Anti-Phishing Working Group
APWG

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

Phishing Activity Trends

Report for the Month of April, 2007

Summarization of April Report Findings

_ The number of unique phishing websites detected by APWG rose to 55,643 in April 2007, a massive jump of nearly 35,000 from March resulting from aggressive sub-domain phishing tactics by which phishers started using the tactic of putting a large numbers of phish URLs on the same domain. _ Similar to tactics employed by phishing gangs in late 2006, APWG researchers encountered phishers placing thousands of phishing URLs under the same domain. _ April 2007 saw a the number of brands being attacked rise 174 and notes that more non-financial brands attacked including social networking, VOIP, and numerous large web-based email providers were attacked. _ Unique phishing reports submitted to APWG in April was 23,656, a drop of over 1,000 from March. _ Financial Services continue to be the most targeted industry sector at 92.5% and the APWG notes that several large US banks are among the most-attacked brands. Furthermore, two top banks have been targeted for at least two months in a row. _ A large number of European banks were targeted in April with seven of the most-targeted 20 brands in that month belonging to European banks. In addition, one of the top 20 was a Canadian financial institution.

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 April 2007

• Number of unique phishing reports received in April:	**23656**
• Number of unique phishing sites received in April:	**55643**
• Number of brands hijacked by phishing campaigns in April:	**172**
• Number of brands comprising the top 80% of phishing campaigns in April:	**11**
• Country hosting the most phishing websites in April:	**United States**
• Contain some form of target name in URL:	**13.5 %**
• No hostname just IP address:	**6 %**
• Percentage of sites not using port 80:	**1.5 %**
• Average time online for site:	**3.8 days**
• Longest time online for site:	**27 days**

Methodology

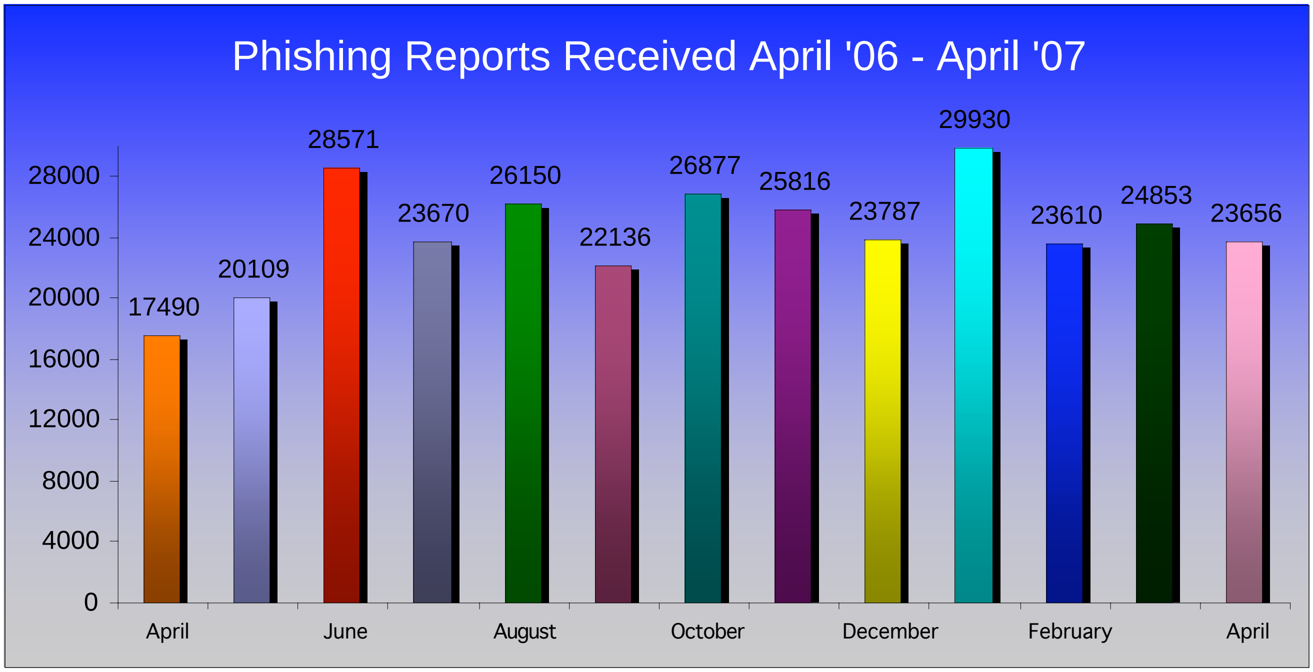
APWG is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to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

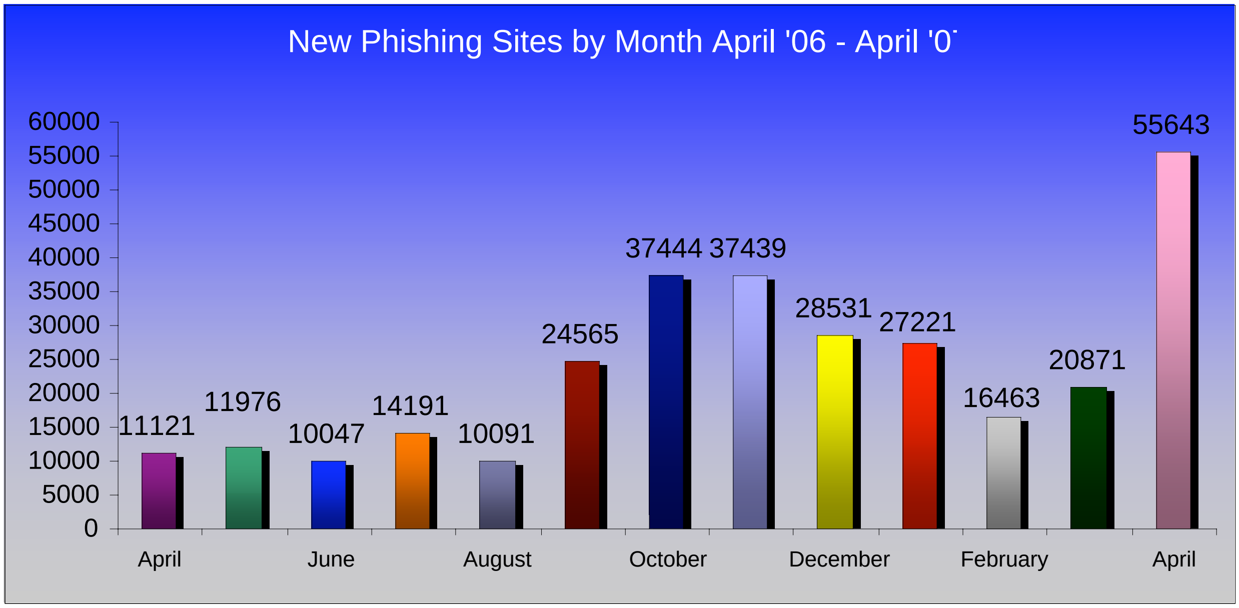
The total number of *unique* phishing reports submitted to **APWG** in April 2007 was **23,656**, a drop of over 1,000 from the previous month. This is a count of ***unique*** phishing email reports received by the APWG from the public, its members and its research partners.



The **Phishing Attack Trends Report** is published monthly by the Anti-Phishing Working Group, an industry 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 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.

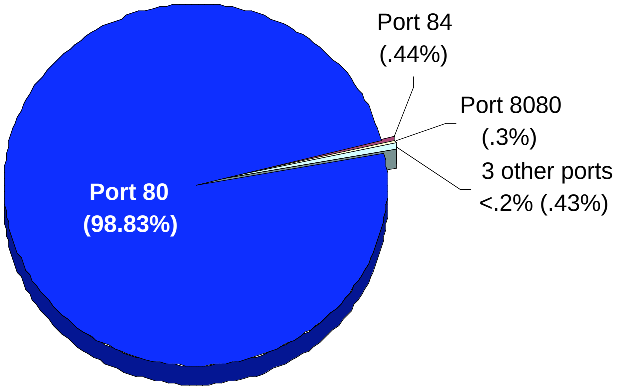
The number of *unique* phishing websites detected by **APWG** was 55,643 in April 2007, a massive increase of nearly 35,000 from March, the result of from aggressive tactics used to establish multiple URLs on a common domain. Laura Mather, Ph.D., Senior Scientist at MarkMonitor said, "In April the phishers started using the tactic of putting a large numbers of phish URLs on the same domain, similar to what they were doing in late 2006. We have seen cases where the phisher will put thousands of URLs on the same domain. They do this to get around website blocking that Internet Explorer 7.0 and Firefox 2 have deployed to protect consumers from phish sites."



Typically, URL multiplying techniques involve apparently automated creation of subdomains (xxxx.fakedomain.com) to establish discrete hosts for phishing sites or the use of different directories on the same domain (www.fakedomain.com/xxxx). APWG researchers have watched these tactics increase in frequency since last fall and, after a lull this spring, phishers have returned to these techniques with redoubled effort. Phish sites rose 166% in April from the previous month and 48% from the previous high for phishing URLs in October, 2006.

Top Used Ports Hosting Phishing Data Collection Servers in April 2007

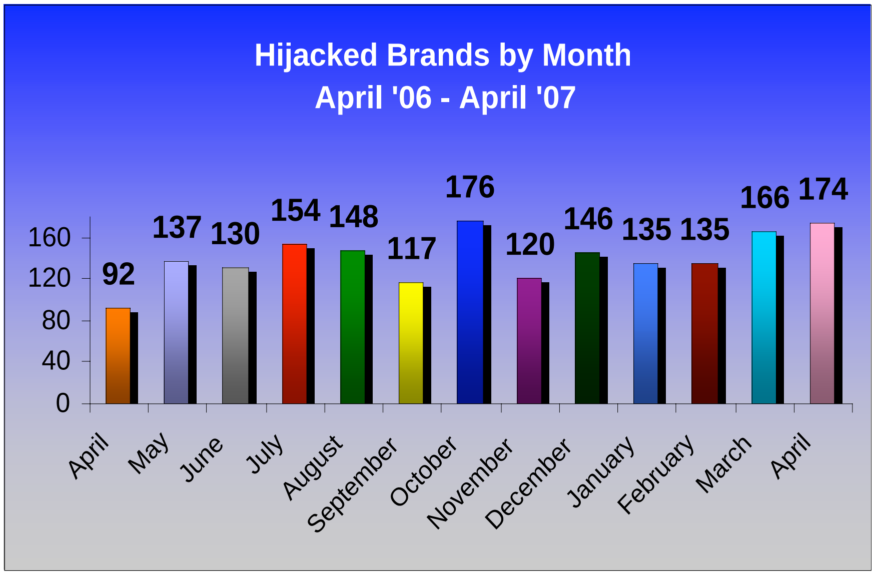
April saw a continuation of HTTP port 80 being the most popular port used at 98.83% of all phishing sites reported.



Brands & Legitimate Entities Hijacked By Email Phishing Attacks in April 2007

Number of Reported Brands

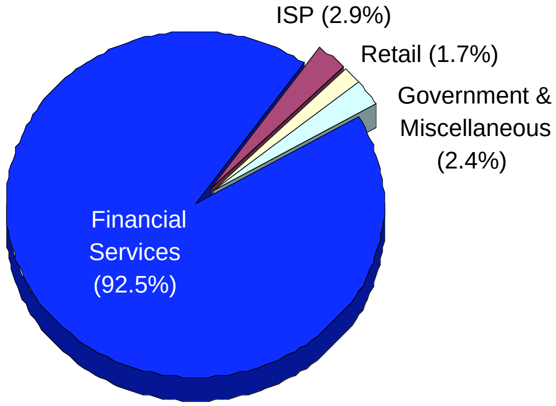
April 2007 saw a continuing increase in hijacked brands that started in February, rising to 174. APWG notes that in April, more non-financial brands were attacked including social networking, VOIP, and numerous large web-based email providers.



Most Targeted Industry Sectors in April 2007

Financial Services continue to be the most targeted industry sector at 92.5% of all attacks in the month of April. APWG notes that several fairly large US banks are the top brands attacked, and these two top banks have been targeted in two consecutive months.

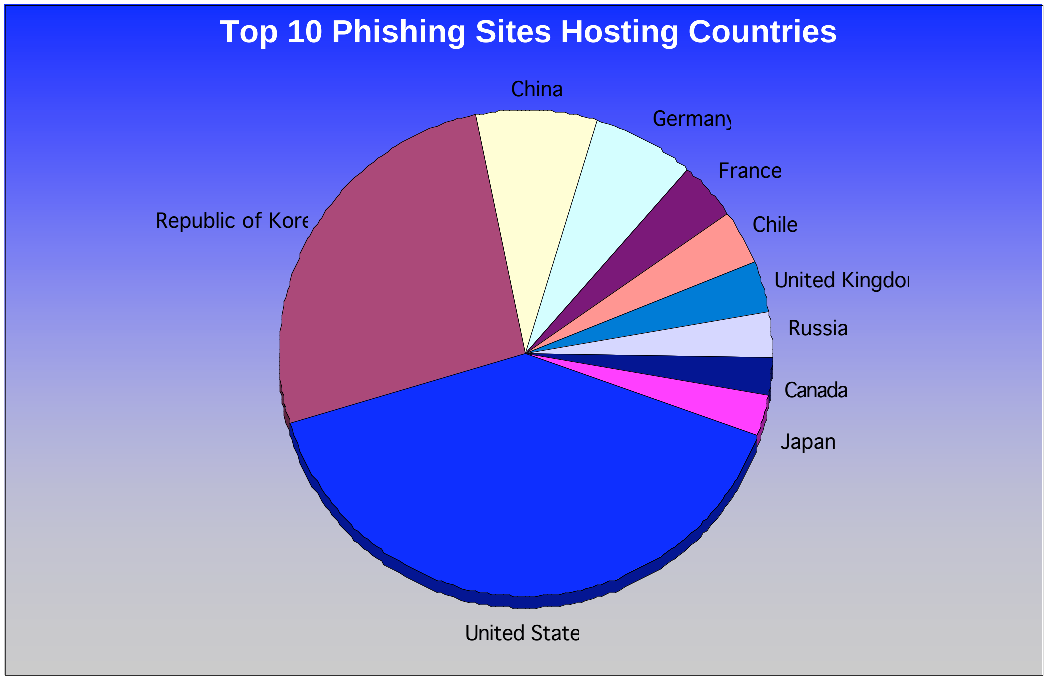
In addition, a large amount of European banks were being targeted and are seven of the top 20 brands attacked in April. In addition, one of the top 20 brands was a Canadian financial institution.



Web Phishing Attack Trends in April 2007

Countries Hosting Phishing Sites

In April, Websense® Security Labs™ saw the United States remain on the top of the list for countries hosting phishing websites with 28.44%. The rest of the top 10 breakdown is as follows: France 26.9%, Republic of Korea 21.05%, Romania 2.04%, China 1.9%, Germany 1.9%, Russia 1.75%, United Kingdom 1.46%, Turkey 1.46%, Netherlands 1.17%.



PROJECT: Crimeware

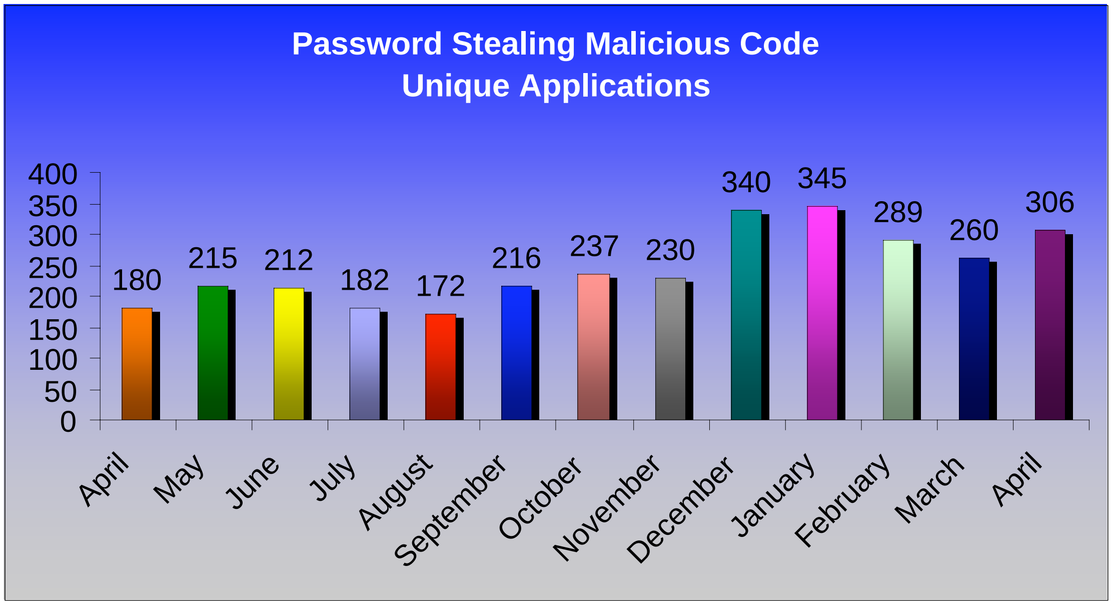
Crimeware Taxonomy & Samples According to Classification in April 2007

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

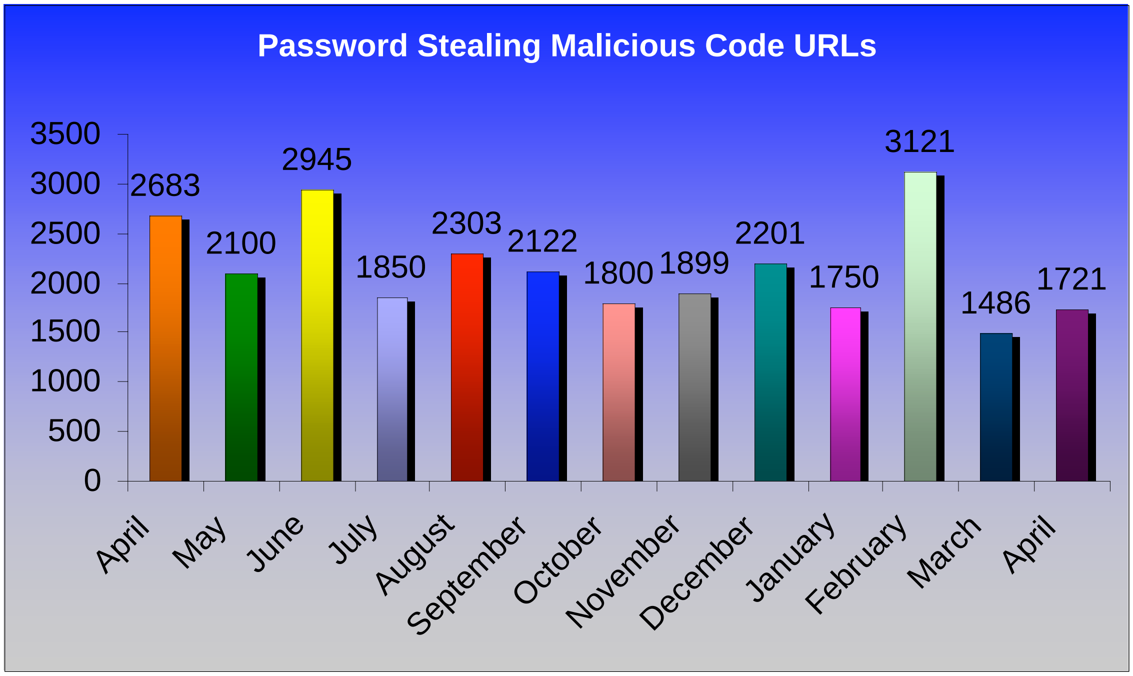
Phishing-based Trojans - Keyloggers

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 April



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



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.

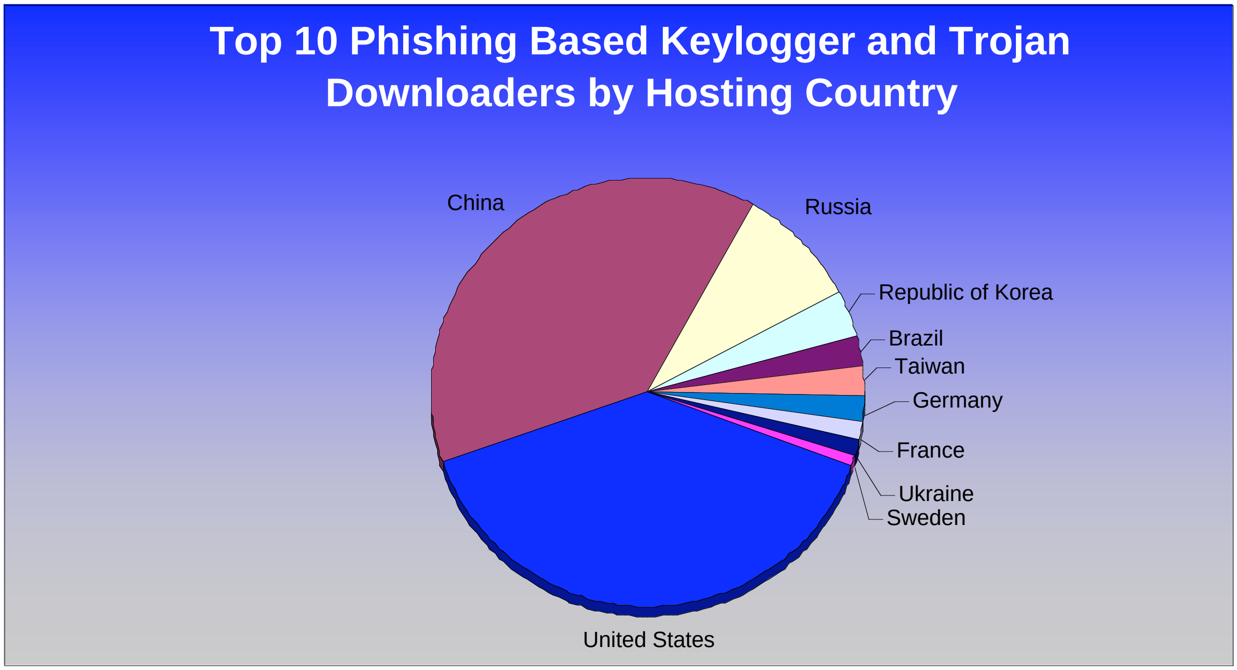
Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server.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

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 continues to be the top hosting country with 38.57%.

The rest of the breakdown was as follows; China 37.64%, Russia 8.87%, Republic of Korea 3.57%, Brazil 2.33% Taiwan 2.02%, Germany 1.87%, France 1.55%, Ukraine 0.93%, Sweden 0.93%.



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 and Cas Purdy at 858.320.9493 or cpurdy@websense.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 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.