Phishing Activity Trends Report

1st Quarter 2013

APWG

Unifying the
Global Response
To Cybercrime

January – March 2013

Published July 23, 2013

Phishing Activity Trends Report, 1st Quarter 2013

Phishing Report Scope

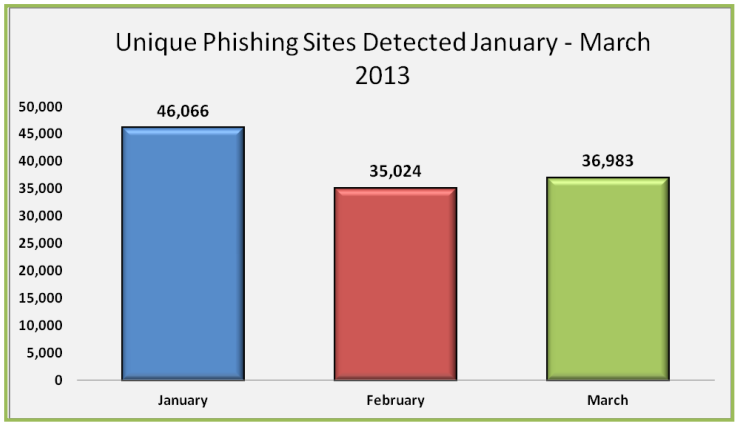
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation,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

Unique Phishing Sites Detected Reached Lowest Point Since Oct. '11



February's 35,024 was the lowest number of phishing sites detected in a month since October 2011. [p. 4]

1st Quarter 2013 Phishing Activity Trends Summary

- Phishing attack numbers declined 20 percent from Q4 2012 to Q1 2013, [p.4], due to a precipitous drop in virtual server phishing attacks. [p. 5]

- Trends indicate phishing levels returning to the levels seen prior to the record-setting highs of 2012. [pp. 4-5]

- The significant drop in the number of phishing-based Trojans and downloaders hosted in the USA, with an increase in Canada, illustrates the migratory patterns of cyber-criminals. [p. 10]

- After reaching an all-time high in November 2012, the number of brands targeted by phishers dropped as low as 348, in February 2013. [p. 6]

- Payment Services jumped back on top as the most-targeted industry sector, after being surpassed by financial services during the fourth quarter of 2012. [p. 7]

- Trojan infections have reached record levels, accounting for almost 80 percent of all infections. [p. 8]

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.

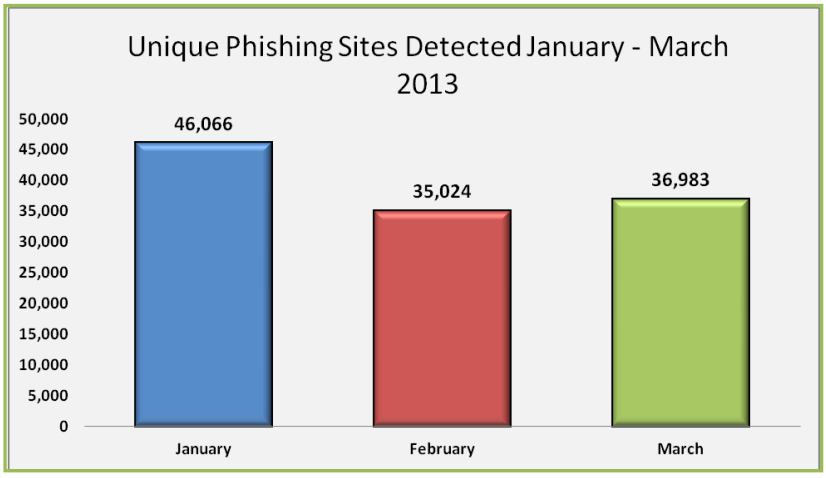
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLS, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances (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 1st Quarter 2013

	January	February	March
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	28,850	25,385	19,892
Number of unique phishing websites detected	46,066	35,024	36,983
Number of brands targeted by phishing campaigns	402	348	405
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	50.03%	50.75%	55.89%
No hostname; just IP address	1.84%	1.92%	5.24%
Percentage of sites not using port 80	1.36%	2.33%	0.64%

Phishing E-mail Reports and Phishing Site Trends – 1st Quarter 2013

Phishing attack numbers declined notably from Q4 2012 to Q1 2013, with APWG seeing a 20 percent decrease between January and March 2013. February's 35,024 was the lowest number of attacks detected since the 36,733 seen in October 2011.



The number of unique phishing reports submitted to APWG each month saw a massive decrease during the quarter, dropping 31 percent from January to March. January's total of 28,850 was 29 percent lower than the all-time high of 40,621 reports, recorded in August 2009.

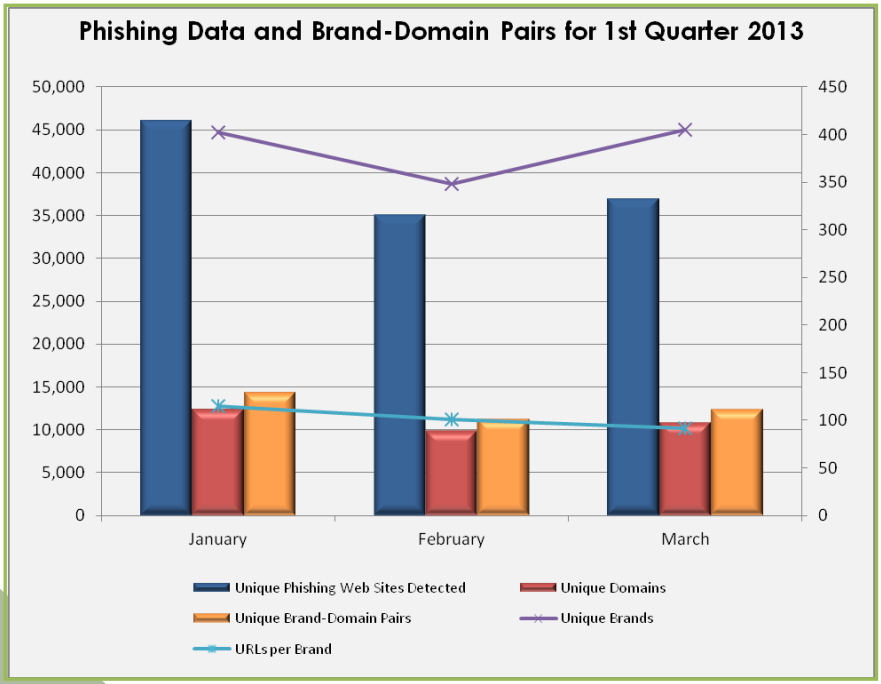
The declines in attacks and reports were mostly due to a precipitous decline in virtual server phishing attacks. A virtual server phishing attack is an incident wherein a cybercriminal breaks into a single web server that hosts a large number of domains, and then creates and hosts phishing pages on each one of those domains. This method can efficiently yield a large number of attacks.

Internet Identity President and *Trends Report* contributing analyst Rod Rasmussen said, by Internet Identity's own count, the number of phishing sites hosted on shared virtual servers plummeted from a high of over 14,400 incidents in October 2012 to just 1,653 in February 2013. "While fluctuations in these statistics can be common, the drastic decrease likely indicates that cybercriminals are utilizing the servers they compromise not for phishing attacks, but rather for more malware or distributed denial of service attacks," Mr. Rasmussen said.

Brand-Domain Pairs Measurement – 1st Quarter 2013

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.) *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.

The number of unique brand-domain pairs fluctuated during first quarter of 2013. The high for the three-month period was 14,365 brand-domain pairs in January, dropping to 11,194 in February.

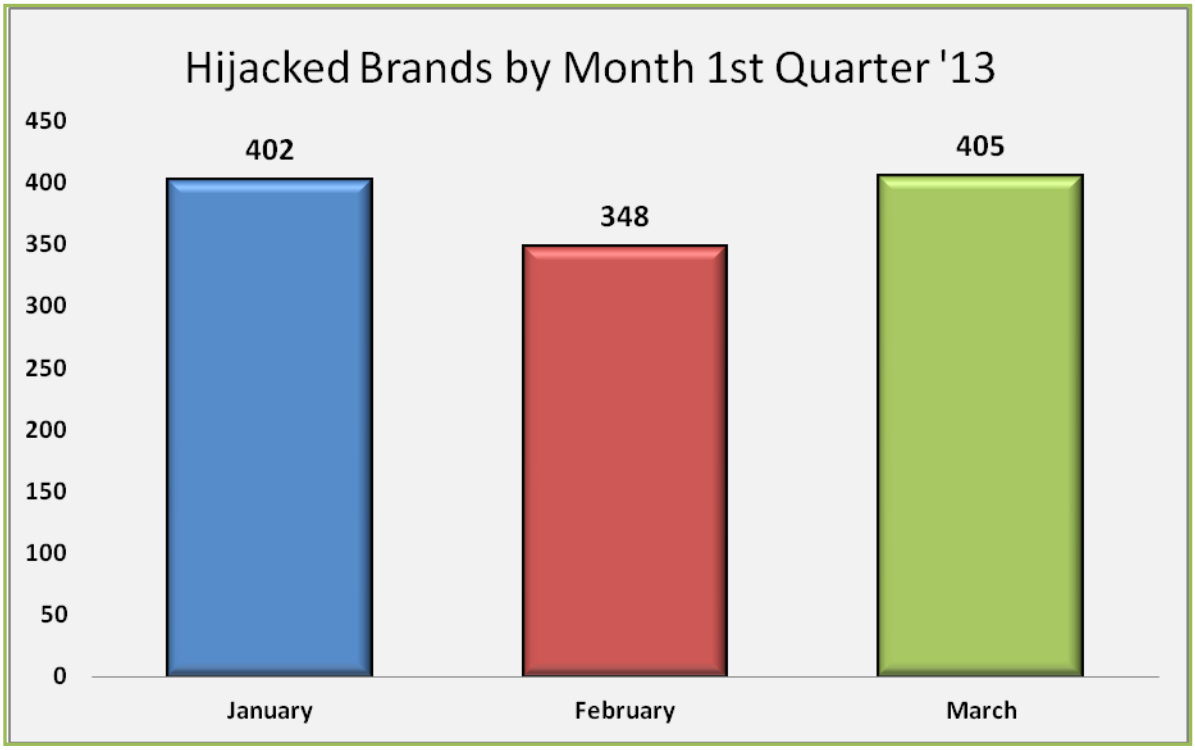


"There was a significant drop in the number of phishing attacks with a 17 per cent decline in Q1 2013 from the previous quarter. This downward trend seems to indicate phishing levels are dropping back toward the levels that we saw prior to the record-setting highs of 2012," said Ihab Shraim, CISO and Vice President Anti-Fraud Engineering and Operations. "These changes are likely due to a shift to more advanced and targeted techniques for credential theft including malware and stealthier spear phishing."

	January	February	March
Number of Unique Phishing Web Sites Detected	46,066	35,024	36,983
Unique Domains	12,358	9,901	10,802
Unique Brand-Domain Pairs	14,365	11,194	12,378
Unique Brands	402	348	405
URLs Per Brand	114.59	100.64	91.31

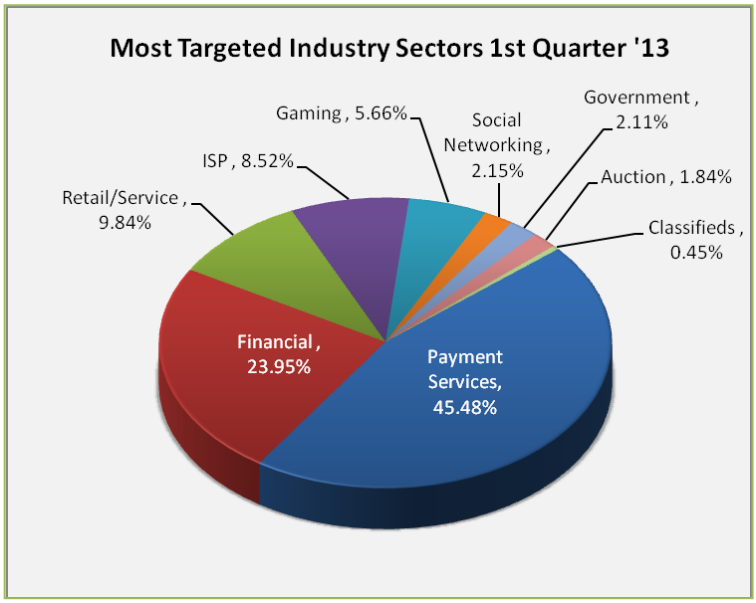
Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 1st Quarter 2013

After reaching a high of 430 in November 2012, the number of brands targeted by phishers dropped. February's total of 348 was anomalously low, the lowest monthly total since November 2011. Otherwise, the number of brands targeted was generally higher than levels seen in 2011 and 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 – 1st Quarter 2013

Payment Services jumped back on top as the most-targeted industry sector, after being surpassed by Financial Services during the fourth quarter of 2012. Attacks against social media dropped nearly 4 percent from the fourth quarter of 2012. Gaming experienced a notable drop from 14.70 percent in Q4 2012 to 5.66 percent in Q1 2013.



Countries Hosting Phishing Sites – 1st Quarter 2013

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 2013. 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.

January		February		March	
United	64.78%	United	54.30%	United	53.18%
Germany	4.34%	Germany	7.98%	Germany	7.40%
China	3.86%	China	5.56%	UK	4.21%
UK	3.57%	Australia	3.64%	Canada	4.15%
Ireland	2.65%	UK	3.33%	Turkey	3.81%
Netherlands	2.30%	Canada	3.16%	France	2.38%
France	2.29%	France	2.28%	Russia	2.34%
Canada	2.04%	Brazil,	1.59%	Brazil	2.33%
Bahamas	1.67%	Russia	1.40%	Latvia	1.29%
Australia	1.12%	Singapore	1.30%	Netherlands	1.26%

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, e-commerce sites, and web-based mail sites.

Malware Infected Countries – 1st Quarter 2013

During the first three months of 2013, PandaLabs collected more than 6.5 million malware samples. Trojans are still the most common, accounting for three out of four cases. The breakdowns are similar to those seen during 2012:

Type of Malware Identified	% of malware samples
Trojans	74.46%
Viruses	12.73%
Worms	11.79%
Rogueware	.79%
Other	.23%

Malware Infections by Type	% of malware samples
Trojans	77.93%
Viruses	7.48%
Worms	5.89%
Rogueware	3.98%
Other	4.72%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, Trojan infections remain near historically high levels. Today most Trojan infections are made through compromised websites, often exploiting some kind of vulnerability in Java or Adobe. This means that in just a few minutes (in the case of a popular Web page) there may be thousands of infections with the same Trojan. Similarly, they could be different Trojans, since attackers can change the Trojan based on parameters such as the victim's location or operating system.

An average of 31 percent of computers worldwide were infected with malware in 1Q 2013. China again topped the infection ranking, and was the only country with an infection rate over 50 percent. Several factors contribute to a high infection rate, including use of unauthorized (and therefore unpatched) operating system software, and sub-par IT management practices in institutions.

Europe continues to have the lowest infection rates. Finland boasts a low 17 percent infection rate. Other countries outside this Top 10 but with infection rates below the average were: Canada (24.89 percent), Denmark (25.72 percent), Portugal (26.91 percent), Costa Rica (27.22 percent), France (27.43 percent), USA (27.79 percent), Mexico (29.91 percent), and Hungary (30.69 percent).

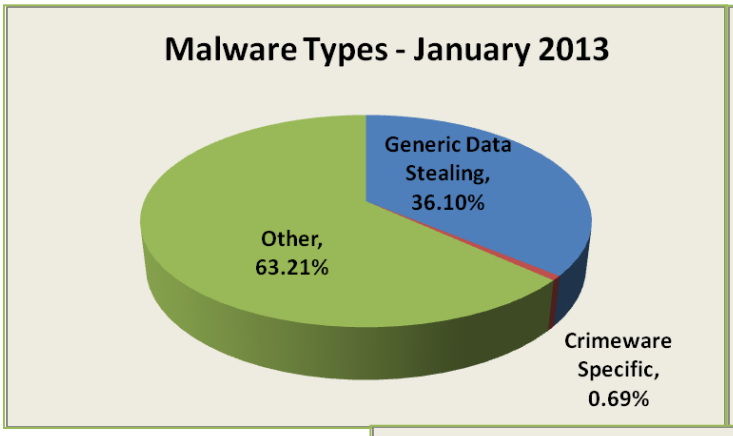
Ranking	Country	Infection Rate
1	China	53.47%
2	Ecuador	41.01%
3	Turkey	40.38%
4	Argentina	37.77%
5	Peru	37.43%
6	Taiwan	36.48%
7	Russia	36.21%
8	Poland	33.79%
9	Spain	33.58%
10	Brazil	33.45%

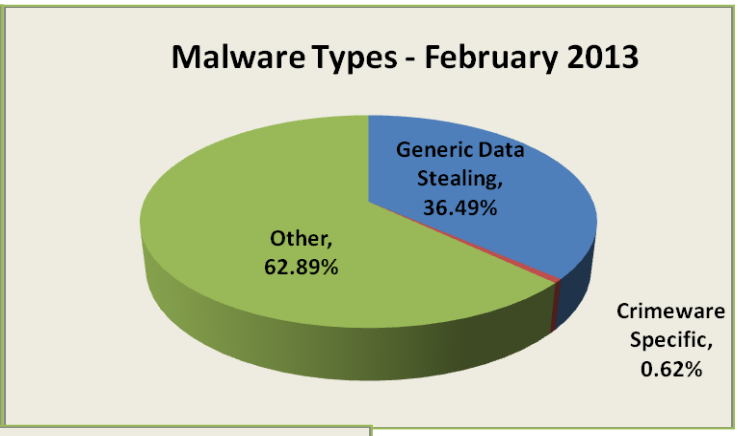
Ranking	Country	Infection ratio
35	Finland	17.07%
36	Sweden	20.01%
37	Switzerland	20.99%
38	UK	21.89%
39	Norway	22.57%
40	Japan	22.82%
41	Germany	22.94%
42	Belgium	23.89%
43	Holland	23.92%
44	Australia	24.32%

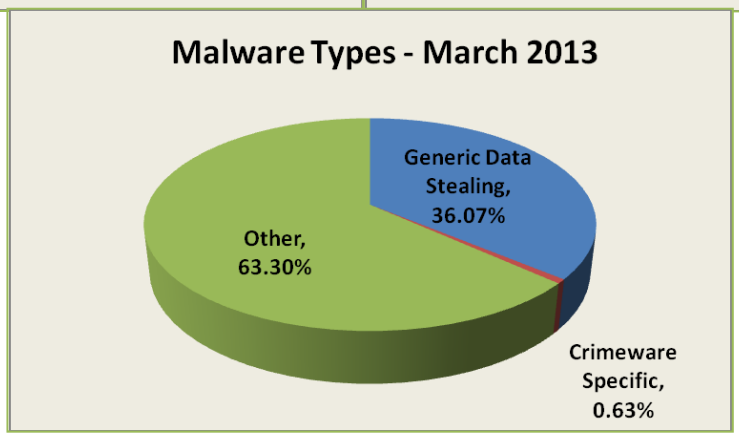
Measurement of Detected Crimeware – 1st Quarter 2013

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.)







"Data-stealing malware has seen a rise indicating the trend of stolen data as a commodity on the black market continues; the use of other malware has seen a slight reduction," said Carl Leonard of Websense Security Labs.

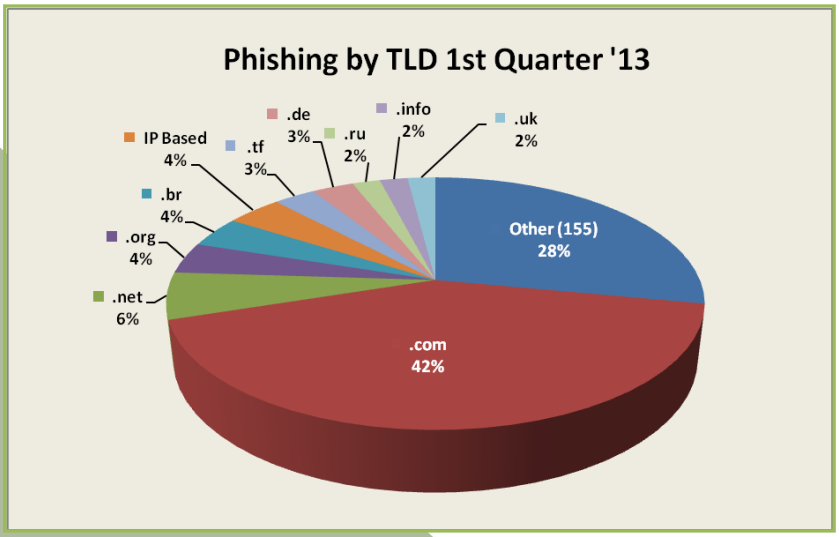
Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

During March, there was a shift in how criminals obtained hosting for their phishing-based Trojans and downloaders. A significant percentage of this activity ceased to be hosted in the USA, dropping from almost 37 percent to less than 20 percent of the world total. "While tracking the decrease in US-hosted phishing websites we noticed a corresponding increase in phishing sites hosted in Canada," said Carl Leonard of Websense. "We saw a decrease in Canadian-hosted phishing in 2012, so we may seeing the beginning of a trend reversal in Q1 2013." The activity points to a rash of compromised web servers in Canada in early 2013, which could be used for phishing and malware distribution. The following chart provides a breakdown of the websites that were classified as hosting malicious code , either a phishing-based keylogger or a Trojan downloader that downloads a keylogger:

January		February		March	
USA	36.79%	USA	28.65%	Germany	21.60%
Germany	23.94%	Germany	25.48%	USA	19.48%
Russian	13.44%	Russia	14.19%	Switzerland	18.97%
Netherlands	6.07%	Romania	5.59%	Russia	18.60%
China	3.97%	China	4.13%	Netherlands	3.35%
Rep of Korea	1.54%	Netherlands	3.84%	China	2.83%
Brazil	1.50%	Malta	2.18%	Ukraine	2.10%
Romania	1.49%	France	2.18%	Romania	1.92%
France	1.25%	Ukraine	1.83%	Rep of Korea	1.05%
Ukraine	1.20%	Rep of Korea	1.29%	B. Virgin Islands	1.03%

Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing sites. Forty-two percent of domains used for phishing were .COM names, down for 49 percent previously. The .COM TLD represents approximately 44 percent of domain names registered worldwide. The TLD of Brazil (.BR) continued to have 4 percent of phishing worldwide, but only 1 percent of the world 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; Websense at publicrelations@websense.com, or ATmedia@internetidentity.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.