



Phishing Activity Trends Report

4th Quarter

2013



Unifying the
Global Response
To Cybercrime

October – December 2013

Published April 7, 2014

Phishing Activity Trends Report, 4th Quarter 2013

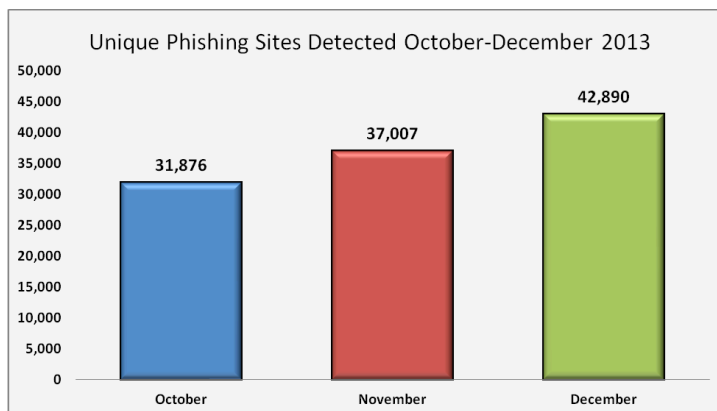
Phishing Report Scope

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).

Fraudsters Look to Profit on the Brands that Deliver the Highest Returns



Overall phishing activity accelerated in the fourth quarter, and 2013 ended as a high-volume year for phishing.

4th Quarter 2013 Phishing Activity Trends Summary

- The number of phishing sites detected rose through the fourth quarter. Overall, there were 22 percent fewer phishing sites in the fourth quarter than there were in the third quarter. Even then, 2013 was one of the most active years on record for phishing. [pp. 4-5]
- During the second half of 2013, 840 unique target institutions were attacked, up significantly from the 720 found in the second half of 2013. [p. 6]
- A number of malware families morphed constantly in efforts to avoid detection by antivirus products. Fully 37 percent of the malware variations spawned during 2013 showed up during Q4. [p. 8]
- The United States continued to be the top country hosting phishing sites during the fourth quarter of 2013. [p. 7]

Table of Contents

Statistical Highlights for 4th Quarter 2013	3
Phishing E-mail Reports and Phishing Site Trends	4
Brand-Domain Pairs Measurement	5
Brands & Legitimate Entities Hijacked by E-mail Phishing Attacks	6
Most Targeted Industry Sectors	7
Countries Hosting Phishing Sites	7
Top Malware Infected Countries	8
Measurement of Detected Crimeware	9
Phishing-based Trojans & Downloader's Host Countries (by IP address)	10
Phishing by Top-Level Domain	10
APWG Phishing Trends Report Contributors	11

Phishing Activity Trends Report, 4th Quarter 2013

Methodology and Instrumented Data Sets

APWG tracks 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.

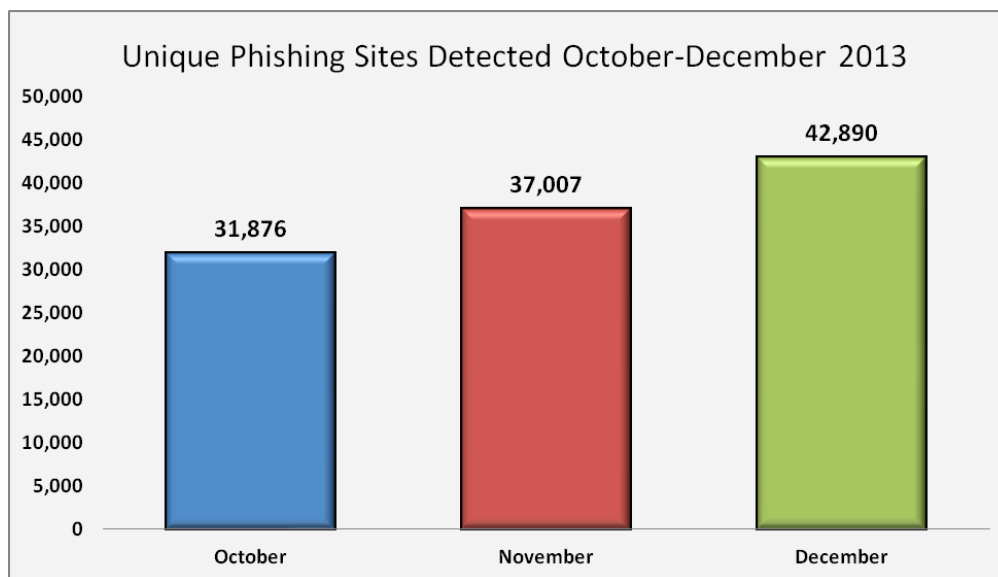
Statistical Highlights for 4th Quarter 2013

	October	November	December
Number of unique phishing websites detected	31,876	37,007	42,890
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	55,241	53,047	52,489
Number of brands targeted by phishing campaigns	350	356	362
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	58.72%	71.04%	74.67%
No hostname; just IP address	1.06%	0.87%	1.60%
Percentage of sites not using port 80	1.65%	0.72%	0.78%

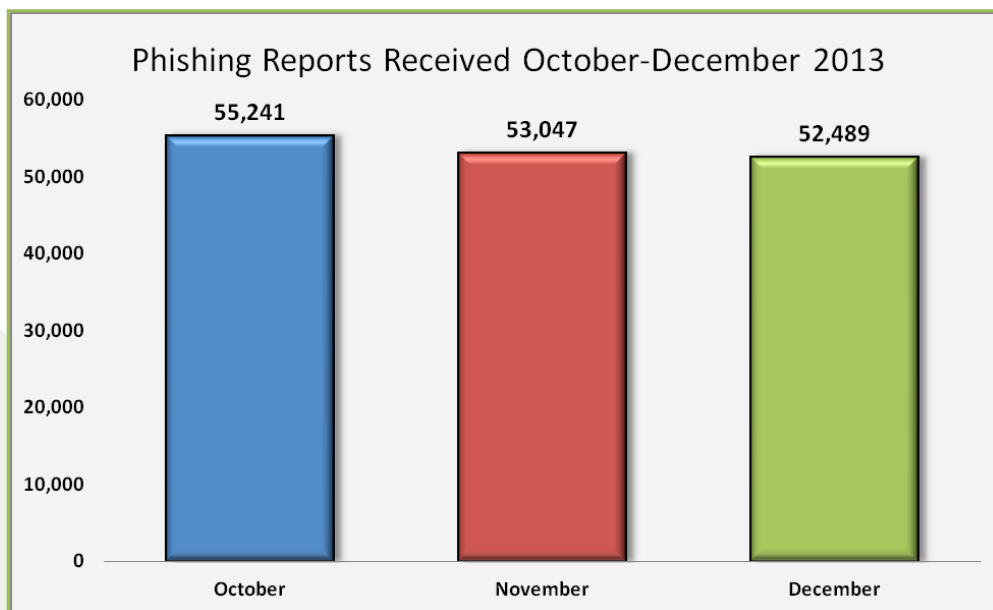
Phishing Activity Trends Report, 4th Quarter 2013

Phishing E-mail Reports and Phishing Site Trends – 4th Quarter 2013

The number of unique phishing sites detected rose over the course of the fourth quarter. The total number of unique phishing sites observed in Q4 was 111,773, which was a 22 percent overall decrease over Q3's 143,353.



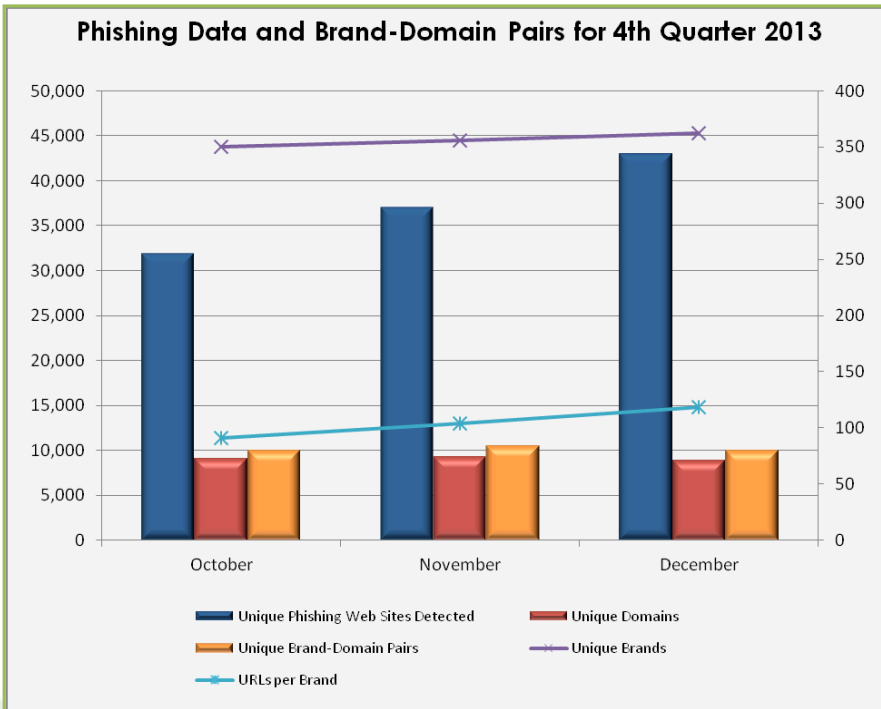
The number of unique phishing reports submitted to APWG during Q4 was 160,777. This was a decline of 12 percent from the 180,012 received in Q3. Some reports duplicate each other, and the number of unique sites detected rose over the course of the quarter while the number of reports declined slightly.



Phishing Activity Trends Report, 4th Quarter 2013

Brand-Domain Pairs Measurement – 4th 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 in order to prevent over-blocking, it is useful to understand the general number of unique URLs that occur per domain.



The number of brands targeted saw a gradual increase during Q4 2013. The number of unique brand-domain pairs remained consistent during Q4.

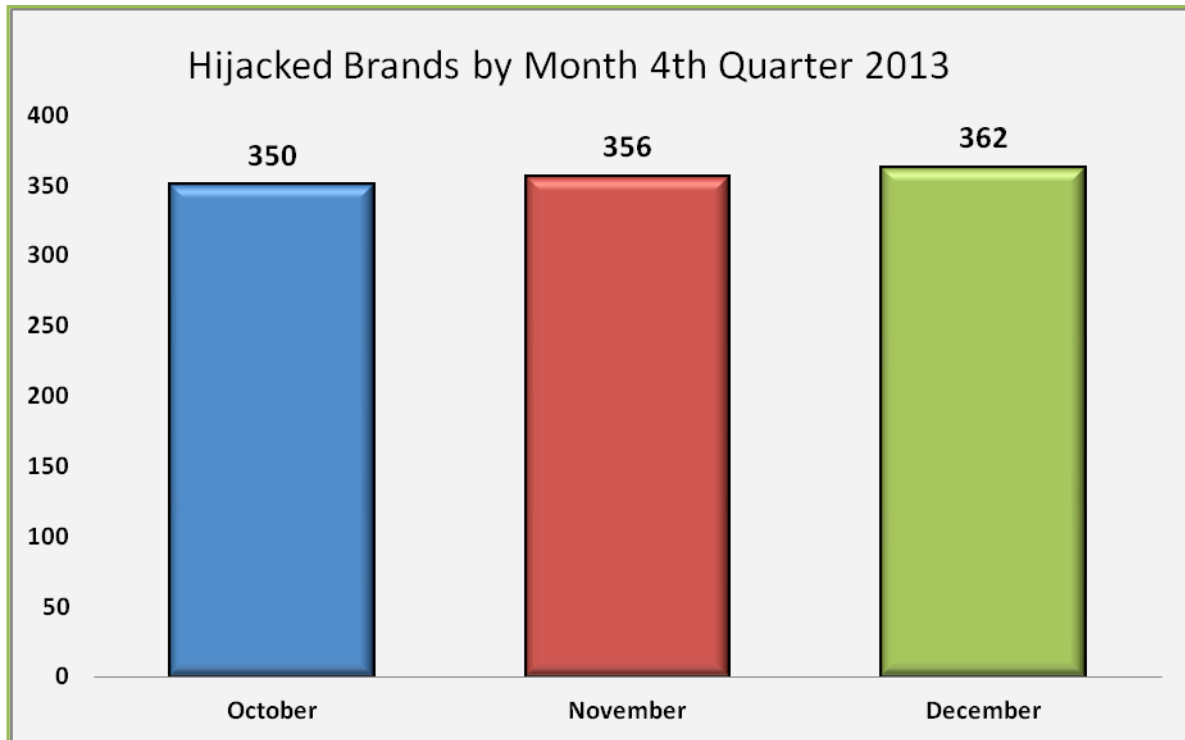
“Two thousand thirteen enters the ‘top three’ of most-phished years since MarkMonitor started tracking statistics almost 10 years ago,” commented Frederick Felman, Chief Marketing Officer, MarkMonitor. “Unfortunately, today’s high levels of phishing attacks are not the result of another unusual spike; it is just the new normal as phishers continue to improve their techniques and broaden their targets.”

	October	November	December
Number of Unique Phishing Web Sites Detected	31,876	37,007	42,890
Unique Domains	9,028	9,211	8,831
Unique Brand-Domain Pairs	9,951	10,466	9,897
Unique Brands	350	356	362
URLs Per Brand	91.07	103.95	118.48

Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 4th Quarter 2013

The number of brands targeted in a month was down from the all-time high of 441 that was recorded in April 2013. The number of hijacked brands remained relatively level during the three-month period.

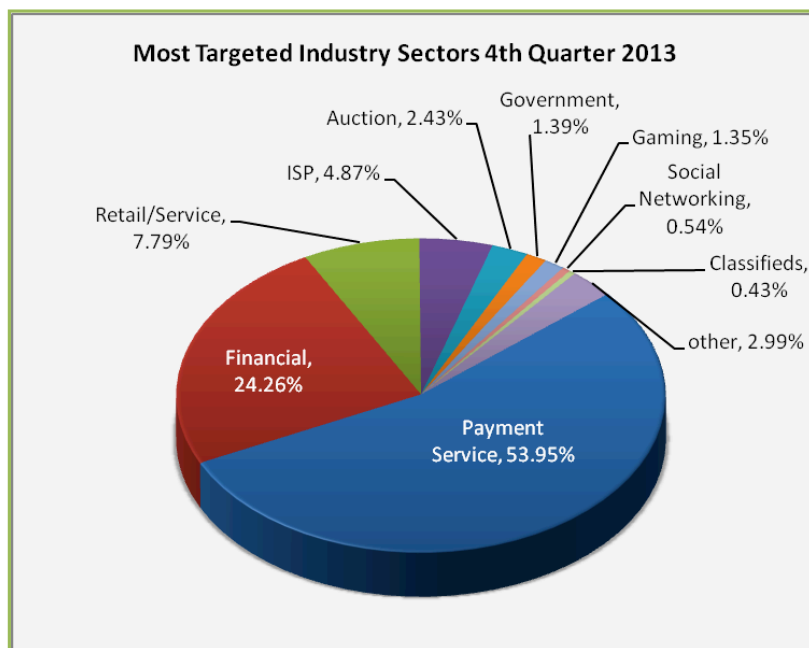
During the second half of 2013, APWG contributor IID observed 840 unique target institutions, up significantly from the 720 found in the second half of 2013. As always, a small number of brands were targeted frequently, with a larger number of brands attacked only once or twice during the period.



Phishing Activity Trends Report, 4th Quarter 2013

Most-Targeted Industry Sectors – 4th Quarter 2013

Payment Services continued to be the most-targeted industry sector throughout 2013, representing nearly 54 percent of attacks in Q4. Attacks targeting ISPs declined from 8.52 percent in Q1 to 4.87 percent in Q4.



Countries Hosting Phishing Sites – 4th Quarter 2013

The United States continued to be the top country where phishing sites are hosted during the fourth quarter of 2013. This is mainly due to the fact that a significant percentage of the world's Web sites and domain names are hosted in the United States, and that most phishing sites sit on compromised web servers.

October		November		December	
United States	54.04%	United States	48.17%	United States	57.56%
China	12.80%	Netherlands	8.01%	Hong Kong	4.56%
Germany	4.01%	Germany	5.83%	Germany	4.26%
United Kingdom	3.24%	France	3.02%	France	3.16%
France	2.96%	Canada	2.79%	United Kingdom	2.83%
Canada	2.69%	United Kingdom	2.75%	Russian Federation	2.63%
Russian Federation	1.71%	Russian Federation	2.72%	Netherlands	2.29%
Brazil	1.50%	Singapore	2.22%	Turkey	1.81%
Netherlands	1.46%	Brazil	1.88%	Canada	1.72%
Spain	1.36%	Turkey	1.39%	Rep. of Korea	1.25%

Phishing Activity Trends Report, 4th Quarter 2013

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 – 4th Quarter 2013

During the last quarter of 2013, APWG member company PandaLabs gathered a record 11.5 million new malware samples. By the end of 2013, PandaLabs' database contained a grand total of approximately 145 million unique malware samples. Many of these were slight variations on a much smaller number of malware families, created when malware morphed its code in order to avoid detection by antivirus programs. This activity accelerated as the year went on, and 37 percent of the malware created during 2013 showed up during Q4.

New Malware Strains in Q4	% of malware samples	Malware Infections by Type	% of malware samples
Trojans	60.76%	Trojans	73.11%
Viruses	4.32%	Viruses	4.99%
Worms	19.25%	Worms	5.01%
Adware/Spyware	19.26%	Adware/Spyware	13.90%
Other	0.09%	Other	2.98%

Trojans continue to be the most common type of malware, and represented 73.11 percent of malware infections. And according to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, PandaLabs has been working to detect and classify more adware/toolbar programs, at the request of customers. Based on this initiative, the share of malware that was adware/spyware found by PandaLabs rose from just 0.57% in Q3 to 13.90 percent in Q3.

In the fourth quarter of 2013, 28.39 percent of the computers analyzed by PandaLabs worldwide appeared to be infected with malware. That global infection rate is one of the lowest that PandaLabs has ever recorded, which is indeed good news. China has the highest infection rate by far -- 53.85 percent of all computers analyzed there were infected. Asia and Latin America were the regions with the highest number of computer infections. Eight of the ten least-infected countries were in Europe.

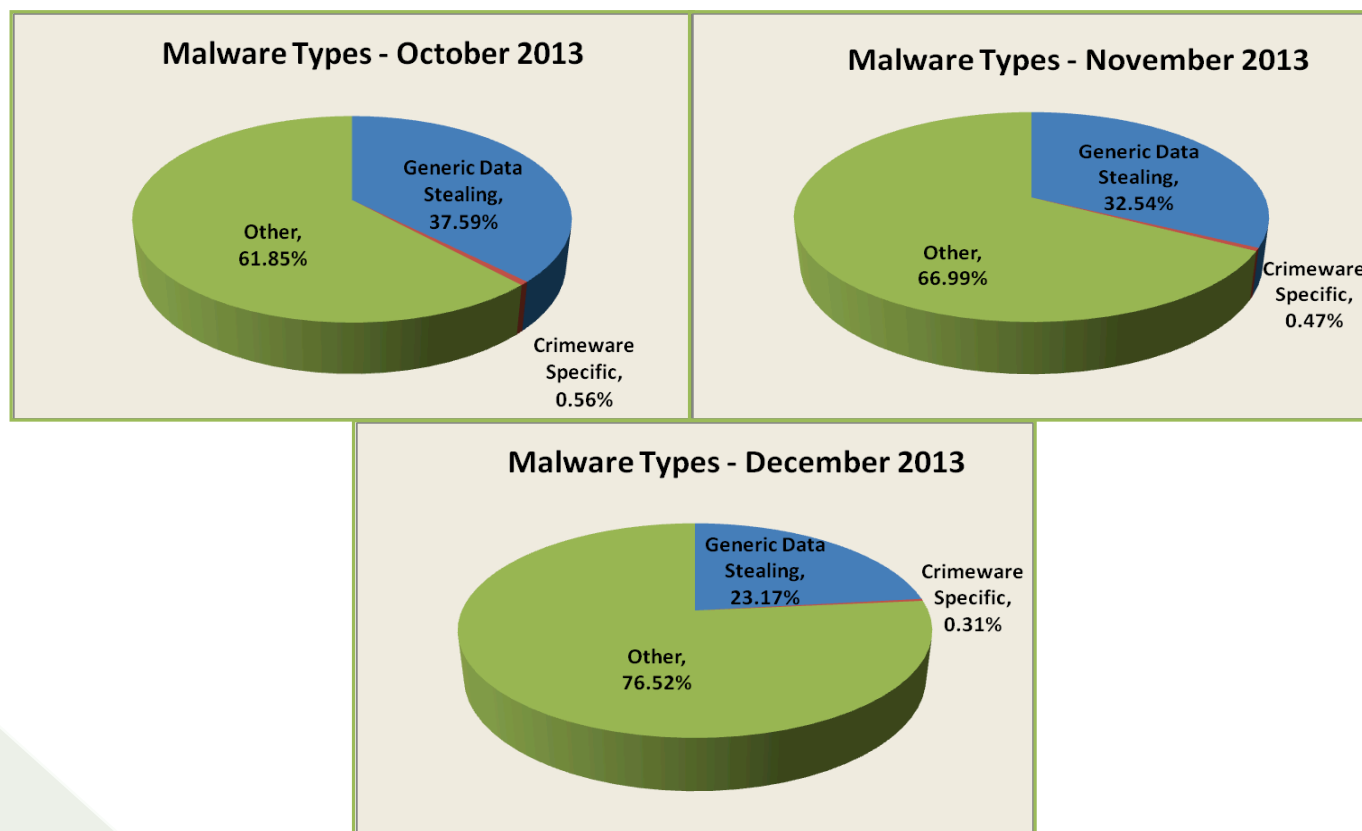
Highest Ranking	Country	Infection Rate	Lowest Ranking	Country	Infection Rate
1	China	53.85%	45	Sweden	16.18%
2	Taiwan	39.57%	44	United Kingdom	18.18%
3	Turkey	37.50%	43	Portugal	18.55%
4	Poland	36.65%	42	Switzerland	19.23%
5	Peru	35.63%	41	Germany	20.69%
6	Russia	34.55%	40	France	21.02%
7	Argentina	34.42%	39	Netherlands	21.07%
8	Canada	34.31%	38	Venezuela	23.13%
9	Colombia	33.33%	37	United States	23.85%
10	Brazil	32.25%	36	Spain	26.82%

Phishing Activity Trends Report, 4th Quarter 2013

Measurement of Detected Crimeware – 4th 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.)



"Phishing emails form a dangerous stage of the attack lifecycle," said Carl Leonard of Websense Security Labs. "Attackers can craft very convincing lures to bypass existing security solutions and deliver their payloads into an organisation. We found that 3.3 percent of all unwanted mail contains malicious links and other malicious content that lead unwary readers to malware download sites. Three percent may not appear to be a large number, but when viewed in light of the billions of spam emails that are sent each year, it is evident that building web intelligence into a security solution can significantly enhance an organisation's security posture."

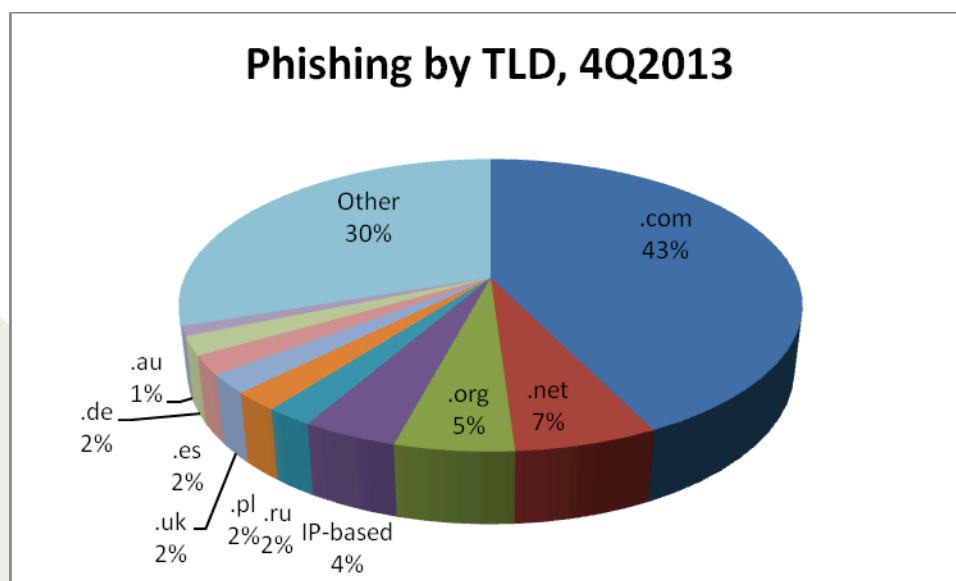
Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

The United States remained the top country that hosted phishing-based Trojans and downloaders during the three-month period. 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, and that much malware is distributed from compromised web servers.

October		November		December	
United States	53.25%	United States	29.05%	United States	44.64%
China	8.48%	China	13.40%	Europe	10.01%
Germany	5.56%	Europe	8.85%	Hungary	8.33%
Spain	4.62%	Ukraine	7.49%	Ukraine	7.87%
Russian Federation	3.96%	Rep. of Korea	7.27%	China	4.82%
Poland	3.57%	Poland	5.25%	Netherlands	4.15%
France	3.28%	Russian Federation	4.88%	Russian Federation	3.62%
Netherlands	3.25%	Ireland	4.31%	Germany	2.22%
Rep. of Korea	2.28%	France	3.77%	Rep. of Korea	1.94%
Ukraine	1.21%	Netherlands	2.49%	France	1.89%






Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing sites. Forty-three percent of domains used for phishing were .COM names; .COM TLD represents approximately 42 percent of domain names registered worldwide. Phishing declined in the TLD of Brazil (.BR), which had 4 percent of phishing worldwide in the third quarter but only about 1 percent in the fourth quarter.



Phishing Activity Trends Report, 4th Quarter 2013

APWG Phishing Activity Trends Report Contributors

 <p>Illumintel provides advising and security services to top-level-domain registry operators, Internet companies, and intellectual property owners.</p>	 <p>Internet Identity (IID) is a US-based provider of technology and services that help organizations secure their Internet presence.</p>	 <p>MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.</p>
 <p>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.</p>	 <p>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.</p>	

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 lcorrns@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.

11

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