Phishing Activity Trends Report

3rd Quarter 2012

APWG

Unifying the
Global Response
To Cybercrime

July – September 2012

Published February 1, 2013

Phishing Activity Trends Report, 3rd Quarter 2012

Phishing Report Scope

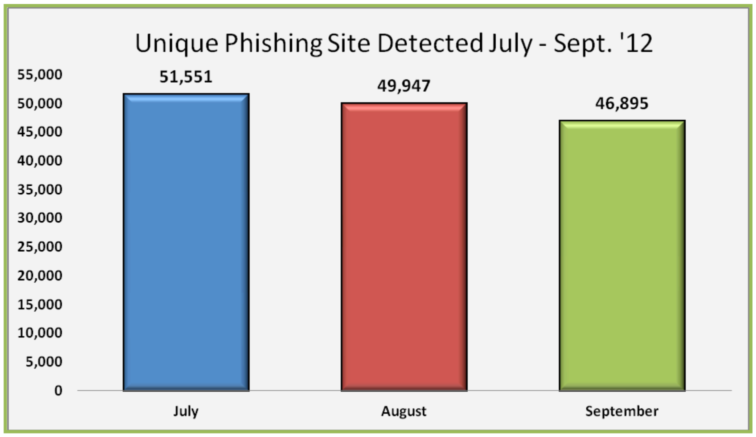
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation,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

Number of Unique Phishing Sites Declines for Six Straight Months



The second and third quarters of 2012 saw a constant decline in the number of unique phishing sites detected by the APWG [p. 4]

3rd Quarter '12 Phishing Activity Trends Summary

● The second and third quarters of 2012 saw a constant decline in the number of unique phishing sites detected by the APWG. This is a return to historical levels after a period of high activity. The decline in traditional phishing is probably due to an increase in malware-based attacks. [p. 4]

● The APWG received reports of 30,955 unique phishing sites in July – 24 percent lower than the all-time high of 40,621 reports recorded in August 2009 [p.4]

● The total number of URLs used to host phishing attacks dropped to 148,393 from 175,229 in Q2 2012, a decline of 15 percent. [p. 5]

● The number of unique phishing e-mail reports (campaigns) received by APWG from consumers dropped from 33,464 in May to 21,684 in September, a decline of 35 percent.

● Financial Services continued to be the most-targeted industry sector in the third quarter of 2012. [p. 7]

● China is back to being the top ranking country most infected by malware at 53.17 percent.

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.

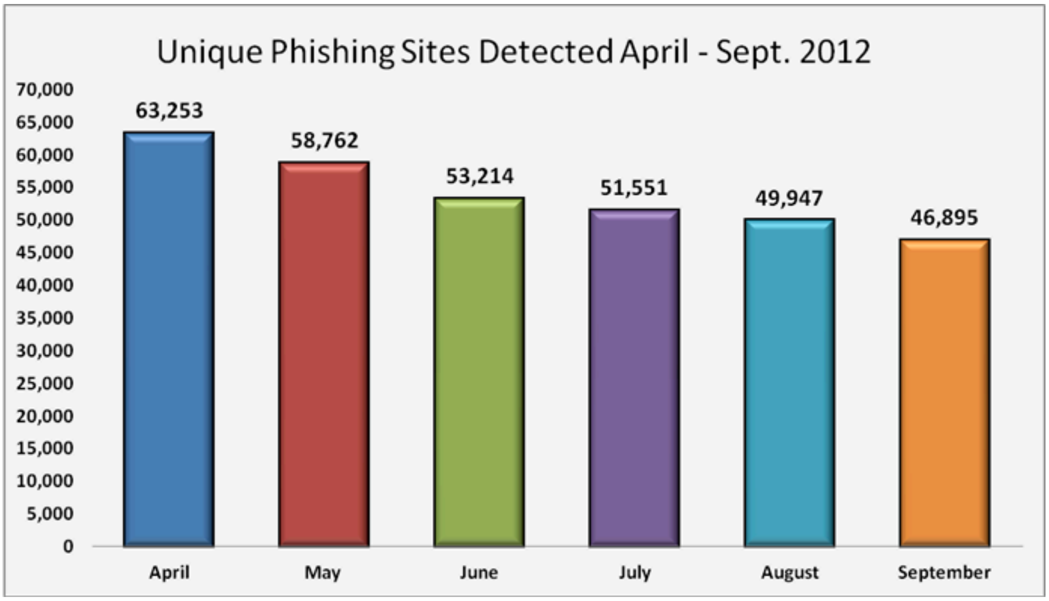
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. APWG additionally tracks crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample), as well as unique sites that are distributing 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 3rd Quarter 2012

	July	August	September
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	30,955	21,751	21,684
Number of unique phishing websites detected	51,551	49,947	46,895
Number of brands targeted by phishing campaigns	426	398	395
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	55.39%	46.24%	46.10%
No hostname; just IP address	2.66%	2.34%	2.17%
Percentage of sites not using port 80	0.41%	0.51%	0.57%

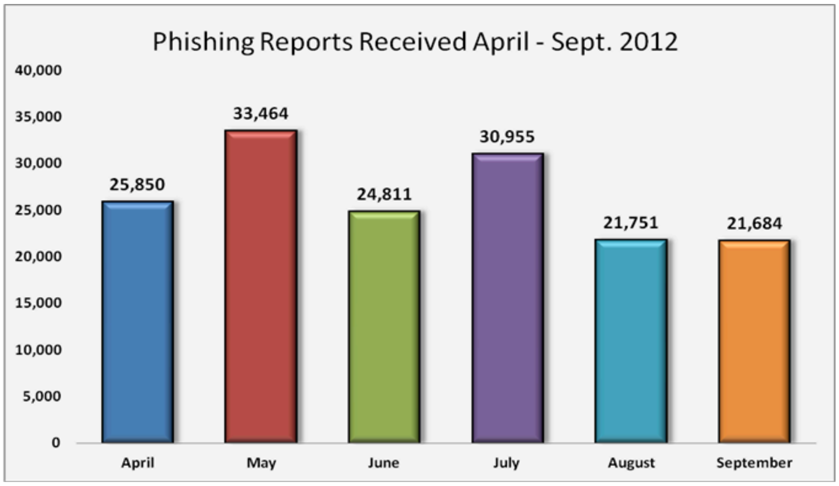
Phishing E-mail Reports and Phishing Site Trends – 3rd Quarter 2012

Phishing attacks targeting consumers remained at high levels during the quarter. There are hundreds of phishing websites established online every day, and each campaign can involve hundreds of thousands or millions of e-mails sent to consumers. During the third quarter, we saw a constant decline of unique phishing sites detected by the APWG, a trend continued from the second quarter. September 2012's 46,895 sites was slightly below September 2011's 48,410 sites, marking a return to historical phishing levels after a period of high activity. The drop from April to September was 26 percent.



"Some professional phishers have moved from perpetrating mass phishing campaigns to exploit-style malware attacks," said Rod Rasmussen, President and CTO of Internet Identity. "These don't show up as traditional phishing attacks. If anything, there are probably more "lures" of all types being generated, but with the destination being an exploit site with a drive-by download that infects users directly with malware, rather than a phishing site that attempts to steal credentials via social engineering."

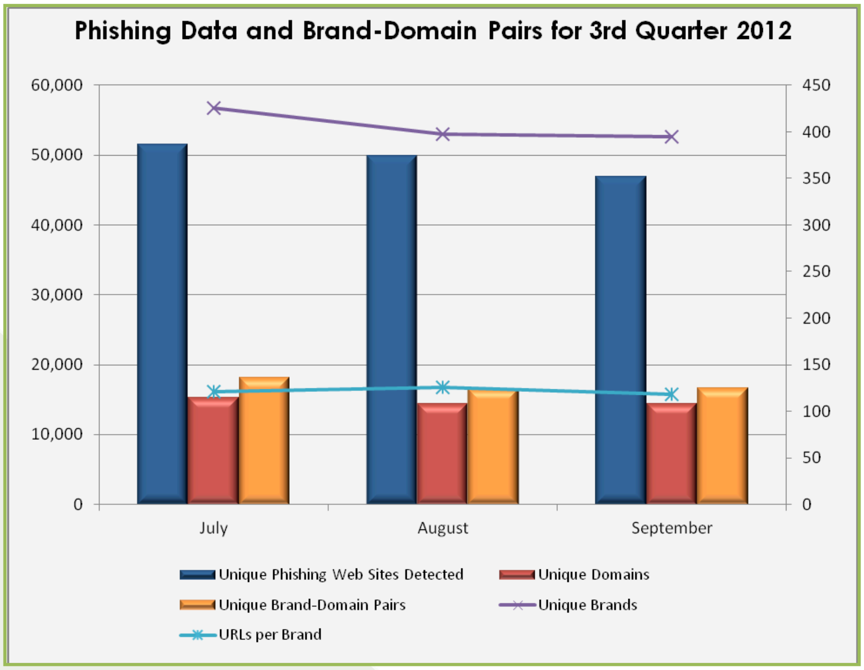
Ihab Shraim, Chief Information Security Officer and VP, Anti-Fraud Engineering & Operations at MarkMonitor, also ascribed the decline to the use of other fraudulent techniques, such as malware attack vectors. "However, it is unlikely that traditional phishing will stop since the cost of producing a phishing attack is almost insignificant," he said. "Also, the decline is not universal across all brands."



The number of unique phishing reports submitted to APWG each month showed the same downward trend. The quarter's high was 30,955 reports in July. May's high was 24 percent lower than the all-time high of 40,621 reports, recorded in August 2009.

Brand-Domain Pairs Measurement – 3rd 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 overall phishing attack levels are down from the record levels seen last quarter. However, phishing attacks are still 45 percent higher than the same period last year" as measured by MarkMonitor, said Ihab Shraim, Chief Information Security Officer and and VP, Anti-Fraud Engineering & Operations at MarkMonitor. "The majority of the drop is due to a dip in attacks against the financial and retail sectors. In general, fraud-centric targeted attacks continue to rise steadily."

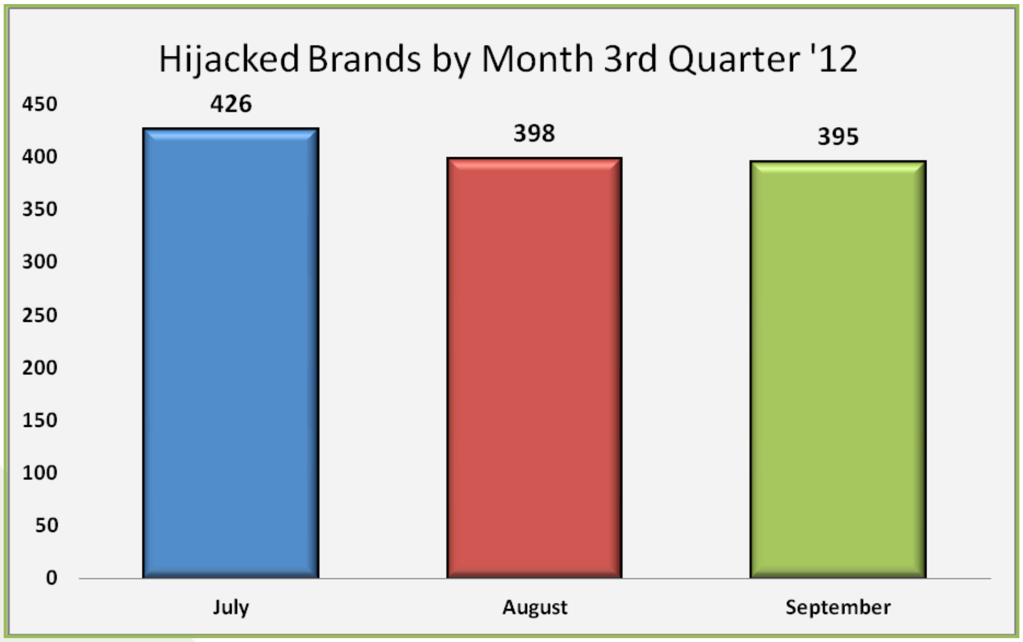
The number of unique brand-domain pairs remained very consistent during the third quarter of 2012. The high for the three-month period was 15,347 brand-domain pairs in July. This was down 37 percent from the record of 24,438 recorded in August 2009.

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.

	July 2012	August	Sept.
Number of Unique Phishing Web Sites Detected	51,551	49,947	46,895
Unique Domains	15,347	14,411	14,380
Unique Brand-Domain Pairs	18,206	16,595	16,695
Unique Brands	426	398	395
URLs Per Brand	121.01	125.49	118.72

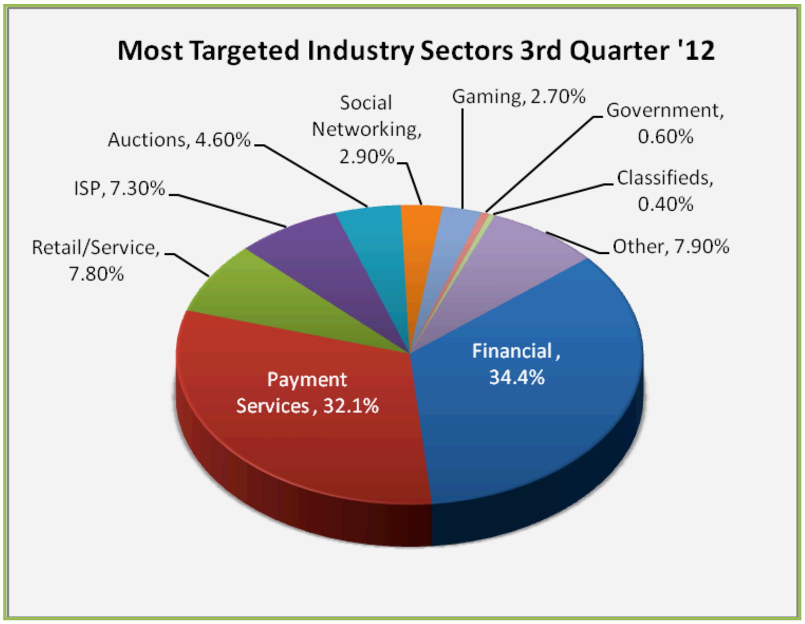
Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 3rd Quarter 2012

July 2012 saw 428 brands targeted by phishers, tying the all-time-high observed in April 2012. The number of brands then declined. APWG members report that smaller institutions such as credit unions are being targeted less frequently.



Most-Targeted Industry Sectors – 3rd Quarter 2012

Financial services continued to be the most-targeted industry sector in the third quarter of 2012. Attacks against financial services and payment services remained steady from the second quarter. Attacks against auctions sites rose from 2.3 percent to 4.5 percent, and attacks against government sites fell slightly.



Countries Hosting Phishing Sites – 3rd 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 third 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. *(*August numbers unavailable.)*

July		August	September	
USA	68.27%	*	USA	73.04%
Russia	4.23%	*	UK	3.69%
Netherlands	3.90%	*	Kazakhstan	2.09%
UK	2.98%	*	Netherlands	1.93%
Germany	2.75%	*	Germany	1.58%
France	2.24%	*	Russia	1.39%
Canada	2.20%	*	Canada	1.25%
Brazil	1.64%	*	France	1.08%
Turkey	0.81%	*	Hong Kong	0.96%
Australia	0.77%	*	Ukraine	0.90%

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 – 3rd Quarter 2012

In the third quarter of 2012 alone, more than six million new malware samples were detected, a similar figure to the first two quarters of the year. Trojans continued to account for most of the new threats:

Type of Malware Identified	% of malware samples
Trojans	72.58%
Virus	14.47%
Worms	10.53%
Rogueware	2.08%
Other	.34%

Malware Infections by Type	% of malware samples
Trojans	78.04%
Virus	6.56%
Worms	6.53%
Rogueware	5.33%
Other	3.33%

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, when it comes to the number of infections caused by each malware category, Trojans once again topped the ranking, accounting for 78 percent of infections in Q3. Data theft continues to be the main reason behind malware creation, as shown by the overwhelming proliferation of Trojans (78.04 percent of all samples detected by PandaLabs).

Which countries were most infected? Which countries were best protected? The average number of infected PCs across the globe stood at 30.68 percent, slightly less than in Q2. Countries in Asia took the top two spots of most infections per country, with China leading the way (53.17 percent of infected PCs), followed by South Korea (52.77 percent). These two were the only countries whose infection rates exceeded 50 percent. Next came Turkey (42.51 percent). As the table shows, there are high-infection countries in every region of the world: Asia, Europe, South America, and Africa as well.

Eight of the ten least-infected countries are in Europe with the only exceptions being Canada and Australia. The country with the fewest infections is Ireland (20 percent of infected PCs), closely followed by Norway (20.16 percent). Sweden takes the third spot (22.46 percent), maintaining its presence as one of the countries least affected by malware infections over the last few years.

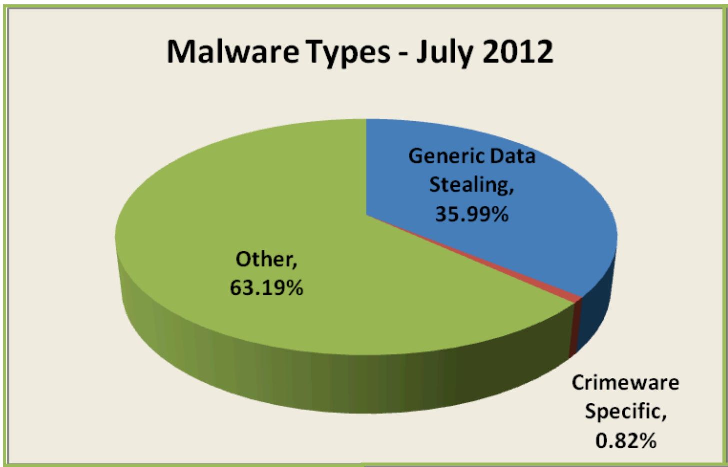
Ranking	Country	Infection Rate
1	China	53.17%
2	South Korea	52.77%
3	Turkey	42.51%
4	Slovakia	40.59%
5	Taiwan	40.20%
6	Romania	37.50%
7	Bolivia	36.07%
8	Poland	35.33%
9	Guatemala	35.14%
10	South Africa	34.57%

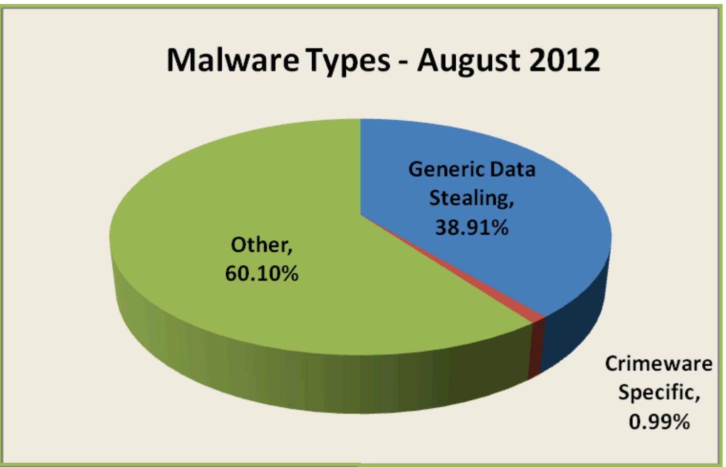
Ranking	Country	Infection ratio
23	Hungary	26.11%
24	Canada	24.33%
25	Australia	23.67%
26	Germany	23.57%
27	Finland	23.26%
28	UK	22.72%
29	Switzerland	22.69%
30	Sweden	22.46%
31	Norway	20.16%
32	Ireland	18.40%

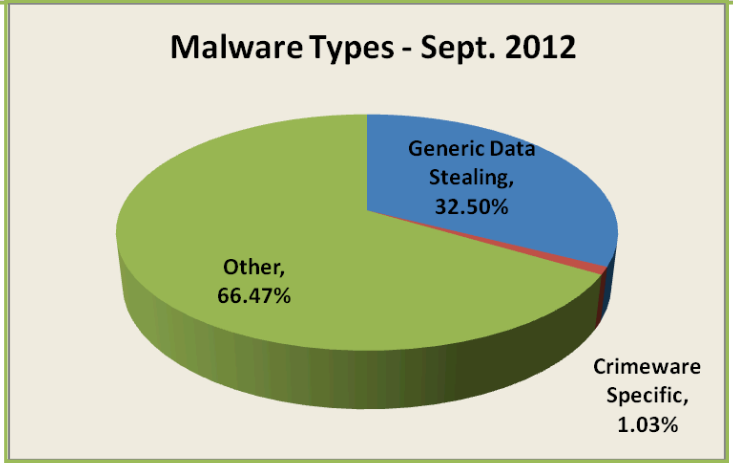
Measurement of Detected Crimeware – 3rd Quarter 2012

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.)







"A form of reconnaissance prior to spear phishing that is termed a 'watering hole attack' has been observed," said Carl Leonard of Websense Security Labs. "Here a site is compromised and the visitors are monitored to see what kind of spear phising attack they may be most susceptible to. Additionally, crimeware has remained statistically the same in this quarter, as has data stealing and the use of other malware."

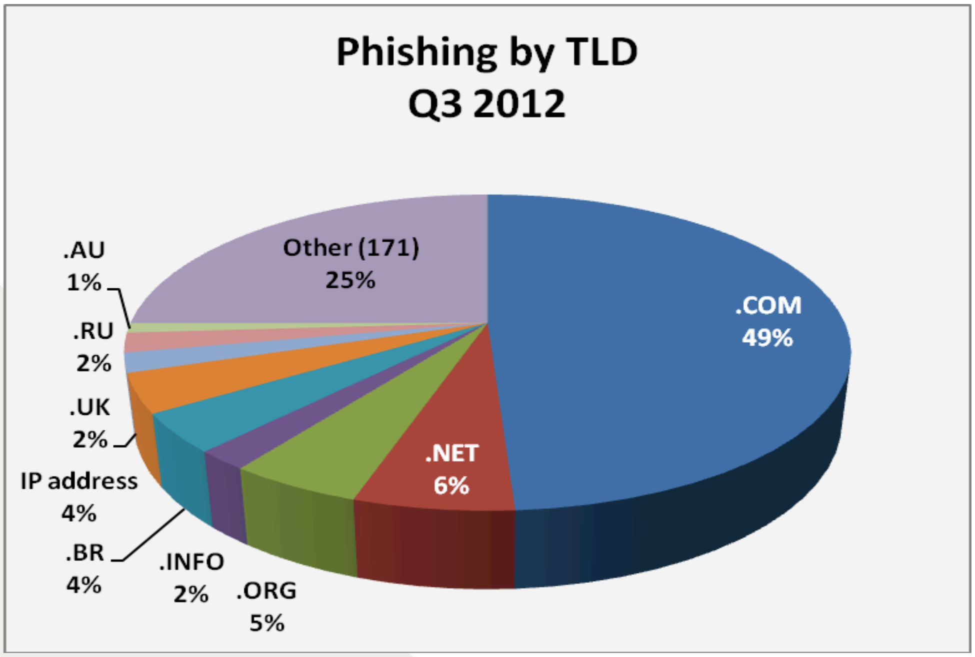
Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

During the three month period, the USA remained the top hosting country of phishing-based Trojans. This chart represents a breakdown of the websites that were classified as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader that downloads a keylogger.

July		August		September	
USA	54.92%	USA	52.91%	USA	50.32%
France	15.41%	France	7.83%	China	15.75%
China	9.08%	UK	7.77%	UK	5.45%
Rep of Korea	2.30%	China	6.24%	Netherlands	4.65%
Netherlands	2.18%	Canada	2.67%	France	3.97%
Germany	2.08%	Germany	2.47%	Germany	2.46%
UK	1.91%	Switzerland	1.65%	Canada	1.58%
Russia	1.84%	Australia	1.64%	Russia	1.58%
Brazil	1.18%	Brazil	1.57%	Rep of Korea	1.54%
Canada	0.98%	Netherlands	1.21%	Brazil	1.30%

Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing. Forty-nine percent of phishing attacks were on .COM names, and .COM represents approximately 44 percent of domain names registered worldwide. The TLD of Brazil (.BR) had 4 percent of phishing worldwide, but only 1 percent of the 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; or Websense at 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.

Statistical analysis by Greg Aaron, Illumintel; *Trends Report* editing by Ronnie Manning, Mynt Public Relations.