

# Phishing Activity Trends Report

**2<sup>nd</sup> Quarter  
2012**

**APWG**

Unifying the  
Global Response  
To Cybercrime

**April – June 2012**

*Published September 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](mailto:reportphishing@antiphishing.org). APWG also measures the evolution, proliferation, and propagation of crimeware by drawing from the research of our member companies.

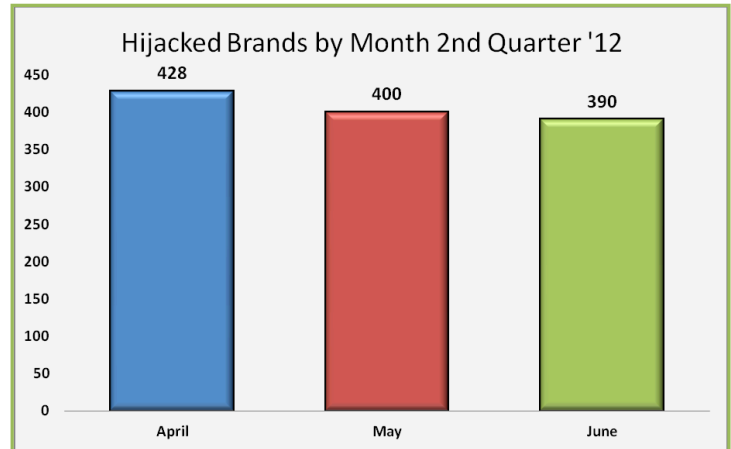
## Phishing Defined

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

<b>Statistical Highlights for 1st Quarter 2012</b>	<b>3</b>
<b>Phishing E-mail Reports and Phishing Site Trends</b>	<b>4</b>
<b>Brand-Domain Pairs Measurement</b>	<b>5</b>
<b>Brands &amp; Legitimate Entities Hijacked by</b>	
<b>E-mail Phishing Attacks</b>	<b>6</b>
<b>Most Targeted Industry Sectors</b>	<b>7</b>
<b>Countries Hosting Phishing Sites</b>	<b>7</b>
<b>Top Malware Infected Countries</b>	<b>8</b>
<b>Measurement of Detected Crimeware</b>	<b>9</b>
<b>Phishing-based Trojans &amp; Downloader's Host</b>	
<b>Countries (by IP address)</b>	<b>10</b>
<b>Top Five Phishing E-mail Subject Lines</b>	<b>10</b>
<b>APWG Phishing Trends Report Contributors</b>	<b>11</b>

## Brands Targeted by Cybercrime Gangs Reach All-Time High in April



April 2012 recorded a new all-time high of 428 brands targeted by phishers, after reaching a new high of 392 brands just in Q1 2012. [p. 6]

## 2nd Quarter '12 Phishing Activity Trends Summary

- The number of unique phishing sites detected by the APWG reached an all-time monthly high of 63,253 in April. [p.4]
- The total number of URLs used to host phishing attacks increased to 175,229 in Q2 2012, up from 164,023 in Q1 2012. [p. 5]
- Financial Services continued to be the most-targeted industry sector in the second quarter of 2012. [p. 7]
- Four out of every five new malware specimens created were Trojans (78.92 percent). [p. 8]
- For the first time, South Korea led the ranking of countries most infected by malware (57.30 percent of infected PCs), followed by China (51.94 percent). [p. 8]
- In the second quarter of 2012, more than six million unique malware samples were identified. [p. 8]
- During the second quarter, the USA remained the top hosting country of phishing-based Trojans, consistent from the first quarter of the year. [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. 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's *Phishing Activity Trends Report* also includes statistics on rogue anti-virus software, desktop infection rates, and related topics. *Issue Note:* Starting with this issue, APWG discontinues the measurement of ports hosting phishing data collection servers. The metric yields little in the way of forensic insights, as Port 43 has consistently mediated some 99 percent or more of web-based phishing since 2003.

## Statistical Highlights for 2<sup>nd</sup> Quarter 2012

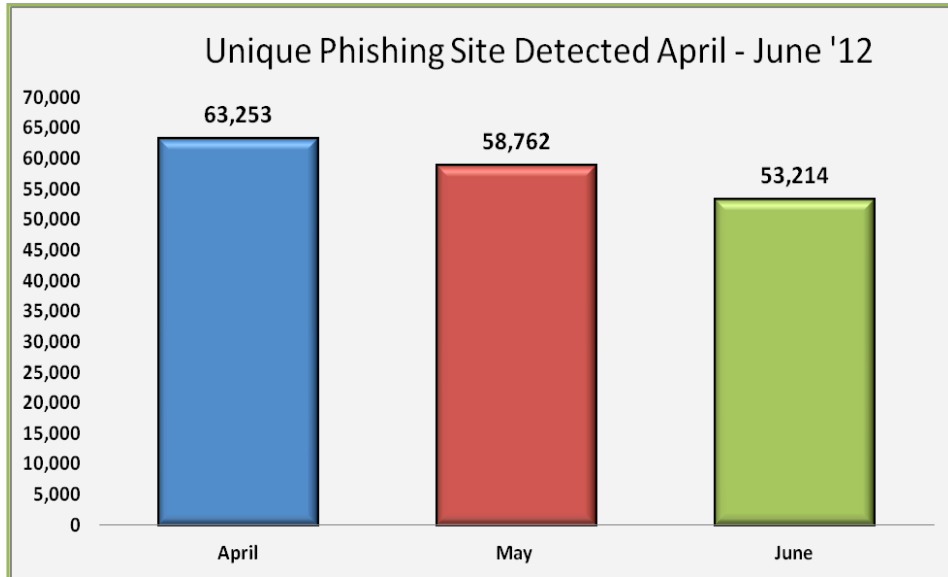
	April	May	June
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	25,850	33,464	24,811
Number of unique phishing websites detected	63,253	58,762	53,214
Number of brands targeted by phishing campaigns	428	400	390
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	46.63%	29.69%	60.39%
No hostname; just IP address	1.04%	0.56%	2.38%
Percentage of sites not using port 80	0.21%	0.31%	0.24%

## Phishing E-mail Reports and Phishing Site Trends – 2nd Quarter 2012

Phishing attacks targeting consumers remained at high levels during the quarter, with 25,000 to 30,000 unique phishing e-mail campaigns documented each month. Each campaign can involve hundreds of thousands or millions of e-mails sent to consumers. There are hundreds of phishing websites established online every day, luring any

number of consumers to trouble and loss.

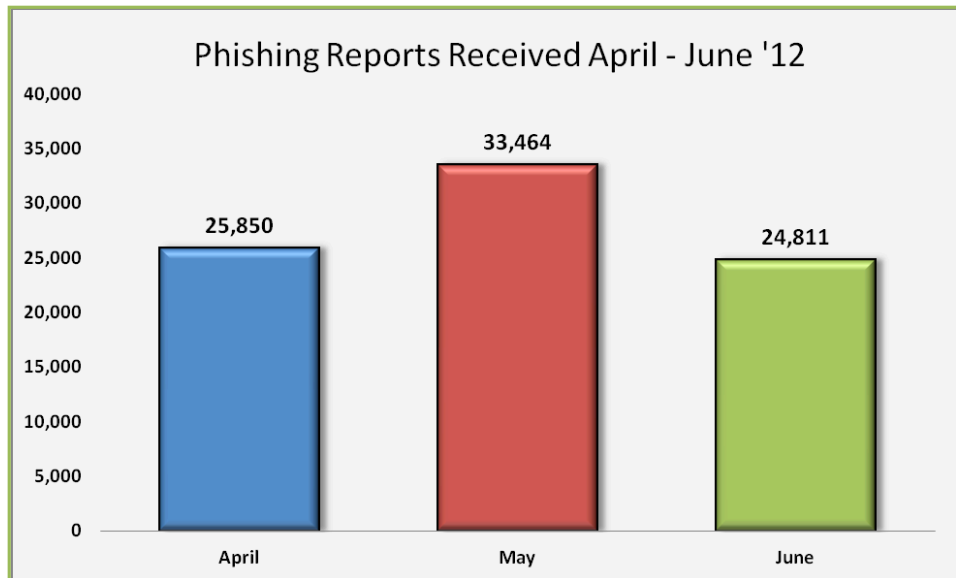
In April, the number of unique phishing sites detected by the APWG reached an all-time high of 63,253. Phishing in the following two months fell off, with June seeing a drop to 53,214 sites, indicating reduced activity by phishers. The April figure eclipsed the previous record high of 56,859, which was recorded in February 2012, by almost 11 percent.



The number of unique phishing reports submitted to APWG each month fluctuated by nearly 8,000 reports from month to month. The quarter's high was 33,464 reports in May. May's high was 18 percent lower than the all-time high of 40,621 reports, recorded in August 2009.

APWG research partner Internet Identity found a major increase in the use of a tactic that allows phishers to create hundreds of phish at once. By adding a phishing

page to all the domains on a vulnerable shared virtual server, a server that hosts multiple web sites, the criminal effectively creates hundreds of phishing pages with unique Internet locations. "Even excluding the thousands of phishing sites created by this tactic, phishing in the second quarter of 2012 was up significantly over the first quarter," said Rod Rasmussen, President and CTO of Internet Identity and *Trends Report* contributing analyst.

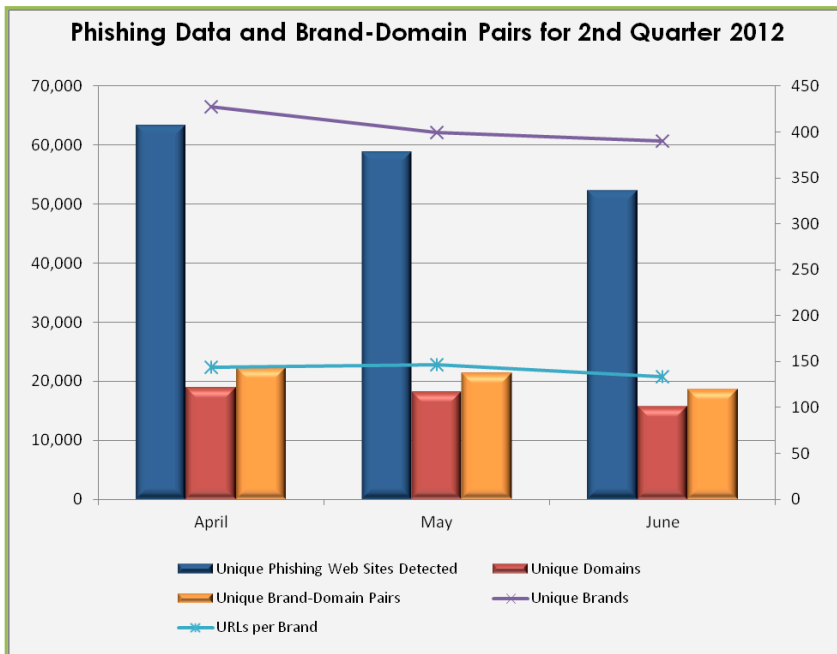


## Brand-Domain Pairs Measurement – 2nd Quarter 2012

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 number of unique brand-domain pairs consistently dropped during the first quarter of 2012. The high for the three-month period was 22,247 brand-domain pairs in April. This was down nine percent from the record of 24,438 recorded in August 2009.



“Targeted attacks remain the favorite attack vector used to launch phishing attacks, as the number of unique brands [during the entire quarter] being targeted rose to 601 in Q2 2012 from 587 in Q1 2012,” said Ihab Shraim, chief information security officer and vice president, anti-fraud engineering and operations at MarkMonitor, and APWG *Trends Report* contributing analyst. “As a corollary, the total number of URLs used to host phishing attacks increased to 175,229 in Q2 2012 from 164,023 in Q1 2012.”

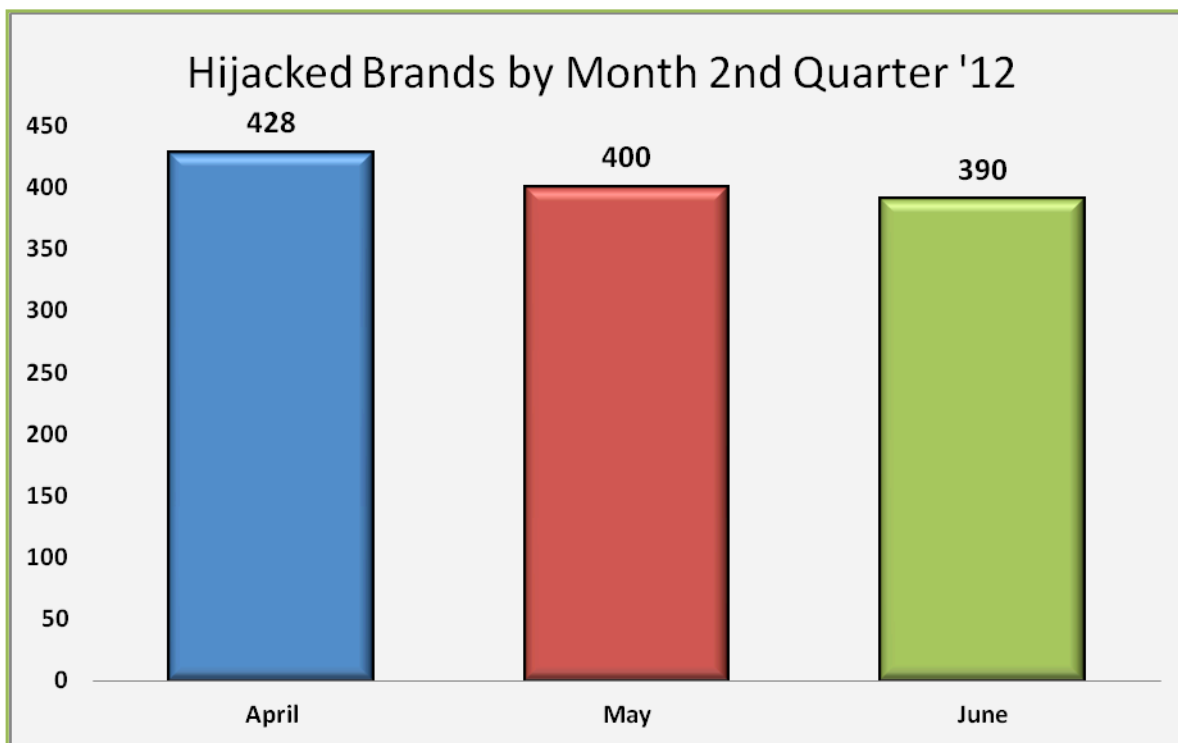
*Forensic utility* of this metric: If the number of unique URLs is greater than the number of brand/domain pairs, it

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.

	April	May	June
Number of Unique Phishing Web Sites Detected	63,253	58,762	52,214
Unique Domains	18,878	18,191	15,637
Unique Brand-Domain Pairs	22,247	21,425	18,532
Unique Brands	428	400	390
URLs Per Brand	143.85	146.90	133.88

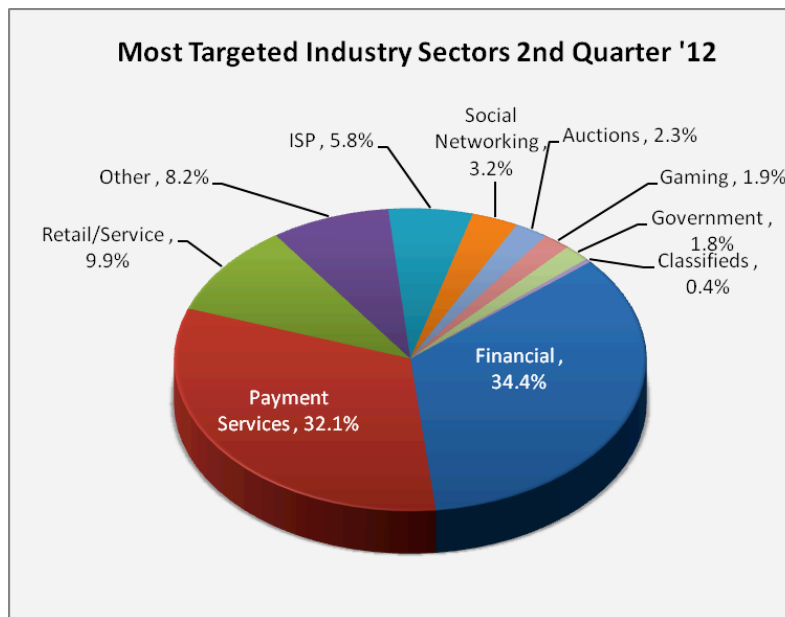
## Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 2nd Quarter 2012

April 2012 saw an all-time high of 428 brands targeted by phishers, after reaching a previous high of 392 brands during February and March 2012. This was a nine percent increase from the previous all-time high of 392. May proved to have even a higher number of brands than the previous high with 400.



## Most Targeted Industry Sectors – 2nd Quarter 2012

Financial Services continued to be the most-targeted industry sector in the second quarter of 2012. Similar to last quarter, during this three-month period, Payment Services remained the second-highest industry sector for targeted attacks.



## Countries Hosting Phishing Sites – 2nd 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 second 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.

April		May		June	
USA	58.45%	USA	87.91%	USA	71.55%
Egypt	6.28%	Bahamas	5.55%	Germany	3.36%
Brazil	4.54%	Germany	0.53%	UK	3.08%
Canada	3.93%	Canada	0.47%	Canada	2.71%
Germany	3.91%	Rep. Korea	0.46%	France	2.17%
UK	2.45%	Switzerland	0.45%	Brazil	1.61%
Netherlands	1.67%	UK	0.44%	Netherlands	1.52%
France	1.56%	Netherlands	0.42%	Czech Rep.	1.34%
Russia	1.14%	Egypt	0.36%	Japan	1.19%
Turkey	1.12%	Belgium	0.34%	Russia	0.94%

## 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 – 2nd Quarter 2012

During the second quarter of 2012, PandaLabs identified more than six million malware strains at its laboratory, a similar figure to the first quarter. The types of malware found were also similar: four out of every five new malware specimens created were Trojans (78.92 percent). This continues the trend established over the last few months:

Type of Malware Identified	% of malware samples
Trojans	78.92%
Worms	10.78%
Virus	7.44%
Rogueware	2.96%
Other	.17%

Malware Infections by Type	% of malware samples
Trojans	76.18%
Worms	6.69%
Virus	7.82%
Rogueware	5.80%
Other	3.51%

According to Luis Corrons, PandaLabs Technical Director and APWG *Trends Report* contributing analyst, Trojans accounted for most infections, as expected. Corrons noted that a relatively small number of PCs are infected by worms—fewer than the number of new worms created over the quarter. The figures corroborate what is well known: massive worm epidemics are a thing of the past and have been replaced by Trojans, more specifically, banking Trojans and the infamous “Police Virus,” crimeware designed to blackmail innocent users into paying a bogus “police” fine.

Let's now look at the geographic distribution of infections. Which countries were most infected? Which countries were best protected? The average number of infected PCs across the globe stood at 31.63 percent, down almost four percentage points compared to Q1. South Korea led the ranking of most affected countries for the first time ever (57.30 percent of infected PCs), followed by China (51.94 percent). These were the only countries whose infection rates exceeded 50 percent. Next came Taiwan (42.88 percent). In the case of China, it is interesting to note that some of the country's most developed regions have much lower infection rates than the rest of the country; that's the case of Hong Kong for example, whose infection rate stands at a mere 23.36 percent.

Ranking	Country	Infection Rate
1	South Korea	57.30%
2	China	51.94%
3	Taiwan	42.88%
4	Bolivia	42.28%
5	Honduras	40.80%
6	Turkey	39.29%
7	Ecuador	37.59%
8	Russia	36.78%
9	Slovakia	36.09%
10	Poland	35.74%

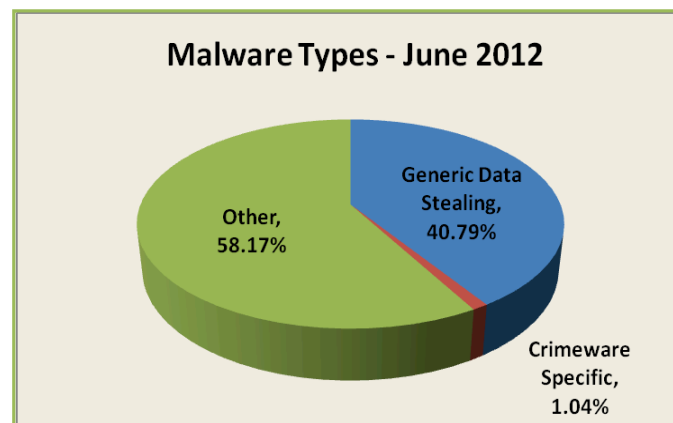
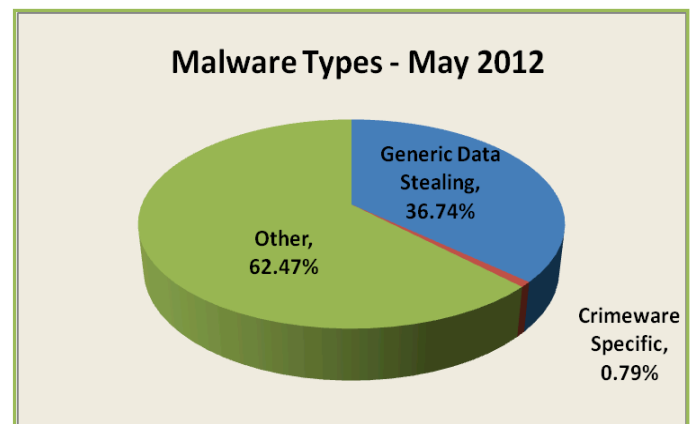
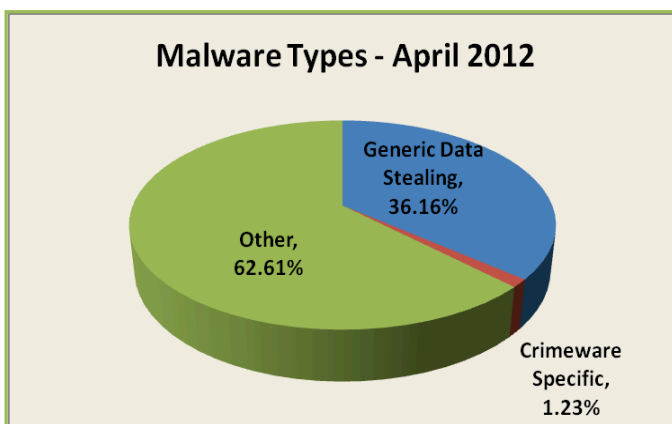
Ranking	Country	Infection ratio
23	Holland	24.74%
24	Hungary	24.54%
25	Finland	24.02%
26	Ireland	23.64%
27	Germany	22.61%
28	Uruguay	21.94%
29	United Kingdom	21.01%
30	Norway	20.50%
31	Sweden	19.07%
32	Switzerland	18.40%



## Measurement of Detected Crimeware – 2nd 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.)



"The top five subject lines in phishing emails this quarter attempted to scare users, similar to fake antivirus campaigns and other computer threats. Even well-trained users forget best practices and will click on pop-ups or follow links in a panic response," said APWG *Trends Report* contributing analyst, Carl Leonard, of Websense Security Labs. [See: Phishing Subject Lines chat, p 10.]

## Top Five Phishing Email Subject Lines – 2nd Quarter 2012

FROM	SUBJECT
Top Phishing Sender 1	Your account has been accessed by a third party
Top Phishing Sender 2	LloydsTSB Internet Banking Customer Service Message
Top Phishing Sender 3	Security Measures
Top Phishing Sender 4	Verify your activity
Top Phishing Sender 5	Account security notification

*Source: Websense Security Labs, Sept. 2012*






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

This chart represents a breakdown of the websites which were classified during the first quarter of 2012 as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. During the three month period, the USA remained the top hosting country of phishing-based Trojans.

April		May		June	
USA	46.44%	USA	78.13%	USA	55.17%
Russia	11.55%	UK	3.77%	France	11.17%
France	7.81%	France	3.64%	China	7.00%
China	4.15%	China	1.75%	Russia	3.73%
Brazil	3.77%	Russia	1.48%	Rep of Korea	2.85%
Netherlands	3.68%	Germany	1.34%	Netherlands	2.63%
Rep of Korea	3.33%	Hong Kong	1.07%	Germany	2.56%
Germany	2.94%	Netherlands	0.80%	Ukraine	1.83%
UK	2.25%	Iceland	0.67%	UK	1.70%
Poland	1.40%	Canada	0.67%	Brazil	1.33%

# Phishing Activity Trends Report, 2<sup>nd</sup> Quarter 2012

## 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](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); or Websense at [publicrelations@websense.com](mailto: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.

11

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