



# **Phishing Activity Trends Report**

**1<sup>st</sup> Quarter  
2012**



**Unifying the  
Global Response  
To Cybercrime**

**January – March 2012**

*Published July 2012*

# Phishing Activity Trends Report, 1<sup>st</sup> 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](mailto:reportphishing@antiphishing.org). APWG also measures the evolution, proliferation, and propagation of crimeware by drawing from the research of our member companies.

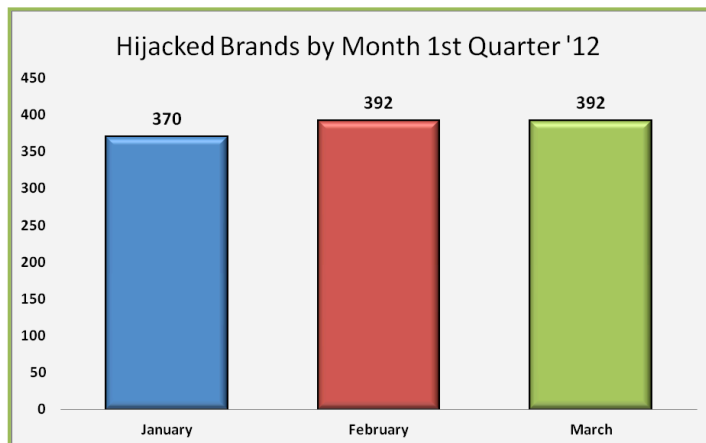
## Phishing Defined

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

<b>Statistical Highlights for 1st Quarter 2012</b>	<b>3</b>
<b>Phishing E-mail Reports and Phishing Site Trends</b>	<b>4</b>
<b>Brand-Domain Pairs Measurement</b>	<b>5</b>
<b>Most Used Ports Hosting Phishing Data</b>	
Collection Servers in 1st Quarter 2012	4
<b>Brands &amp; Legitimate Entities Hijacked by</b>	
E-mail Phishing Attacks	6
<b>Most Targeted Industry Sectors</b>	7
<b>Countries Hosting Phishing Sites</b>	7
<b>Top Malware Infected Countries</b>	8
<b>Measurement of Detected Crimeware</b>	9
<b>Phishing-based Trojans &amp; Downloader's Host</b>	
Countries (by IP address)	10
<b>APWG Phishing Trends Report Contributors</b>	11

## Targeted Brands Reaches Record High in February and March



The all-time high of 392 brands targeted in Feb. and March was an increase of 8 percent from the previous record high recorded just last December. [p. 6]

## 1st Quarter '12 Phishing Activity Trends Summary

- The number of unique phishing sites detected in a month by the APWG reached 56,859 in February, which was an all-time high. [p. 4]
- Financial Services continued to be the most-targeted industry sector in the first quarter of 2012. [p. 7]
- The average number of infected PCs across the globe stands at 35.51 percent, which is more than three percentage points lower than in 2011. [p. 8]
- China continues to be the most affected country (with 54.10 percent of infected PCs), and remains the only country with an infection ratio over 50 percent. [p. 8]
- Brand-Domain Pairs Measurement is up across the board with one of the biggest increases ever seen in a single quarter. [p. 5]
- In the first three months of 2012, more than six million unique malware samples were identified. [p. 8]
- During the quarter, USA remained the top nation for hosting phishing-based Trojans, and Azerbaijan cracked the top 10 for the first time ever, in March 2012. [p. 10]

# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

## 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.

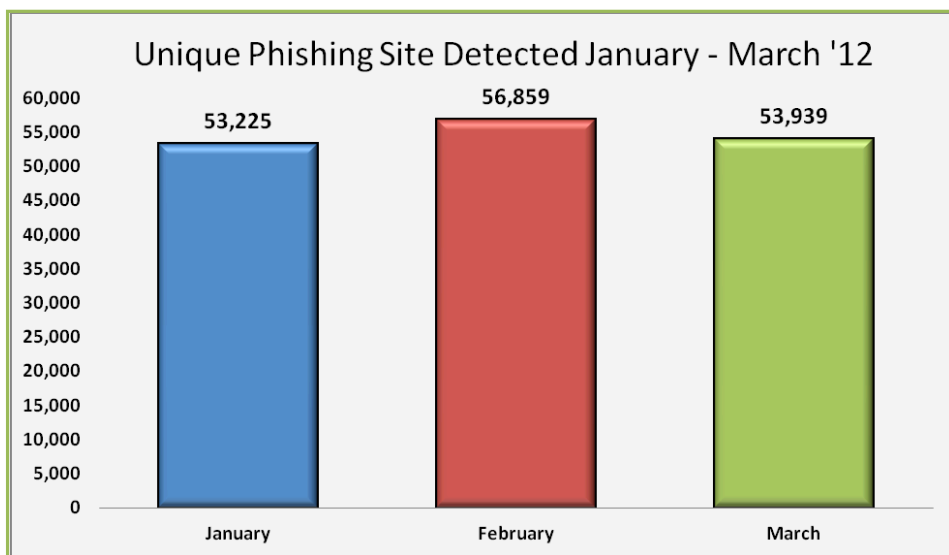
## Statistical Highlights for 1<sup>st</sup> Quarter 2012

	January	February	March
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	25,444	30,237	29,762
Number of unique phishing websites detected	53,225	56,859	53,939
Number of brands hijacked by phishing campaigns	370	392	392
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	49.53%	45.39%	55.42%
No hostname; just IP address	1.19%	1.40%	2.09%
Percentage of sites not using port 80	1.19%	0.68%	0.26%

# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

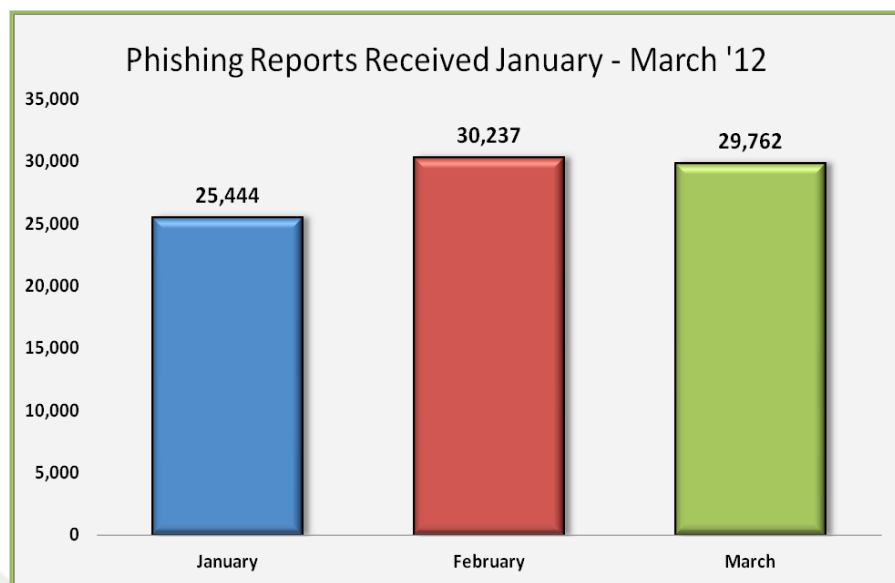
## Phishing E-mail Reports and Phishing Site Trends – 1st Quarter 2012

Phishing attacks targeting consumers remained at high levels during the quarter, with 25,000 to 30,000 unique phishing e-mail campaigns documented each month. Each campaign can involve hundreds of thousands or millions of e-mails sent to consumers. There are hundreds of phishing websites established online every day, luring any number of consumers to trouble and loss.



The number of unique phishing sites detected in a month by the APWG was 56,859 in February, which was an all-time high. The total remained relatively consistent during the three-month period, indicating sustained and regular activity by phishers. The February figure eclipsed the previous record high of 56,362, which was recorded in August 2009, by almost 1 percent.

The number of unique phishing reports submitted to APWG each month fluctuated by less than 5,000 reports from month to month. The quarter's high was 30,237 reports in February. February's high was 25 percent lower than the all-time high of 40,621 reports, recorded in August 2009.



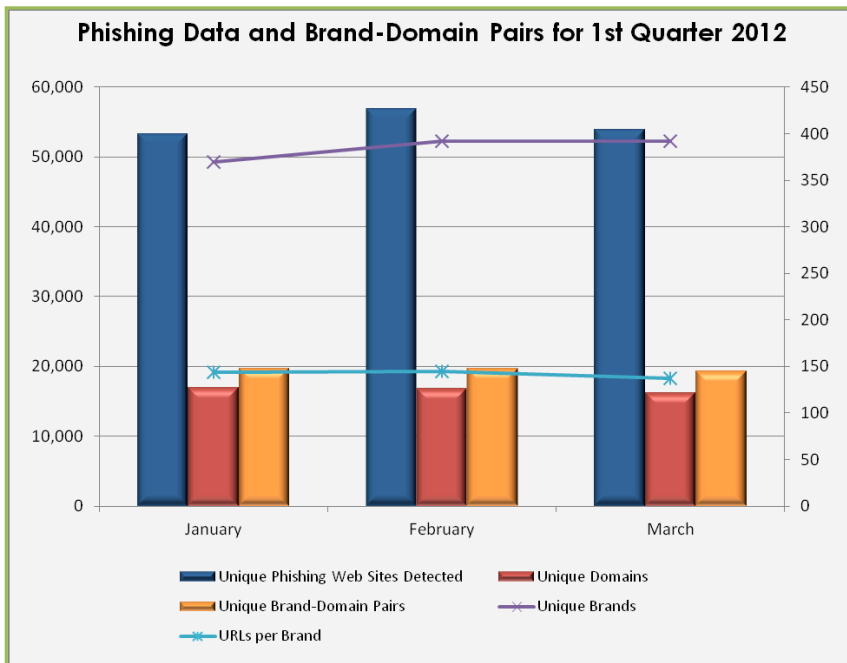


# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

## Brand-Domain Pairs Measurement – 1st 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 had a slight fluctuation during the first quarter of 2012. The high for the three-month period was 19,702 brand-domain pairs in January. This was down 19 percent from the record of 24,438 recorded in August 2009.



“Phishing measurements are up across the board, with one of the biggest increases we have ever seen in a single quarter, said Ihab Shraim, CISO and VP, AntiFraud Operations and Engineering, MarkMonitor. “While this increase is chiefly due to new phishing detection technology that we began rolling out early in 2012, we also observed the payment services category returning to its position as the second-most-popular phishing sector and large increases in activity in the social networking, ISP, and government sectors, too.”

*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.

	January	February	March
Number of Unique Phishing Web Sites Detected	53,225	56,859	53,939
Unique Domains	16,965	16,804	16,233
Unique Brand-Domain Pairs	19,702	19,619	19,299
Unique Brands	370	392	392
URLs Per Brand	143.85	145.05	137.59

# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

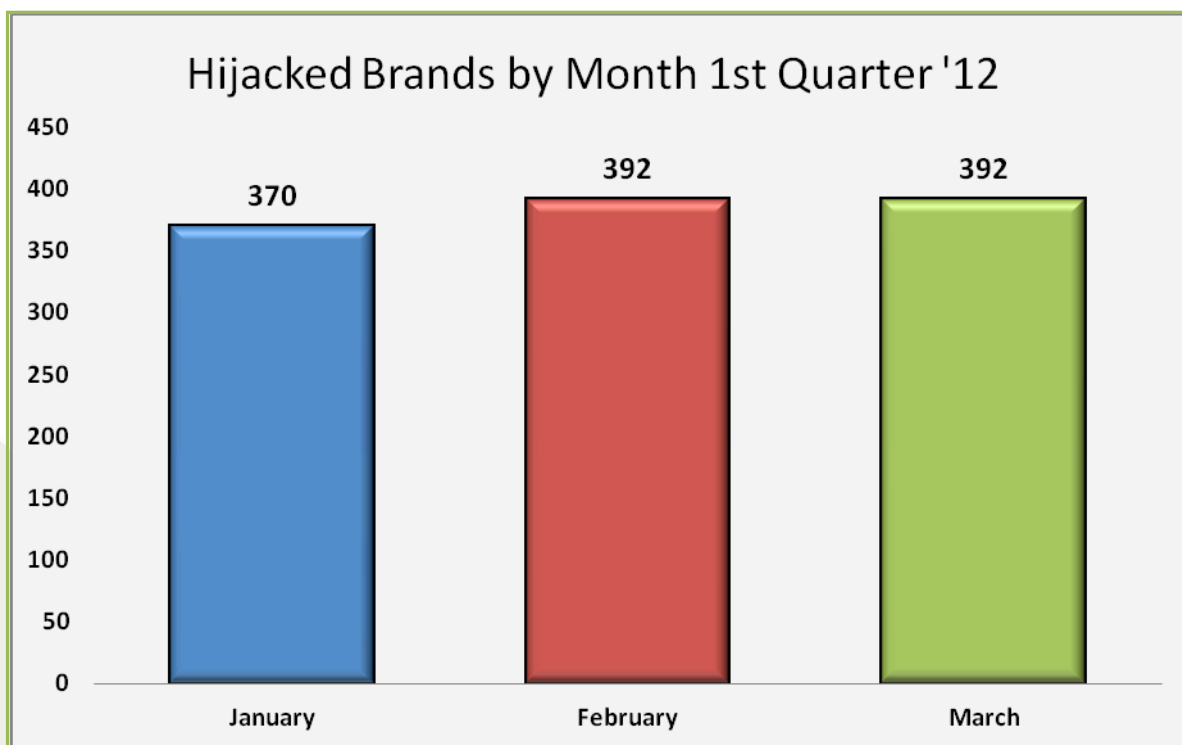
## Most Used Ports Hosting Phishing Data Collection Servers – 1st Quarter 2012

The first quarter of 2012 saw a continuation of HTTP port 80 being the most popular port used of all phishing sites reported, a trend that has been consistent since APWG began tracking and reporting in 2003.

January		February		March	
Port 80	98.418%	Port 80	99.324%	Port 80	99.739%
Port 443	1.581%	Port 443	.673%	Port 443	.259%
		Port 21	.003%	Port 21	.002%

## Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 1st Quarter 2012

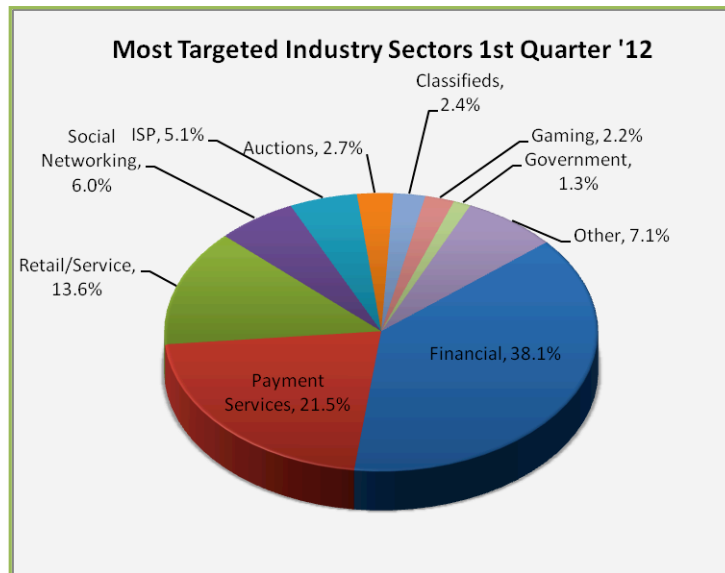
February and March 2012 both presented a new all-time high of 392 brands targeted by phishers. This was an 8 percent increase from the previous all-time high of 362, recorded in December 2011. The previous high before December was 356, reached in October 2009.



# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

## Most Targeted Industry Sectors – 1st Quarter 2012

Financial Services continued to be the most-targeted industry sector in the first quarter of 2012. During this three month period, Payment Services eclipsed Retail/Services to come in as the second-highest industry sector for targeted attacks.



## Countries Hosting Phishing Sites – 1st 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 first 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. Canada was briefly at #2 in January, but that spate of phishing subsided in February.

January		February		March	
USA	68.92%	USA	70.86%	USA	66.20%
Canada	11.20%	Romania	3.25%	Germany	3.04%
Egypt	4.32%	Germany	2.66%	B. Virgin Il.	2.63%
Germany	1.85%	UK	2.62%	Brazil	2.54%
France	1.35%	Russia	1.78%	Egypt	1.98%
Israel	1.29%	France	1.73%	UK	1.91%
Netherlands	1.19%	Canada	1.66%	Netherlands	1.84%
Russia	0.68%	Netherlands	1.51%	Canada	1.83%
UK	0.68%	Brazil	1.35%	Turkey	1.54%
Turkey	0.63%	Australia	1.01%	France	1.51%

# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

## Crimeware Taxonomy and Samples According to Classification

The APWG's Crimeware statistics categorize crimeware attacks as follows, though 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 – 1st Quarter 2012

In the first three months of 2012, PandaLabs identified more than six million unique malware samples, which is in line with the overwhelming number of malware strains detected over the last few years. Most of the infections were caused by Trojans (80 percent of all new malware samples), setting a new record high. This is a continuation of the trend established over the last few months:

Type of Malware Identified	% of malware samples
Trojans	80.77%
Worms	9.31%
Virus	6.43%
Rogueware	2.89%
Other	.60%

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, one of the characteristics of Trojans is that they cannot replicate automatically, so they are less capable of triggering massive infections than viruses or worms, which can infect a large number of PCs by themselves. While Trojans account for most infections, it is worth noting the relatively small number of PCs infected by worms. This demonstrates that massive worm epidemics have become a thing of the past, and have been replaced by a silent Trojan invasion.

The average number of infected PCs across the globe stands at 35.51 percent, which is more than three points lower than in 2011. China continues to be the most affected country (54.10 percent of PCs there are infected), and remains the only country with an infection ratio over 50 percent. China is followed by Taiwan (47.15 percent) and Turkey (42.75 percent). The list of the least malware-infected nations is topped by European countries, with the exception of Japan. Sweden came in lowest with less than 18 percent of its computers infected (setting a new record).

Ranking	Country	Infection Rate
1	China	54.10%
2	Taiwan	47.15%
3	Turkey	42.75%
4	Russia	41.22%
5	Peru	39.99%
6	Ecuador	38.03%
7	Spain	37.93%
8	Argentina	37.52%
9	Poland	36.90%
10	Chile	36.63%

Ranking	Country	Infection ratio
23	Finland	28.53%
24	Portugal	28.38%
25	Denmark	27.73%
26	Germany	27.20%
27	Japan	25.50%
28	Netherlands	24.85%
29	United Kingdom	24.17%
30	Norway	22.29%
31	Switzerland	20.02%
32	Sweden	17.94%



# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

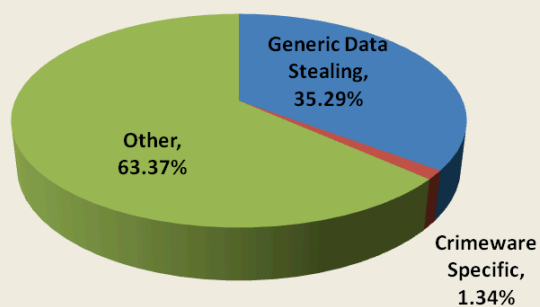
## Measurement of Detected Crimeware – 1<sup>st</sup> Quarter 2012

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

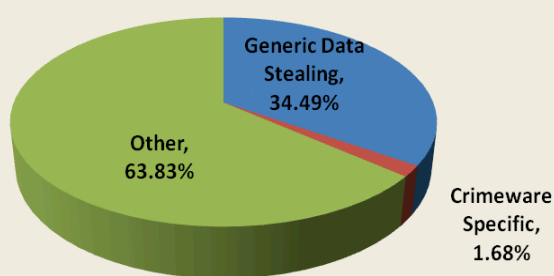
- *Crimeware* (data-stealing malicious code designed specifically to be used to victimize financial institutions' customers and to co-opt those institutions' identities);
- *Data Stealing and Generic Trojans* (code designed to send information from the infected machine, control it, and open backdoors 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.)

"This quarter, we saw an interesting scam using a pdf attachment as a lure to capture personally identifiable information (PII). The information in that pdf file was a faked signed document from a popular global banking institution," said Carl Leonard of Websense Security Labs.

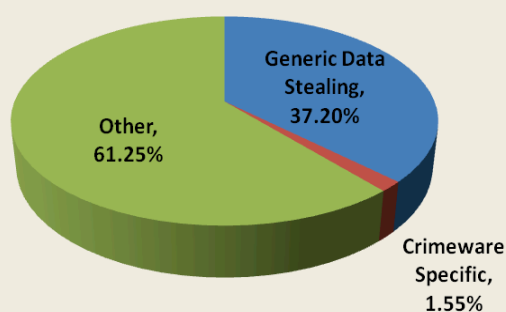
Malware Types - January 2012



Malware Types - February 2012



Malware Types - March 2012



# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012






## Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

This chart represents a breakdown of the websites which were classified during the first quarter of 2012 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. During the three month period, the USA remained the top hosting country of phishing-based Trojans, and Azerbaijan cracked the top 10 for the first time ever, in March 2012.

January		February		March	
USA	71.27%	USA	55.37%	USA	47.25%
France	6.79%	Russia	7.31%	France	9.53%
Russia	2.78%	China	4.65%	China	5.92%
Germany	2.63%	France	3.43%	Azerbaijan	5.19%
Rep of Korea	2.29%	Netherlands	3.33%	Russia	4.92%
Netherlands	2.09%	Rep of Korea	2.93%	Canada	4.86%
China	1.99%	Brazil	2.69%	Germany	3.39%
UK	1.18%	Germany	2.68%	Netherlands	2.78%
Ukraine	1.08%	UK	2.50%	Rep of Korea	2.21%
Canada	0.95%	Panama	2.13%	Ukraine	1.98%

# Phishing Activity Trends Report, 1<sup>st</sup> Quarter 2012

## APWG Phishing Activity Trends Report Contributors

  Illumintel Inc. provides advising and security services to top-level-domain registry operators and other Internet companies.	  Internet Identity (IID) is a US-based provider of technology and services that help organizations secure their Internet presence.	  MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.
	  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, 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](mailto: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](mailto:Te.Smith@markmonitor.com); Luis Corrons of Panda at [lcorrns@pandasoftware.es](mailto:lcorrns@pandasoftware.es); or Websense at [publicrelations@websense.com](mailto: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.

11

Statistical analysis by Greg Aaron, [Illumintel](http://www.illumintel.com); Trends Report editing by Ronnie Manning, [Mynt Public Relations](http://www.mynt.com).