# Phishing Activity Trends Report

## 4th Quarter 2014

APWG

Unifying the
Global Response
To Cybercrime

October – December 2014

*Published April 29, 2015*

## Phishing Report Scope

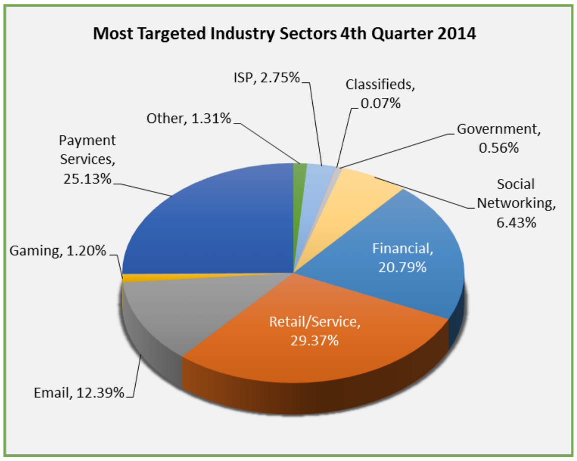
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation,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

## Retail/Service Was Most-Targeted Industry Sector in Q4



*Retail/Service was the most-targeted industry sector in the fourth quarter of 2014, with Payment Services close behind. [pg. 7]*

### 4th Quarter 2014 Phishing Activity Trends Summary

- During the 4th quarter of 2014, a record number of malware variants were detected – an average of 255,000 new threats each day. [p. 8]
- The number of unique phishing reports submitted to APWG during Q4 was 197,252. This was an increase of 18 percent from the 163,333 received in Q3 of 2014. [p. 4]
- The total number of phish observed in Q4 was 46,824. [p. 4]
- A total of 437 brands were targeted by phishers in Q4. [p. 6]
- The United States continued to be the top country hosting phishing sites. [p. 7]
- The United States remained the top country hosting phishing-based Trojans and downloaders during the three month period. [p. 10]

## Methodology and Instrumented Data Sets

The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. Sampling change note for this and subsequent editions: Beginning with this report, we have updated some of our data collection and measurement techniques. APWG member Internet Identity is now assisting with the following metrics for the *Trends Report*: unique phishing websites detected; domain names used; brands targeted and brand-domain pairs; phishing by country; and phishing by industry sector. The new collection and measurement process means that while there may be some discontinuity from our Q3 report statistics, we think the new data adds greater precision in enumeration and categorization.

APWG tracks the number 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.

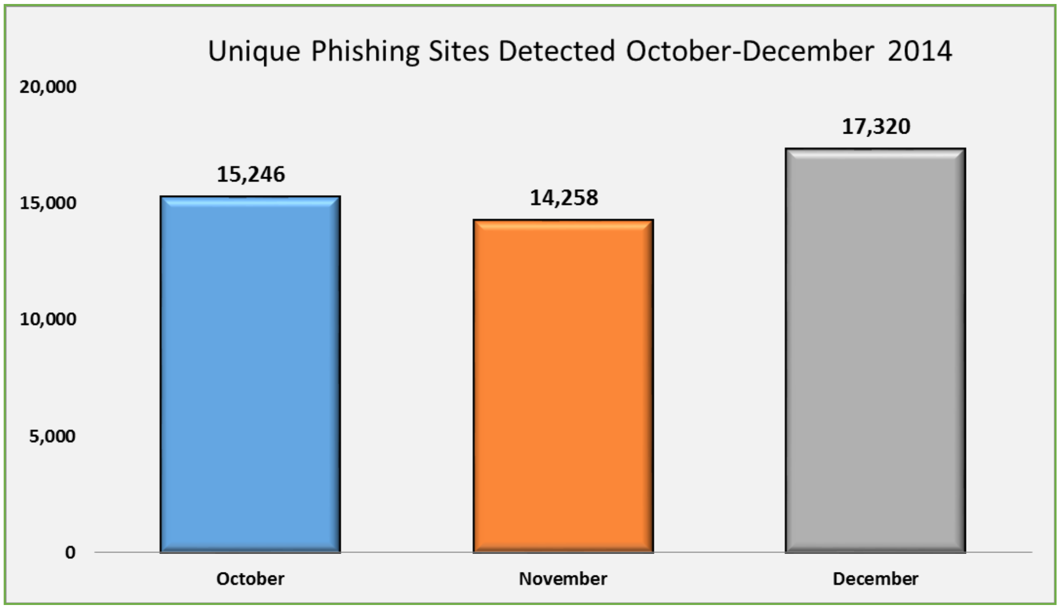
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLS, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances (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 4th Quarter 2014

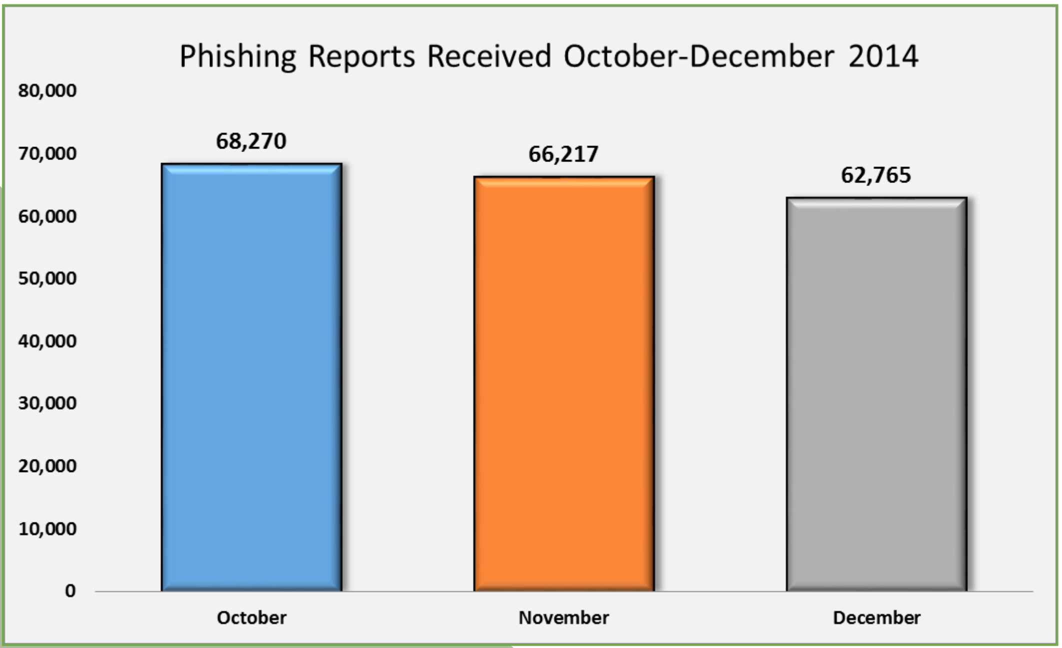
| | October | November | December |
|---|---|---|---|
| Number of unique phishing websites detected | 15,246 | 14,528 | 17,320 |
| Number of unique phishing e-mail reports (campaigns) received by APWG from consumers | 68,270 | 66,217 | 62,765 |
| Number of brands targeted by phishing campaigns | 271 | 273 | 300 |
| Country hosting the most phishing websites | USA | USA | USA |
| Contain some form of target name in URL | 44.88% | 50.40% | 50.37% |
| Percentage of sites not using port 80 | 0.72% | 0.35% | 1.04% |

## Phishing E-mail Reports and Phishing Site Trends – 4th Quarter 2014

The total number of unique phishing sites observed in Q4 was 46,824. This number is substantially lower than in Q3 by roughly half, a shift attributable to methodological refinements in how phishing sites were verified and URLs were de-duplicated to identify truly unique phishing sites. [See methology notes, p. 3.]

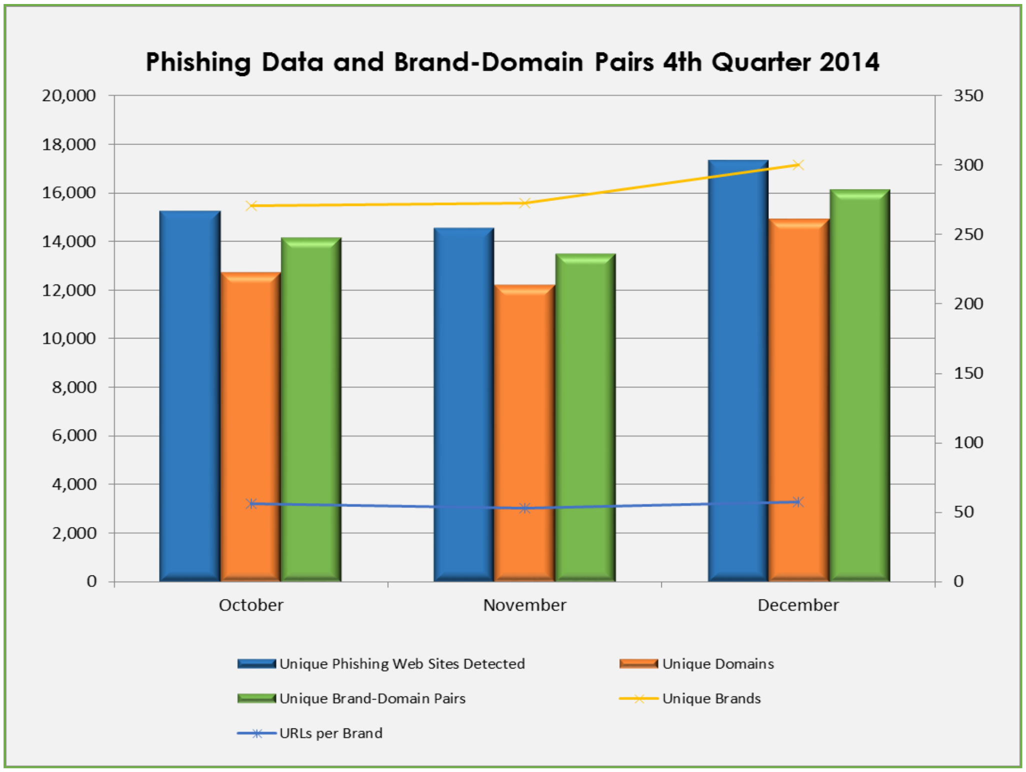


The number of unique phishing reports submitted to APWG during Q4 was 197,252. This was an increase of 18 percent from the 163,333 received in Q3 of 2014. The number of unique phishing reports submitted to APWG remained consistent during the three-month period.



## Brand-Domain Pairs Measurement – 4th 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.

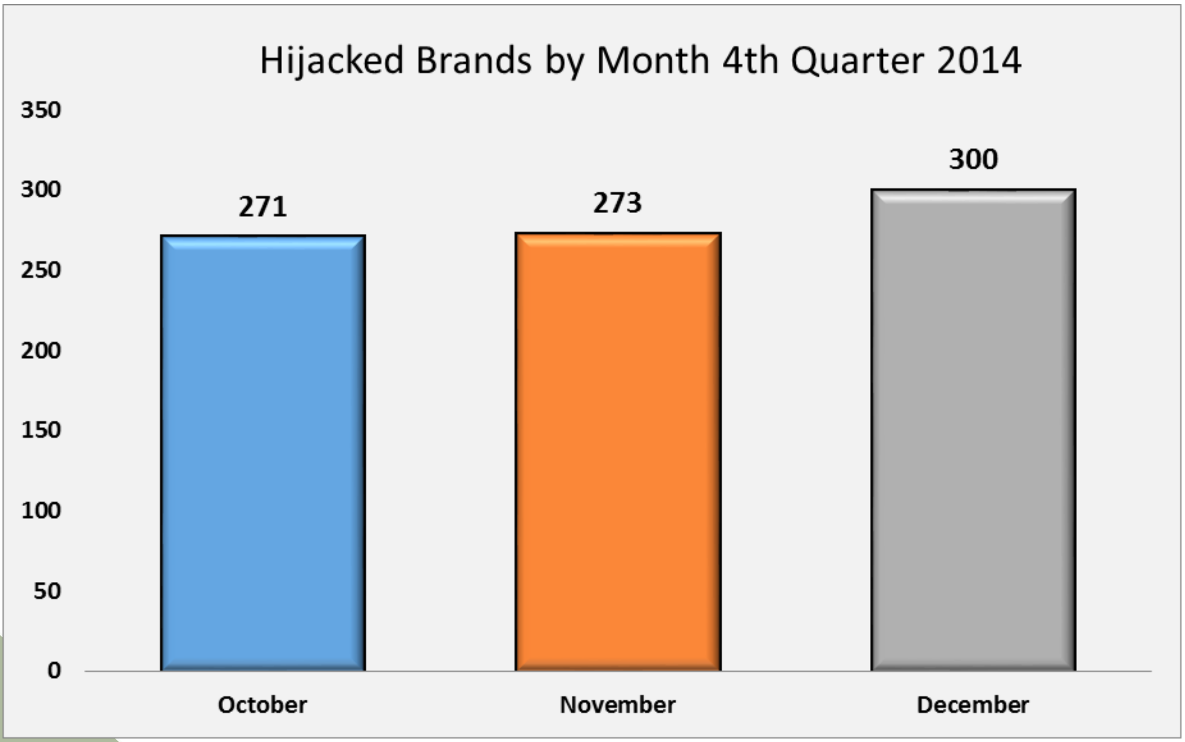


| | October | November | December |
|---|---|---|---|
| Number of Unique Phishing Web Sites Detected | 15,246 | 14,528 | 17,320 |
| Unique Domains | 12,722 | 12,187 | 14,900 |
| Unique Brand-Domain Pairs | 14,148 | 13,470 | 16,124 |
| Unique Brands | 271 | 273 | 300 |
| URLs Per Brand | 56.25 | 53.21 | 57.73 |

## Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 4th Quarter 2014

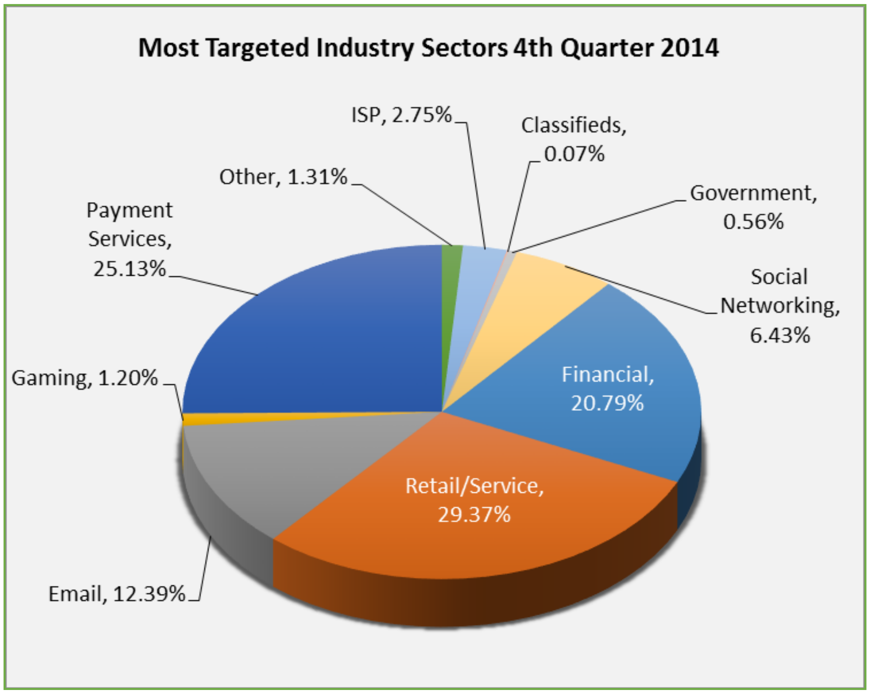
A total of 437 brands were targeted by phishers in Q4. This is lower than in Q3, and the difference is attributable to methodological refinements, namely how phishing sites were verified and classified. [See methology notes, p. 3.]

"The final quarter of 2014 witnessed a raft of email-based phishing attempts against well-established financial institutions, possibly timed to coincide with both the holiday spending increase and heightened consumer fears in the wake of corporate security breaches," said Carl Leonard, Principal Security Analyst, Websense Security Labs. "The UK financial market featured heavily, and high-profile targets such as Barclays, Halifax, and Santander were phished significantly. Phishing attacks also targeted speakers of the Dutch language , with financial services providers ING and SNS banks among those impersonated. Webmail and Apple-themed account verification attempts continued to be popular methods to obtain personal information."



## Most-Targeted Industry Sectors – 4th Quarter 2014

Retail/Service was the most-targeted industry sector in the fourth quarter of 2014, with 29.37 percent of phishing sites. Payment Services continued to be popular targets, with 29.37 percent of attacks during the three-month period.



## Countries Hosting Phishing Sites – 4th Quarter 2014

The United States continued to be the top country where phishing sites were hosted during the third quarter of 2014. Phishers break into vulnerable web hosting to find hosting for the phishing sites, and the USA hosts a large percentage of the world's web sites.

| October | | November | | December | |
|---|---|---|---|---|---|
| United States | 42.69% | United States | 45.90% | United States | 52.13% |
| Poland | 7.60% | Poland | 8.53% | United Kingdom | 3.47% |
| China | 5.96% | France | 3.90% | Bulgaria | 3.44% |
| Germany | 3.96% | Germany | 3.82% | Germany | 3.42% |
| Russian Federation | 3.57% | Netherlands | 3.71% | France | 2.83% |
| France | 3.35% | United Kingdom | 3.33% | Russian Federation | 2.70% |
| Netherlands | 2.95% | Turkey | 2.66% | Turkey | 2.64% |
| Canada | 2.90% | Russian Federation | 2.46% | Canada | 2.48% |
| United Kingdom | 2.85% | Canada | 2.13% | Netherlands | 2.04% |
| Turkey | 2.23% | Hong Kong | 1.60% | Brazil | 1.87% |

## Crimeware Taxonomy and Samples According to Classification

The APWG's Crimeware statistics categorize crimeware attacks as follows. 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, such as access to financial-based websites, e-commerce sites, and web-based mail sites.

## Malware Infected Countries – 4th Quarter 2014

APWG member PandaLabs tracks the number of malware variants detected, which has been growing each quarter. During the 4th quarter of 2014 this figure broke a new record, with 23,500,000 malware samples detected, an average of 255,000 new threats each day. Never in the history of computer security has the amount of new malware created been so high. However we should remark that we are talking about new malware binaries, which does not mean that each and every one of them is a completely new threat. In fact, the vast majority are just variants of existing malware modified by their creators to evade signature-based detection systems, while the functionality is the same. Still, the escalating numbers illustrate the adaptability of the code and the creativity of the malware authors.

This technique can sometimes defeat anti-malware protection, and the cost for the malware authors to create such a huge number of variants is effectively zero, since they have built automatic systems that take care of this task. Trojans are the most common type of malware, accounting for 82.18% of the new malware strains put in circulation, while traditional computer viruses came in second at a far-off 9.34%.

| New Malware Strains in Q4 | % of malware samples |
|---:|---:|
| Trojans | 82.18% |
| Viruses | 9.34% |
| Worms | 3.45% |
| Adware/Spyware | 1.27% |
| Other | 3.76% |

| Malware Infections by Type | % of malware samples |
|---|---:|
| Trojans | 76.63% |
| Viruses | 2.03% |
| Worms | 2.28% |
| Adware/Spyware | 5.05% |
| Other | 14.01% |

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, the global infection rate was 33.21%, lower than in the last quarters even though the number of malware samples has increased.

It's clear that the highest positions in the ranking are held by Asian and Latin American countries. Other countries with rates above the global average include: Poland (34.90%), Brazil (34.82%), Italy (34.50%), Colombia (34.12%), Spain (34.01%), Costa Rica (33.90%), Chile (33.55%) and Slovenia (33.22%). In general, Europe is the area with the lowest infection rates.

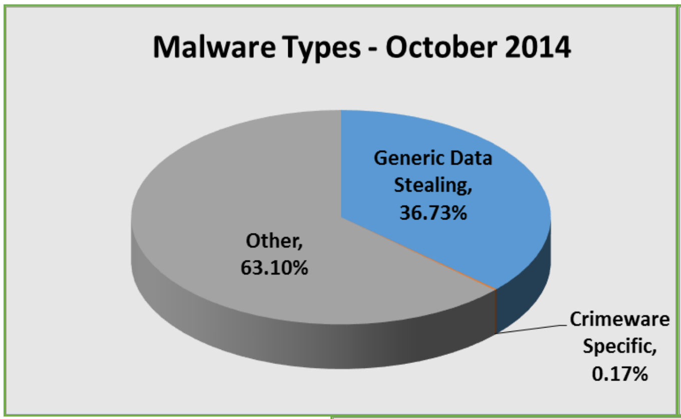
| Ranking | Country | Infection Rate |
|---:|---|---:|
| **1** | China | 47.22% |
| **2** | Taiwan | 45.92% |
| **3** | Turkey | 42.33% |
| **4** | Russia | 41.45% |
| **5** | Bolivia | 41.38% |
| **6** | Argentina | 41.16% |
| **7** | Ecuador | 39.47% |
| **8** | Peru | 37.11% |
| **9** | El Salvador | 35.02% |
| **10** | Guatemala | 34.98% |

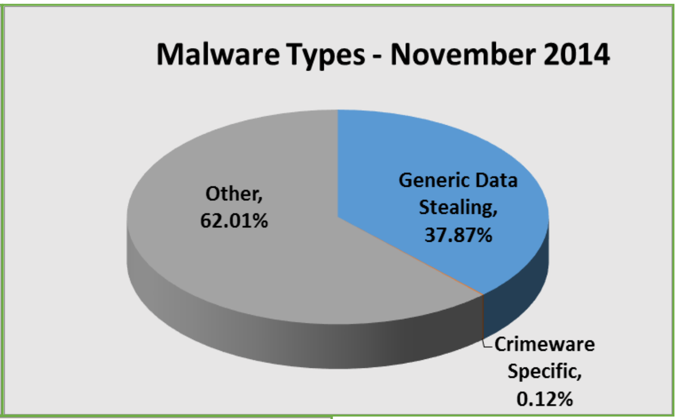
| Ranking | Country | Infection Rate |
|---:|---|---:|
| **45** | Switzerland | 27.83% |
| **44** | Belgium | 26.39% |
| **43** | Portugal | 25.56% |
| **42** | Germany | 24.81% |
| **41** | France | 23.37% |
| **40** | UK | 22.93% |
| **39** | Netherlands | 22.36% |
| **38** | Japan | 21.34% |
| **37** | Norway | 21.02% |
| **36** | Sweden | 20.07% |

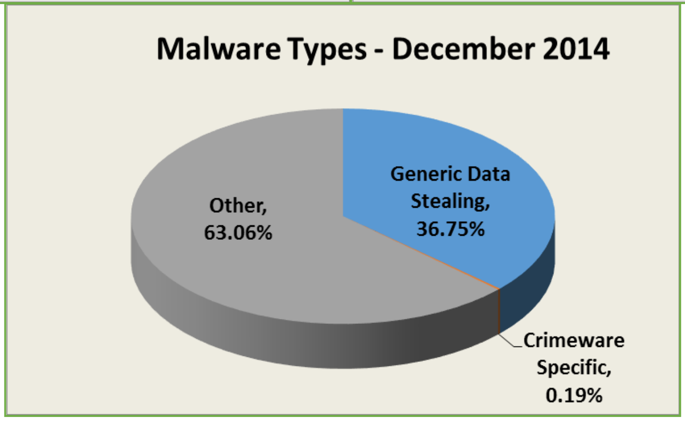
## Measurement of Detected Crimeware – 4th Quarter 2014

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.)


Malware Types - October 2014


Malware Types - November 2014


Malware Types - December 2014

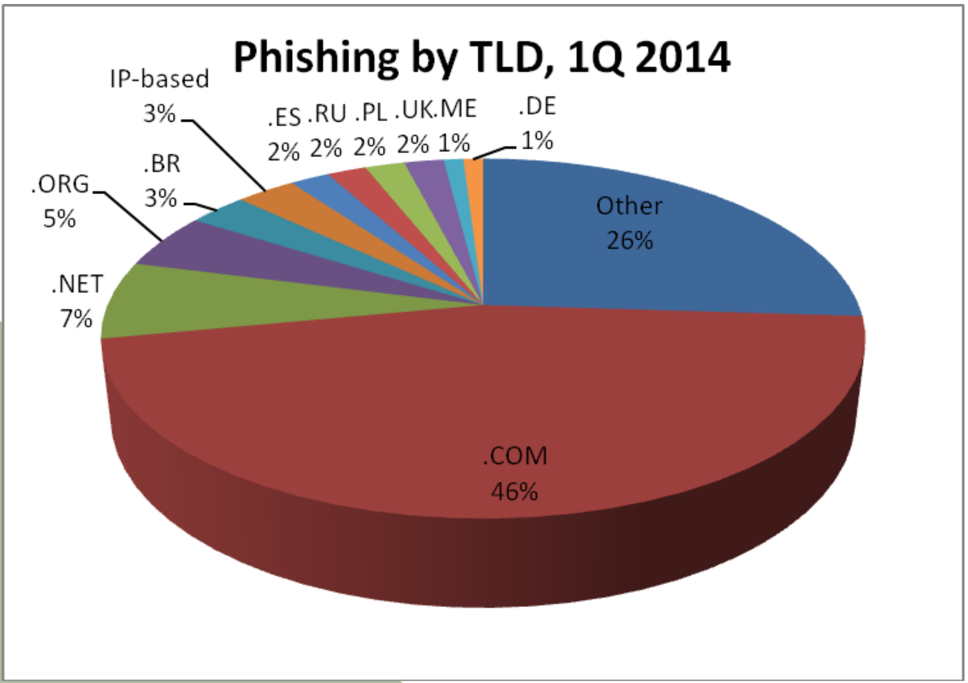
## Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

The United States remained the top country hosting phishing-based Trojans and downloaders during the three month period.

| October | | November | | December | |
|---|---|---|---|---|---|
| United States | 67.34% | United States | 50.76% | United States | 40.56% |
| China | 5.09% | France | 5.58% | Czech Republic | 16.01% |
| Netherlands | 3.63% | Netherlands | 5.27% | France | 8.38% |
| Russian Federation | 2.92% | Germany | 3.53% | China | 7.49% |
| France | 2.67% | China | 3.48% | Netherlands | 3.17% |
| Brazil | 1.86% | Turkey | 3.04% | Germany | 2.28% |
| Germany | 1.81% | United Kingdom | 2.37% | Russian Federation | 2.13% |
| Switzerland | 1.71% | Russian Federation | 2.28% | Turkey | 1.83% |
| Czech Republic | 1.56% | Brazil | 1.83% | Thailand | 1.69% |
| Ukraine | 1.06% | Spain | 1.47% | Poland | 1.39% |

## Phishing by Top-Level Domain

Internet Identity records the top-level domains (TLDs) used to host phishing sites. Forty-six percent of domains used for phishing were .COM names, down from 55% 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.



## APWG Phishing Activity Trends Report Contributors

| | |
|---|---|
| ILLUMINTEL<br>Illumintel Inc. provides advising and security services to top-level-domain registry operators, Internet companies, and intellectual property owners. | IID<br>Internet Identity (IID) is a US-based provider of technology and services that help organizations secure their Internet presence. |
| PANDA SECURITY<br>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!<br>ESSENTIAL INFORMATION PROTECTION™<br>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 + 1 617.669.1123; Mark Foege of IID at mark.foege@internetidentity.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 USA 501(c)6 tax-exempted corporation, was founded by Tumbleweed Communications, financial services institutions and e-commerce providers. APWG.EU was founded in 2013 as a Spanish non-profit scientific research foundation.  Its mission is to engage European businesses and organizations in the fight against identity theft.

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