Phishing Activity Trends Report

2nd Quarter 2013

APWG

Unifying the
Global Response
To Cybercrime

April – June 2013

Published November 5 , 2013

Phishing Activity Trends Report, 2nd 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.

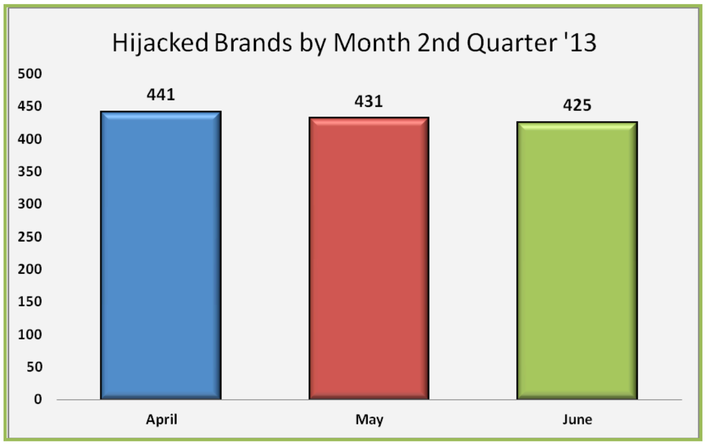
Phishing Defined

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 2nd 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

Fraudsters Seek New Victims and Brands in Untapped Markets



Some 441 brands were hijacked in April, a record high that surpassed the previous monthly high of 430 in November 2012 [p. 6]

2nd Quarter 2013 Phishing Activity Trends Summary

● During the second quarter of 2013, a total of 639 unique brands were targeted by phishing attacks. This number topped the previous high of 614 seen in Q4 2012. [p. 6]

● Phishing hosted in Russia almost disappeared in June, replaced by phishing hosted in Kazakhstan. This was a temporary shift highlighting the mobility of criminal infrastructure. [p. 7]

● The number of unique phishing reports submitted to APWG saw a steady decrease during the quarter, dropping nearly 27 percent from April to June. [p. 4]

● The number of new malware samples continues to rise. In Q2 2013, some 12 percent more malware samples were captured than in the same period last year. [p. 8]

● The online game sector experienced a notable drop in phishing, from 5.66 percent in Q1 2013 down to 2.03 percent in Q2 2013. [p. 7]

● In May, Germany surpassed the United States as the top country hosting phishing-based Trojans and downloaders. [p. 10]

Methodology and Instrumented Data Sets

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.

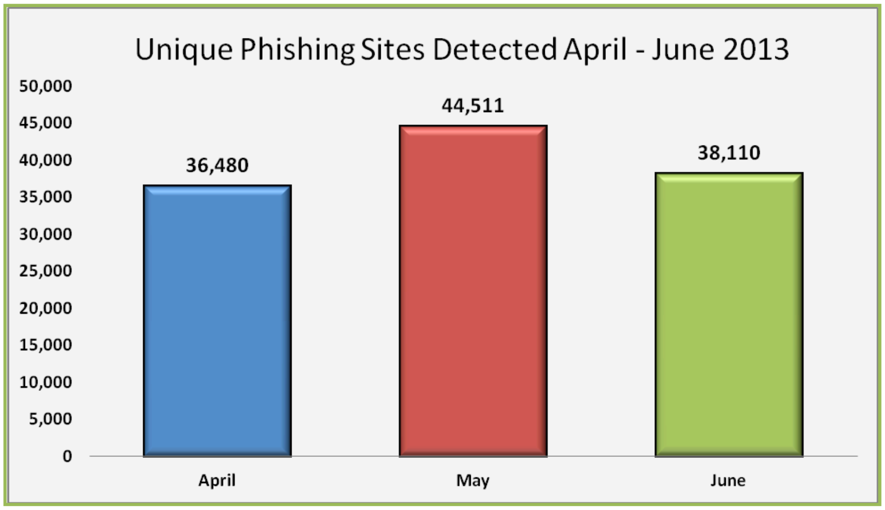
Special Note for Readers of Q2 2013 *Trends Report*: The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (e-mail campaigns) in addition to unique phishing sites with this quarterly report. We plan on reviewing our metrics and reporting systems over the next six months, in order to keep pace with change in the environment and continue to provide fresh insights to the public.

Statistical Highlights for 2nd Quarter 2013

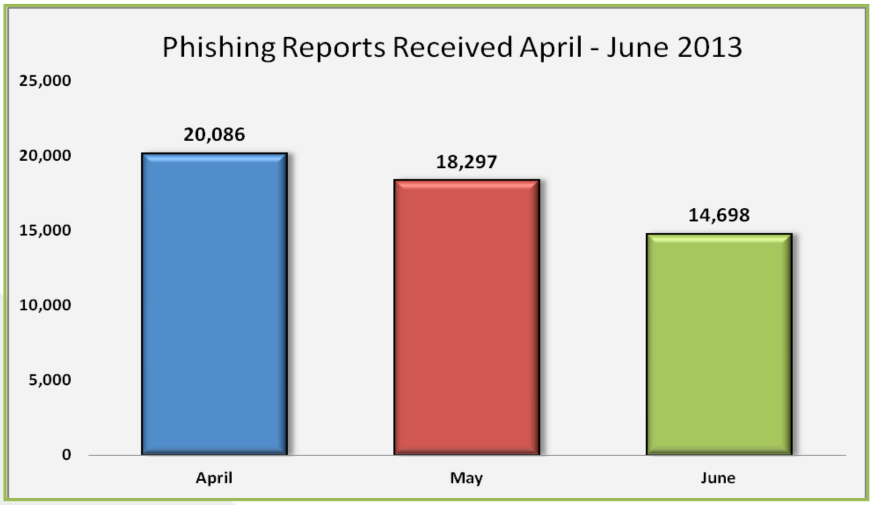
	April	May	June
Number of unique phishing websites detected	36,480	44,511	38,110
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	20,086	18,297	14,698
Number of brands targeted by phishing campaigns	441	431	425
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	50.92%	57.45%	51.52%
No hostname; just IP address	4.57%	5.23%	5.26%
Percentage of sites not using port 80	0.38%	0.45%	0.80%

Phishing E-mail Reports and Phishing Site Trends – 2nd Quarter 2013

The number of phishing sites detected fluctuated by nearly 10,000 sites month to month during both Q1 and Q2, with APWG seeing a 18 percent increase from April to May, 2013. April's 36,480 was the second-lowest number on record, a little higher than the historical low of 35,024 recorded in February 2013.



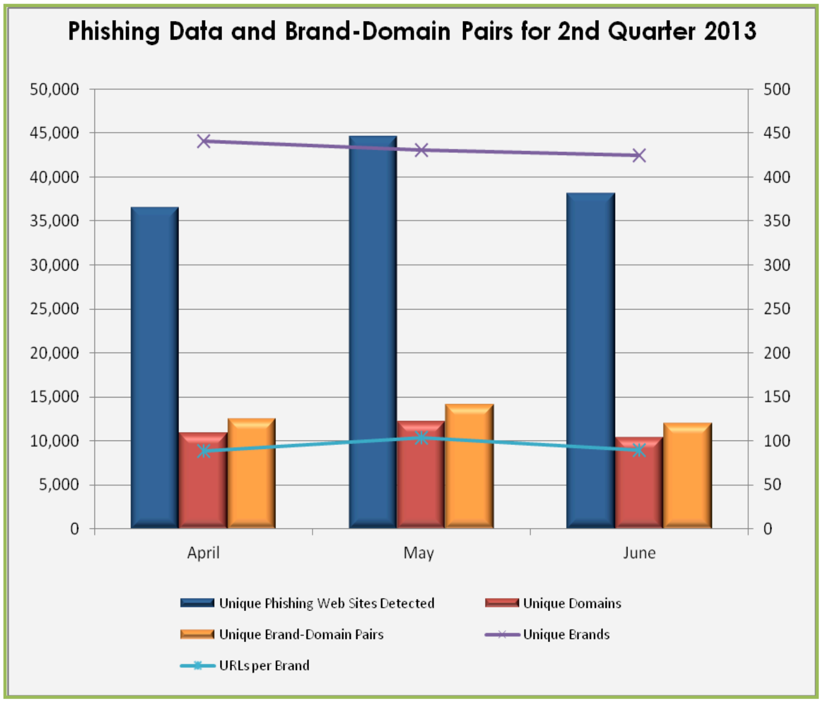
The number of unique phishing reports submitted to APWG each month saw a steady decrease during the quarter, dropping nearly 27 percent from April to June. June's total of 14,698 was 63 percent lower than the all-time high of 40,621 reports, recorded in August 2009. It is not unusual for phishing activity to decline a bit in the summer months.



Brand-Domain Pairs Measurement – 2nd 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, it is useful to understand the general number of unique URLs that occur per domain.

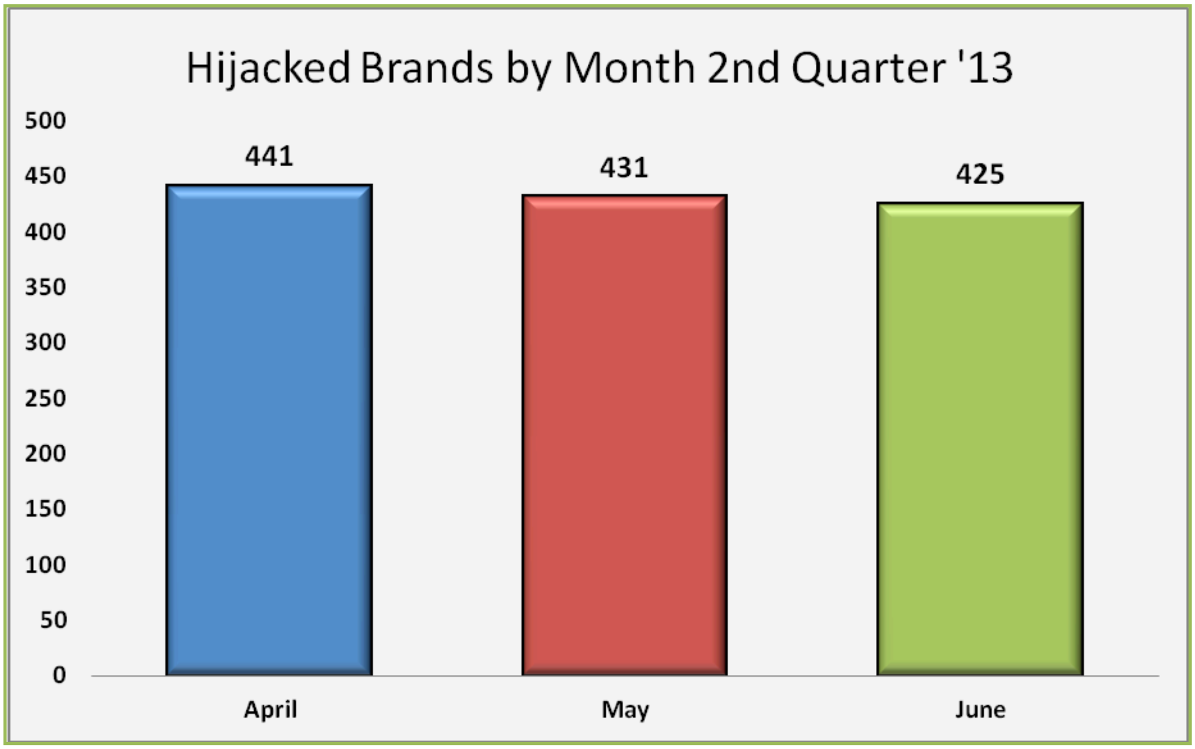
The number of unique brand-domain pairs fluctuated during second quarter of 2013. The high for the three-month period was in May, with 14,033 brand-domain pairs, dropping back to 11,960 in June.



	April	May	June
Number of Unique Phishing Web Sites Detected	36,480	44,511	38,110
Unique Domains	10,849	12,180	10,329
Unique Brand-Domain Pairs	12,460	14,033	11,960
Unique Brands	441	431	425
URLs Per Brand	88.75	103.27	89.64

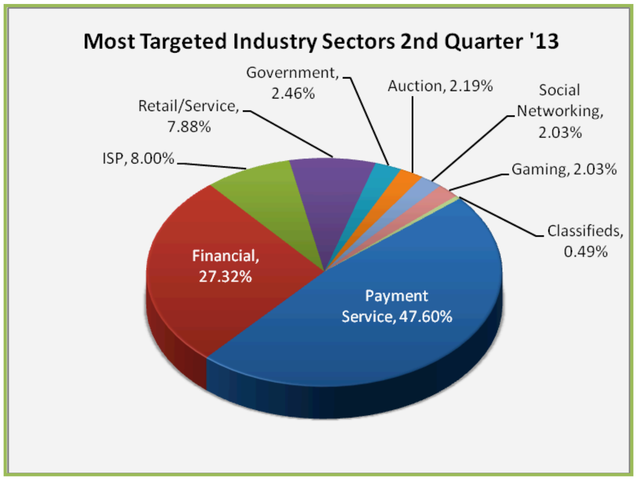
Brands Targeted by E-mail Phishing Attacks – 2nd Quarter 2013

The number of brands targets by phishers reached an all-time high of 441 in April, surpassing the old monthly record of 430 seen in November 2012. "The landscape continues to evolve as fraudsters seek new victims in untapped markets by targeting more brands," said Ihab Shraim, *Trends Report* contributing analyst and CISO and Vice President Anti-Fraud Engineering and Operations at MarkMonitor. "During the second quarter of 2013, a total 639 unique brands were targeted by phishing attacks. This number topped the previous high of 614 seen in Q4 2012."



Most-Targeted Industry Sectors – 2nd Quarter 2013

Payment Services continued to be the most-targeted industry sector. Most sectors remained consistent with the first quarter of 2013, except for computer and online gaming, which experienced a notable drop from 5.66 percent in Q1 2013 to 2.03 percent in Q2 2013.



Countries Hosting Phishing Sites – 2nd Quarter 2013

Russia has traditionally been near the top of the list of countries where phishing sites have been hosted. But in June 2013, phishing on Russian hosting almost disappeared, with Kazakhstan suddenly appearing in the #2 spot:

April		May		June	
United States	36.21%	United States	44.03%	United States	45.47%
Hong Kong	19.38%	Russian Federation	11.58%	Kazakhstan	7.11%
Russian Federation	7.67%	United Kingdom	4.79%	France	6.78%
Germany	4.37%	Germany	4.43%	Germany	5.73%
Canada	3.96%	Finland	3.92%	Canada	4.31%
Brazil	3.54%	Turkey	3.67%	United Kingdom	3.11%
Angola	2.68%	Canada	3.38%	Brazil	2.45%
United Kingdom	2.42%	Brazil	2.17%	Turkey	1.70%
France	2.33%	Indonesia	1.90%	Malaysia	1.58%
Thailand	2.15%	Ireland	1.56%	Ukraine	1.40%

"We know that Kazakhstan is enjoying an uptake in the adoption of mobile payments, so it's not a surprise that phishers have sought to move to this area," said *Trends Report* contributing analyst Carl Leonard of Websense Security Labs. "A spate of phishing hosted in Hong Kong also disappeared in late April. The portability of a phishing infrastructure is well-documented, and criminals continue to attempt to evade detection and shut-downs by moving their infrastructure around."

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 – 2nd Quarter 2013

The amount of new malware samples continued to rise. In the second quarter of 2013, 12 percent more unique malware samples were identified than in the same period last year, and an increase of 17 percent in 2013 so far. Trojans were the most popular, accounting for 77.2 percent of all new malware created. According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, Trojans have reached record-setting popularity as a form of malware.

Type of Malware Identified	% of malware samples
Trojans	77.20%
Viruses	11.28%
Worms	10.29%
Rogueware	1.09%
Other	.15%

Malware Infections by Type	% of malware samples
Trojans	79.70%
Viruses	6.06%
Worms	6.71%
Rogueware	3.62%
Other	3.91%

Cyber-criminals use Trojans as a key tool to infect users' computing devices, and continually introduce changes to evade the signature-based detection used by antivirus firms. The process is often automated, changing the binaries run on victims' computers and leading to more unique signatures and samples.

PandaLabs estimates that in the second quarter of 2013, the percentage of infected computers worldwide was 32.77 percent, which was up on the first quarter. More than half of the computers in China are infected. China was followed by Turkey (43.59%). A number of Latin American countries have infection rates over the global average: Peru (42.14%), Brazil (35.83%), Guatemala (35.51%), Colombia (33.86%), Costa Rica (33.33%), and Chile (33.22%).

Europe and Japan continue to have the lowest infection rates. The USA fell in the middle of the rankings, with a 31.16 percent infection rate.

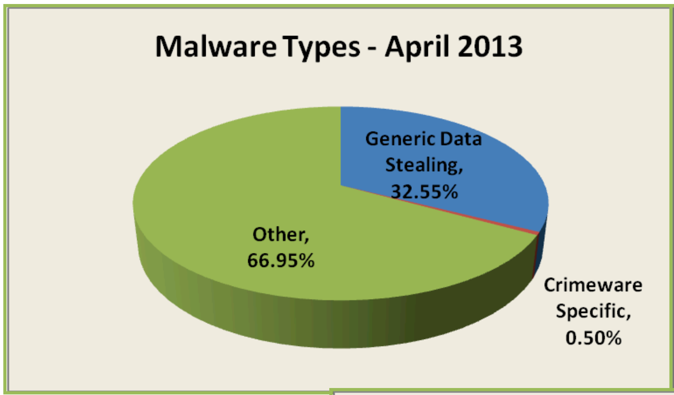
Ranking	Country	Infection Rate
1	China	52.36%
2	Turkey	43.59%
3	Peru	42.14%
4	Bolivia	41.67%
5	Ecuador	41.13%
6	Russia	41.08%
7	Argentina	39.36%
8	Taiwan	38.65%
9	Slovenia	38.00%
10	El Salvador	37.29%

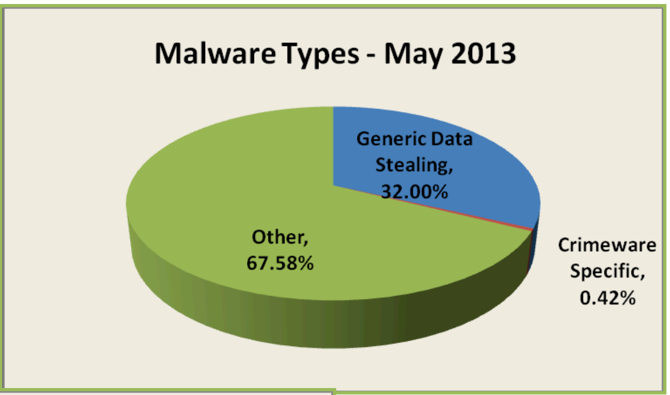
Ranking	Country	Infection ratio
35	Portugal	26.79%
36	Netherlands	25.82%
37	Switzerland	25.60%
38	Belgium	24.87%
39	France	24.54%
40	UK	24.48%
41	Japan	24.21%
42	Germany	24.18%
43	Norway	21.14%
44	Sweden	21.03%

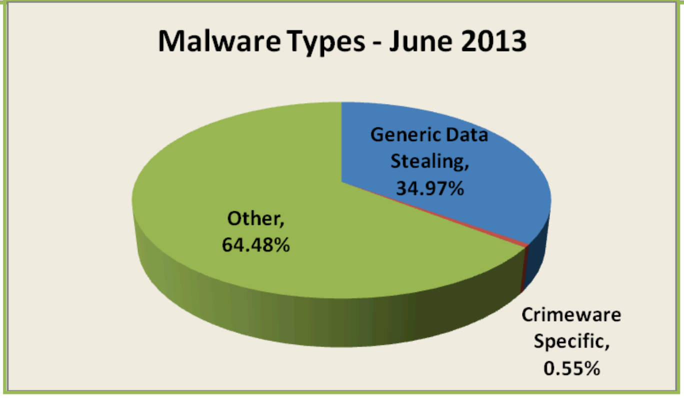
Measurement of Detected Crimeware – 2nd Quarter 2013

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.)


Malware Types - April 2013


Malware Types - May 2013


Malware Types - June 2013

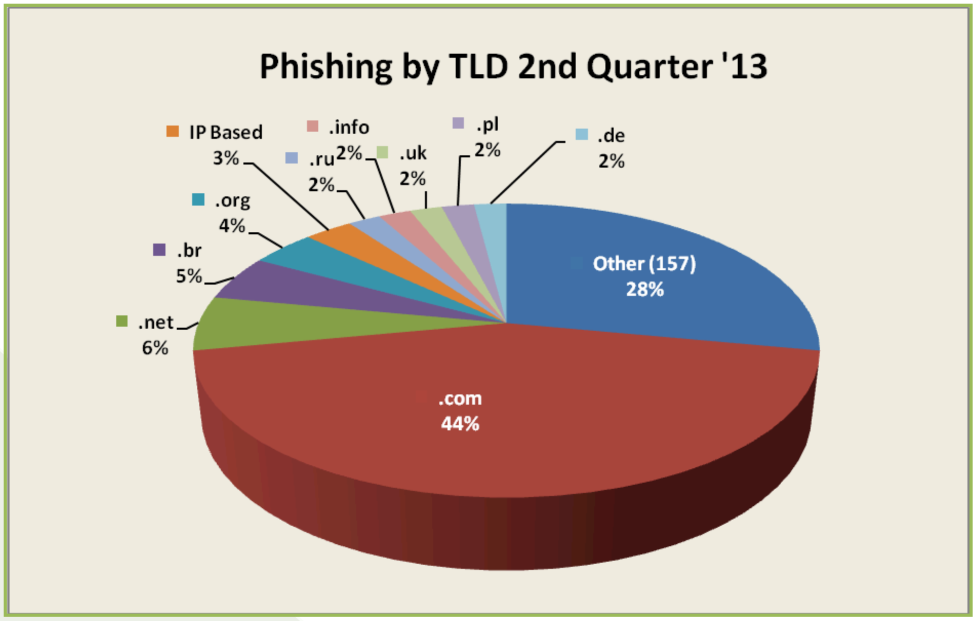
Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

In May, Germany surpassed the United States as the top country hosting phishing-based Trojans and downloaders. This is the first time that Germany has been ranked at the top. The United States returned to the top spot in June.

April		May		June	
United States	26.80%	Germany	28.59%	United States	40.66%
Switzerland	24.58%	United States	27.18%	Germany	30.42%
Germany	18.33%	China	8.50%	Netherlands	4.31%
Russian Federation	8.01%	Russian Federation	6.38%	China	4.25%
China	3.87%	Netherlands	6.10%	Russian Federation	3.35%
Ukraine	2.78%	Switzerland	3.99%	Rep. of Korea	2.30%
Spain	2.35%	France	3.98%	Romania	1.40%
Netherlands	1.99%	Ukraine	2.95%	Switzerland	1.20%
Romania	1.44%	Romania	2.03%	France	1.17%
United States	26.80%	Spain	1.74%	Brazil	1.13%

Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing sites. Forty-four percent of domains used for phishing were .COM names, up for 42 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.



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; 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.

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