Phishing Activity Trends Report

4th Quarter 2015

APWG

Unifying the
Global Response
To Cybercrime

October – December 2015

Published March 22, 2016

Phishing Report Scope

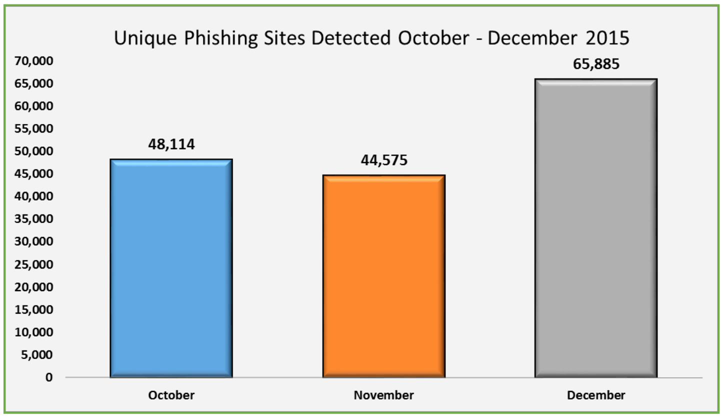
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, 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

Phishers Upped Attacks During the 2015 Holiday Season



Phishers unleashed a barrage with phishing scams in December 2015, in an annual attempt to part consumers from their money. [p. 4]

4th Quarter 2015 Phishing Activity Trends Summary

- Another holiday phenomenon was that the Retail / Service sector became the most-targeted industry sector in the fourth quarter of 2015, with 24.03% of all phishing attacks. [p. 7]
- There has been a notable increase in software bundlers, which install unwanted programs without the user's consent. [p. 8]
- Belize and the United States topped the list of countries that hosted phishing sites. [p. 7]
- The USA remained the top country hosting phishing-based Trojans and downloaders during the three-month period. [p. 10]
- The number of brands targeted by phishing remained constant throughout 2015, although new companies and institutions were always being targeted. [p. 6]
- In Q4 2015, 14 million new malware samples were captured. [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.

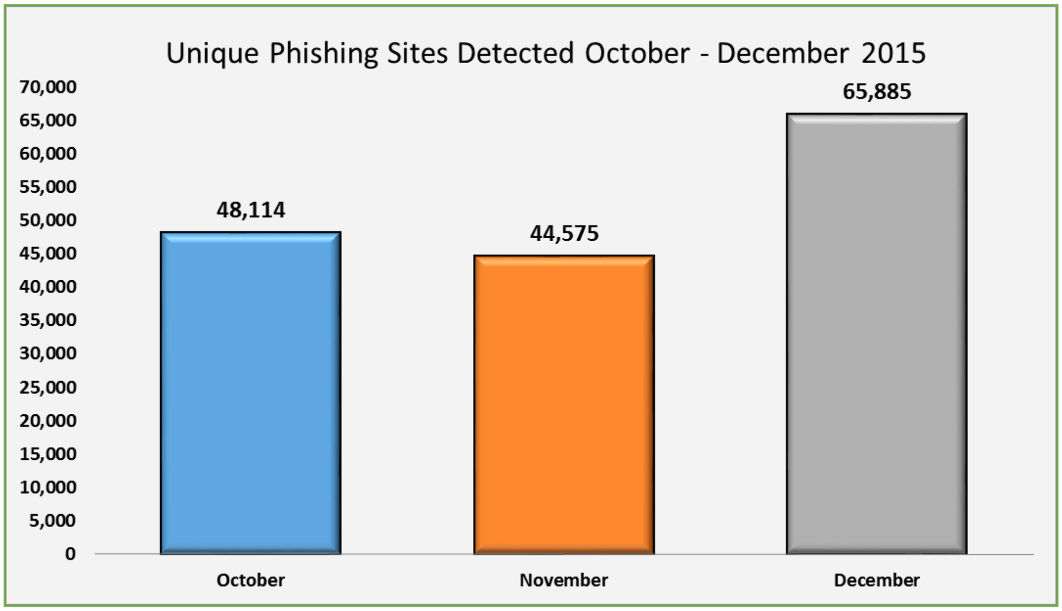
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances (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 4th Quarter 2015

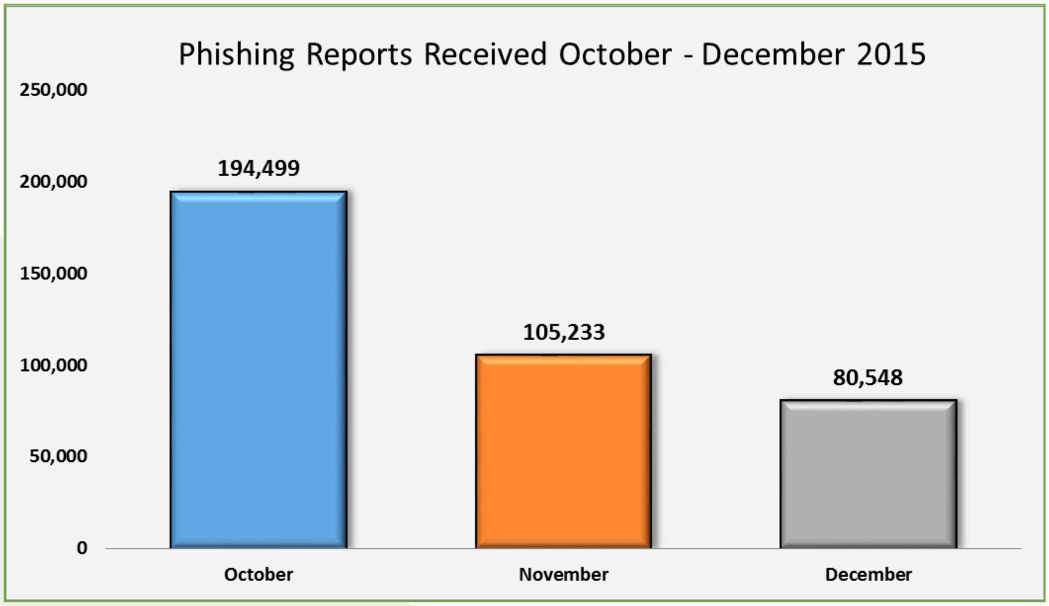
	October	November	December
Number of unique phishing websites detected	48,114	44,575	65,885
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	194,499	105,233	80,548
Number of brands targeted by phishing campaigns	391	408	406
Country hosting the most phishing websites	Belize	USA	USA
Phishing URL contains some form of target name	78.51%	72.61%	52.3%
Percentage of sites not using port 80	2.91%	3.98%	7.50%

Phishing E-mail Reports and Phishing Site Trends – 4th Quarter 2015

The total number of phishing attacks observed in Q4 was 158,574. APWG noted a large spike in phishing from November to December 2015, with an increase of over 21,000 phishing sites detected during the holiday season.

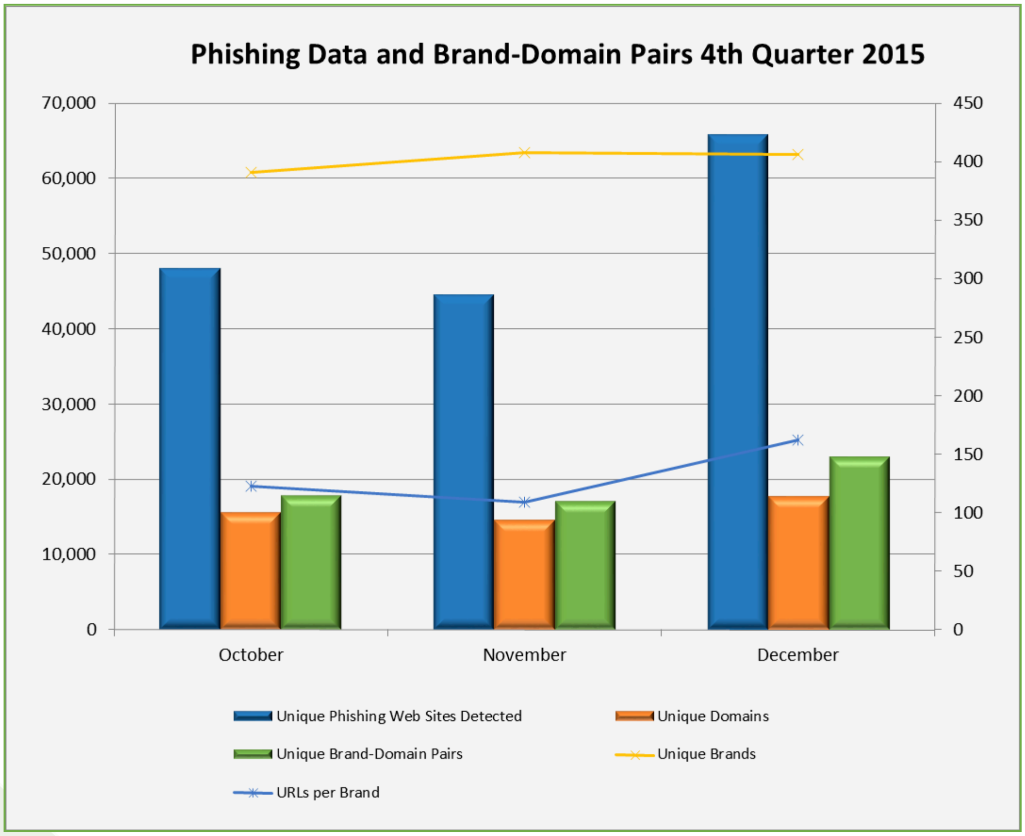


The number of unique phishing reports submitted to APWG during Q4 was 173,262. The number of unique phishing reports submitted to APWG saw a drop of nearly 15,000 from November to December.



Brand-Domain Pairs Measurement – 4th Quarter 2015

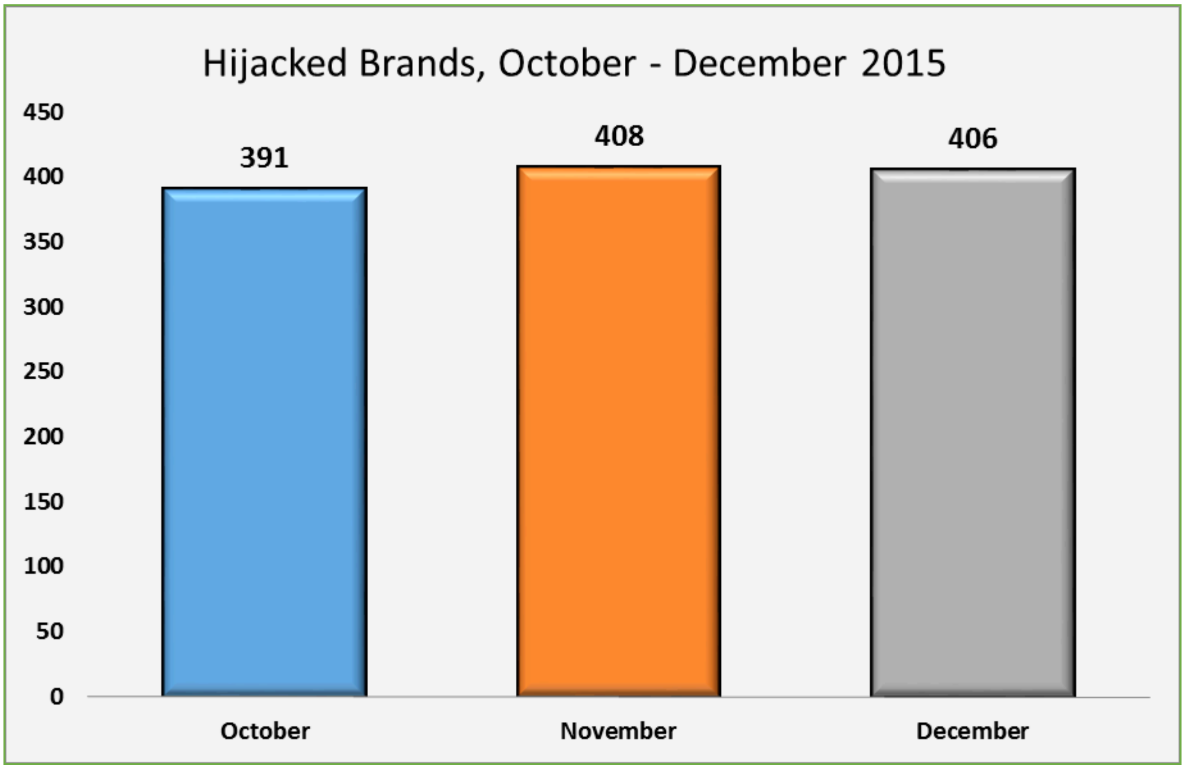
The following chart combines statistics based on brands phished, unique domains, unique domain/brand pairs, and unique URLs. Brand/domain pairs count the unique instances of a domain being used to target a specific brand. (*Example*: if several URLs are targeting a brand – but are hosted on the same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



	October	November	December
Number of Unique Phishing Web Sites Detected	48,114	44,575	65,885
Unique Domains	15,477	14,457	17,689
Unique Brand-Domain Pairs	17,711	17,032	22,882
Unique Brands	391	408	406
URLs Per Brand	123	109	162

Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 4th Quarter 2015

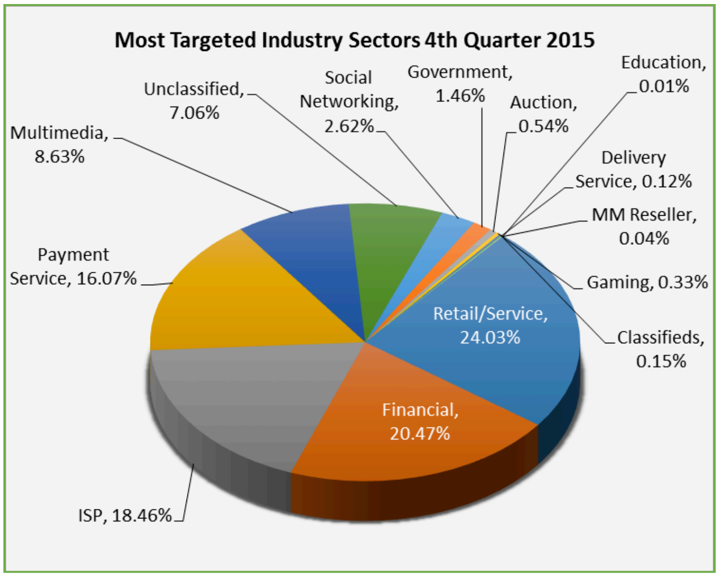
The number of brands targeted by phishers in each month of the quarter remained constant. Across 2015, phishers targeted between 393 and 442 unique brands in any given month. However, there was turnover among the companies that were targeted – a stream of new companies and institutions were phished for the first time.



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 are no reliable numbers regarding how many companies are being attacked in that fashion.

Most-Targeted Industry Sectors – 4th Quarter 2015

The Retail / Service sector became the most-targeted industry sector in the fourth quarter of 2015, with 24.03 percent of attacks, followed closely by Financial Services. In the first three quarters of 2015, ISPs had been the most-targeted industry segment.



Countries Hosting Phishing Sites – 4th Quarter 2015

Phishers often break into vulnerable web hosting networks to provision phishing sites. Belize was the top country hosting phishing sites in September and October, surpassing the United States. Web servers in Belize were broken into by phishers, leading to the temporary increase. According to Carl Leonard, Principal Security Analyst at Forcepoint, the US bias was due to a plethora of sites set up for fake Tech Support scams and fake anti-virus scams (often called “rogue anti-virus). These sites are designed to defraud people (encouraging them to pay a fee to "clean" their machine), or to install malware instead of the proffered anti-virus software.

October		November		December	
Belize	42.75%	United States	50.90%	United States	83.58%
United States	42.56%	Belize	27.22%	Netherlands	1.95%
Belgium	2.58%	Europe	4.65%	United Kingdom	1.51%
Europe	2.38%	Hong Kong	4.57%	Germany	1.26%
Germany	0.99%	China	1.14%	Australia	1.12%
United Kingdom	0.81%	Canada	1.09%	Hong Kong	0.86%
Canada	0.71%	Italy	0.88%	China	0.82%
Brazil	0.63%	Germany	0.86%	France	0.73%
Hong Kong	0.60%	United Kingdom	0.81%	Russian Federation	0.60%
France	0.50%	Australia	0.76%	Ireland	0.57%

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 – 4th Quarter 2015

In 2015, APWG member PandaLabs captured 84 million new malware samples, with 14 million of those captured in the fourth quarter of 2015. Most of them were variants of a much smaller number of pieces of malware, changed in small ways to avoid anti-malware defenses. By the end of 2015 PandaLabs had 304 million malware samples on file. There was a major increase in PUPs (Potentially Unwanted Programs) via software bundlers, which install programs without the user's consent. And there was a rise in different variants of Cryptolocker (ransomware) in the fourth quarter. The latter caused mayhem worldwide by locking users out of their data and demanding ransom payments.

New Malware Strains in Q4	% of malware samples
Trojans	53.05%
Viruses	23.48%
Worms	13.38%
Adware/Spyware	1.83%
PUP	8.26%

Malware Infections by Type	% of malware samples
Trojans	61.28%
Viruses	2.02%
Worms	2.40%
Adware/Spyware	5.25%
PUP	29.05%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, PUPs placed second, accounting for nearly a third of infections. Corrons noted: "Aggressive distribution techniques and software programs used by PUPs means that they achieve a high rate of installation in users' computers. If we look at the global percentage of infected computers, which is 35.45 percent, we can see that it increased compared to previous quarters, and this was mainly driven by PUPs. We must point out, however, that this figure represents computers that have had any type of malware encounter, but doesn't necessarily mean that they became infected."

Asia and Latin America were the regions that registered the highest infection rates. The countries with the lowest infection rates are generally in Europe, with Japan also appearing in the bottom ten.

Ranking	Country	Infection Rate
1	China	57.24%
2	Taiwan	49.15%
3	Turkey	42.52%
4	Guatemala	39.09%
5	Russia	38.01%
6	Ecuador	37.51%
7	Mexico	37.28%
8	Peru	37.06%
9	Poland	36.83%
10	Brazil	36.34%

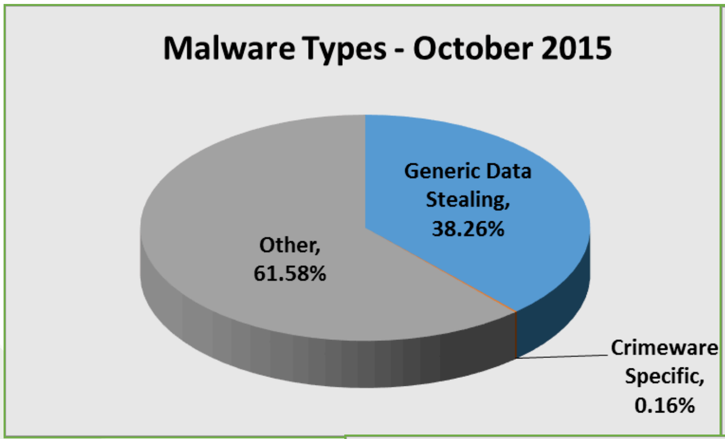
Ranking	Country	Infection ratio
45	Netherlands	26.51%
44	Japan	25.34%
43	Denmark	24.84%
42	Belgium	23.46%
41	Switzerland	23.16%
40	Germany	22.78%
39	UK	21.34%
38	Sweden	20.88%
37	Norway	20.51%
36	Finland	20.32%

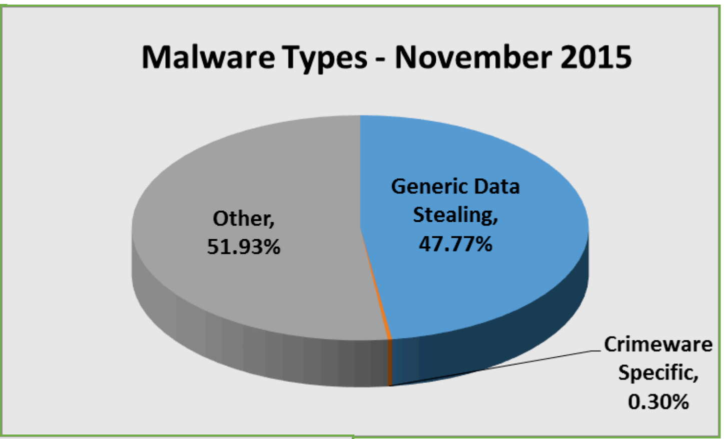
Measurement of Detected Crimeware – 4th Quarter 2015

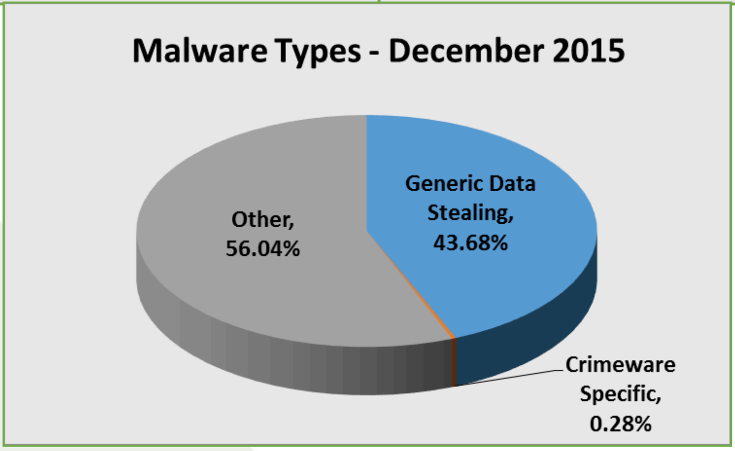
Using data contributed from APWG founding member Forcepoint regarding the proliferation of malevolent software, this metric measures proportions of three genera of malevolent code:

- *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.)

Accoring to Carl Leonard, Principal Security Analyst, Forcepoint, "In October 2015 the U.S. Department of Justice announced the arrest of the administrator of the Dridex or Bugat botnet. This botnet spread a malware package. Victims would see an email lure arrive into their inboxes, purporting to be an invoice or parcel delivery notification. The malware would then attempt to silently steal the recipient's online bank credentials." The botnet was allegedy used to steal at least US$10 million, and was disrupted by the FBI, Europol, GCHQ and the UK's National Crime Agency with assistance from private security organizations.







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.

October		November		December	
United States	67.52%	United States	70.12%	United States	71.09%
Canada	8.68%	Rep. of Korea	8.39%	China	6.80%
China	5.14%	China	6.82%	Rep. of Korea	3.23%
Netherlands	3.22%	Netherlands	3.01%	Netherlands	3.06%
Germany	2.25%	Germany	1.97%	Canada	2.72%
United Kingdom	1.93%	France	1.57%	Germany	2.04%
Portugal	1.29%	Canada	1.05%	Russian Federation	1.87%
Thailand	1.29%	Russian Federation	1.05%	France	1.53%
Ukraine	0.96%	Ukraine	0.66%	Singapore	0.51%
Vietnam	0.96%	Romania	0.52%	Israel	0.51%

APWG Phishing Activity Trends Report Contributors

iThreat Cyber Group iThreat provides risk data, intelligence tools, and analysis to help its clients protect their intellectual & Internet properties.	IID An Infoblox company, IID is a provider of technology and services that help organizations secure their Internet presence.	MarkMonitor MarkMonitor, a 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.	FORCEPOINT POWERED BY Raytheon Forcepoint brings a fresh approach to address the constantly evolving cybersecurity challenges and regulatory requirements facing businesses and government agencies.	

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; Carl Leonard at Forcepoint CLeonard@forcepoint.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 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.

Analysis by Greg Aaron, iThreat Cyber Group; editing by Ronnie Manning, Mynt Public Relations.