were classified during June 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 hosting country with 48.02%.

The rest of the breakdown was as follows; China 12.73%, Russia 12.19%, Italy 9.52%, Brazil 4.6%, France 3.42%, Republic of Korea 3.1%, Malaysia 2.67%, Germany 2.03%, Canada 1.71%.



# 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.