Phishing Activity Trends Report

1st Quarter 2014

Unifying the Global Response To Cybercrime

January – March 2014

Published June 23, 2014

Phishing Activity Trends Report, 1st Quarter 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.

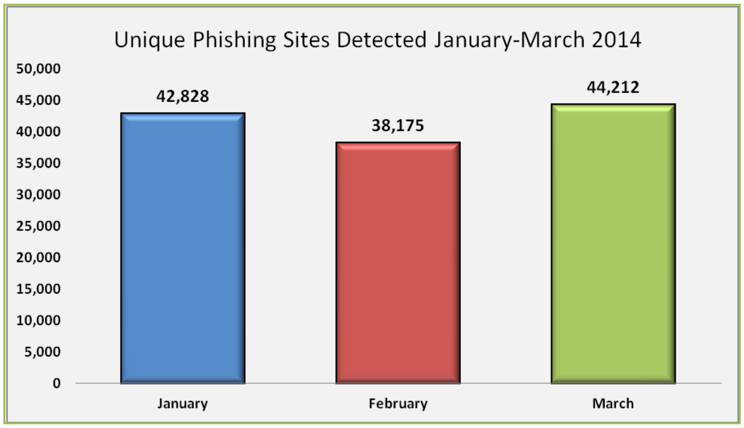
Phishing Defined

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 1st 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

High First Quarter Detections Predict Active 2014 for Phishers Worldwide



The first quarter of 2014 saw the second highest number of phishing attacks ever recorded in a first quarter by the APWG in its Phishing Activity Trends Report. [p. 5]

1st Quarter 2014 Phishing Activity Trends Summary

- The number of phishing sites leaped by 10.7 percent over the fourth quarter of 2013. [p. 4]
- The number of brands targeted by phishers was up, from 525 targeted in the fourth quarter of 2013 to 557 in the first quarter of 2014. [p. 6]
- The number of phishing attacks observed in Q1 was 125,215. That is the second-highest number of sites detected in a first quarter, eclipsed only by the 164,032 seen in the first quarter of 2012. [p. 5]
- Payment Services continued to be the most-targeted industry sector. [p. 7]
- The United States continued to be the top country hosting phishing sites. [p. 7]
- 32.7 percent of personal computers around the world were infected with malware, aware, or spyware. [p. 8]

www.apwg.org

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.

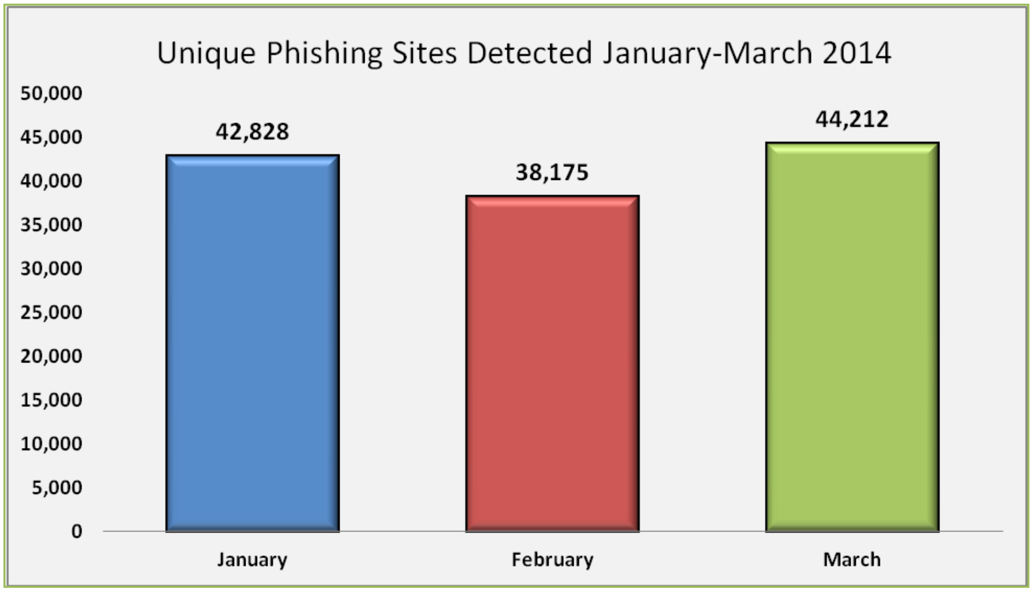
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLS, all leading to basically the same attack destination.) APWG additionally tracks crimeware instances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

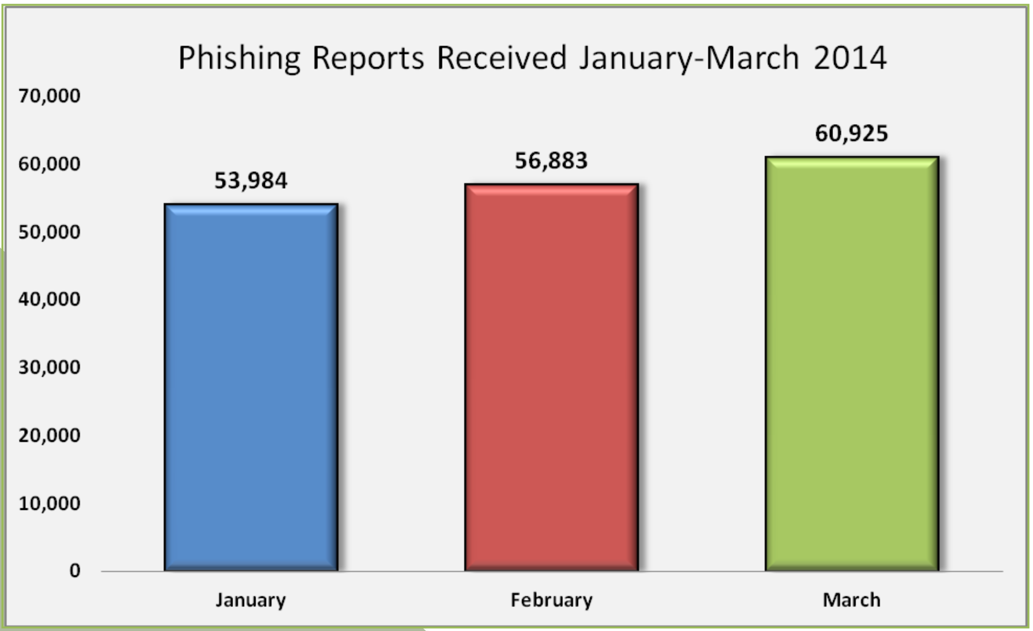
	January	February	March
Number of unique phishing websites detected	42,828	38,175	44,212
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	53,984	56,883	60,925
Number of brands targeted by phishing campaigns	384	355	362
Country hosting the most phishing websites	USA	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 – 1st Quarter 2014

The total number of phish observed in Q1 was 125,215, a 10.7 percent increase over Q4 2013, when a total of 111,773 were observed. The 125,215 is the second-highest number of sites detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012.

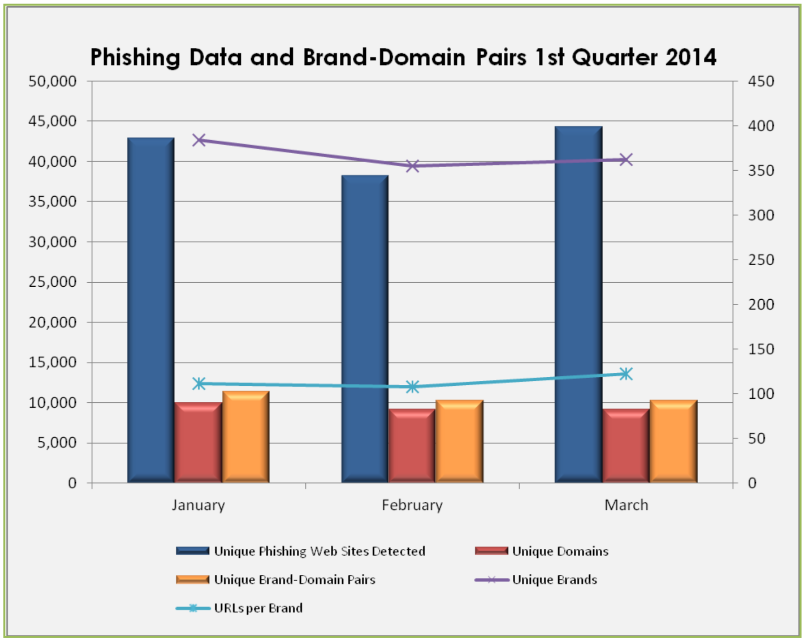


The number of unique phishing reports submitted to APWG during Q1 was 171,792. This was an increase for the 6.8 percent increase from 160,777 received in Q4 of 2013. The number of unique phishing reports submitted to APWG rose by nearly 7,000 during the three month period:



Brand-Domain Pairs Measurement – 1st 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.



The number of unique phishing web sites detected in the first quarter was 125,215. This is the second-highest number of sites detected in first a quarter, eclipsed only by the 164,032 detected in the first quarter of 2012.

"As Q1 levels are typically lower than what we see later in the year, we expect this to be a very active year for phishers worldwide," said Frederick Felman, chief marketing officer, MarkMonitor.

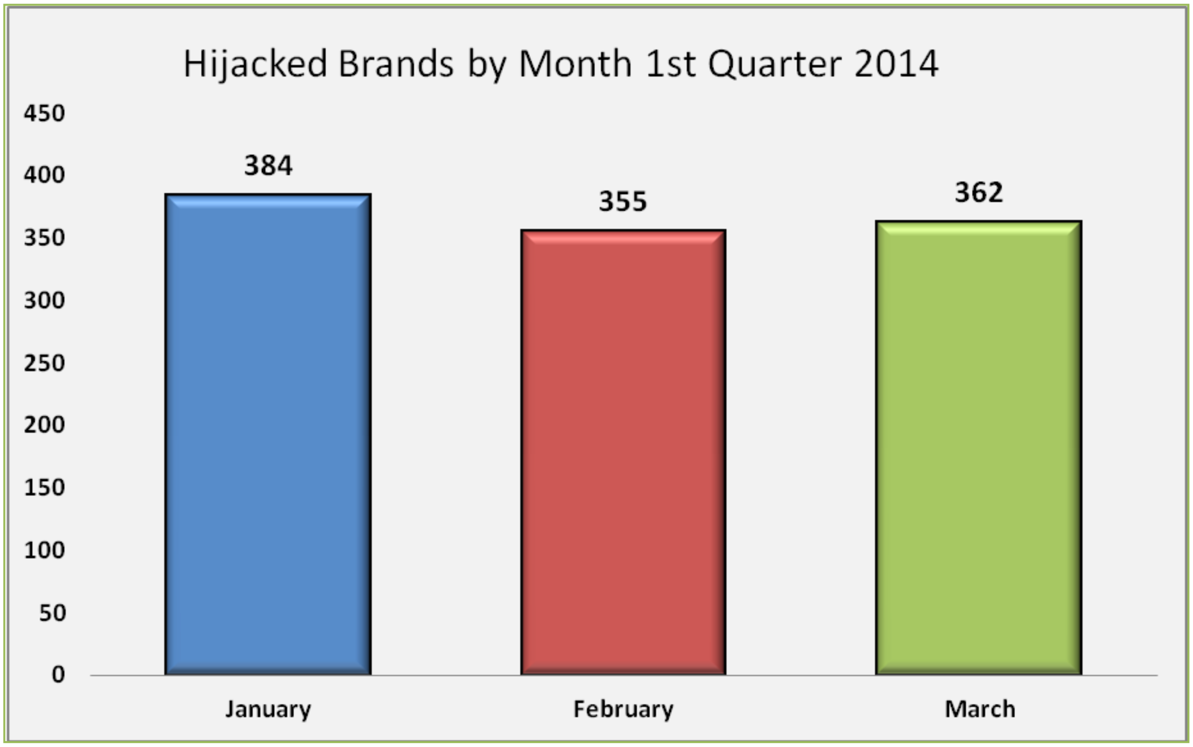
The number of brands targeted remained relatively consistent during Q1 2014.

	January	February	March
Number of Unique Phishing Web Sites Detected	42,828	38,175	44,212
Unique Domains	9,918	9,088	9,152
Unique Brand-Domain Pairs	11,351	10,214	10,275
Unique Brands	384	355	362
URLs Per Brand	111.53	107.53	122.13

Brands and Legitimate Entities Targeted by E-mail Phishing Attacks – 1st Quarter 2014

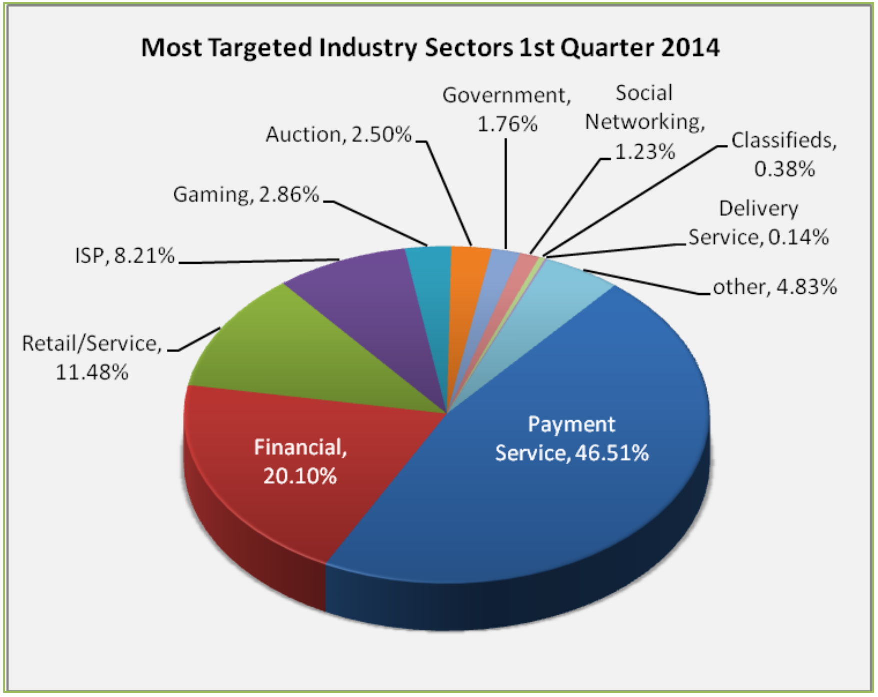
A total of 557 brands were targeted by phishers in Q1. This was up from the 525 targeted in the fourth quarter of 2013. The number of brands targeted in any given month remained below the all-time high of 441 that was recorded in April 2013.

“The number and diversity of phishing targets is increasing,” said Greg Aaron, President of Illumintel and APWG Senior Research Fellow. “Almost any enterprise that takes in personal data via the Web is a potential target.”



Most-Targeted Industry Sectors – 1st Quarter 2014

Payment Services continued to be the most-targeted industry sector at the beginning of 2014, with 46.51 percent of attacks during the three-month period.



Countries Hosting Phishing Sites – 1st Quarter 2014

The United States continued to be the top country hosting phishing sites during the first 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. A spate of phishing hit Turkey-based hosters in February and March.

January		February		March	
United States	56.30%	United States	46.29%	United States	40.21%
United Kingdom	5.17%	France	5.88%	Turkey	4.40%
Hong Kong	3.86%	Turkey	4.11%	Hong Kong	4.13%
Germany	3.52%	Germany	4.04%	Russian Federation	4.00%
France	3.40%	Netherlands	3.39%	Germany	3.87%
Russian Federation	2.62%	United Kingdom	3.37%	Netherlands	3.69%
Netherlands	2.49%	Russian Federation	2.87%	France	3.28%
Canada	2.12%	Canada	2.40%	Japan	2.88%
Turkey	1.95%	Japan	1.96%	United Kingdom	2.86%
Brazil	1.36%	Poland	1.89%	Poland	2.76%

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 – 1st Quarter 2014

During the first quarter of 2014, APWG member company PandaLabs gathered 4.8 million new malware samples, with its library reaching 15 million new malware samples total. Many 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. Trojans continue to be the most common type of malware, constituting 71.85% of all malware captured during this quarter. PandaLabs' Collective Intelligence platform found that that almost four out of every five malware infections were caused by Trojans (79.70%).

New Malware Strains in Q1	% of malware samples
Trojans	71.85%
Viruses	10.45%
Worms	12.25%
Adware/Spyware	5.26%
Other	0.19%

Malware Infections by Type	% of malware samples
Trojans	79.70%
Viruses	6.71%
Worms	6.06%
Adware/Spyware	3.62%
Other	3.91%

According to Luis Corrons, PandaLabs Technical Director and *Trends Report* contributing analyst, the percentage of infected computers around the world in Q1 has increased, reaching 32.77%. The countries leading the list are China (with 52.36% of computers in the country infected), followed by Turkey (43.59%) and Peru (42.14%).

Asia and Latin America continue to be the regions with the highest number of computer infections. The rest of the top ten have a rather lower infection rate, although higher than the average. Nine of the ten least-infected countries are in Europe, with the exception being Japan. The ranking is topped by Sweden (21.03% of its PCs are infected), followed by Norway (21.14%) and Germany (24.18%).

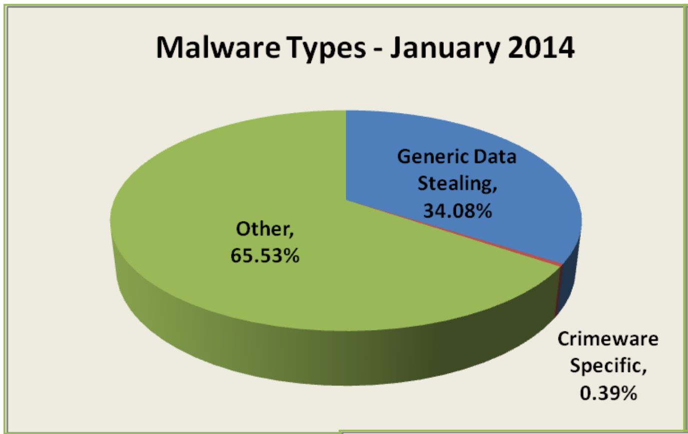
Ranking	Country	Infection Rate
1	China	52.36%
2	Turkey	43.59%
3	Peru	42.14%
4	Bolivia	41.67%
5	Ecuador	41.13%
6	Russia	41.08%
7	Argentina	39.36%
8	Taiwan	38.65%
9	Slovenia	38.00%
10	El Salvador	37.29%

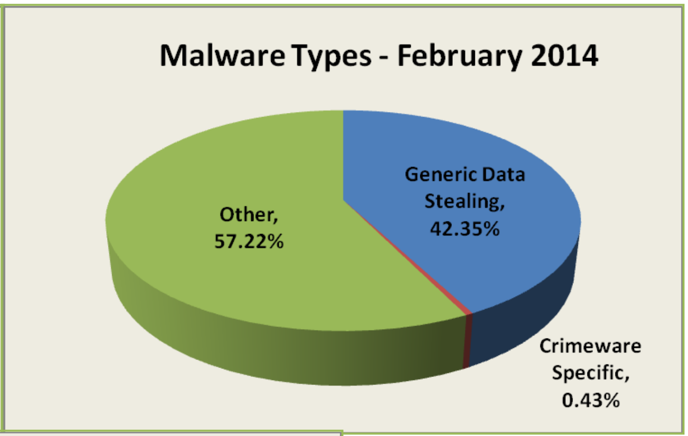
Ranking	Country	Infection ratio
45	Portugal	26,79%
44	Netherlands	25,82%
43	Switzerland	25,60%
42	Belgium	24,87%
41	France	24,54%
40	United Kingdom	24,48%
39	Japan	24,21%
38	Germany	24,18%
37	Norway	21,14%
36	Sweden	21,03%

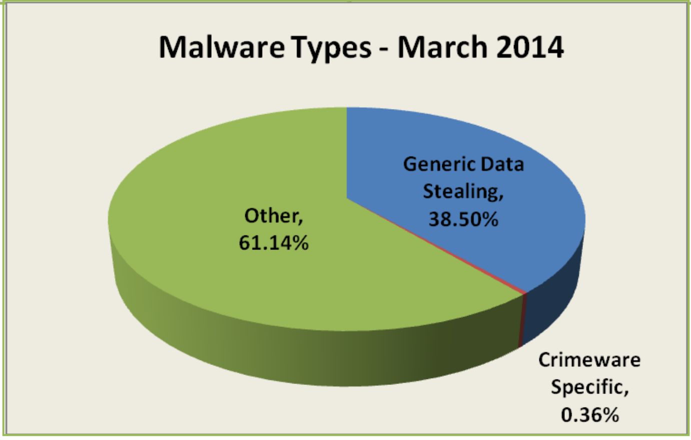
Measurement of Detected Crimeware – 1st Quarter 2014

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.)







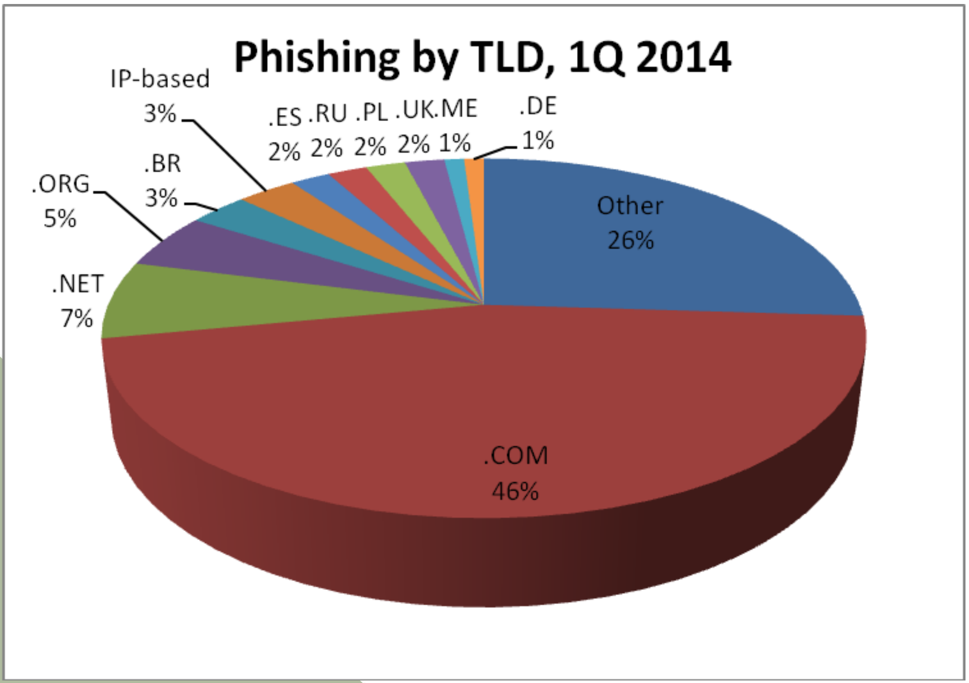
Phishing-based Trojans and Downloader's Hosting Countries (by IP address)

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

January		February		March	
United States	50.86%	United States	64.17%	United States	46.21%
Hungary	13.28%	Netherlands	8.89%	Netherlands	26.12%
China	6.32%	Ukraine	3.94%	China	4.20%
Ukraine	5.95%	China	3.20%	France	3.45%
Netherlands	4.38%	Germany	2.94%	Germany	3.42%
Europe	2.39%	France	2.59%	Ukraine	3.37%
Germany	2.34%	Russian Federation	1.77%	Poland	1.32%
Russian Federation	2.21%	Rep. of Korea	1.59%	United Kingdom	1.22%
France	1.64%	Brazil	1.20%	Rep. of Korea	0.98%
Rep. of Korea	1.50%	Europe	0.97%	Russian Federation	0.93%

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, up from 43 percent in the previous quarter. The .COM TLD represents approximately 44 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

Illumintel Inc. provides advising and security services to top-level-domain registry operators, Internet companies, and intellectual property owners.

IID

Internet Identity (IID) is a US-based 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.

Yes! websense® ESSENTIAL INFORMATION PROTECTION™

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 617.669.1123; Te Smith of MarkMonitor at 831.818.1267 or Te.Smith@markmonitor.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 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.

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