

Phishing Activity Trends Report

1st-3rd Quarters

APWG

2015

Unifying the
Global Response
To Cybercrime

January – September 2015

Published December 23, 2015

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.

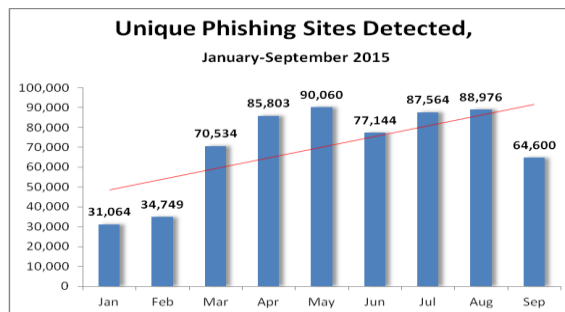
Phishing Defined

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 1st – 3rd Quarters 2015	3
Phishing Site Trends 1st-3rd Quarters 2015	4
Brand-Domain Pairs Measurement	5
Brands & Entities Hijacked by E-mail	
Phishing Attacks	6
Most Targeted Industry Sectors	8
Countries Hosting Phishing Sites	9
Malware-Infected Countries	10
Measurement of Detected Crimeware	12
Phishing-based Trojans & Downloaders Host	
Countries (by IP address)	13
APWG Phishing Trends Report Contributors	14

Phishing Not Showing Any Signs of Slowing in 2015



Both consumer-facing phishing and spear-phishing that targets specific business employees increased in 2015.

Q1 – Q3 2015 Phishing Activity Trends Summary

- "Business email compromise" (or BEC) scams became a major problem in 2015. These attacks often use spear-phishing techniques, and fool companies into transferring large amounts of money to criminals. [pp. 6-7]
- The total number of unique phishing sites detected from Q1 through Q3 was 630,494. [p. 4]
- ISPs were the most-targeted industry sector during the first three quarters of 2015, surpassing the banking and financial services sectors. [p. 8]
- In September, Belize became the top country hosting phishing sites, briefly surpassing the United States. [p. 9]
- Computers around the world continue to be infected with malware at a high rate. The global infection rate was 36.51% in Q1, 32.21% in Q2, and 32.12% in Q3 of 2015 [pp. 10-11]

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

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 1st – 3rd Quarters 2015

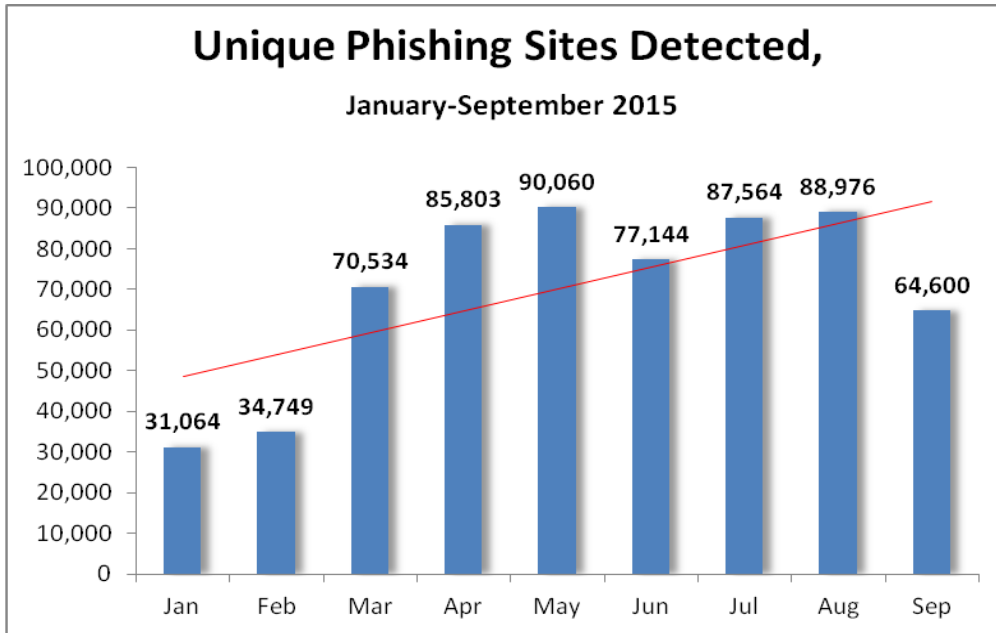
	Jan	Feb	Mar	April	May	June	July	Aug	Sept
Number of unique phishing websites detected	31,064	34,749	70,534	85,803	90,060	77,144	87,564	88,976	64,600
Number of unique phishing e-mail reports (campaigns) received	49,608	55,795	115,808	142,099	149,616	125,757	142,155	146,439	106,421
Number of brands targeted by phishing campaigns	420	438	421	393	404	420	434	442	402
Country hosting the most phishing websites	USA	USA	USA	USA	USA	USA	USA	USA	Belize
Contain some form of target name in URL	60.4%	67.4%	76.8%	69.2%	65.0%	73.1%	76.1%	76.8%	81.3%
Percentage of sites not using port 80	0.60%	1.56%	1.46%	2.19%	2.55%	2.73%	3.49%	3.68%	2.73%

Below we provide additional insights about these statistics.

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

Phishing Site Trends and E-mail Reports: 1st – 3rd Quarters 2015

The total number of unique phishing sites detected from Q1 through Q3 was 630,494. The total number detected in Q2 was 253,007, and the number detected in Q3 was 241,140.



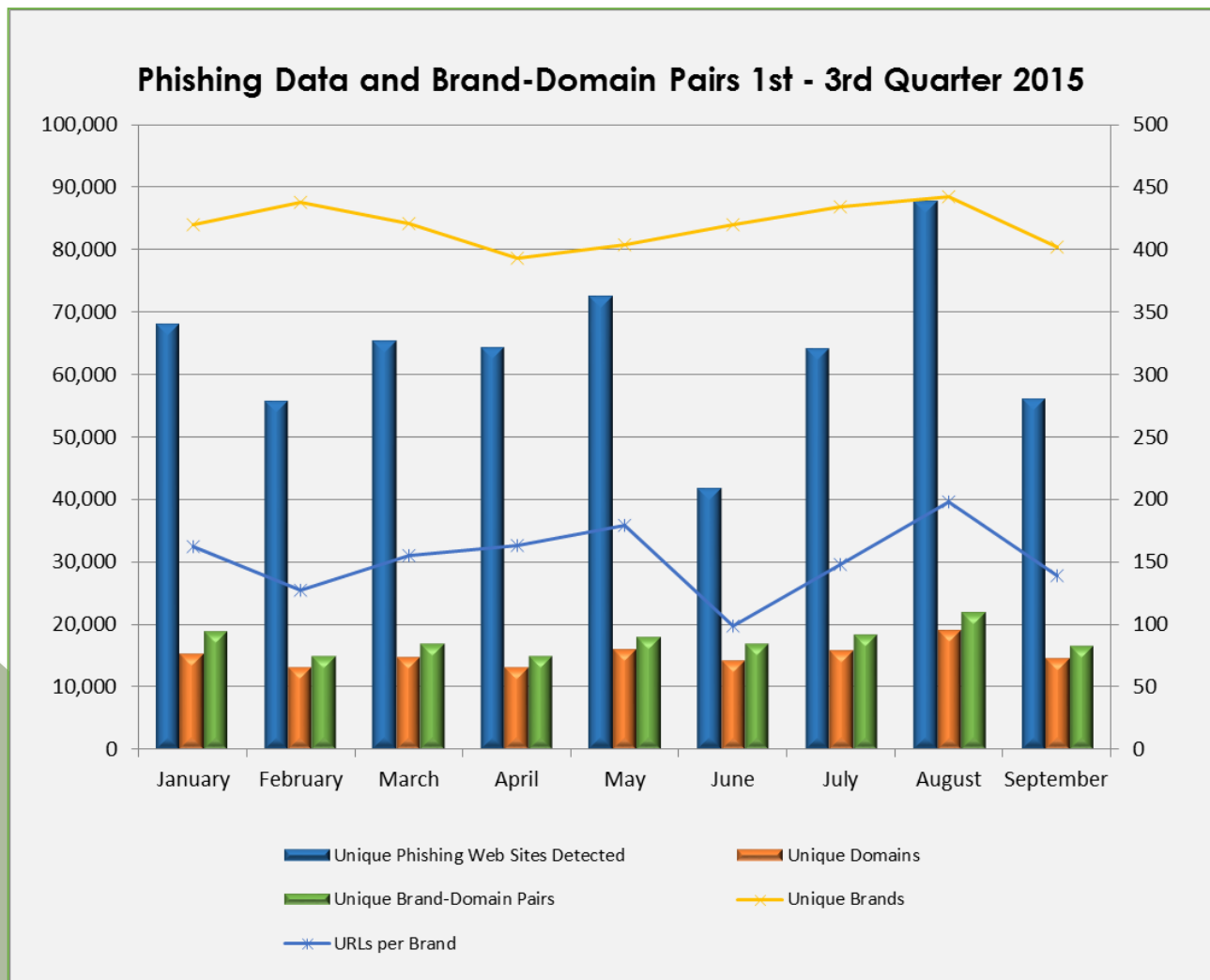
The number of unique phishing reports submitted to APWG from Q1 through Q3 was 1,033,698. APWG is now receiving twice as many reports as it did in 2014.



Phishing Activity Trends Report, 1st – 3rd Quarters 2015

Brand-Domain Pairs Measurement: 1st – 3rd Quarters 2015

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.

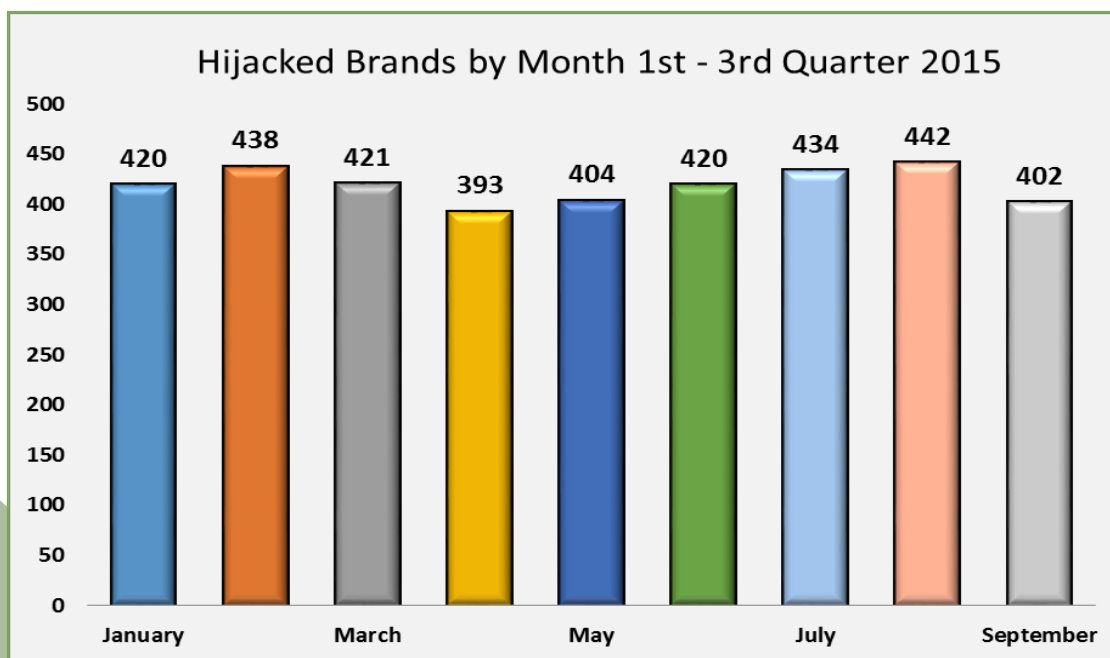


Phishing Activity Trends Report, 1st – 3rd Quarters 2015

	Jan	Feb	Mar	April	May	June	July	Aug	Sept
Number of Unique Phishing Web Sites	68,185	55,869	65,530	64,328	72,709	41,852	64,275	87,801	56,196
Unique Domains	15,122	13,032	14,700	12,980	15,944	14,138	15,789	18,912	14,377
Unique Brand-Domain Pairs	18,791	14,741	16,821	14,750	17,932	16,705	18,177	21,839	16,463
Unique Brands	420	438	421	393	404	420	434	442	402
URLs Per Brand	162	127	155	163	179	99	148	198	139

Brands and Entities Targeted by E-mail Phishing Attacks: 1st – 3rd Quarters 2015

The number of brands attacked per month remained steady month-to-month across the first three quarters of 2015:



The above numbers measure widely distributed, general attacks against online companies. They do not measure “spear-phishing” attacks, which are highly selective attacks that target specific employees at specific companies. Because such attacks are not widely broadcast via mass spamming, and may involve only a few email lures, there

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

are no reliable numbers regarding how many companies are being attacked in this fashion. However, we do know that Business Email Compromise (BEC) scams were a scourge to many businesses in 2015, with the FBI reporting a 270% increase in reported global losses from January to August 2015. [<https://www.ic3.gov/media/2015/150122.aspx>]

“BEC scams seek to socially engineer the employees of a business to perform a wire transfer to an account under the control of the attacker,” according to Carl Leonard, Principal Security Analyst at APWG member Raytheon|Websense. “The attacks use a form of spear-phishing, and initial attacks sent the spear-phishing emails from free domain names that closely resembled the victim company's domain name. Later attacks used a forged “from” address that matched the victim’s domain, with reply-to headers forcing the victim’s email client to reply to an external email address. We strongly encourage that businesses educate their employees about the dangers of these scams and implement technologies that intercept the incoming emails.”

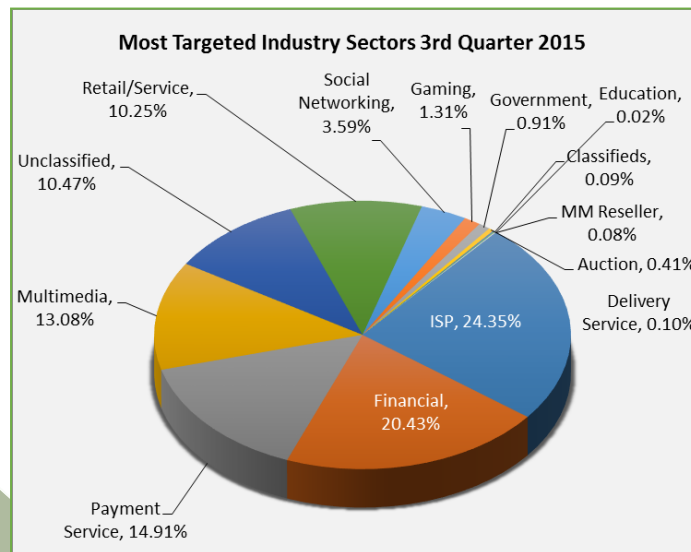
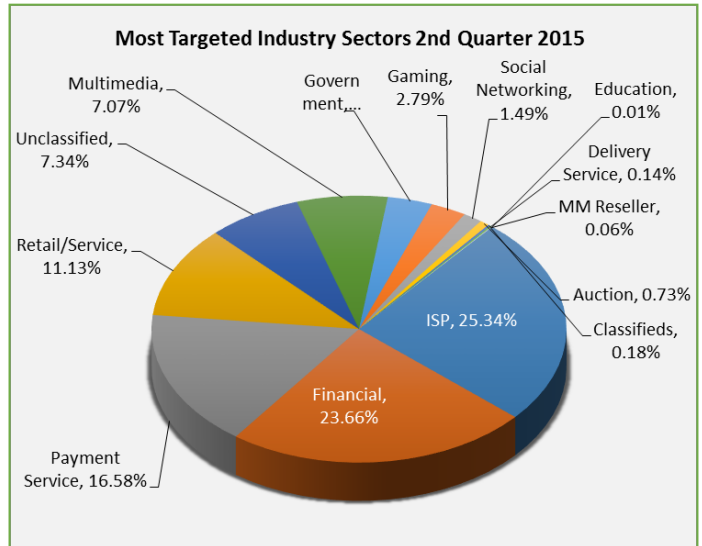
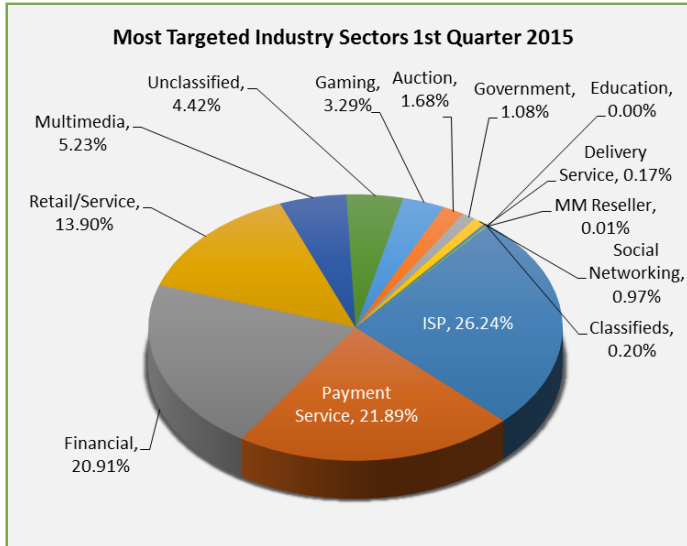
APWG Senior Research Fellow Greg Aaron noted: “All types of companies are vulnerable to BEC scams. It’s not just large companies – I’ve seen companies with under eight employees being targeted. All businesses should assume that they have been researched by a criminal. Businesses can protect themselves by allowing bank transfers only after multiple approvals.”

Leonard added: “Beyond phishing for bank account details we have seen that attackers adopt numerous tactics to solicit email address and password combination from employees. Typically they lure an end-user to a web page designed to capture the user’s email account credentials. The compromised email account is then used to attack more businesses by sending spam, phishing, and malicious emails. It is therefore vitally important to disrupt the attack in the early stages of the threat lifecycle.”

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

Most-Targeted Industry Sectors: 1st – 3rd Quarter 2015

According to contributing member MarkMonitor, Internet Service Providers (ISPs) became the most-targeted industry sector during the first three quarters of 2015, with the Payment Services and Financial (banks) sectors coming in second and third during the nine-month period. Phishers sometimes break into ISP accounts so that they can send spam from those user accounts. ISP accounts can also contain other things that phishers want: personally identifiable information, credit card details, and access to domain name and hosting management.



Phishing Activity Trends Report, 1st – 3rd Quarters 2015

Countries Hosting Phishing Sites: 1st – 3rd Quarters 2015

Phishers often break into vulnerable web hosting to find hosting for their phishing sites. Belize was the top country hosting phishing sites in September, surpassing the United States. Web servers in Belize were broken into by phishers, leading to the temporary increase. The USA hosts a large percentage of the world's web sites.

January		February		March	
United States	35.47%	United States	64.16%	United States	60.30%
Chile	32.97%	Hong Kong	4.03%	Sweden	13.48%
Germany	2.89%	Germany	3.06%	Belize	7.01%
United Kingdom	2.75%	Belize	2.55%	Belgium	2.16%
Russia	2.15%	United Kingdom	2.51%	United Kingdom	1.97%
France	1.96%	France	2.17%	France	1.41%
Canada	1.71%	Canada	1.80%	Germany	1.26%
Turkey	1.66%	Belgium	1.67%	Canada	0.84%
Netherlands	1.42%	Russia	1.55%	Turkey	0.82%
Bulgaria	1.27%	Netherlands	1.42%	Hong Kong	0.71%

April		May		June	
United States	61.92%	United States	54.09%	United States	60.99%
Belize	10.94%	Belize	13.27%	Belize	15.39%
France	2.40%	Italy	3.89%	Belgium	3.95%
Hong Kong	2.33%	United Kingdom	2.64%	Hong Kong	3.03%
United Kingdom	1.89%	France	2.09%	United Kingdom	1.65%
Italy	1.72%	Germany	2.00%	France	1.32%
Poland	1.54%	Belgium	1.78%	Germany	1.25%
China	1.38%	Russia	1.68%	Netherlands	1.08%
Germany	1.34%	Netherlands	1.56%	Italy	0.92%
Russia	1.22%	Turkey	1.44%	Canada	0.74%

July		August		September	
United States	54.29%	United States	45.52%	Belize	52.65%
Belize	26.28%	Belize	37.25%	United States	36.69%
Belgium	3.89%	Europe	2.62%	United Kingdom	0.97%
Hong Kong	3.11%	Belgium	1.99%	Netherlands	0.86%
France	1.48%	Hong Kong	1.89%	Canada	0.72%
United Kingdom	0.97%	United Kingdom	1.13%	Germany	0.69%
Germany	0.89%	Canada	0.90%	France	0.60%
Canada	0.85%	Germany	0.85%	India	0.52%
Italy	0.83%	France	0.60%	Russia	0.48%
Netherlands	0.74%	Netherlands	0.59%	Turkey	0.36%

Crimeware Taxonomy and Samples According to Classification

The APWG's Crimeware statistics categorize crimeware attacks as follows. 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: 1st – 3rd Quarters 2015

APWG member PandaLabs tracks the number of malware variants detected. PandaLabs detected 21 million unique malware samples during the third quarter of this year, down slightly from the 23.5 million seen in 4Q 2014. These are new malware binaries, which does not mean that each and every one of them is a completely new and original threat. The vast majority are variants of existing malware modified by their creators to evade signature-based detection systems.

New Malware Strains in Q1	% of malware samples
Trojans	72.75%
Viruses	14.85%
Worms	4.52%
Adware/Spyware	4.51%
Other	3.37%

New Malware Strains in Q2	% of malware samples
Trojans	71.16%
Viruses	10.83%
Worms	5.68%
Adware/Spyware	4.32%
Other	7.57%

New Malware Strains in Q3	% of malware samples
Trojans	69.15%
Viruses	11.34%
Worms	6.23%
Adware/Spyware	5.32%
Other	7.96%

Malware Infections by Type Q1	% of malware samples
Trojans	76.05%
Viruses	1.68%
Worms	2.57%
Adware/Spyware	5.17%
Other	14.53%

Malware Infections by Type Q2	% of malware samples
Trojans	76.25%
Viruses	1.53%
Worms	2.63%
Adware/Spyware	5.43%
Other	14.39%

Malware Infections by Type Q3	% of malware samples
Trojans	77.64%
Viruses	1.57%
Worms	3.20%
Adware/Spyware	4.74%
Other	12.85%

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, the global infection rate was 36.51% in Q1, 32.21% in Q2, and 32.12% in Q3 – steady from 2014. The highest infection rates were in Asian and Latin American countries. In general, Europe is the region with the lowest infection rates.

"Companies must be prepared as attacks are becoming more complex and hard to distinguish," Corrons stated. "Spear phishing campaigns are growing, all of them with the same goal: set a foot on corporate networks to perpetrate large attacks to steal all kind of financial and confidential information. New approaches are needed, such as having advanced threat detection capabilities. CISOs need to know what is being executed in all servers and endpoints, with forensics capabilities in case an intrusion takes place."

Countries with the Highest Infection Rates – Q1	
China	48.01%
Turkey	43.33%
Peru	42.18%
Bolivia	41.45%
Russia	41.38%
Argentina	41.03%
Ecuador	40.57%
Taiwan	40.21%
El Salvador	39.89%
Guatemala	39.58%

Countries with the Lowest Infection Rates – Q1	
Portugal	27.83%
Belgium	27.39%
Netherlands	26.96%
Germany	26.52%
France	25.87%
UK	25.11%
Switzerland	24.61%
Japan	23.97%
Sweden	22.42%
Norway	20.07%

Countries with the Highest Infection Rates – Q2	
China	47.53%
Turkey	43.11%
Peru	41.97%
Russia	41.15%
Argentina	40.93%
Bolivia	40.13%
Taiwan	39.57%
Guatemala	39.21%
El Salvador	39.02%
Ecuador	38.89%

Countries with the Lowest Infection Rates – Q2	
Netherlands	27.83%
Portugal	27.39%
Belgium	26.96%
France	26.52%
Germany	25.87%
UK	25.17%
Switzerland	24.41%
Japan	23.57%
Norway	22.22%
Sweden	21.57%

Countries with the Highest Infection Rates – Q3	
China	45.35%
Turkey	42.89%
Peru	40.99%
Russia	38.32%
Taiwan	37.82%
Bolivia	37.13%
Guatemala	36.75%
El Salvador	35.32%
Ecuador	35.02%
Argentina	34.78%

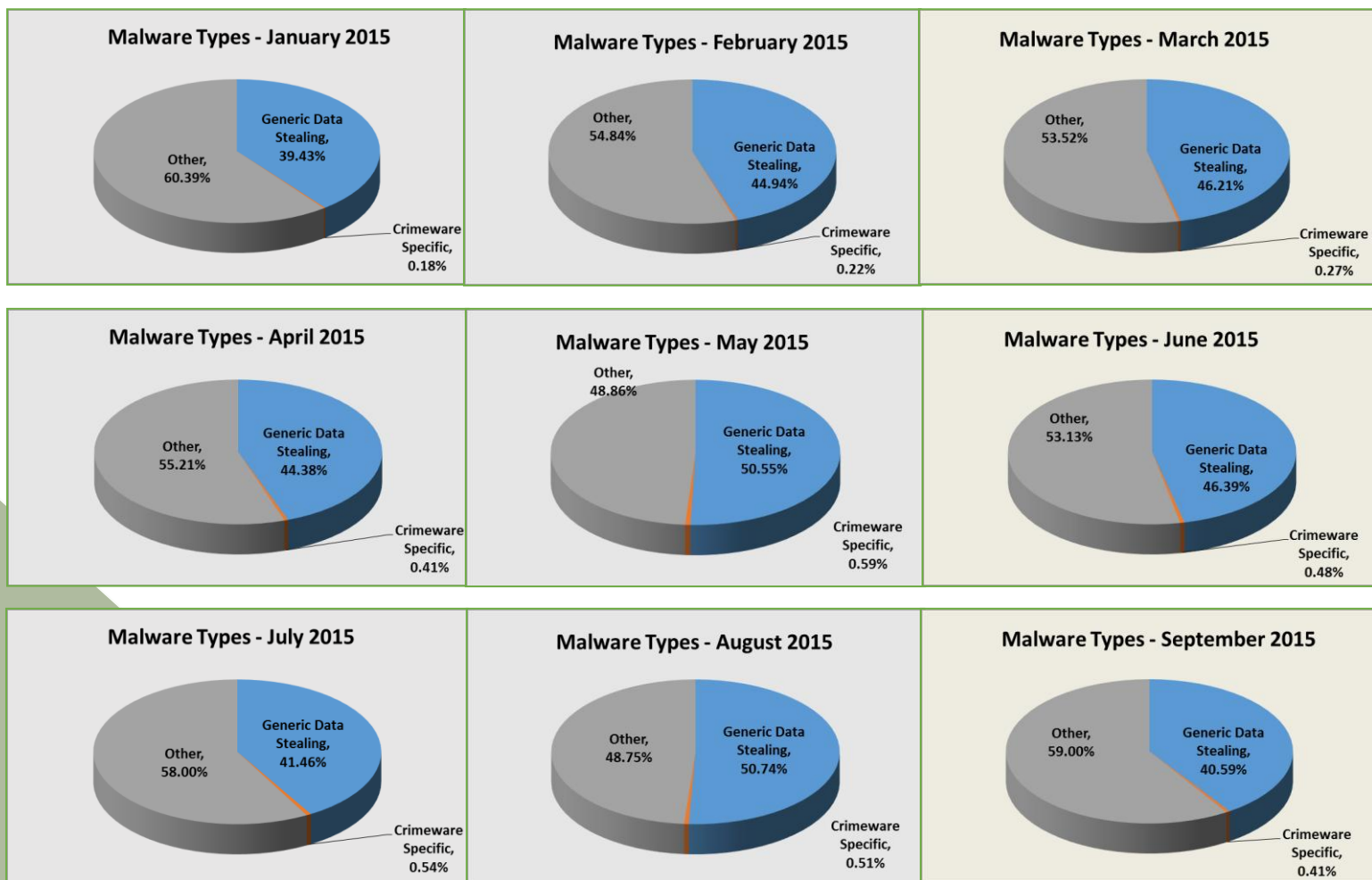
Countries with the Lowest Infection Rates – Q3	
Portugal	26.38%
Netherlands	26.22%
Belgium	25.96%
France	25.02%
Germany	24.87%
UK	24.17%
Switzerland	23.57%
Japan	22.75%
Sweden	21.33%
Norway	20.12%

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

Measurement of Detected Crimeware: 1st – 3rd Quarters 2015

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 Activity Trends Report, 1st – 3rd Quarters 2015

Phishing-based Trojans and Downloaders Hosting Countries (by IP Address)

The USA remained the top country hosting phishing-based Trojans and downloaders during the nine-month period.






January		February		March	
United States	34.24%	United States	40.22%	United States	57.82%
Netherlands	18.53%	China	26.05%	China	10.41%
China	8.34%	Germany	3.14%	Germany	3.50%
Georgia	6.85%	Netherlands	2.92%	Netherlands	3.46%
Ukraine	3.78%	Russia	2.81%	Russia	3.24%
Thailand	3.42%	France	2.70%	United Kingdom	2.46%
France	3.07%	Georgia	2.27%	Thailand	2.03%
Russia	2.99%	Brazil	2.16%	Brazil	1.86%
Germany	2.46%	Canada	1.95%	France	1.73%
United Kingdom	1.76%	Thailand	1.73%	Rep. of Korea	1.56%

April		May		June	
United States	49.13%	United States	48.20%	United States	59.52%
China	17.51%	China	19.73%	Netherlands	4.76%
Germany	4.12%	Russia	3.77%	Rep. of Korea	4.76%
Russia	3.62%	France	3.09%	Germany	4.37%
Thailand	3.33%	Ireland	2.23%	China	3.97%
United Kingdom	2.97%	United Kingdom	2.06%	United Kingdom	3.17%
Netherlands	2.39%	Germany	2.06%	Vietnam	1.98%
France	2.24%	Poland	1.72%	Australia	1.59%
Canada	1.52%	Rep. of Korea	1.72%	Brazil	1.59%
Brazil	1.37%	Netherlands	1.37%	Ireland	1.59%

July		August		September	
United States	60.29%	United States	57.23%	United States	72.01%
China	14.26%	China	10.69%	China	6.69%
France	3.26%	Germany	4.40%	Canada	4.75%
Ireland	2.85%	Ukraine	4.40%	Russia	2.11%
Russia	2.44%	United Kingdom	4.40%	Netherlands	1.94%
Netherlands	2.04%	Netherlands	3.14%	United Kingdom	1.76%
Rep. of Korea	1.83%	Ireland	2.52%	France	1.76%
United Kingdom	1.63%	Hong Kong	1.89%	Germany	1.06%
Germany	1.63%	France	1.89%	Ukraine	1.06%
Canada	1.02%	Rep. of Korea	1.89%	Ireland	0.88%

Phishing Activity Trends Report, 1st – 3rd Quarters 2015

APWG Phishing Activity Trends Report Contributors

 <p>Illumintel Inc. provides advising and security services to Internet companies, intellectual property owners, and domain name registries.</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>Raytheon Websense 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.

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