

Phishing Activity Trends Report

2nd Quarter

2014

APWG

Unifying the
Global Response
To Cybercrime

April – June 2014

Published August 28, 2014

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.

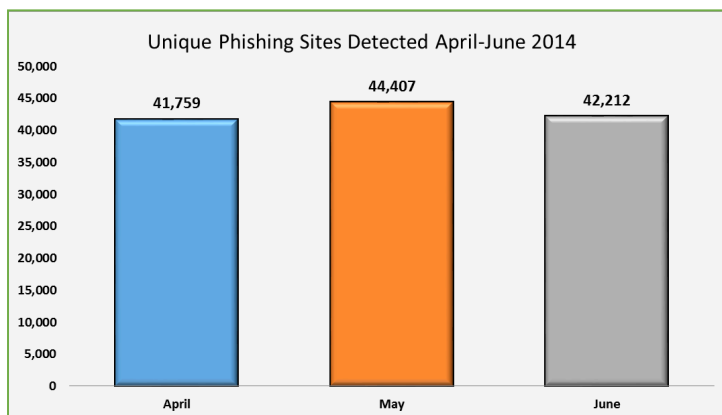
Phishing Defined

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 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

2014 Brand Attacks Aim at the Most Vulnerable Targets



April through June 2014 saw the second-highest number of phishing sites ever observed in a quarter. [p. 4]

2nd Quarter 2014 Phishing Activity Trends Summary

- The 128,378 phishing sites were observed in Q2. This is the second-highest number of phishing sites detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012. [p. 4]
- New online payment services and crypto-currency sites are being targeted more frequently. [pp. 6-7]
- There has been a recent increase in PUPs (Potentially Unwanted Programs) such as spyware and adware. This contributed to higher global infection rates. [p. 8]
- The total number of brands targeted dropped to 531 brands, down from the 557 targeted in the first quarter of 2014. [p. 6]
- The United States continued to be the top country hosting phishing sites. [p. 7]

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.

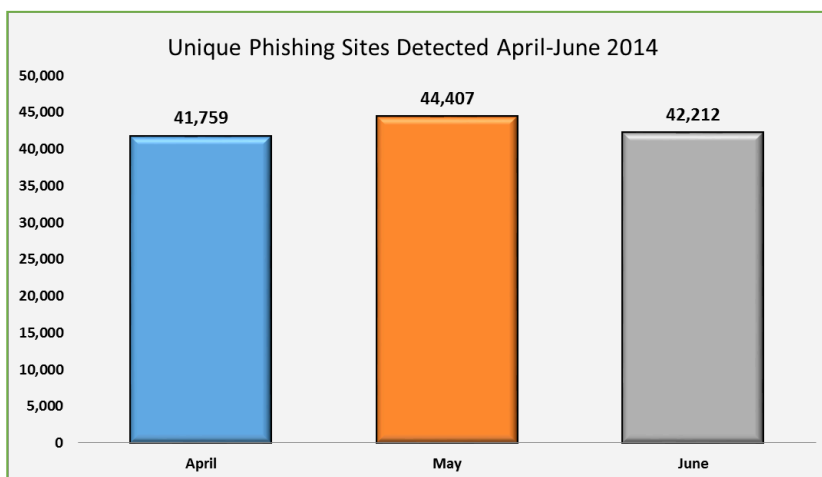
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances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

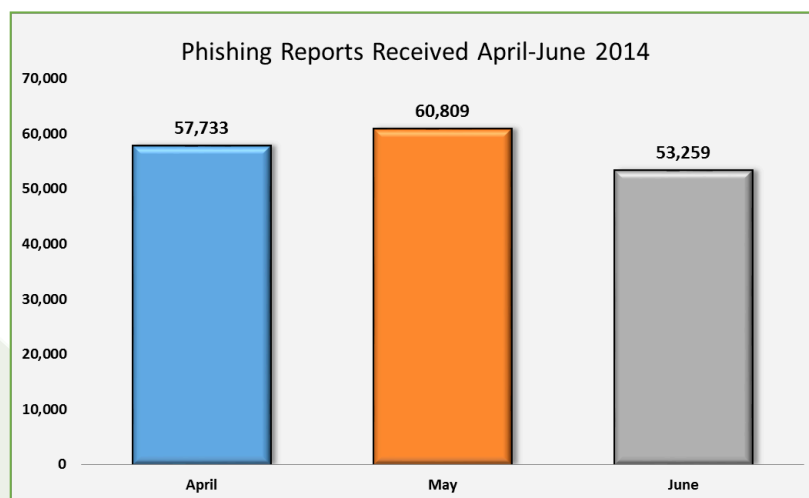
	April	May	June
Number of unique phishing websites detected	41,759	44,407	42,212
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	57,733	60,809	53,259
Number of brands targeted by phishing campaigns	332	357	345
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	56.76%	54.31%	64.47%
Percentage of sites not using port 80	0.85%	0.42%	0.56%

Phishing E-mail Reports and Phishing Site Trends – 2nd Quarter 2014

The total number of phish observed in Q2 was 128,378, a 3 percent increase over Q1 2014, when a total of 125,215 were observed. The 128,378 is the second-highest number of phishing sites detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012.

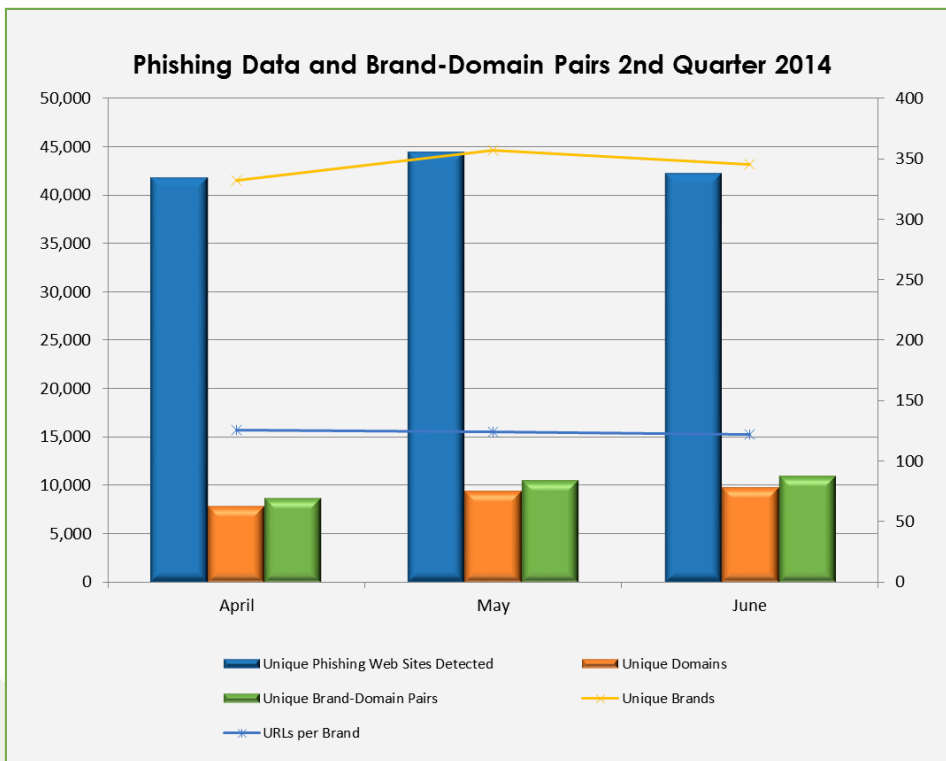


The number of unique phishing reports submitted to APWG during Q2 was 171,801. This was almost identical to the 171,792 reports received in Q1 of 2014. The number of unique phishing reports submitted to APWG dropped by more than 7,500 from May to June:



Brand-Domain Pairs Measurement – 2nd 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.



"Overall phishing volumes experienced a mild increase from the previous quarter and remain at one of the highest levels of activity we have seen," said Frederick Felman, Chief Marketing Officer, MarkMonitor.

The number of targets dropped slightly from 1Q 2014. Year-over-year, the number of targets was down 17% from the 639 observed in Q2 of 2013 to the 531 seen in Q2 of 2014. "This indicates a higher concentration of attacks on more vulnerable brands," said Felman.

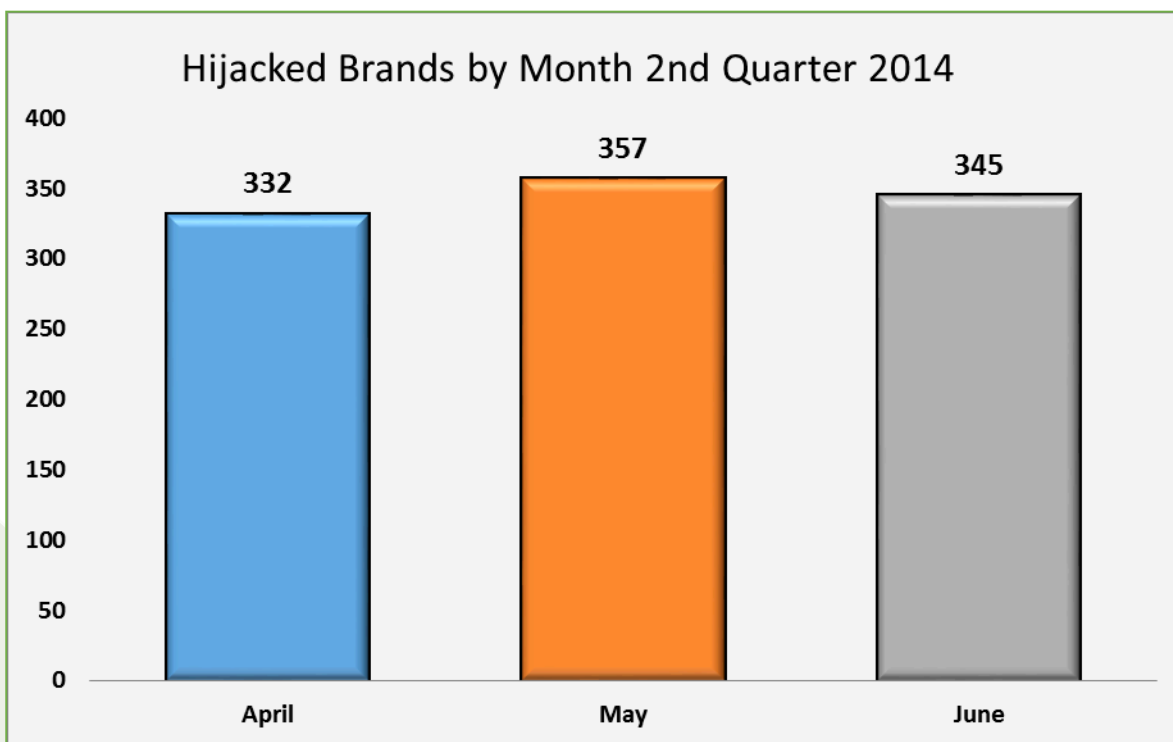
	April	May	June
Number of Unique Phishing Web Sites Detected	41,759	44,407	42,212
Unique Domains	7,847	9,405	9,801
Unique Brand-Domain Pairs	8,753	10,503	10,986
Unique Brands	332	357	345
URLs Per Brand	125.78	124.38	122.35

Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 2nd Quarter 2014

A total of 531 brands were targeted by phishers in Q2. This was down slightly from the 557 targeted in the first quarter of 2014. The number of brands targeted in any given month remained below the all-time high of 441 that was recorded in April 2013.

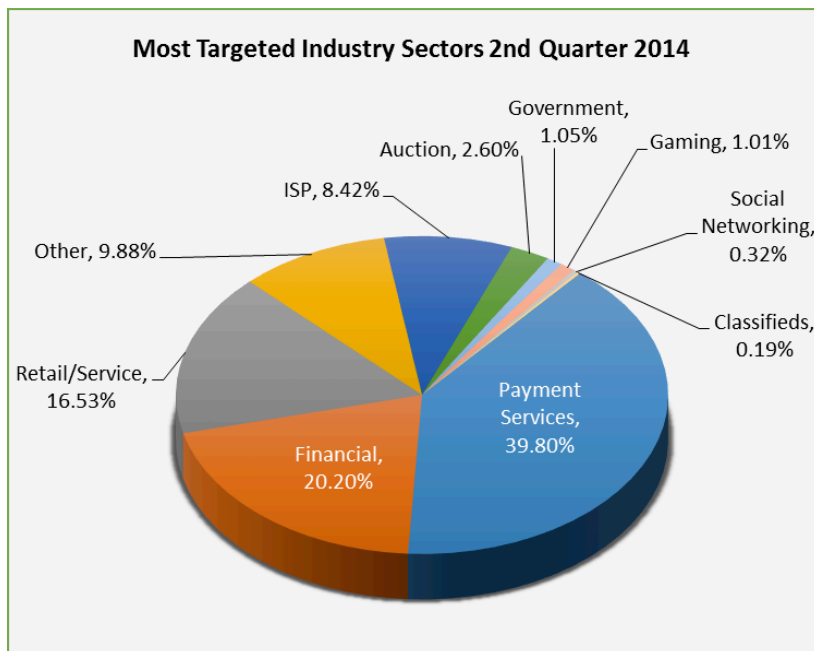
“So far in 2014 we have seen a number of new targets that we did not see in 2013,” said Greg Aaron, President of Illumintel and APWG Senior Research Fellow. “New online payment services are getting phished. Examples include the Austrian cashless payments site PayLife, Hong Kong-based alternate payment system Perfect Money, and Payoneer, an Internet-based financial services business that allows users to transfer money and receive payments through re-loadable prepaid MasterCard debit cards. We’re also seeing an uptick in phishing attacks against the users of Bitcoin sites, notably wallet service Blockchain and the exchange site Coinbase.”

In related news, cryptocurrency was the target of an innovative crime recently [described](#) by Dell SecureWorks. Between February and May 2014, a criminal hijacked traffic from several large ISPs, redirecting cryptocurrency miners' connections to a location controlled by the criminal. This allowed the criminal to collect an estimated \$83,000 in stolen mining profits.



Most-Targeted Industry Sectors – 2nd Quarter 2014

Payment Services continued to be the most-targeted industry sector in the second quarter of 2014, with 39.80 percent of attacks during the three-month period.



Countries Hosting Phishing Sites – 2nd Quarter 2014

The United States continued to be the top country hosting phishing sites during the second quarter of 2014. 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. Month-to-month variations are often attributable to mass breaches at hosting providers.

April		May		June	
United States	35.64%	United States	48.22%	United States	35.79%
Ukraine	17.29%	Germany	7.61%	China	4.32%
Hong Kong	10.36%	Russian Federation	4.86%	Germany	4.19%
United Kingdom	7.25%	United Kingdom	3.49%	Turkey	3.92%
Canada	3.03%	France	2.79%	Russian Federation	3.30%
Netherlands	0.54%	Hong Kong	2.53%	United Kingdom	2.80%
Russian Federation	0.43%	Turkey	2.36%	France	2.03%
France	0.39%	Canada	2.25%	Netherlands	1.85%
Germany	0.39%	Netherlands	2.07%	Poland	1.71%
Japan	0.24%	Poland	1.96%	Canada	1.67%

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 2014

During the second quarter of 2014, APWG member company PandaLabs gathered 15 million new malware samples, which represents an average of over 160,000 new samples created every day. (Most of these were slight variations on a much smaller number of malware families, created when malware morphed its code in order to avoid detection by antivirus programs.) While Trojans are still the most common type of malware, accounting for 58.20% of newly detected threats, this is notably lower than the percentage recorded in the previous quarter (71.85%). This is due to a substantial increase in PUPs (Potentially Unwanted Programs) such as spyware and adware.

There has been a significant increase in the creation of software bundlers: programs that install PUPs on computers along with the programs that the user actually wants to install, but without asking for the user's consent.

New Malware Strains in Q2	% of malware samples	Malware Infections by Type	% of malware samples
Trojans	58.20%	Trojans	62.80%
Viruses	0.38%	Viruses	2.68%
Worms	19.68%	Worms	2.66%
Adware/Spyware	0.39%	Adware/Spyware	7.09%
Other	21.35%	Other	24.77%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, the global infection rate was 36.87%, a significant rise on recent quarters, once again due to the emergence of PUPs. Regarding the data across different countries, China is once again at the top of chart, with an infection rate of 51.05%. China is followed by Peru (44.34%) and Turkey (44.12%).

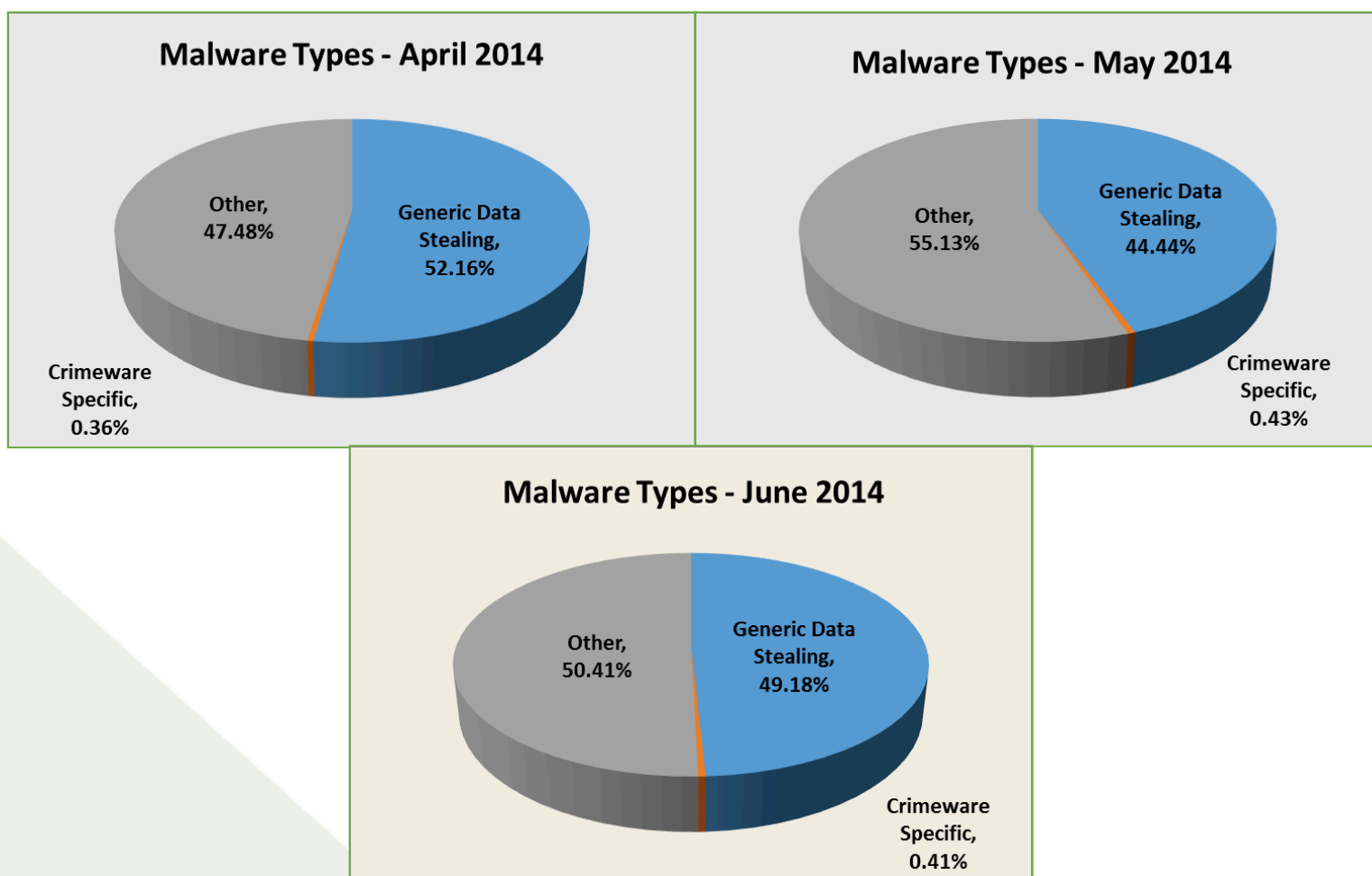
Europe in general is the area with the lowest infection rates. Sweden (22.13%), Norway (22.26%) and Germany (22.88%) are the countries with least infections worldwide. The only non-European country in the top ten most-secure is Japan, which is in fourth place at 24.21%.

Ranking	Country	Infection Rate	Ranking	Country	Infection ratio
1	China	51.05%	45	Netherlands	26.97%
2	Peru	44.34%	44	Portugal	26.28%
3	Turkey	44.12%	43	Belgium	26.06%
4	Bolivia	43.76%	42	Switzerland	25.78%
5	Ecuador	43.13%	41	UK	25.45%
6	Russia	42.89%	40	France	24.88%
7	Argentina	40.57%	39	Japan	24.21%
8	Taiwan	39.63%	38	Germany	22.88%
9	El Salvador	38.51%	37	Norway	22.26%
10	Slovenia	38.25%	36	Sweden	22.13%

Measurement of Detected Crimeware – 2nd 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.)



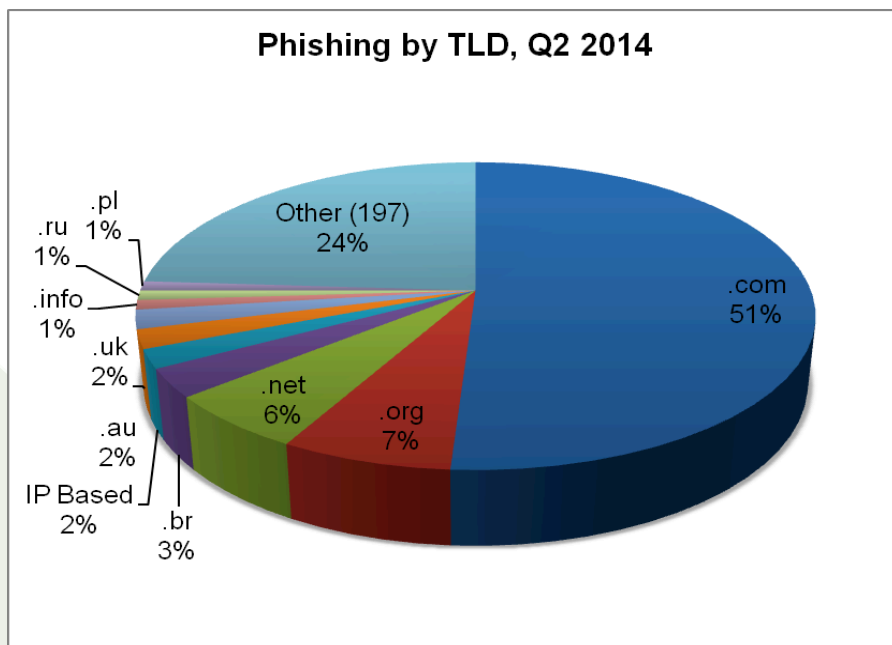
Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

The United States remained the top country hosting phishing-based Trojans and downloaders during the three month period. 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	
United States	77.35%	United States	64.41%	United States	60.20%
China	5.82%	Germany	12.32%	China	8.29%
Russian Federation	1.70%	China	6.11%	Germany	7.47%
Ukraine	1.68%	Russian Federation	2.02%	Netherlands	2.60%
Germany	1.49%	Ukraine	1.84%	Brazil	2.39%
Rep. of Korea	1.38%	France	1.57%	Russian Federation	2.17%
France	1.20%	United Kingdom	1.29%	France	1.74%
Netherlands	0.98%	Brazil	1.26%	Thailand	1.30%
Brazil	0.98%	Rep of Korea	1.11%	Rep. of Korea	1.26%
United Kingdom	0.85%	Netherlands	1.02%	United Kingdom	1.22%






Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing sites. Fifty-one percent of domains used for phishing were .COM names, up from 46 percent in the previous quarter. The .COM TLD represents approximately 42 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, 2nd 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. 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 lcorrns@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.mynt.com).