Phishing Activity Trends Report

4th Quarter 2012

APWG

Unifying the Global Response To Cybercrime

October – December 2012

Published April 24, 2013

Phishing Activity Trends Report, 4th Quarter 2012

Phishing Report Scope

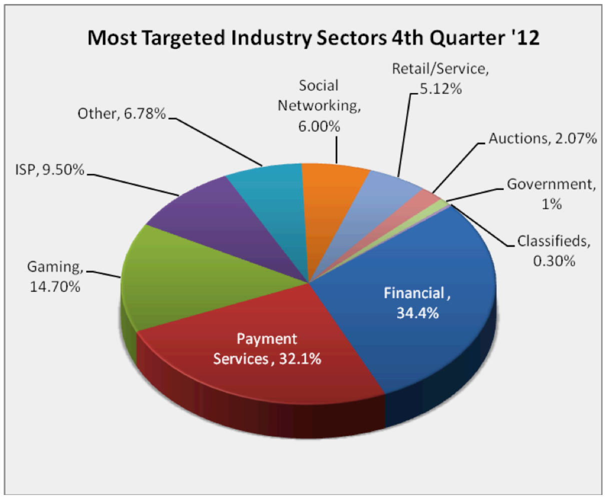
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of crimeware by drawing from the research of our member companies.

Phishing Defined

Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Phishers Shift to Target Online Game Players



Phishing attacks against online game players saw a massive increase, from 2.7 percent of all phishing attacks in Q3 to 14.7 percent in Q4. Financial services continued to be the most-targeted industry sector in the fourth quarter of 2012 with payment services close behind. *[p. 7]*

4th Quarter '12 Phishing Activity Trends Summary

- During Q4, about 30 percent of personal computers worldwide were infected with malware. More than 57 percent of PCs in China may have been infected, while PCs in European nations were infected least-often. [p. 8]

- Except for October 2012, the number of phishing sites declined every month from April 2012 through December 2012. April 2012 saw 63,253 unique phishing sites detected, falling to 45,628 in December 2012. [p. 4]

- The APWG received reports of 28,195 unique phishing sites in December. December's total was 31 percent lower than the high of 40,621 reports in August 2009. [p. 4]

- Use of crimeware dipped slightly in this quarter from the previous, as did the use of data-stealing malware. The use of other malware has increased by a statistically significant amount from the previous quarter. [p. 9]

APWG
www.apwg.org

Methodology and Instrumented Data Sets

The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (e-mail campaigns) in addition to unique phishing sites. An e-mail campaign is a unique e-mail 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 e-mails as those in a given month with the same subject line in the e-mail.

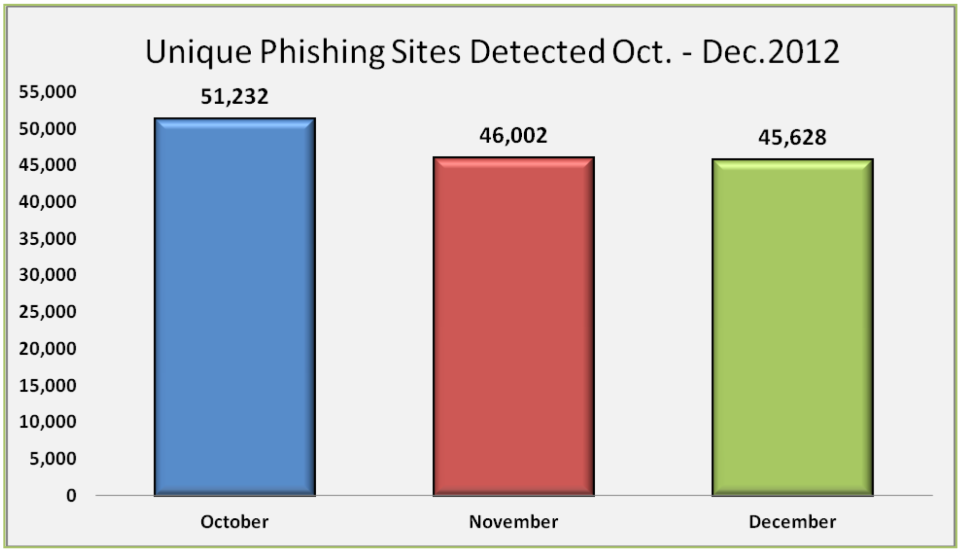
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. APWG additionally tracks crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample), as well as unique sites that are distributing crimeware (typically via browser drive-by exploits). The *APWG Phishing Activity Trends Report* also includes statistics on rogue anti-virus software, desktop infection rates, and related topics.

Statistical Highlights for 4th Quarter 2012

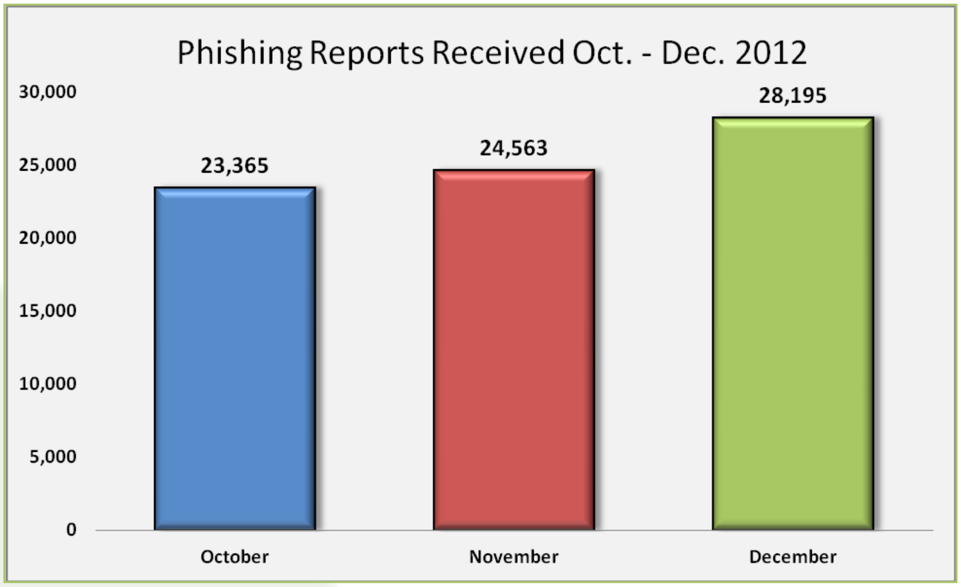
	October	November	December
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	23,365	24,563	28,195
Number of unique phishing websites detected	51,232	46,002	45,628
Number of brands targeted by phishing campaigns	401	430	418
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	60.31%	54.23%	53.59%
No hostname; just IP address	1.63%	1.87%	1.93%
Percentage of sites not using port 80	0.30%	0.24%	1.04%

Phishing E-mail Reports and Phishing Site Trends – 4th Quarter 2012

Except for October 2012, the number of phishing sites declined every month from April 2012 through December 2012. April 2012 saw 63,253 unique phishing sites detected, falling to 45,628 in December 2012. The drop from October to December was 11 percent, and the decline from the 2nd quarter through the fourth quarter was 28 percent. The decline continues to be mainly in phishing against the retail and financial services sectors.



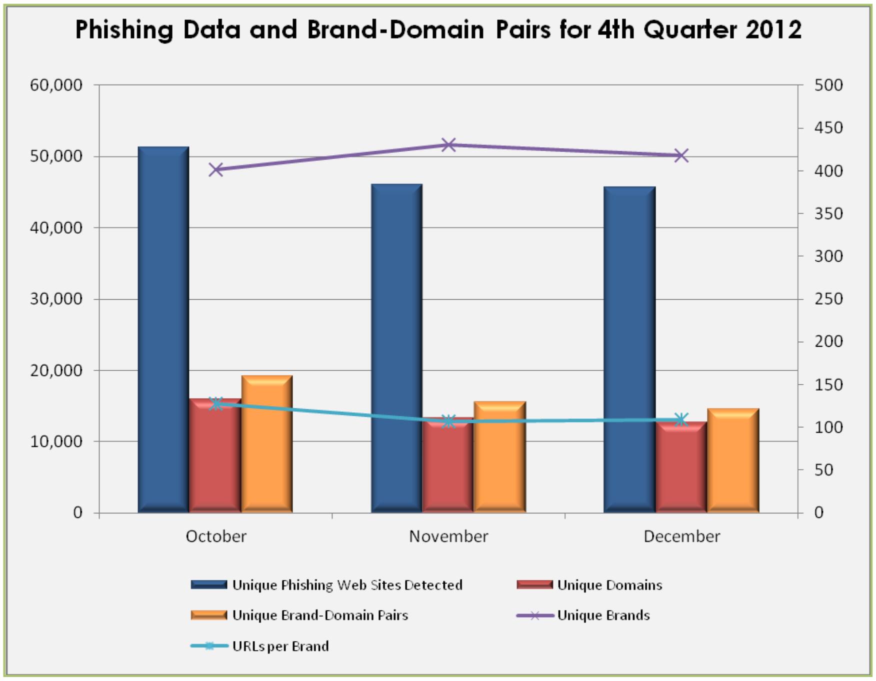
The number of unique phishing reports submitted to APWG each month saw a gradual increase during the quarter. The quarter's high was 28,195 reports in December. December's high was 31 percent lower than the all-time high of 40,621 reports, recorded in August 2009.



Brand-Domain Pairs Measurement – 4th Quarter 2012

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 are targeting a brand – but are hosted on the same domain – this brand/domain pair would be counted as one instead of several.

The number of unique brand-domain pairs saw a massive drop during the fourth quarter of 2012. The high for the three-month period was 19,140 brand-domain pairs in October, dropping down nearly 5,000 to 14,637 in December.



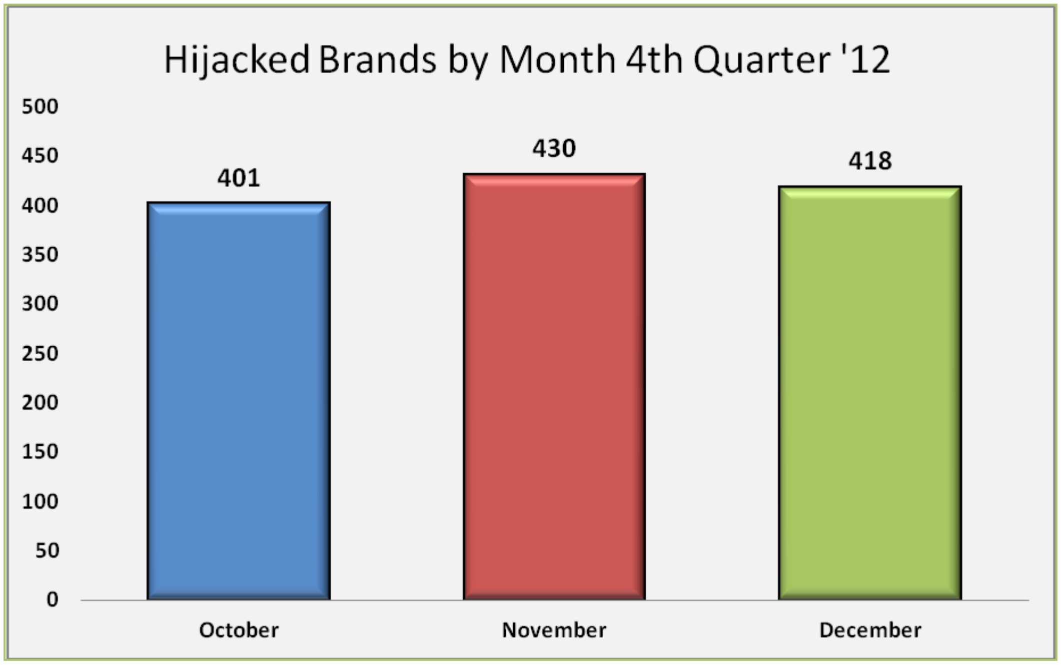
"The total number of phishing attacks detected in Q4 2012 dropped compared to the all-time high in Q2, but the total number of brands targeted by phishers increased in Q4 when compared to Q3 of 2012," said Ihab Shraim, chief information security officer and vice president, anti-fraud engineering and operations, MarkMonitor. "These shifts are due to fraudsters using more advanced phishing techniques, such as geo-IP blocking, and malware. They are also taking advantage of the availability of non-traditional platforms such as social media and mobile to launch newer types of targeted phishing attacks."

Forensic utility of this metric: 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 brand-holding victim needs to locate and neutralize. Since phishing-prevention technologies (like browser and e-mail blocking) require the full URL, it is useful to understand the general number of unique URLs that occur per domain.

	October	November	December
Number of Unique Phishing Web Sites Detected	51,232	46,002	45,628
Unique Domains	15,899	13,351	12,728
Unique Brand-Domain Pairs	19,140	15,579	14,637
Unique Brands	401	430	418
URLs Per Brand	127.76	106.98	109.15

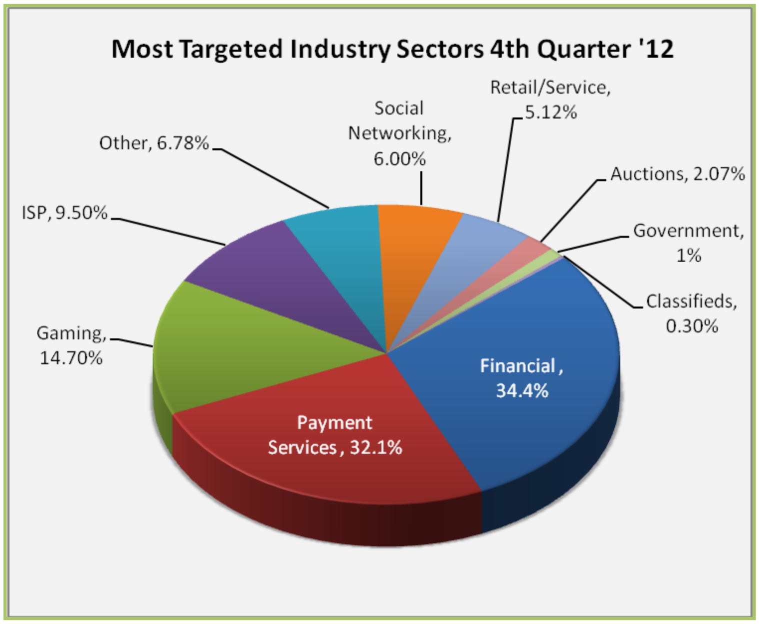
Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 4th Quarter 2012

November 2012 saw 430 brands targeted by phishers. This was an all-time high, surpassing the 428 observed in April and July 2012. APWG members report that sophisticated targeted content continues to make email a highly effective attack vector for phishing, malware, and spam.



Most-Targeted Industry Sectors – 4th Quarter 2012

Financial services continued to be the most-targeted industry sector in the fourth quarter of 2012 with payment services close behind. Attacks against online gaming sites such as Battle.net saw a massive increase, from 2.7% in Q3 to 14.7% in Q4. Online gaming credentials are valuable to certain criminals, who sell them on the black market. In-game items held in those accounts can also be sold by phishers for real-world cash. Victims can even have their real-life identities stolen. Attacks against social media doubled to 6%, up from 3% in the third quarter.



Countries Hosting Phishing Sites – 4th Quarter 2012

Most phishing occurs on hacked or compromised Web servers. The United States continued to be the top country hosting phishing sites during the fourth quarter of 2012. This is mainly due to the fact that a large percentage of the world's Web sites and domain names are hosted in the United States.

October		November		December	
USA	73.93%	USA	73.87%	USA	63.85%
UK	4.52%	China	5.65%	China	6.22%
Germany	2.20%	Russia	2.33%	UK	3.12%
Canada	1.91%	Thailand	1.76%	Germany	2.84%
China	1.70%	Australia	1.59%	Canada	2.68%
Netherlands	1.21%	Netherlands	1.39%	Rep. of Korea	2.60%
Australia	1.13%	Germany	1.37%	Russia	1.32%
Ireland	0.97%	Canada	1.33%	Br. Virgin Isl.	1.17%
France	0.94%	UK	1.19%	Netherlands	1.04%
Br. Virgin	0.92%	Czech Rep.	1.19%	Hungary	1.04%

Crimeware Taxonomy and Samples According to Classification

The APWG's Crimeware statistics categorize crimeware attacks as follows; the taxonomy will grow as variations in attack code are spawned. Definition: Crimeware is code designed with the intent of collecting information on the end-user in order to steal the user's credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components, which attempt to monitor specific actions (and specific organizations, such as financial institutions, retailers, and e-commerce merchants) in order to target specific information. The most common types of information are access to financial-based websites, ecommerce sites, and web-based mail sites.

Malware Infected Countries – 4th Quarter 2012

In the fourth quarter of 2012, 7 million new malware samples were detected by PandaLabs. The categorization was a follows:

Type of Malware Identified	% of malware samples
Trojans	73.69%
Virus	14.60%
Worms	10.32%
Rogueware	1.17%
Other	.21%

Malware Infections by Type	% of malware samples
Trojans	77.06%
Virus	8.95%
Worms	6.21%
Rogueware	4.67%
Other	3.11%

According to Luis Corrons, PandaLabs Technical Director and *APWG Trends Report* contributing analyst, the percentage of Trojans grew slightly, from 72.58 percent in the 3rd quarter to 73.69 percent in the 4th quarter of 2012, and Trojans continue to account for most of the new threats. Virus infections increased, from 6.56 percent in Q3 to 8.95 percent in Q4 2012.

Which countries were most infected? Which countries were best protected? The average number of infected PCs across the globe stood at 29.86 percent percent, similar to Q3. China, as usual, is "leading" the way (57.62 percent of infected PCs), followed by Honduras (42.86 percent) and Turkey (41.60 percent). Depending upon the malware used, infected PCs can then be used to attack other computers or send spam to other computers around the world.

As the table shows, there are high-infection countries in almost every part of the world: Asia, Europe, and South America. However, if we take a look at the least-infected countries, all of them are European with the only exception of South Africa. The country with the fewest infections is Finland (18.20 percent of infected PCs), followed by Switzerland (20.13 percent). Sweden takes the third spot (20.75 percent), maintaining its presence as one of the countries least affected by malware infections over the last few years.

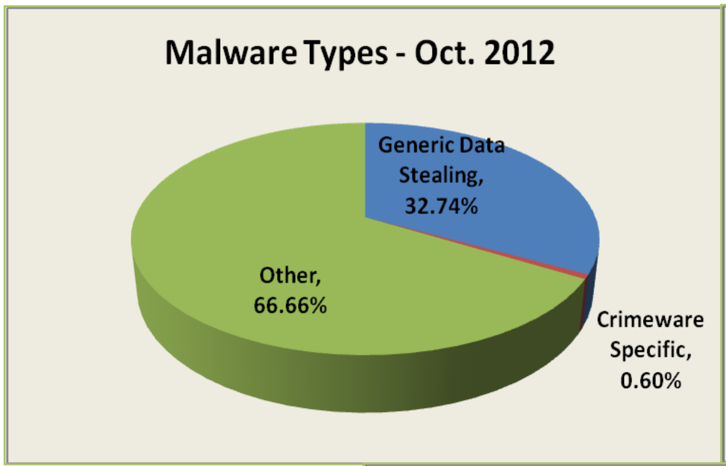
Ranking	Country	Infection Rate
1	China	57.62%
2	Honduras	42.86%
3	Turkey	41.60%
4	Bolivia	41.46%
5	Poland	36.33%
6	Taiwan	36.20%
7	Peru	34.33%
8	Argentina	33.46%
9	Czech Republic	33.00%
10	El Salvador	32.63%

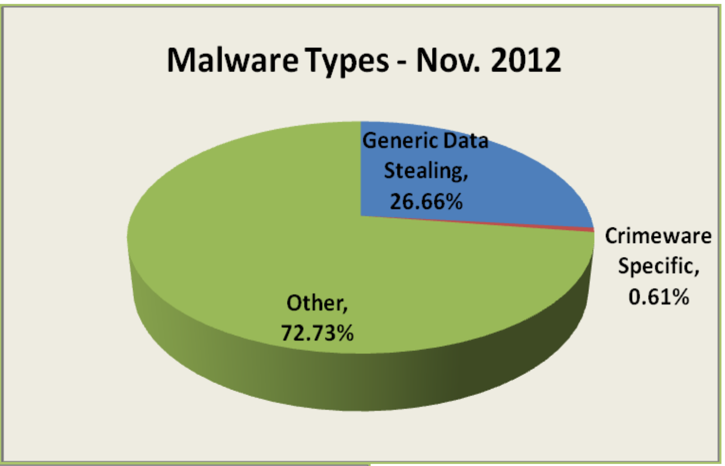
Ranking	Country	Infection ratio
35	Denmark	23.31%
36	Austria	23.31%
37	United Kingdom	23.17%
38	South Africa	22.01%
39	Netherlands	21.91%
40	Germany	21.65%
41	Norway	21.61%
42	Sweden	20.75%
43	Switzerland	20.13%
44	Finland	18.20%

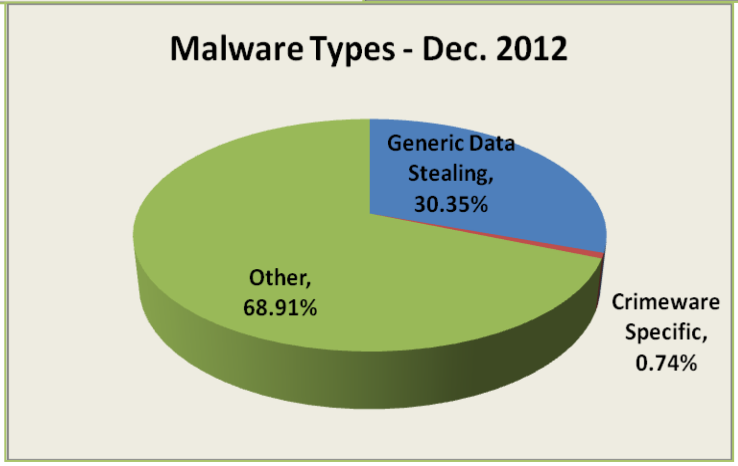
Measurement of Detected Crimeware – 4th Quarter 2012

Using data contributed from APWG founding member Websense regarding the proliferation of malevolent software, this metric measures proportions of three genera of malevolent code:

- *Crimeware* (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt those institutions' identities);
- *Data Stealing and Generic Trojans* (code designed to send information from the infected machine, control it, and open backdoors on it); and
- *Other* (the remainder of malicious code commonly encountered in the field such as auto-replicating worms, dialers for telephone charge-back scams, etc.)







Carl Leonard of Websense Security Labs said: "Continuing with the data collected for the last quarter of 2012, use of crimeware dipped slightly in the fourth quarter from the previous, as has data-stealing malware. The use of other malware has increased by a statistically significant amount from the previous quarter."

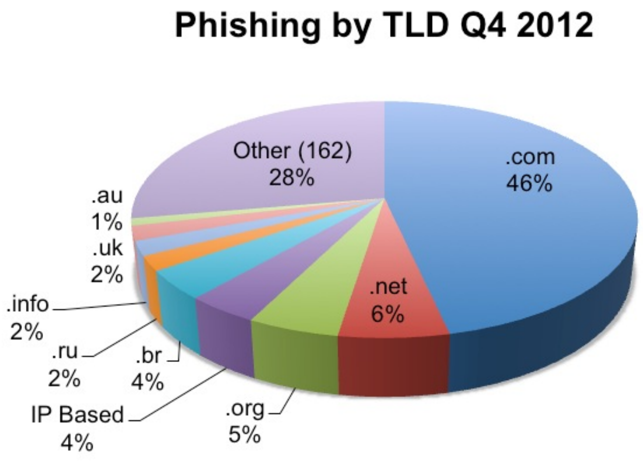
Hosting of Phishing-based Trojans and Downloaders by Country (by IP address)

During the three-month period, USA and China still ranked as the top two countries for hosting phishing sites respectively, with the Netherlands making a second place appearance in November. The following chart represents a breakdown of the websites that were classified as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader that downloads a keylogger.

October		November		December	
USA	65.79%	USA	67.96%	USA	50.32%
China	10.43%	Netherlands	5.92%	China	15.75%
Netherlands	5.34%	China	5.29%	UK	5.45%
France	2.67%	Lithuania	3.92%	Netherlands	4.65%
Germany	2.13%	Germany	2.39%	France	3.97%
Rep. of Korea	2.12%	Rep. of Korea	2.13%	Germany	2.46%
Russia	1.80%	Russia	1.80%	Canada	1.58%
Brazil	0.97%	France	1.38%	Russia	1.58%
UK	0.77%	UK	0.99%	Rep of Korea	1.54%
Br. Virgin Isl.	0.64%	Brazil	0.91%	Brazil	1.30%

Phishing by Top-Level Domain

APWG member Internet Identity records the top-level domains (TLDs) used to host phishing. Forty-six percent of phishing attacks were on .COM names, and .COM represents approximately 42 percent of domain names registered worldwide. The TLD of Brazil (.BR) had 4 percent of phishing worldwide, but only 1 percent of the total global domain name market.



APWG Phishing Activity Trends Report Contributors

ILLUMINTEL

Illumintel Inc. provides advising and security services to top-level-domain registry operators and other Internet companies.

IID

Internet Identity (IID) is a US-based provider of technology and services that help organizations secure their Internet presence.

MarkMonitor®

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PANDA SECURITY

Panda Security's mission is to keep our customers' information and IT assets safe from security threats, providing the most effective protection with minimum resource consumption.

websense® Yes! ESSENTIAL INFORMATION PROTECTION™

Websense, Inc. is a global leader in secure Web gateway, data loss prevention, and e-mail security solutions, protecting more than 43 million employees at organizations worldwide.

The *APWG Phishing Activity Trends Report* is published by the APWG. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver at 404.434.7282 or foy@apwg.org. For media inquiries related to the content of this report, please contact APWG Secretary General Peter Cassidy at 617.669.1123; Te Smith of MarkMonitor at 831.818.1267 or Te.Smith@markmonitor.com; Luis Corrons of Panda at lcorrons@pandasoftware.es; or Websense at publicrelations@websense.com.

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail spoofing. Membership is open to qualified financial institutions, retailers, ISPs, solutions providers, the law enforcement community, government agencies, multi-lateral treaty organizations, and NGOs. There are more than 2,000 enterprises worldwide participating in the APWG. Because electronic crime is a sensitive subject, APWG maintains a policy of confidentiality of member organizations.

Websites of APWG public-service enterprises include its public website, <http://www.antiphishing.org>; the Website of public awareness program, STOP. THINK. CONNECT. Messaging Convention <http://www.stopthinkconnect.org> and the APWG's research website <http://www.ecrimeresearch.org>. These serve as resources about the problem of phishing and electronic frauds perpetrated against personal computers and their users – and resources for countering these threats. The APWG, a 501c6 tax-exempted corporation, was founded by Tumbleweed Communications, financial services institutions and e-commerce providers. APWG's first meeting was in November 2003 in San Francisco and in June 2004 was incorporated as an independent corporation controlled by its board of directors, its executives and its steering committee.

Analysis by Greg Aaron, Illumintel; *Trends Report* editing by Ronnie Manning, Mynt Public Relations.