

Phishing Activity Trends Report

2nd Quarter
2016

APWG

Unifying the
Global Response
To Cybercrime

April – June 2016

Published Oct. 3, 2016

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.

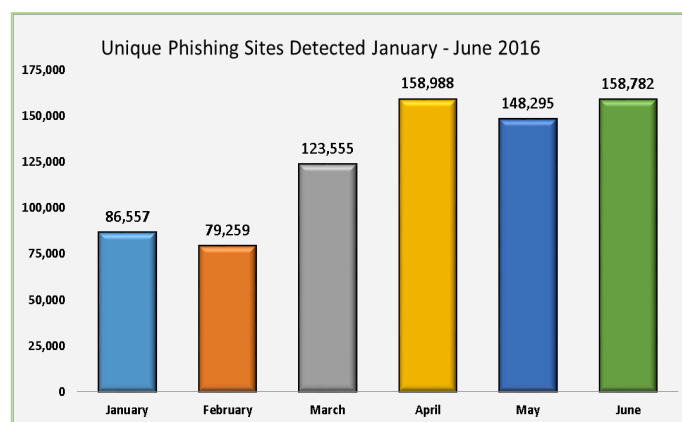
Phishing Defined

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 2016	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
Top Malware Infected Countries	8
APWG Phishing Trends Report Contributors	9

Phishing Attacks In Q2 2016 Shatter All Records to Reach All-Time High



The total number of unique phishing sites observed in the second quarter of 2016 was 466,065. This was 61% higher than the previous quarterly record in Q4, 2015. [pg. 4]

2nd Quarter 2016 Phishing Activity Trends Summary

- The Retail/Service sector remained the most-targeted industry sector during the second quarter of 2016, suffering 43% of attacks [pg. 7]
- The number of brands targeted by phishers in the second quarter remained consistent – ranging from 411 to 425 different brands each month [p. 6]
- Ransomware continued to be a pervasive threat. 18 million new malware samples were found in Q2, an average of +200,000 a day [p. 8]
- The country most infected with malware was China, where 49.02 percent of computers encountered infections, followed by Taiwan (47.34%) and Turkey with 40.99% [p. 8]
- The countries with the lowest infection rates were generally European, with the Scandinavian countries having the lowest percentages of infections [p. 8]

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 tracks and reports the number of unique phishing reports (email campaigns) it receives, in addition to the number of unique phishing sites found. 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 found in a given month that have 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 2016

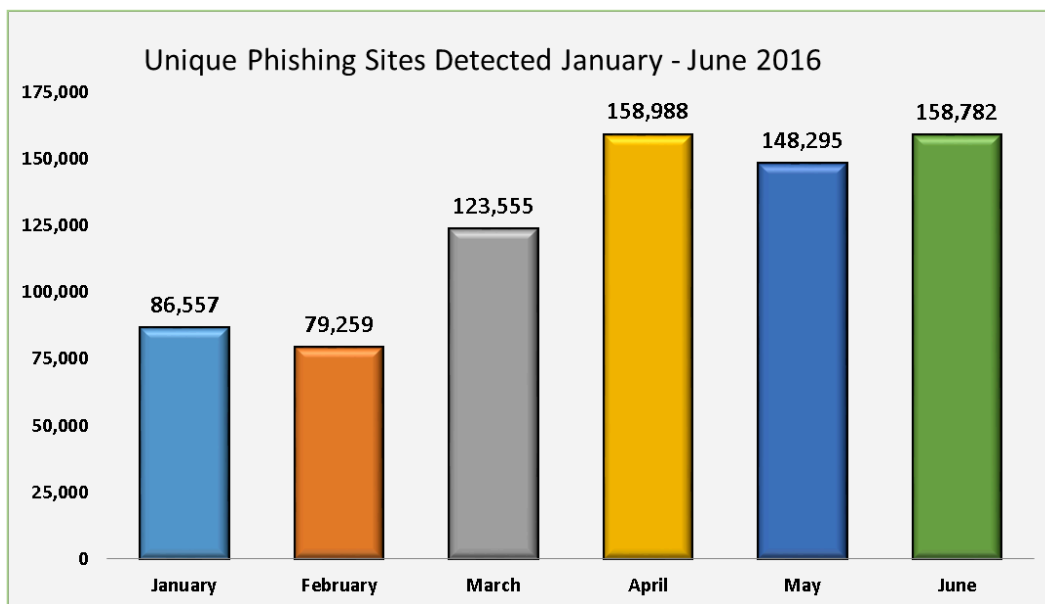
	April	May	June
Number of unique phishing websites detected	158,988	148,295	158,782
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	121,028	96,490	98,006
Number of brands targeted by phishing campaigns	411	425	418

Phishing Activity Trends Report, 2nd Quarter 2016

Phishing E-mail Reports and Phishing Site Trends – 2nd Quarter 2016

The total number of unique phishing sites observed in the second quarter of 2016 was 466,065. This was an all-time high. The second quarter's total was up 61% from the 289,371 phish found in the first quarter of 2016, which was the previous high. The Q2 total was almost three times the 158,574 phishing websites found in Q4 2015.

According to Stefanie Ellis, AntiFraud Product Marketing Manager at MarkMonitor, "In Q2, MarkMonitor saw the highest phishing volumes we have ever detected. While some of the increase can be attributed to enhancements to our data technologies, some of the activity was tied to big campaigns that attacked service or cloud organizations."



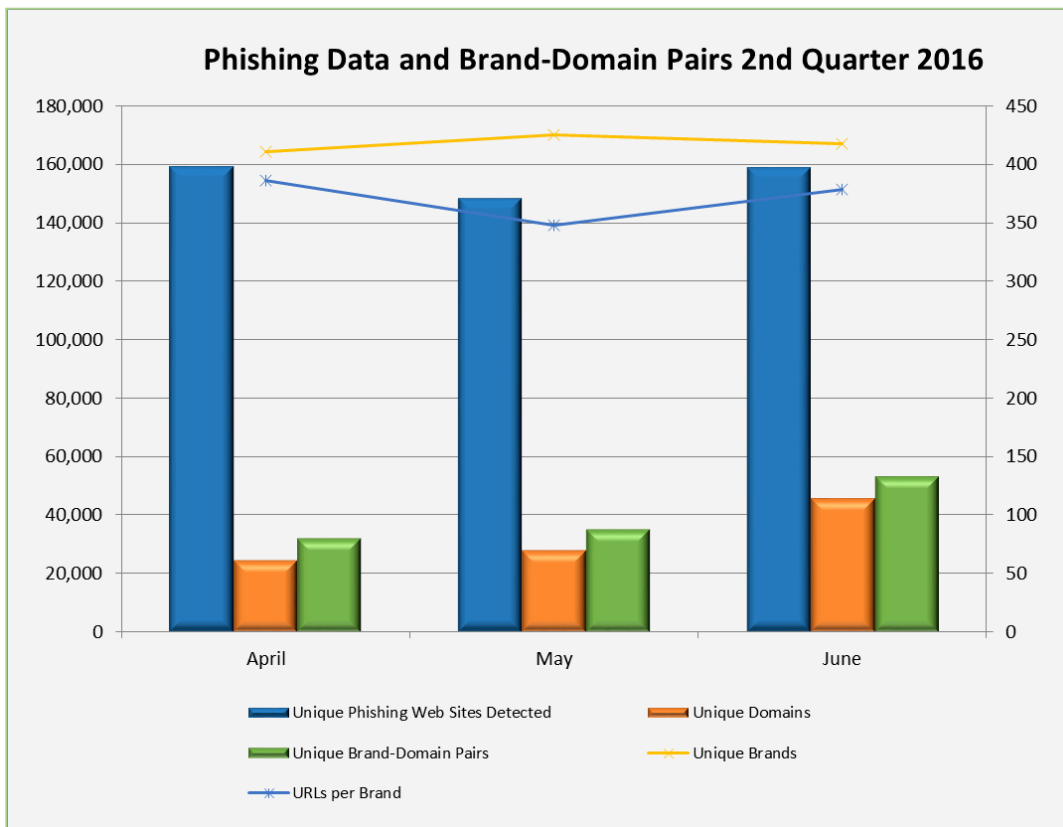
The number of unique phishing reports submitted to APWG during Q2 was 315,524. Additional historical reports were submitted during research for this report and were not counted in the totals below.



4

Brand-Domain Pairs Measurement – 2nd Quarter 2016

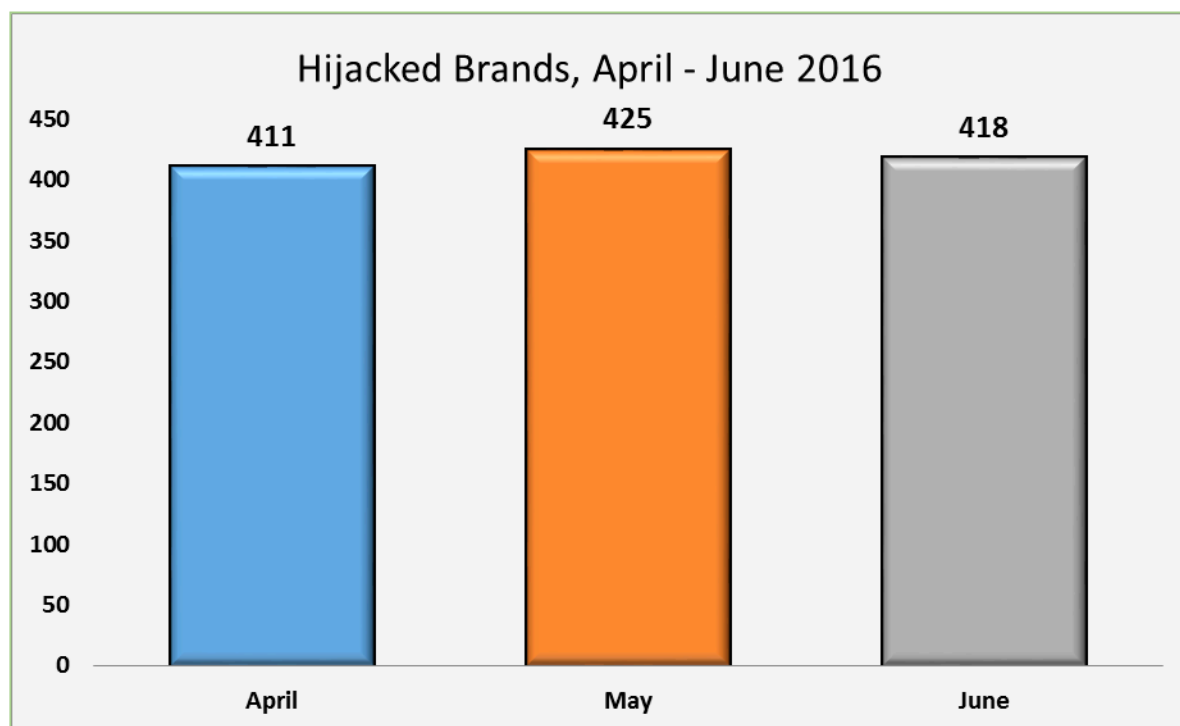
The following chart combines statistics based on brands phished, unique domains, unique domain/brand pairs, and unique URLs. Brand/domain pairs count the unique instances of a domain being used to target a specific brand. (*Example:* if several URLs are targeting a brand – but are hosted on the same 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.



	April	May	June
Number of Unique Phishing Web Sites Detected	158,988	148,295	158,782
Unique Domains	24,771	27,971	45,683
Unique Brand-Domain Pairs	32,188	35,332	53,209
Unique Brands	411	425	418
URLs Per Brand	386	348	379

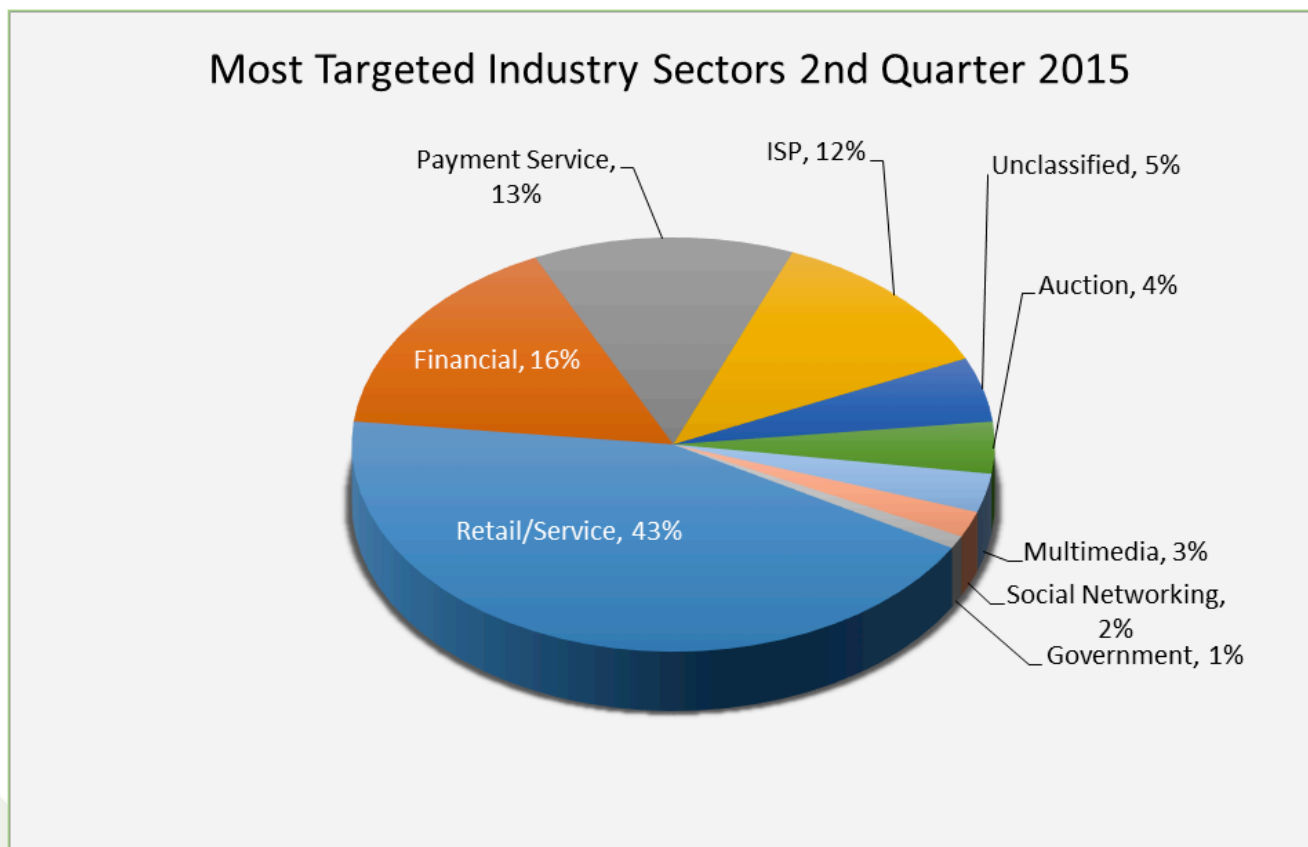
Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 2nd Quarter 2016

The number of brands targeted by phishers in the second quarter remained consistent – ranging from 411 to 425 brands each month. Across 2015 and through the first half of 2016, phishers targeted between 393 and 442 unique brands in any given month.



Most-Targeted Industry Sectors – 2nd Quarter 2016

The Retail/Service sector was the most-targeted industry sector during the second quarter of 2016, as it also was in the first quarter of the year. About 43 percent of phishing attacks targeted the Retail/Service sector. The Financial Services and Payment Service sectors were second and third, suffering an additional 16 percent and 13 percent of attacks respectively.



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 2016

APWG member PandaLabs found 18 million new malware samples in Q2, an average of more than 200,000 a day. This is 10 percent lower than in the previous quarter, when 20 million new samples were found. Trojans are the most pervasive type of malware and have been leading these statistics for years. Ransomware malware attacks, which are included in the same category, have increased markedly.

New Malware Strains in Q1	% of malware samples
Trojans	71.53%
Virus	12.36%
Worms	10.05%
Adware / Spyware	2.01%
PUPs	4.05%

Malware Infections by Type	% of malware samples
Trojans	67.01%
Virus	1.54%
Worms	3.33%
Adware / Spyware	1.09%
PUPs	27.03%






According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, the overall percentage of infected computers was 29.05 percent, lower than the previous quarter. The world's most-infected country was China, where 49.02 percent of machines are infected, followed by Taiwan (47.34%) and Turkey (40.99%).

The countries with the lowest infection rates were mostly in western Europe. Scandinavian countries had the lowest infection rates: Sweden had just a 19.88 percent infection rate, followed by Finland with 20.65 percent; and Norway with 21.63 percent.

Ranking	Country	Infection Rate
1	China	49.02%
2	Taiwan	47.34%
3	Turkey	40.99%
4	Russia	38.95%
5	Guatemala	37.56%
6	Mexico	36.89%
7	Peru	36.23%
8	Guatemala	36.22%
9	Brazil	34.68%
10	Poland	33.01%

Ranking	Country	Infection ratio
45	The Netherlands	24.86%
44	Denmark	24.34%
43	Germany	24.12%
42	Switzerland	23.94%
41	United Kingdom	23.38%
40	Belgium	22.78%
39	Japan	22.24%
38	Norway	21.63%
37	Finland	20.65%
36	Sweden	19.88%

APWG Phishing Activity Trends Report Contributors

 <p>iThreat provides risk data, intelligence tools, and analysis to help its clients protect their intellectual & Internet properties.</p>	 <p>An Infoblox company, IID is a 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>Forcepoint brings a fresh approach to address the constantly evolving cybersecurity challenges and regulatory requirements facing businesses and government agencies.</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; Stefanie Ellis at Stefanie.ellis@markmonitor.com; or Luis Corrons of Panda Security at lcorrns@pandasoftware.es.

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry and international affairs 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.

Websites of APWG public-service enterprises include its public website, <<http://www.apwg.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 501(c)6 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 was incorporated in 2004 as an independent corporation controlled by its board of directors, its executives and its steering committee.

9

Analysis by Greg Aaron, [iThreat Cyber Group](http://www.ithreat.com); editing by Ronnie Manning, [Mynt Public Relations](http://www.mynt.com).