APWG

Committed to wiping out Internet scams and fraud

Phishing Activity Trends

Report for the Month of December, 2007

Summarization of December Report Findings

► The total number of unique phishing reports submitted to APWG in December 2007 was 25,683, a decrease of more than 2,300 reports from the previous month. ► The number of brands targeted by phishers in December dropped to 144, down from a record high in November of 178. ► In the month of December, the number of websites that were hosting keyloggers dropped by 1250, reducing the number to 2260. ► The number of unique phishing websites detected by the APWG rose to 25,328 in December 2007, an increase of nearly 1,700 from the month of November. ► APWG reports of Government and Misc. brands under attack rose to 5.5% with a number of tax agencies in Anglophone democracies being spoofed worldwide, the highest proportion for that segment since Oct. 2005. ► The APWG notes an increase in phishing campaigns spoofing the US Internal Revenue Service (IRS) and phishing campaigns co-opting the brands of tax authorities in the UK and Australia. Additionally, APWG notes increased numbers of phishing campaigns against non-traditional sites such as automotive associations. ► In December, the United States moved back to the top spot for countries hosting phishing sites with 32.5%, after being eclipsed by China in November. ►In contrast, in December China surpassed the United States as the top hosting country for password-stealing malicious code with 46.62%.

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 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 December 2007

- Number of unique phishing reports received in December: **25683**
- Number of unique phishing sites received in December: **25328**
- Number of brands hijacked by phishing campaigns in December: **144**
- Number of brands comprising the top 80% of phishing campaigns in December: **16**
- Country hosting the most phishing websites in December: **United States**
- Contain some form of target name in URL: **42.1 %**
- No hostname; just IP address: **12 %**
- Percentage of sites not using port 80: **.49 %**
- Average time online for site: **3 days**
- Longest time online for site: **31 days**

Methodology

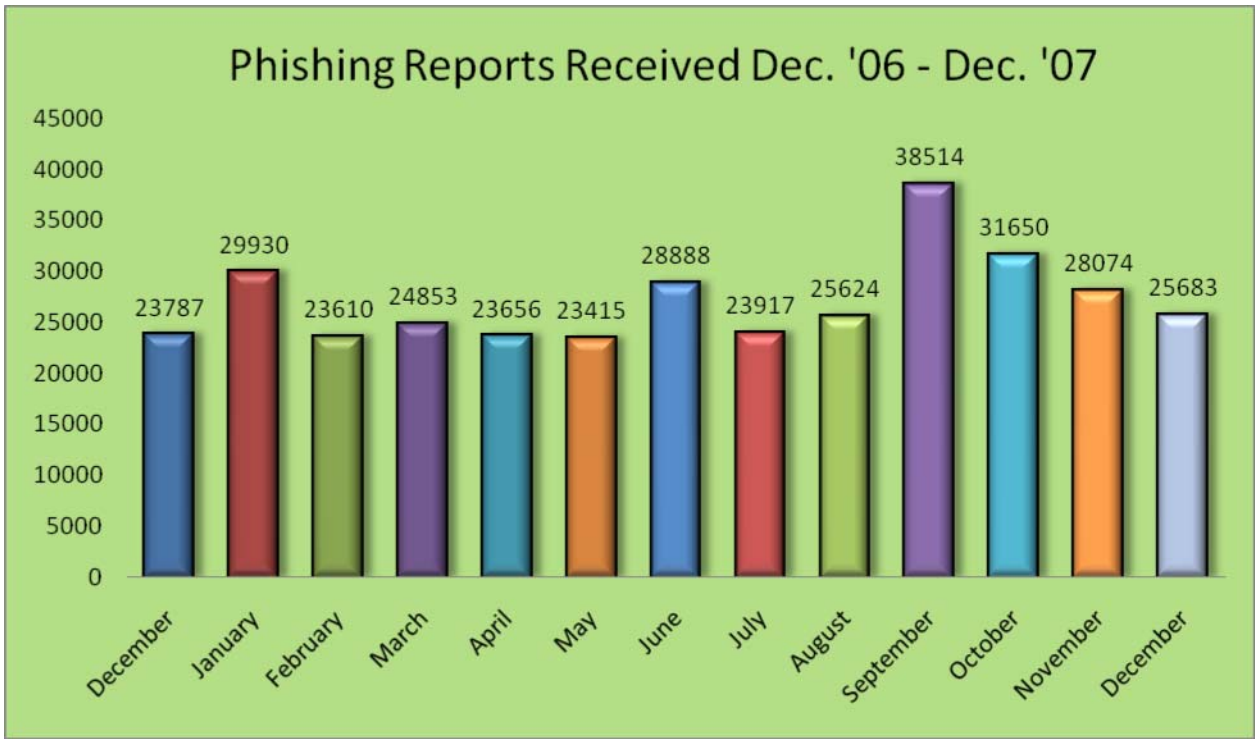
APWG is continuing to refine and develop our tracking and reporting methodology. We have recently re-instated the tracking and reporting of unique phishing reports (email campaigns) in addition to unique phishing sites. An email campaign is a unique email sent out to multiple users, directing them to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

The total number of *unique* phishing reports submitted to **APWG** in December 2007 was **25,683**, a decrease of over 2,300 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.



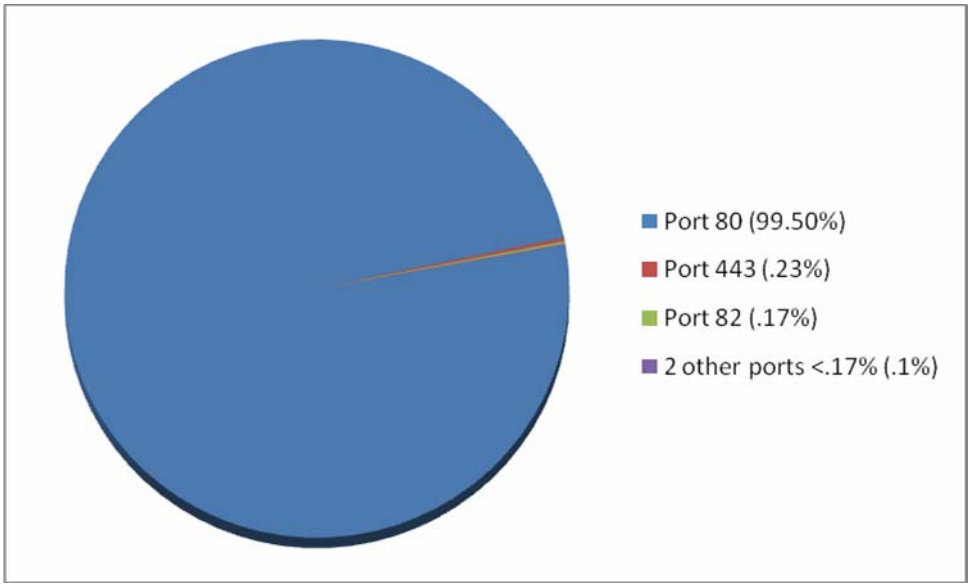
The **Phishing Attack Trends Report** is published monthly by the APWG, an industry and law enforcement association focused on eliminating the identity theft and fraud that result from the growing problem of phishing, crimeware and email spoofing. For further information, please contact APWG Deputy Secretary 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 **25,328** in December 2007, an increase of nearly 1,700 from the month of November.

Top Used Ports Hosting Phishing Data Collection Servers in December 2007

December saw a continuation of HTTP port 80 being the most popular port used at 99.50% of all phishing sites reported.



April - December 2007 Brand-Domain Pairs Measurement

The following chart combines statistics 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.

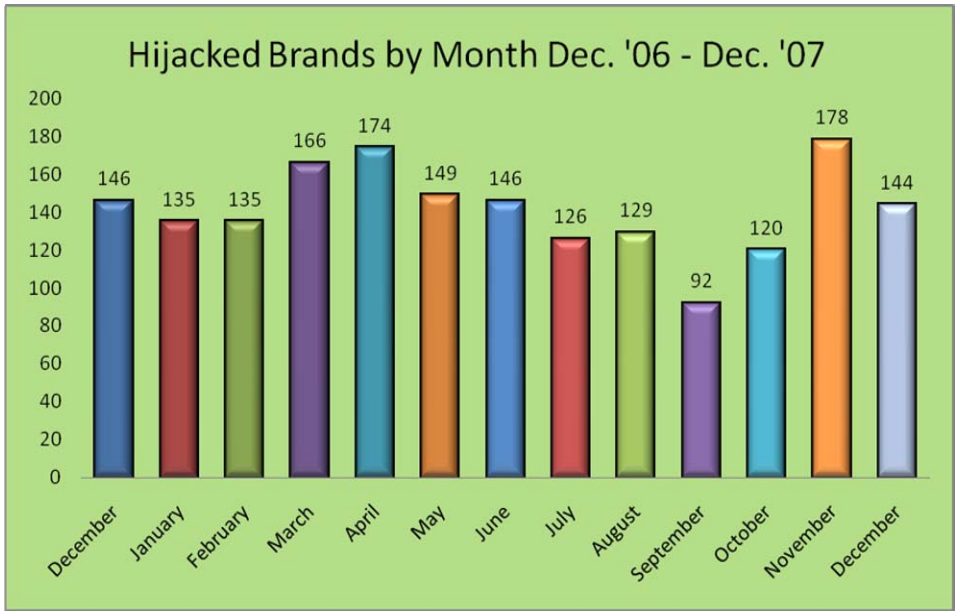
"There appears to be an endless stream of phishers and previously unphished companies to target." said John LaCour, CISSP & Director of AntiPhishing Solutions at MarkMonitor. "In December we saw a small increase in the number of unique phishing URLs and a 10% drop in attacks as measured by domain name-brand pairs. This indicates that phishers have found fertile fields in their favorite targets while they continue to aggressively seek new and previously unphished organizations, albeit at a slower rate than in recent months."

	April	May	June	July	August	September	October	November	December
Unique URLs	55643	37438	31709	30999	32079	28015	34226	23630	25328
Unique Domains	6637	5967	6006	6005	5023	5058	5472	5551	4973
Unique Brand-Domain Pairs	7622	7092	7359	7538	6580	6465	6704	6936	6222
Unique Brands	174	149	146	126	129	92	120	178	144
URLs per Brand	319.79	251.26	217.18	246.02	248.67	304.51	285.22	132.76	175.89

Brands & Legitimate Entities Hijacked By Email Phishing Attacks in Dec. 2007

Number of Reported Brands

After reaching a previous yearly high in November, December reported a drop of more than 30 brands to 144.

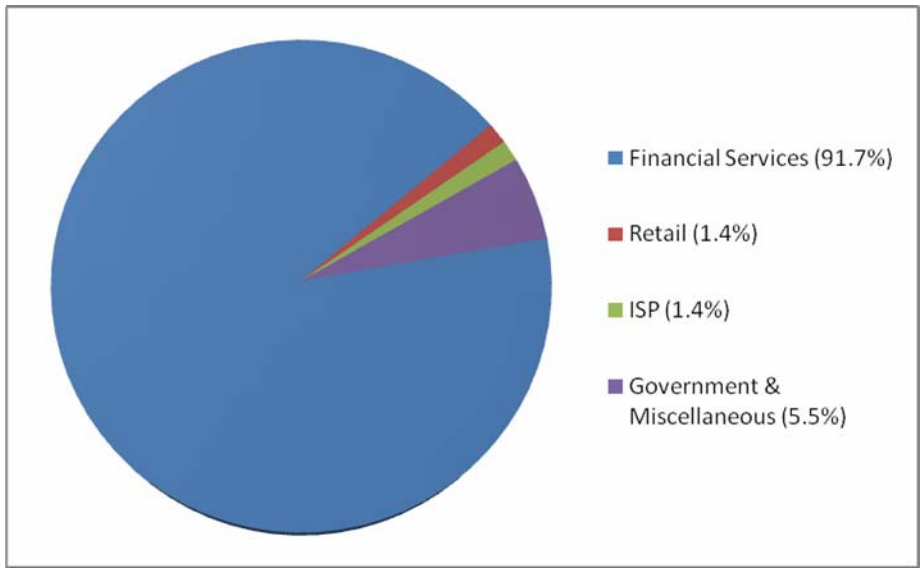


Most Targeted Industry Sectors in December 2007

Financial Services continue to be the most targeted industry sector at 91.7% of all attacks recorded in the month of December.

However, the Government and Miscellaneous segment saw an increase to 5.5%. The APWG noted an increase in phishing campaigns spoofing the IRS in the US and phishing campaigns spoofing tax authorities in the UK and in Australia. (This was the highest proportion for this segment since October, 2005 when it reached 6% of all reported phishing attacks.)

Additionally, APWG notes increased phishing against brands such as automotive associations previously untargeted by phishers.



Web Phishing Attack Trends in December 2007

Countries Hosting Phishing Sites

In December, Websense Security Labs saw the United States move back to the top of countries hosting phishing sites with 32.5%, after a brief one month stay by China in November. The rest of the top 10 breakdown is as follows: China 22.38%, Russian Federation 9.32%, Thailand 5.52%, Israel 5.03%, Egypt 3.6%, Germany 2.92%, France 2.52%, Republic of Korea 1.8% and India with 1.65%.

PROJECT: Crimeware

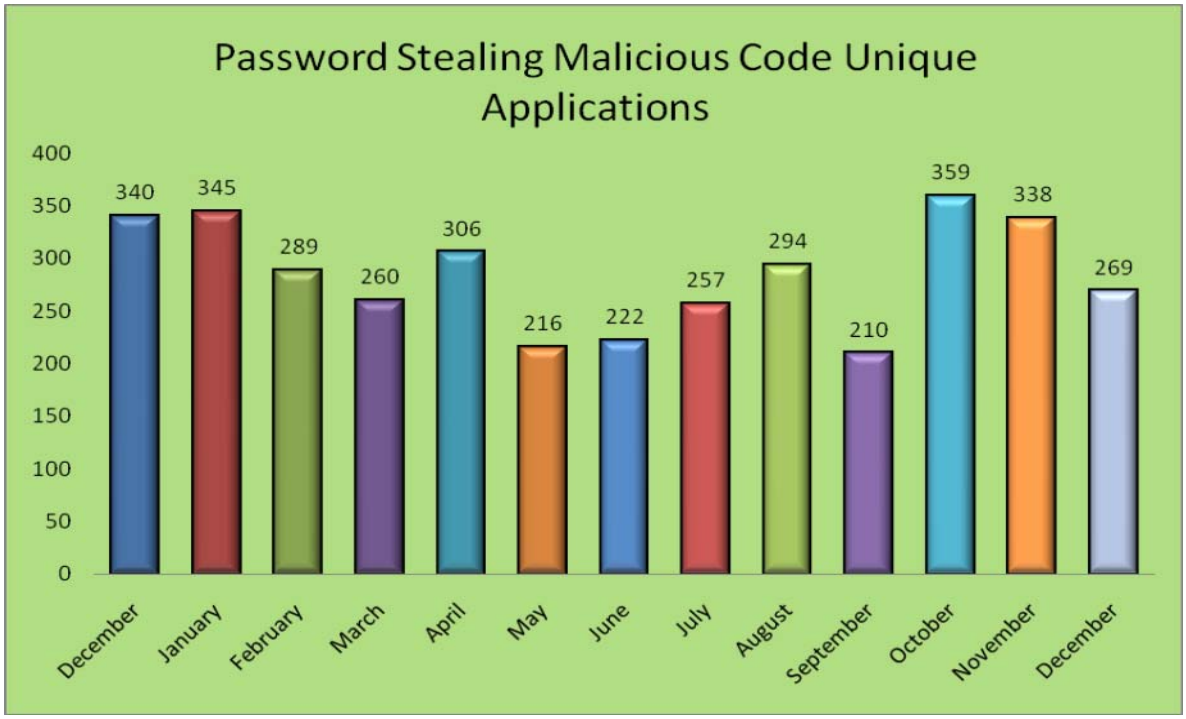
Crimeware Taxonomy & Samples According to Classification in December 2007

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

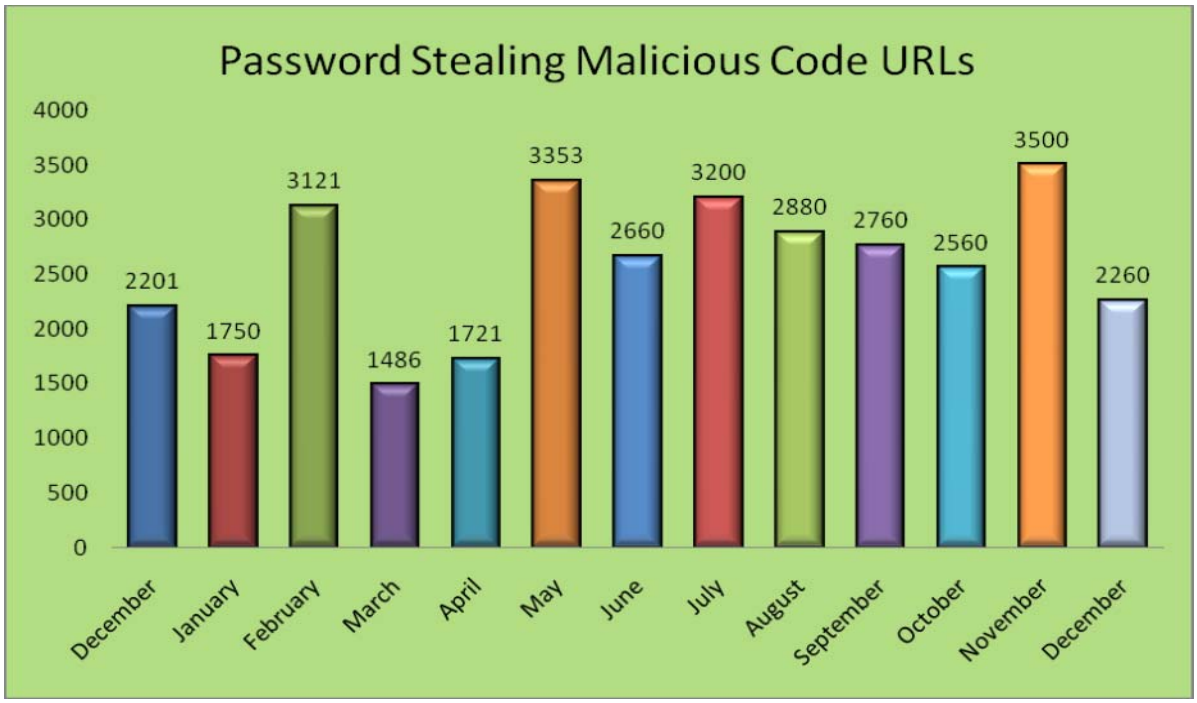
Phishing-based Trojans - Keyloggers

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 December



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



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.

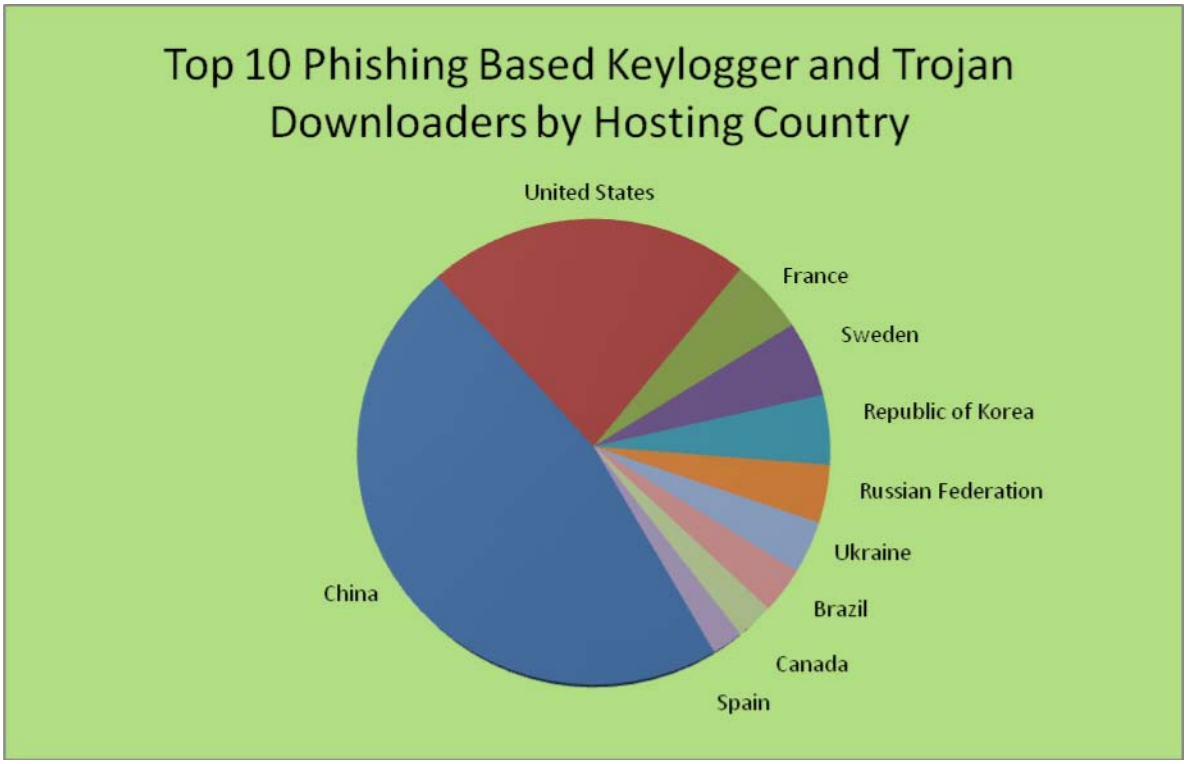
Along with phishing-based keyloggers we are seeing high increases in traffic redirectors. In particular the highest volume is in malicious code which simply modifies your DNS server settings or your hosts file to redirect either some specific DNS lookups or all DNS lookups to a fraudulent DNS server.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

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

In December, China surpassed the United States as the top hosting country with 46.62%.

The rest of the breakdown was as follows; United States 22.57%, France 5.27%, Sweden 5.27%, Republic of Korea 4.85%, Russian Federation 4.01%, Ukraine 3.59%, Brazil 3.16%, Canada 2.53% and Spain with 2.11%



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 APWG Deputy Secretary General Foy Shiver at 404.434.7282 or Cas Purdy at 858.320.9493 or cpurdy@websense.com or Te Smith at 831.818.1267 or Te.Smith@markmonitor.com.

APWG

About the APWG

The APWG, founded as the Anti-Phishing Working Group in 2003, 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 to 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 3000 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 APWG 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.