

# Phishing Activity Trends Report

3<sup>rd</sup> Quarter

2014

APWG

Unifying the  
Global Response  
To Cybercrime

July – September 2014

*Published March 30, 2015*

## 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.

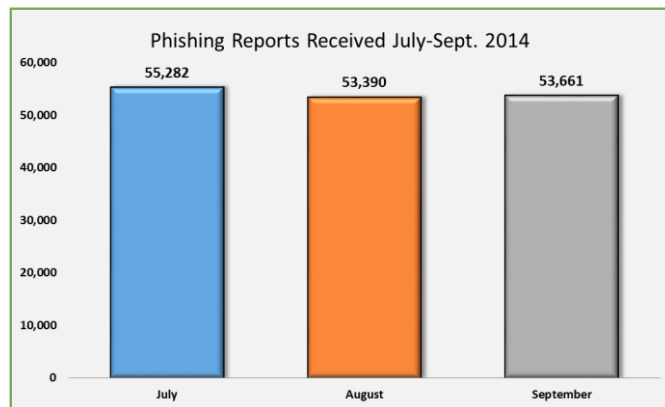
## Phishing Defined

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

Statistical Highlights for 3rd Quarter 2014	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

## Number of Phishing Email Reports Steady in Q3 2014



The number of unique phishing reports submitted to APWG during Q3 was 163,333. This was a decrease of 5 percent from the 171,801 received in Q2 of 2014. [p. 4]

## 3rd Quarter 2014 Phishing Activity Trends Summary

- A total of 549 brands were targeted by phishers in Q4, up from the 531 targeted in the second quarter of 2014. [p. 6]
- The total number of phish observed in Q3 was 92,473, a 28 percent decrease from Q2 2014, although this may be a statistical anomaly. [p. 4]
- In July, phishers broke into Polish servers, with the result that Poland jumped to #2 in the global ranking of countries that hosted phishing content. The United States continued to be ranked number one. [p.7]
- Over 20 million new malware samples were discovered during Q3, an average of 227,747 new malicious files every day. [p. 8]
- The United States remained the top country for hosting phishing-based Trojans and downloaders during the three month period. [p. 10]

## 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.

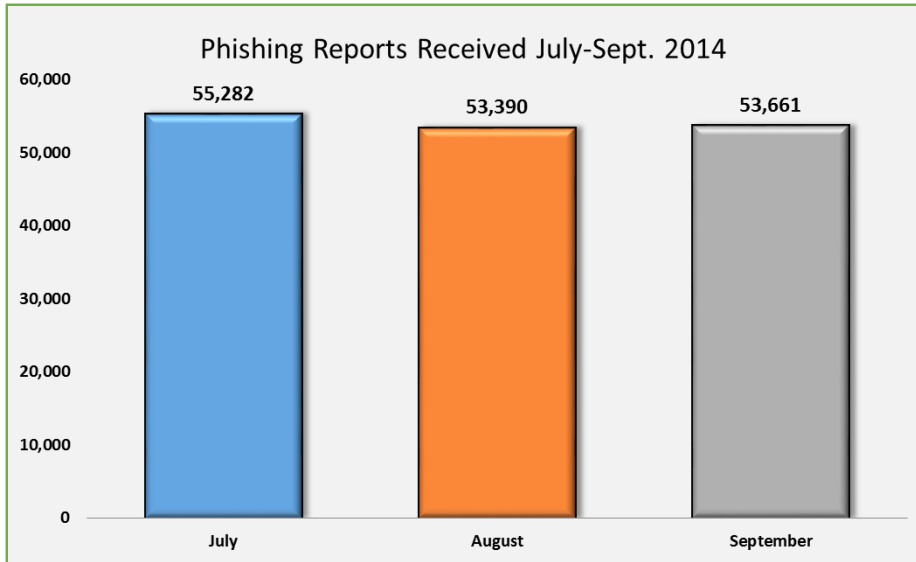
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances (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 3rd Quarter 2014

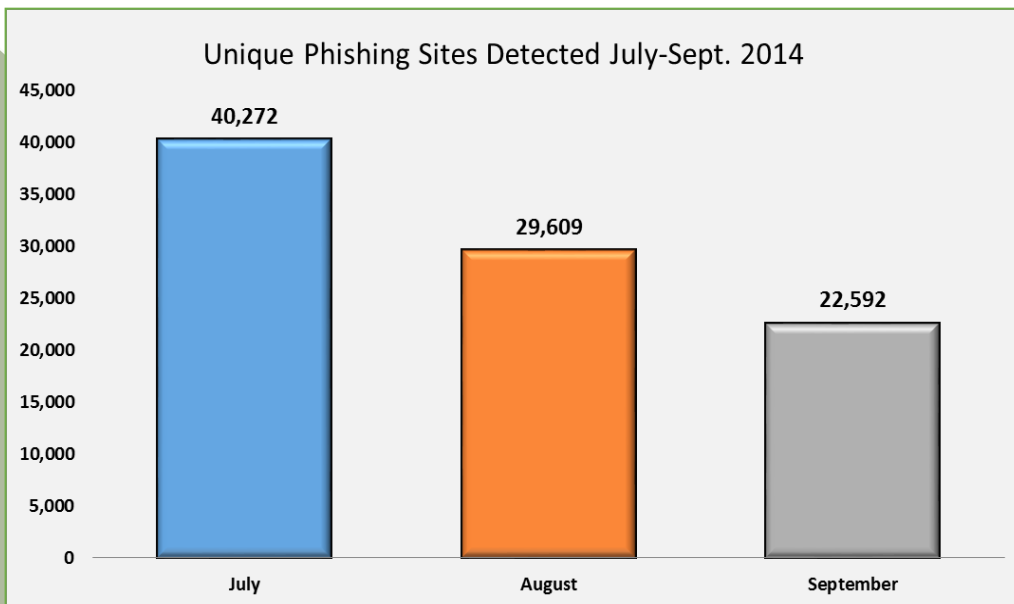
	July	August	September
Number of unique phishing websites detected	40,272	29,609	22,592
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	55,282	54,390	53,661
Number of brands targeted by phishing campaigns	361	349	340
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	43.20%	47.70%	45.97%
Percentage of sites not using port 80	0.52%	0.51%	0.83%

## Phishing E-mail Reports and Phishing Site Trends – 3<sup>rd</sup> Quarter 2014

The number of unique phishing reports submitted to APWG during Q3 was 163,333, a decrease of 5 percent from the 171,801 received in Q2 of 2014. The number of unique phishing reports submitted to APWG remained consistent during the three-month period, between a high of 55,282 in July to 53,661 in September.

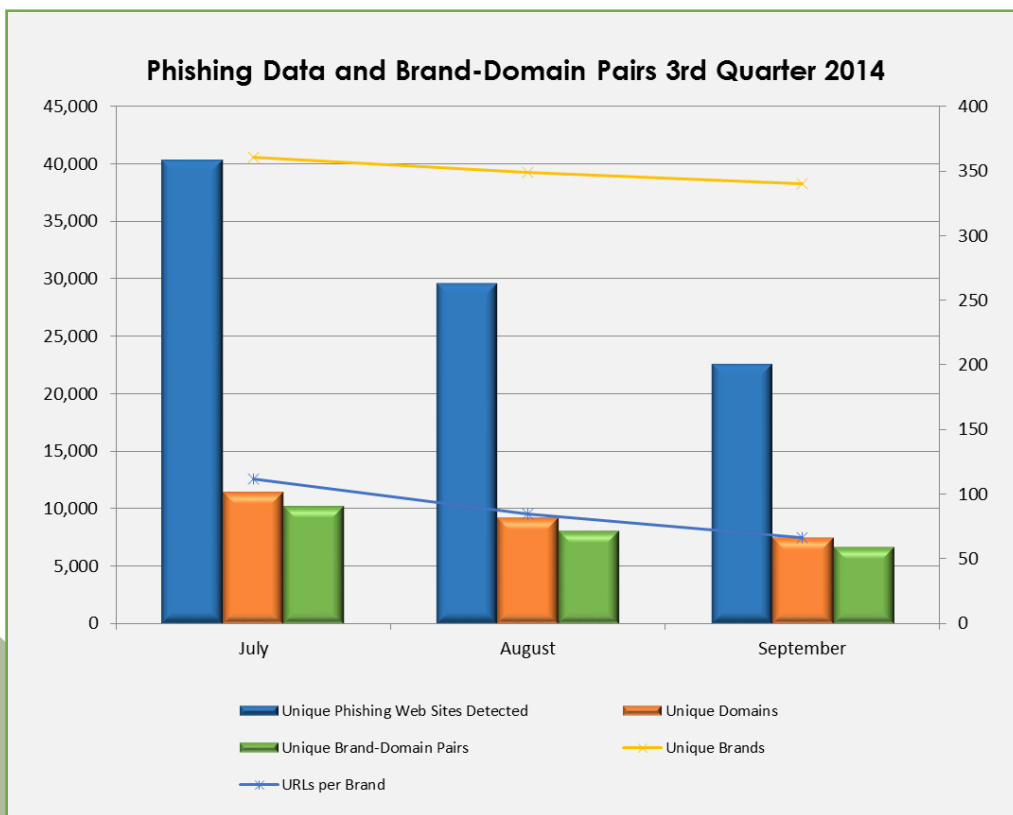


The total number of phish observed in Q3 was 92,473, a 28 percent decrease from Q2 2014, when a total of 128,378 were observed. The quarter saw a drop from July to September, with a decline of over 17,600 sites. Note: The decrease is due in part to a shift in measurement methodology by APWG member MarkMonitor.



## Brand-Domain Pairs Measurement – 3<sup>rd</sup> Quarter 2014

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.

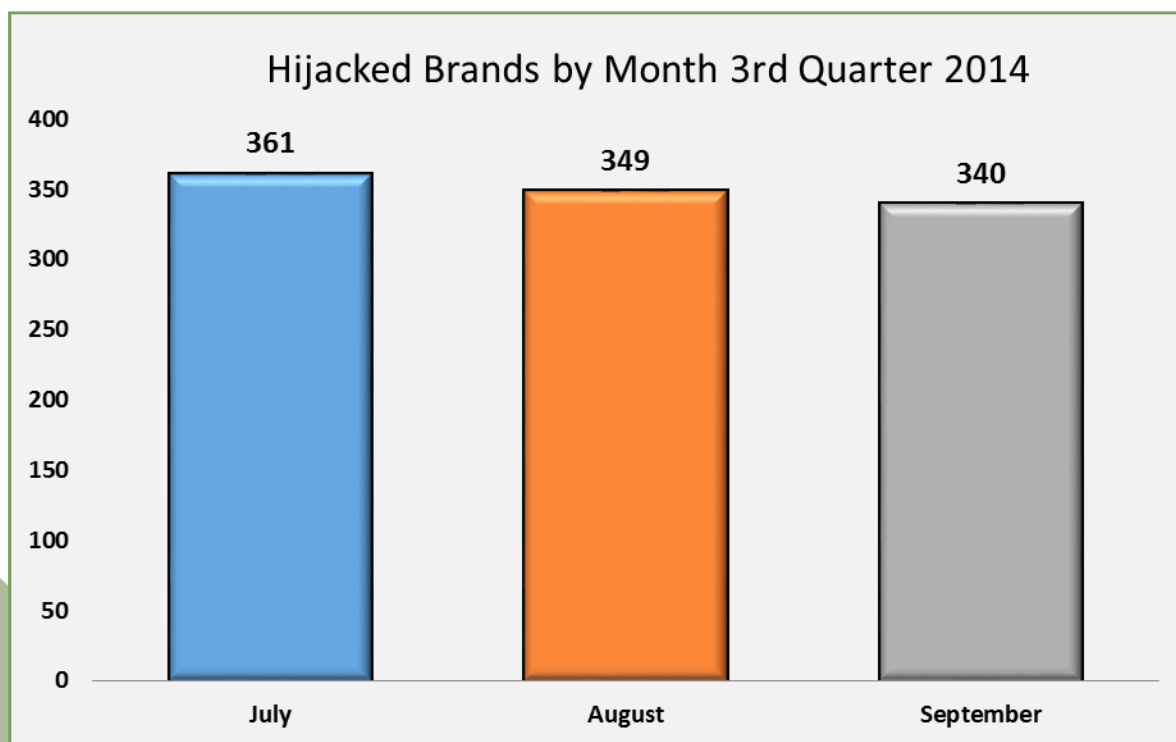


	July	August	September
Number of Unique Phishing Web Sites Detected	40,272	29,609	22,592
Unique Domains	11,500	9,225	7,531
Unique Brand-Domain Pairs	10,265	8,075	6,688
Unique Brands	361	349	340
URLs Per Brand	111.55	84.83	66.44



## Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 3<sup>rd</sup> Quarter 2014

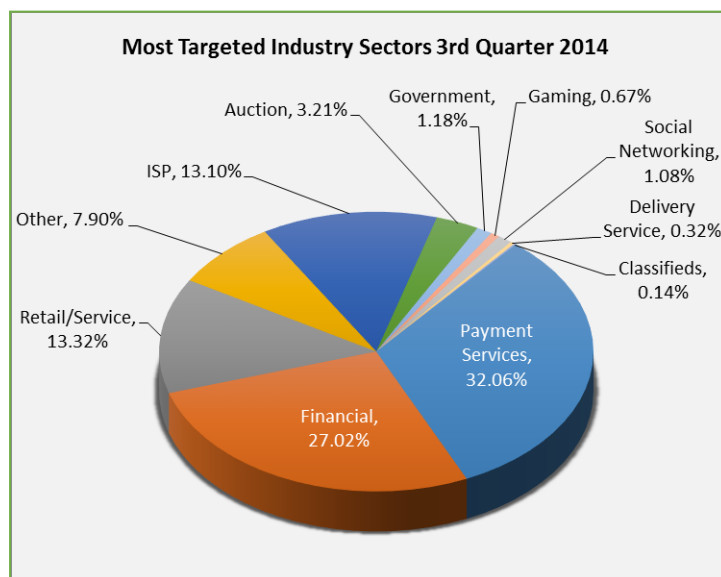
A grand total of 549 brands were targeted by phishers in Q4, up from the 531 targeted in the second quarter of 2014. The monthly high for the quarter was July with 361 brands reportedly targeted by phishers. The number of brands targeted in any given month remained below the all-time high of 441, which was recorded in April 2013.



# Phishing Activity Trends Report, 3<sup>rd</sup> Quarter 2014

## Most-Targeted Industry Sectors – 3rd Quarter 2014

Payment Services continued to be the most-targeted industry sector in the third quarter of 2014, with 32 percent of attacks during the three-month period.



“Healthcare records hold a treasure trove of data that is valuable to an attacker,” said Carl Leonard of Websense Security Labs. “That data can be used in a multitude of different follow-up attacks and fraud. In a break-in we observed, the method of entry was a phishing email purporting to be from the employees’ local IT team, asking the team members to log in to their corporate email system. The resulting webpage served to end users being a fraudulent login page under the control of the attackers.”

## Countries Hosting Phishing Sites – 3rd Quarter 2014

The United States continued to be the top country where phishing sites were hosted during the third quarter of 2014. Websense Security Labs noticed that phishers broke into Polish servers in July 2014, with the result that Poland briefly jumped to the #2 spot:

	July	August	September	
United States	31.48%	United States	32.43%	
Poland	22.01%	Netherlands	8.61%	
Lithuania	6.57%	China	6.57%	
China	6.18%	Slovakia	6.29%	
Germany	4.28%	France	5.21%	
Norway	4.16%	Lithuania	4.83%	
United Kingdom	2.51%	Norway	3.47%	
Hong Kong	2.14%	Germany	3.09%	
France	2.13%	United Kingdom	2.88%	
Canada	1.75%	Canada	2.40%	
			United States	43.97%
			Ukraine	7.30%
			Netherlands	4.87%
			Hong Kong	3.52%
			France	3.48%
			United Kingdom	2.91%
			Germany	2.68%
			Canada	2.35%
			Poland	2.28%
			Czech Republic	2.13%

## 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 – 3rd Quarter 2014

According to APWG member PandaLabs, the number of new malware samples in circulation rose significantly during the first half of the year, doubling last year's figure and reaching an average of 160,000 new samples created every day. In Q3, PandaLabs recorded over 20 million new malware samples, at an average of 227,747 new malicious items per day.

The majority of these malware threats do not belong to new families developed from scratch, but are variants of well-known malware specimens modified by their creators to evade detection systems. The malware included in the "Other" (which includes PUP - Potentially Unwanted Programs) and "Adware/Spyware" categories seems to be particularly efficient, as these specimens are capable of infecting proportionately more computers with fewer samples. This is software that uses aggressive means to reach computers, from bundling with free applications to using installers that distribute legitimate software but install other types of applications without user consent.

New Malware Strains in Q3	% of malware samples
Trojans	78.08%
Viruses	8.89%
Worms	3.92%
Adware/Spyware	2.19%
Other	6.92%

Malware Infections by Type	% of malware samples
Trojans	75.00%
Viruses	1.47%
Worms	2.09%
Adware/Spyware	6.88%
Other	14.55%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, the global infection rate was 37.93 percent, slightly up from past quarters. China is once again in pole position, with an infection rate of 49.83 percent. This is the first time in a long while that China has an infection ratio below 50 percent.

The highest positions in the ranking are held by Asian and Latin American countries. Other countries with rates above the global average include: Poland (39.48%), Brazil (39.21%), Slovenia (39.05%), Colombia (38.86%), Spain (38.37%), Costa Rica (38.19%), Chile (38.05%) and Italy (37.97%). Europe in general is the area with the lowest infection rates.

Ranking	Country	Infection Rate
1	China	49.83%
2	Peru	42.38%
3	Bolivia	42.12%
4	Turkey	41.45%
5	Russia	41.38%
6	Argentina	41.03%
7	Ecuador	40.57%
8	Taiwan	40.21%
9	El Salvador	39.89%
10	Guatemala	39.58%

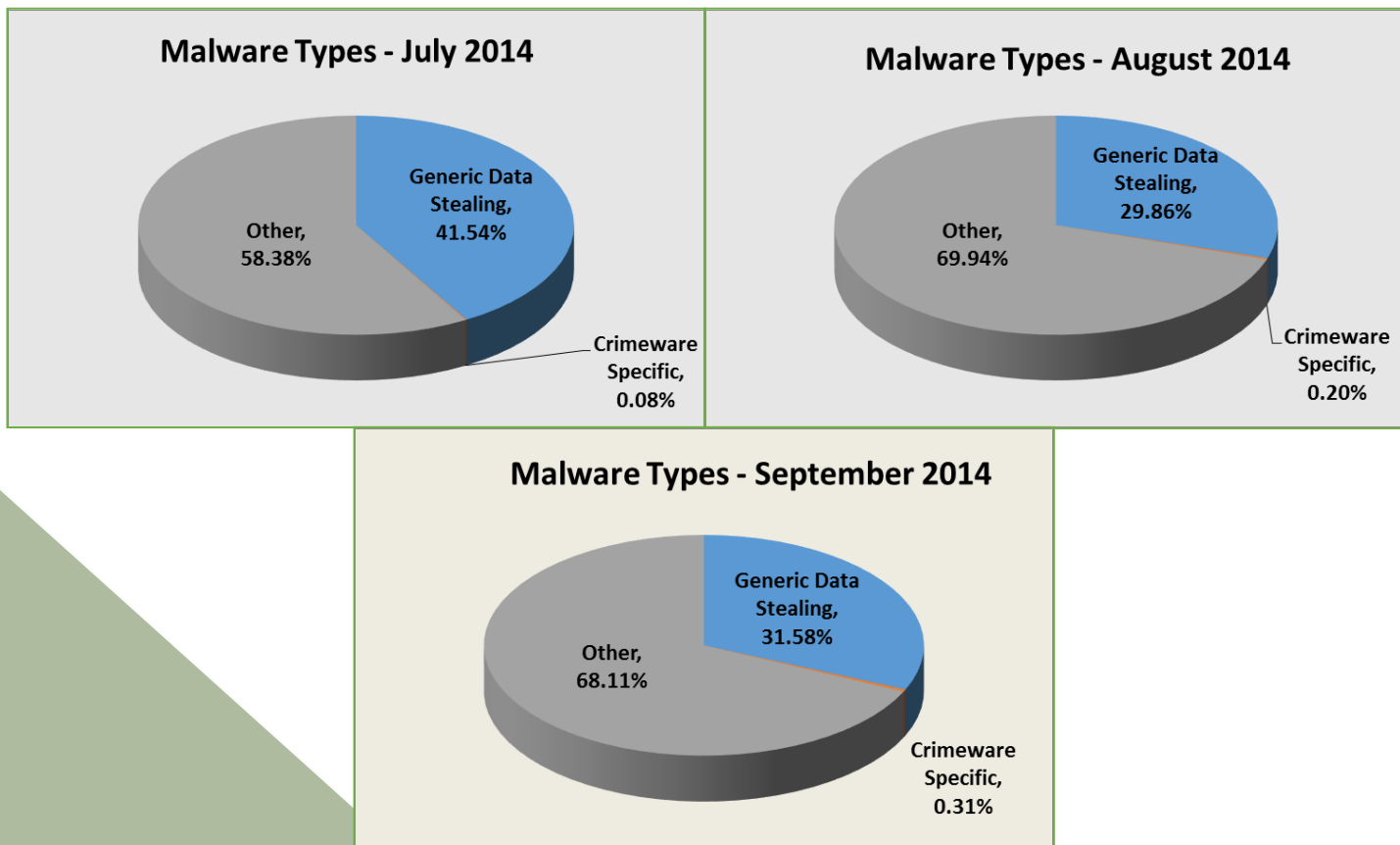
Ranking	Country	Infection ratio
45	Portugal	27.83%
44	Belgium	27.39%
43	Netherlands	26.96%
42	Germany	26.52%
41	France	25.87%
40	UK	25.11%
39	Switzerland	24.61%
38	Japan	24.02%
37	Sweden	23.44%
36	Norway	23.07%



## Measurement of Detected Crimeware – 3<sup>rd</sup> Quarter 2014

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.)



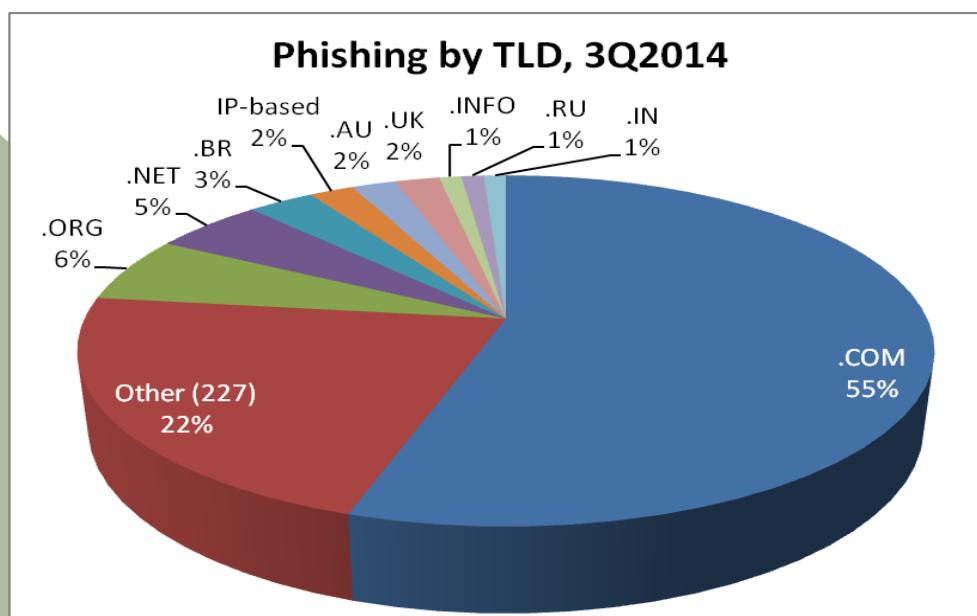
## Phishing-based Trojans and Downloader Hosting Countries (by IP address)

The United States remained the top country where phishing-based Trojans and downloaders were hosted during the three-month period. This is due to the sheer amount of hosting located in the USA, which is vulnerable to break-in.

July		August		September	
United States	61.32%	United States	69.31%	United States	77.44%
China	10.35%	China	6.96%	China	5.82%
Netherlands	3.21%	France	2.66%	Netherlands	1.83%
Russian Federation	2.33%	Germany	2.15%	Ukraine	1.83%
France	1.99%	Russian Federation	1.74%	France	1.51%
Czech Republic	1.90%	Netherlands	1.74%	Switzerland	1.24%
Republic of Korea	1.85%	Ukraine	1.74%	Brazil	1.19%
Germany	1.80%	Brazil	1.56%	Russian Federation	1.10%
Brazil	1.36%	Republic of Korea	1.51%	Germany	0.96%
Poland	1.31%	United Kingdom	1.10%	Poland	0.78%






## Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing sites. Fifty-five percent of domains used for phishing were .COM names, up from 46 percent in the previous quarter. The .COM TLD represents approximately 44 percent of domain names registered worldwide. The TLD of Brazil (.BR) continued to have 3 percent of phishing worldwide, but only 1 percent of the world domain name market.



# Phishing Activity Trends Report, 3<sup>rd</sup> Quarter 2014

## APWG Phishing Activity Trends Report Contributors

 <p>Illumintel Inc. 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, a 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](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); Websense at [publicrelations@websense.com](mailto:publicrelations@websense.com), or [ATmedia@internetidentity.com](mailto:ATmedia@internetidentity.com)

## About the APWG

Founded in 2003 as the Anti-Phishing Working Group, APWG is a non-profit industry association focused on eliminating the identity theft and fraud that result from phishing, crimeware, and message spoofing. Membership is open to qualified financial institutions, retailers, ISPs, solutions providers, law enforcement, government agencies, multi-lateral treaty organizations, and NGOs. More than 2,000 enterprises worldwide are APWG members. eCrime being a sensitive subject, APWG maintains a policy of member confidentiality.

Websites of APWG public-service enterprises include its public website, <http://www.apwg.org> and its European chapter <http://www.apwg.eu>; the 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 computing devices and their users – and advisories 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, APWG was established as an independent corporation controlled by its board of directors, its executives and its steering committee.

11

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