



Phishing Activity Trends Report

3rd Quarter

2013

APWG

Unifying the
Global Response
To Cybercrime

July – September 2013

Published February 10, 2014

Phishing Activity Trends Report, 3rd 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.

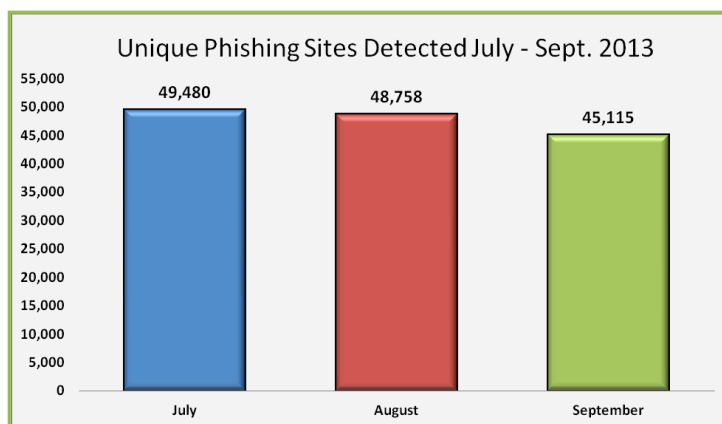
Phishing Defined

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

Statistical Highlights for 3rd 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 Up 20%; Fraudsters Seek Targets of Highest Return



Overall phishing activity was up by 20 percent from the previous quarter despite an 8 percent decline in the number of brands targeted.

3rd Quarter 2013 Phishing Activity Trends Summary

- The number of unique phishing websites detected jumped from June to July, and stayed at relatively elevated levels through the third quarter. [p. 4]
- The number of hijacked brands declined slightly, as phishers stopped targeting less-lucrative targets. [pp. 5-6]
- Trojans remained the most popular form of malware, and a record number of new malware strains were detected in the third quarter. [p. 8]
- More than 59 percent of computers in China appeared to be infected with malware, a record high for any country. [p. 8]
- Forty-two percent of domains used for phishing were .COM names, down from 44 percent in the previous quarter [p. 10]
- The United States continued to be the top country hosting phishing sites during the third quarter of 2013. [p. 7]

Phishing Activity Trends Report, 3rd Quarter 2013

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.

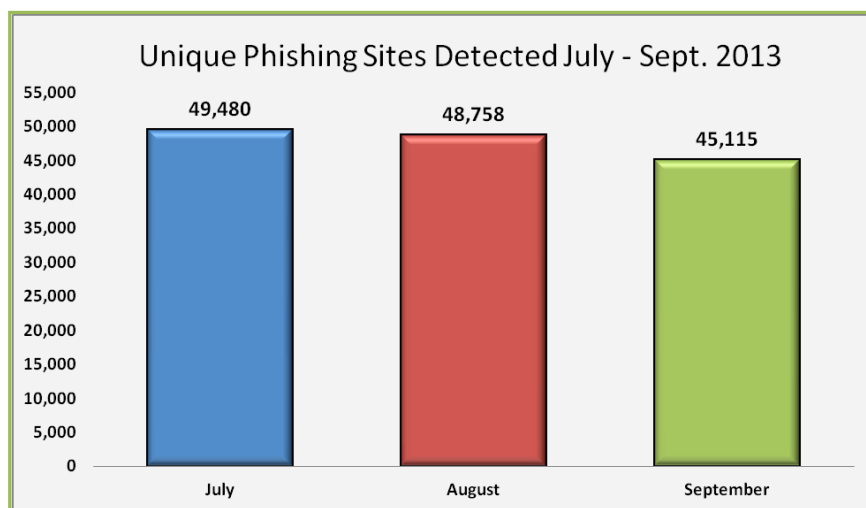
Statistical Highlights for 2nd Quarter 2013

	July	August	September
Number of unique phishing websites detected	49,480	48,758	45,115
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	61,453	61,792	56,767
Number of brands targeted by phishing campaigns	390	400	379
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	35.24%	73.51%	56.22%
No hostname; just IP address	0.15%	3.20%	1.73%
Percentage of sites not using port 80	0.04%	0.32%	0.86%

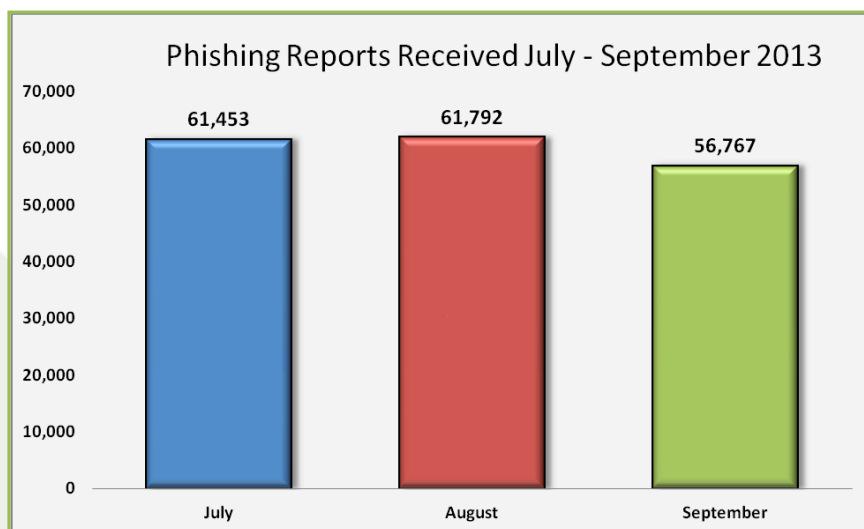
Phishing Activity Trends Report, 3rd Quarter 2013

Phishing E-mail Reports and Phishing Site Trends – 3rd Quarter 2013

The number of phishing sites detected jumped almost 30 percent, from 38,110 in June 2013 to 49,480 in July 2013, and stayed at the higher rate through the third quarter. The total number of phish observed in Q3 was 143,353, a 20 percent increase over Q2's 119,101. The rise is generally attributable to an increased number of attacks against money transfer sites and retail/e-commerce sites (see page 7).



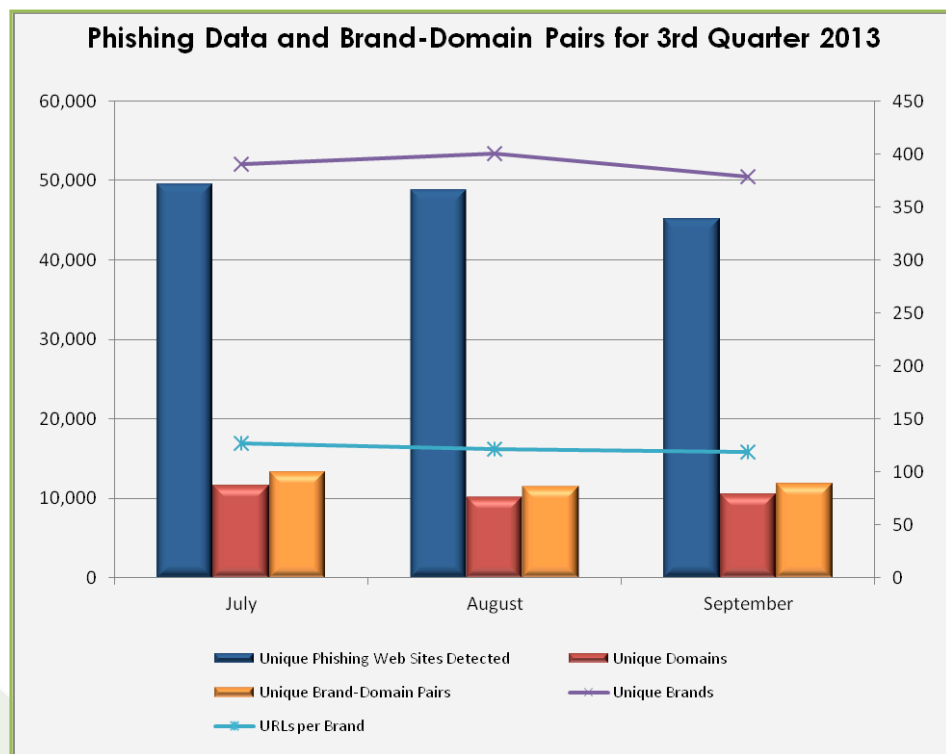
The APWG recently updated its database of phishing signatures. This allows us to better examine incoming e-mail reports from consumers and confirm which contained phishing attempts as opposed to other types of spam and scams. The revisions did not notably affect the number of confirmed phishing sites found, but did validate a higher number of incoming reports than in previous quarters. The number of unique phishing reports submitted to APWG during the quarter remained relatively consistent.



Phishing Activity Trends Report, 3rd Quarter 2013

Brand-Domain Pairs Measurement – 3rd 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 fell from an all-time high of 441 in April 2013 to 379 in September. The number of unique brand-domain pairs dropped during Q3 as well.

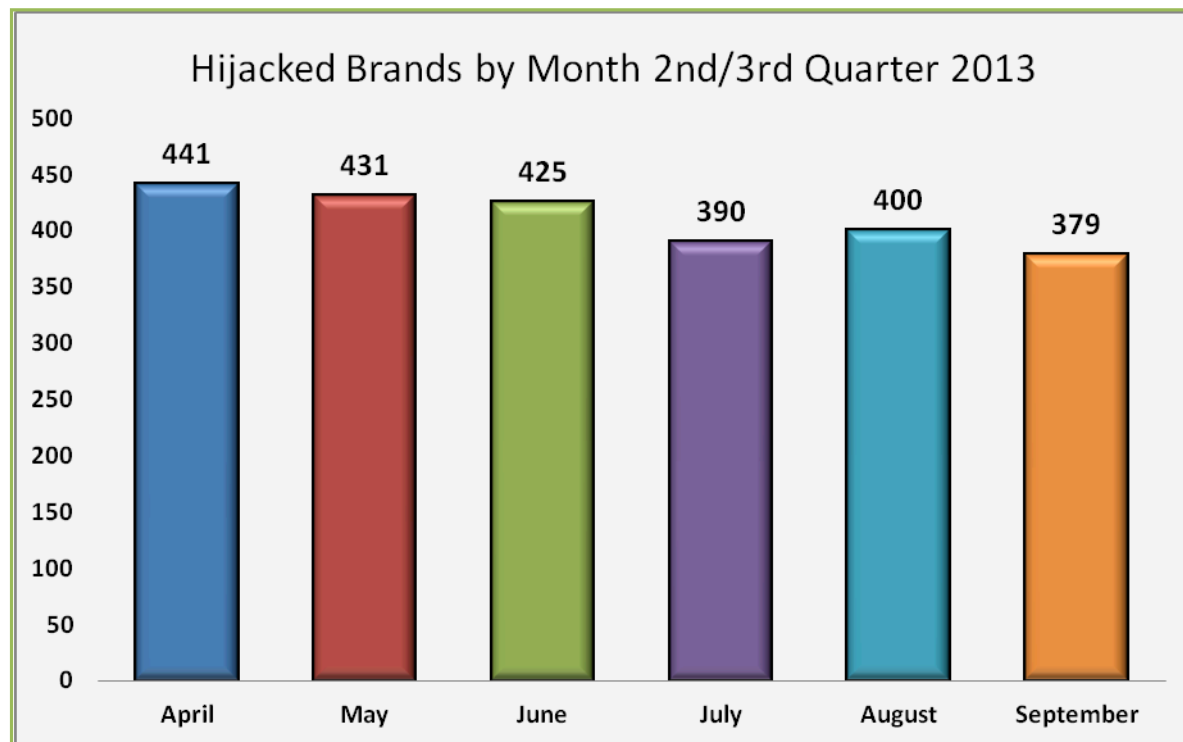
"Overall phishing activity is up by 20 percent from the previous quarter despite an 8 percent decline in the number of brands targeted. Fraudsters look for profit and zoomed in on the brands that deliver the highest returns," said Ihab Shraim, CISO and Vice President Anti-Fraud Engineering and Operations, MarkMonitor.

	July	August	September
Number of Unique Phishing Web Sites Detected	49,480	48,758	45,115
Unique Domains	11,607	10,051	10,419
Unique Brand-Domain Pairs	13,252	11,395	11,803
Unique Brands	390	400	379
URLs Per Brand	126.87	121.89	119.03

Phishing Activity Trends Report, 3rd Quarter 2013

Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 3rd Quarter 2013

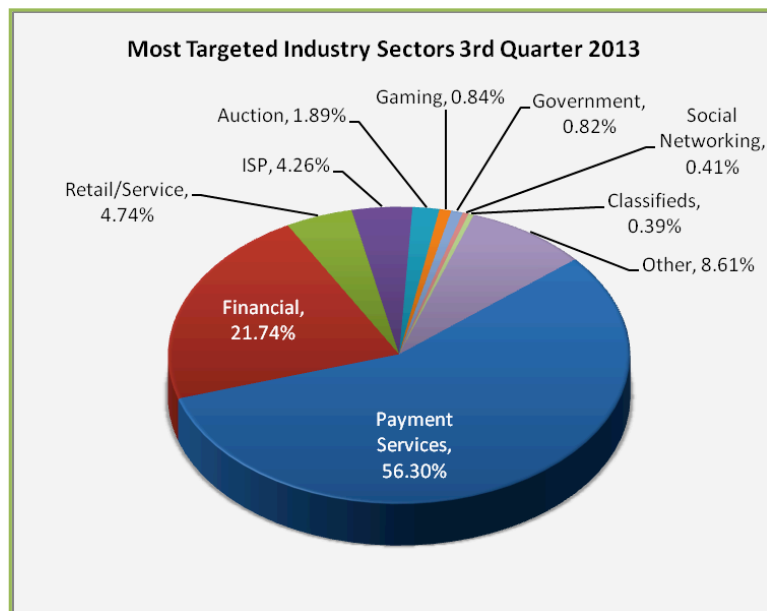
The number of brands targeted fell from an all-time high of 441 in April 2013 to 379 in September 2013. Month to month, the number of hijacked brands remained relatively consistent, while maintaining a high level of total brands that was also consistent with Q2 2014.



Phishing Activity Trends Report, 3rd Quarter 2013

Most-Targeted Industry Sectors – 3rd Quarter 2013

Payment Services continued to be the most-targeted industry sector throughout 2014. Gaming has experienced the most drastic changes during 2014, dropping from 5.66 percent in Q1 2013 to 0.84 percent in Q3 2013.



Countries Hosting Phishing Sites – 3rd Quarter 2013

The United States continued to be the top country hosting phishing sites during the third 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 there.

July		August		September	
United States	58.78%	United States	50.60%	United States	52.58%
Canada	4.21%	France	5.85%	Germany	5.68%
Germany	3.55%	Canada	4.56%	United Kingdom	5.15%
Ukraine	3.32%	Netherlands	4.23%	France	3.35%
Russian Federation	3.05%	Germany	4.08%	Brazil	3.21%
United Kingdom	2.47%	Romania	3.83%	Russian Federation	3.03%
Brazil	2.35%	Russian Federation	3.16%	Netherlands	2.60%
Turkey	2.32%	China	2.89%	Canada	2.21%
France	2.21%	United Kingdom	2.49%	Romania	1.58%
Netherlands	2.21%	Turkey	2.47%	Turkey	1.37%

Phishing Activity Trends Report, 3rd 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 – 3rd Quarter 2013

Malware creation hit a new record high in the third quarter of 2013. APWG member PandaLabs cataloged nearly 10 million new malware samples from July to September, and PandaLabs observed that the number of new malware samples in circulation in the first nine months of 2013 was larger than the total for all of 2012.

Type of Malware Identified	% of malware samples
Trojans	76.85%
Worms	13.12%
Viruses	9.23%
Adware/Spyware	0.57%
Other	0.23%

Malware Infections by Type	% of malware samples
Trojans	78.00%
Worms	5.67%
Viruses	6.63%
Adware/Spyware	6.05%
Other	3.65%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, Trojans were once again the most prevalent type of malware, accounting for 76.85 percent of all new samples identified, and continued to be the weapon of choice for malware writers. It is worth noting the slight increase in the number of adware and spyware infections, at 6.05 percent.

In the third quarter of 2013, 31.88 percent of computers worldwide appeared to be infected with some sort of malware or adware/spyware, almost a full point lower than in the second quarter. As for individual countries, China once again topped the list — 59.36 percent of computers there appeared to be infected according to PandaLabs, a record high. China was followed by Turkey (46.58 %), Peru (42.55 %), and several other Latin American countries.

Europe continued to have the lowest infection rates. Netherlands (19.19 %), UK (20.35 %) and Germany (20.60 %) were the countries with the fewest infections. The only non-European country in the Top Ten was Australia, in ninth place with 26.67 percent. Other countries outside this Top 10 but with infection rates below the average were: Japan (26.84 percent), Hungary (27.56 %), Venezuela (27.82 %), Colombia (29.14 %), Belgium (29.14 %), Italy (30.16 %), United States (30.58 %), Mexico (31.49 %) and Spain (31.74 %).

Ranking	Country	Infection Rate
1	China	59.36%
2	Turkey	46.58%
3	Peru	42.55%
4	Russia	41.80%
5	Taiwan	39.06%
6	Argentina	38.50%
7	Brazil	38.21%
8	Chile	36.02%
9	Poland	35.45%
10	Canada	33.83%

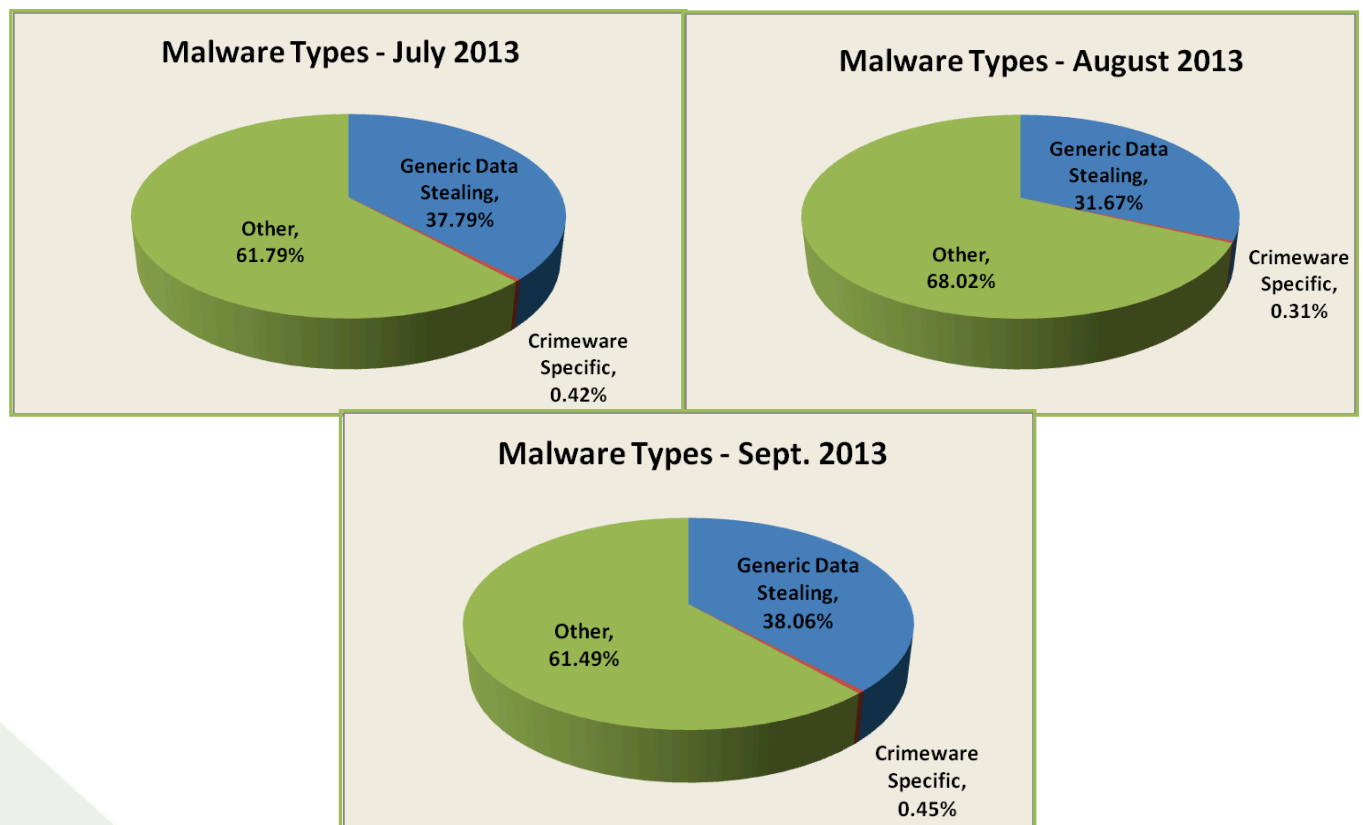
Ranking	Country	Infection ratio
35	Netherlands	19.19%
36	UK	20.35%
37	Germany	20.60%
38	Sweden	21.09%
39	Finland	21.77%
40	Portugal	21.79%
41	Denmark	23.70%
42	France	26.04%
43	Australia	26.67%
44	Switzerland	26.72%

Phishing Activity Trends Report, 3rd Quarter 2013

Measurement of Detected Crimeware – 3rd 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.)



"In the third quarter of 2013 we saw a change in the phishing themes used by malware authors. An emphasis on social media-themed subjects, such as 'Invitation to connect on LinkedIn', was used to entice users who would be used to seeing such subjects," said Carl Leonard of Websense Security Labs.

Phishing Activity Trends Report, 3rd Quarter 2013

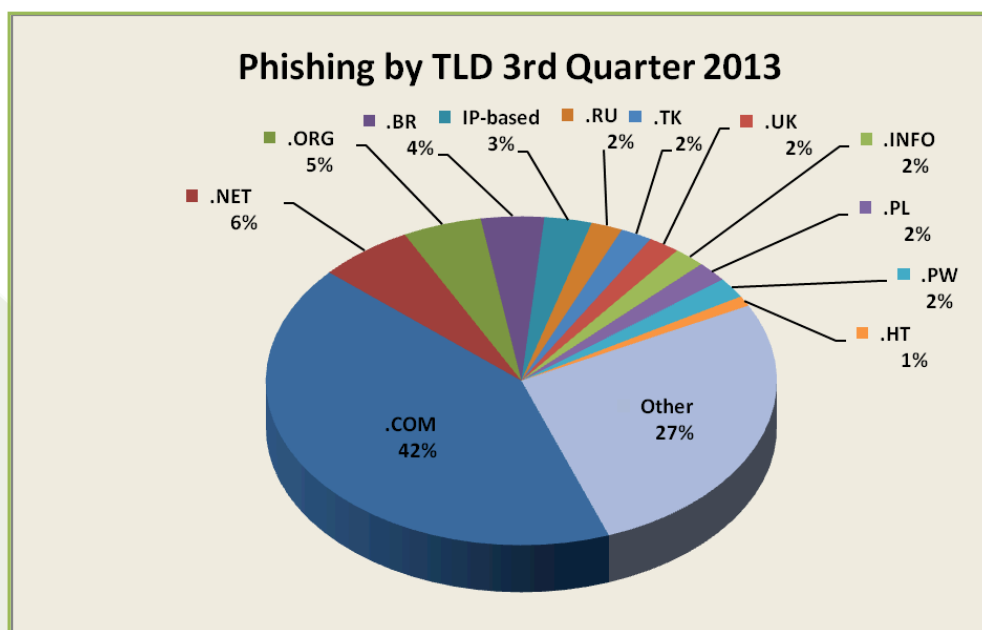
Phishing-based Trojans and Downloaders' Hosting Countries (by IP address)

The United States remained on top during the three-month span after being briefly overtaken last May by Germany as the top country hosting phishing-based Trojans and downloaders. Germany remained ranked in the top three during the quarter.

July		August		September	
United States	36.32%	United States	62.32%	United States	44.67%
Germany	25.12%	Germany	8.90%	Russian Federation	22.00%
Switzerland	11.92%	Russian Federation	6.46%	Germany	6.49%
Russian Federation	4.94%	Netherlands	4.50%	China	6.15%
Netherlands	3.87%	Switzerland	3.80%	Spain	4.26%
China	3.54%	China	3.04%	France	3.52%
Spain	2.23%	Spain	1.81%	Netherlands	2.18%
Korea Republic	1.84%	Ukraine	1.24%	Luxembourg	1.53%
France	1.07%	France	1.13%	Korea Republic	1.42%
Taiwan	0.85%	Korea Republic	1.02%	Ireland	0.81%






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 from 44 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 4 percent of phishing worldwide, but only 1 percent of the world domain name market.



Phishing Activity Trends Report, 3rd Quarter 2013

APWG Phishing Activity Trends Report Contributors

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

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