Phishing Activity Trends Report

1st Quarter 2018

APWG

Unifying the
Global Response
To Cybercrime

Activity January – March 2018

Published July 31, 2018

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

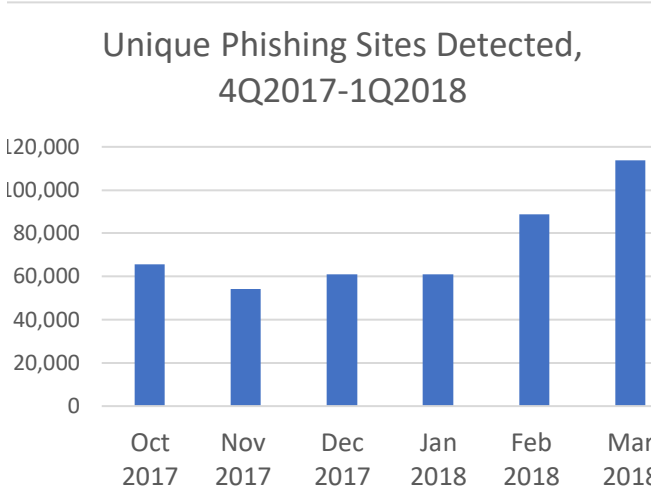
Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit Web sites 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 Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Statistical Highlights for 1st Quarter 2018	**3**
Phishing Site and Phishing E-mail Trends	**4**
Most-Targeted Industry Sectors	**5**
Use of Domain Names for Phishing	**7**
How Phishers use Encryption to Fool Users	**9**
Phishing and Identity Theft in Brazil	**11**
APWG Phishing Trends Report Contributors	**14**

Phishing Attacks Surge in First Quarter of 2018

The number of phish detected in the first quarter of 2018 was up 46% over the last quarter of 2017. [p. 4]



1st Quarter 2018 Phishing Activity Trends Summary

- The online payment sector was targeted by phishing more than in any other industry sector. [p. 5]
- Phishers continue to fool Internet users into complacency by using HTTP protection on phishing sites. [p. 9]
- The APWG's observer in Brazil recorded significant increases in web-based scams on sites like Facebook, and is seeing phishing advertised via text messages. [p. 11]
- By the second quarter of 2018, more than a third of phishing attacks were hosted on Web sites that had HTTPS and SSL certificates: [p.9]
- Phishers are generally using domain names in the largest top-level domains, and at the largest registrars. [p.7]

Statistical Highlights for 1st Quarter 2018

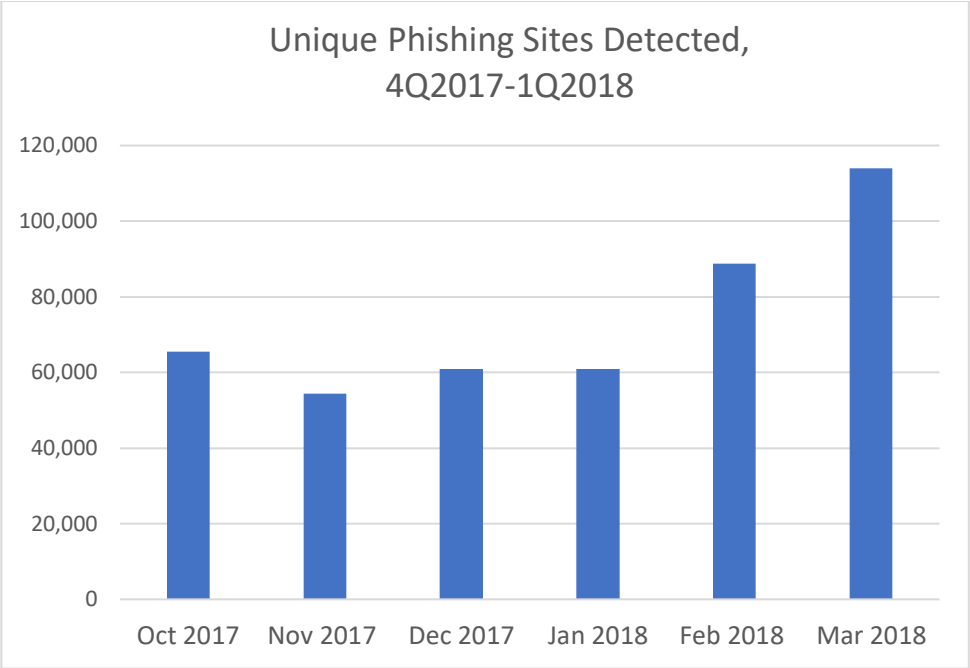
	January	February	March
Number of unique phishing Web sites detected	60,887	88,754	113,897
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	89,250	89,010	84,444
Number of brands targeted by phishing campaigns	235	273	238

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. 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 Web sites. 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's contributing members also track a variety of additional metrics and data sets in order to track the fast-paced nature of cybercrime.

Phishing Site and Phishing E-mail Trends – 1st Quarter 2018

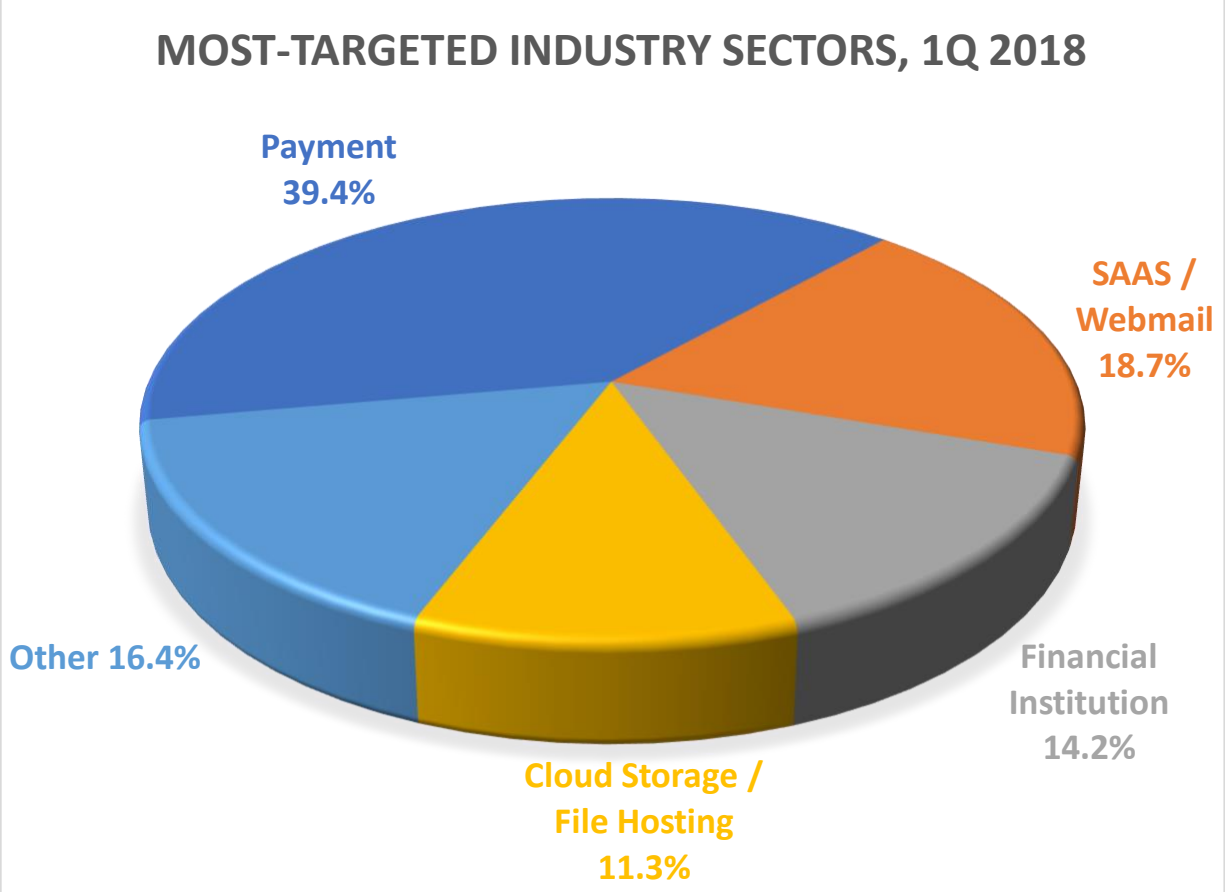
The total number of phish detected in 1Q 2018 was 263,538. This was up 46 percent from the 180,577 observed in 4Q 2017. It was also significantly more than the 190,942 seen in 3Q 2017.



The number of unique phishing reports submitted to APWG during 1Q 2018 was 262,704, compared to 233,613 in 4Q 2017 and 296,208 in 3Q 2017.

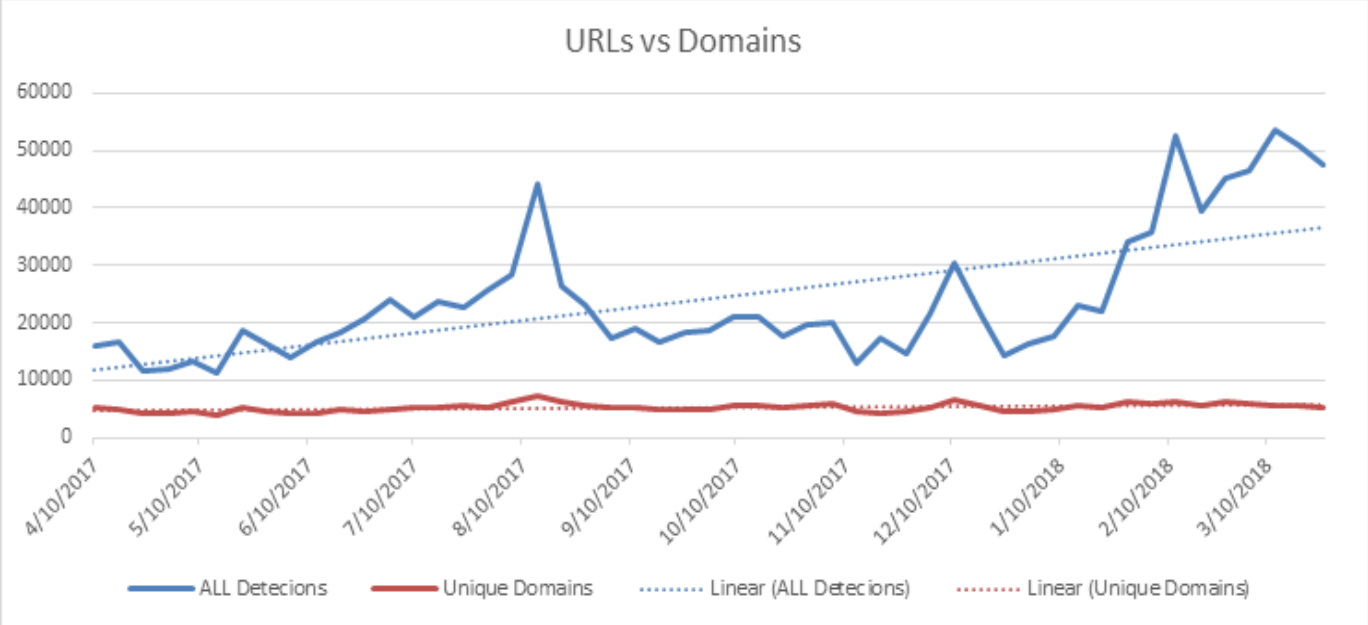
Most-Targeted Industry Sectors – 1st Quarter 2018

APWG member MarkMonitor saw increases in phishing that targeted SAAS/webmail providers and file hosting/sharing sites. Phishing against payment services and banks dropped slightly. Founding APWG member MarkMonitor is an online brand protection organization, securing intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.



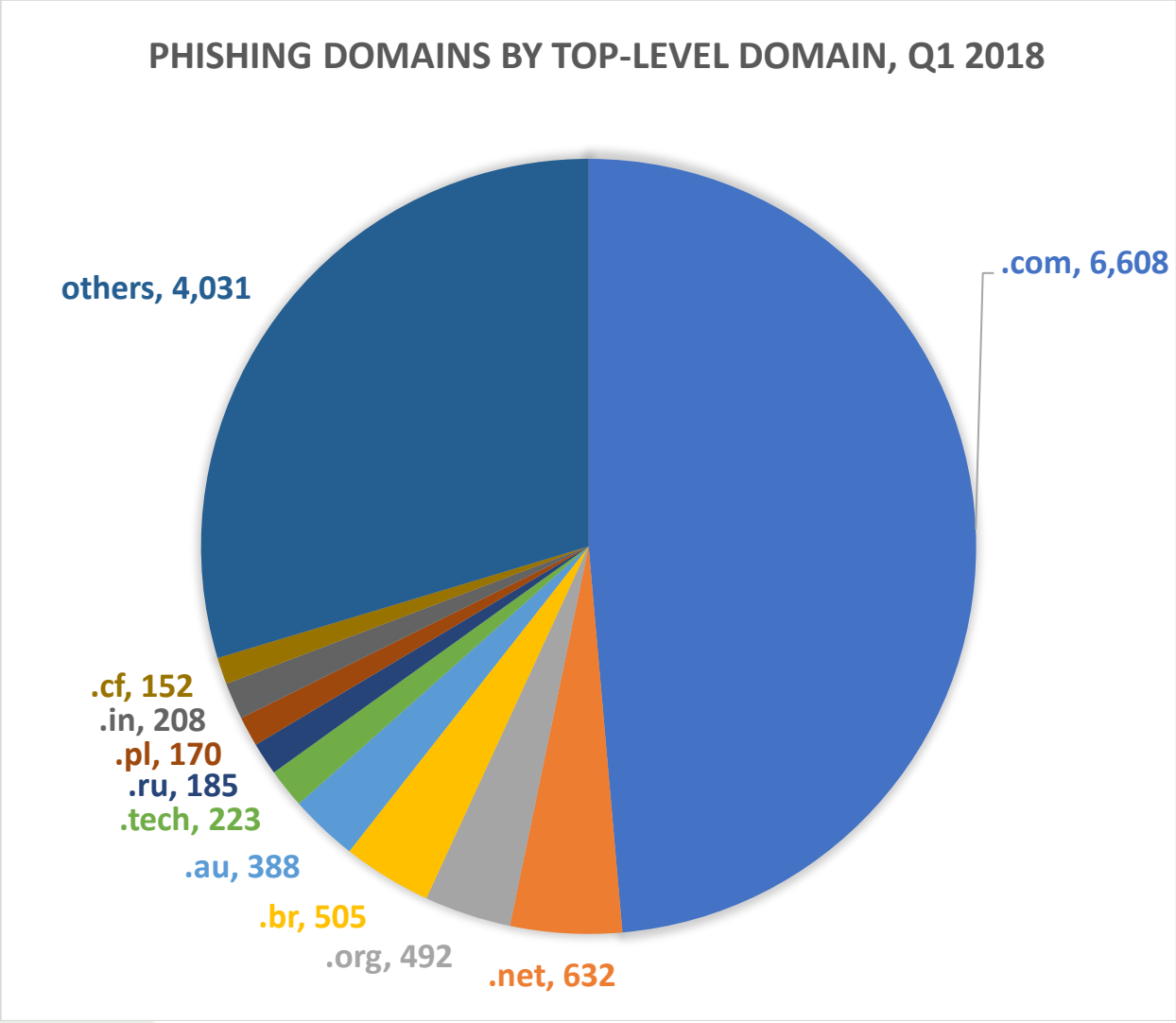
"In Q1 2018, there was a marked increase in URL detections starting in February and ramping up through March, but the number of unique phishing domains remained flat," said Stefanie Ellis, AntiFraud Product Marketing Manager, MarkMonitor. "This increase in URLs can largely be attributed to one-time-use URLs. These unique URLs are automatically generated by phishers to allow for a one-time access by victims to a unique phishing URL."

The increase in URL detections (the blue line below) in 2018 is based in the increase of one-time use URLs. The spikes in August and December of 2017 was more related to increased subdomain URLs rather than one-time use URLs.



Use of Domain Names for Phishing

APWG member RiskIQ monitors for code-level threats, malware, phishing, social media attacks, and fraud to protect corporate customers. RiskIQ's analysts examined thousands of phishing attack URLs that were submitted to the APWG's data repository in Q1 2018. RiskIQ found 13,594 unique domains used in phishing attacks:



The distribution above roughly follow is TLD market share, with .BR, .AU, .IN, and .TECH having more than their share of phishing for their sizes. Several very large TLDs such as .UK and .CN did not appear close to the top ten, indicating much less phishing relative to their sizes.

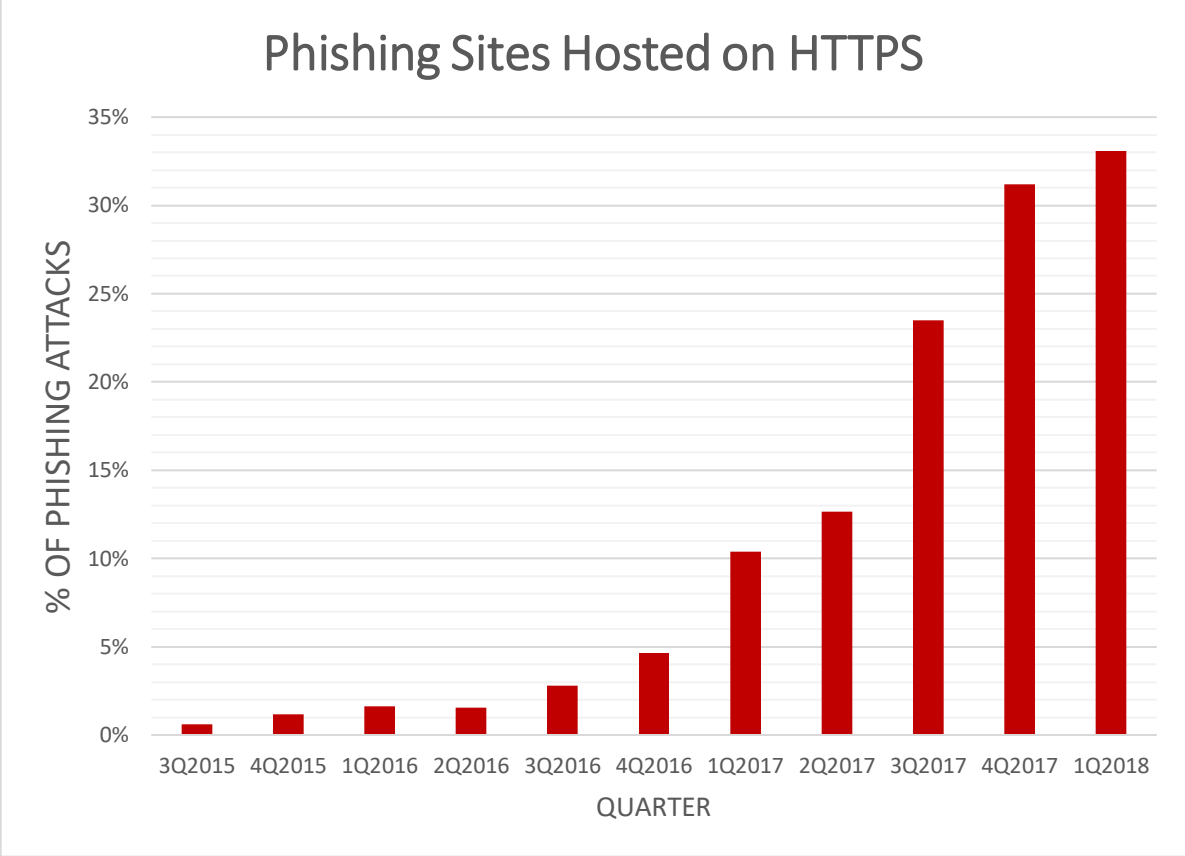
The domains were distributed at several hundred different registrars. RiskIQ was able to identify the registrars for most of the domains; it was not possible to identify a registrar especially in the cases of some ccTLD domains. The top four registrars below are among the largest in the world.

Registrar	Phishing Domains	% of total
GoDaddy.com, LLC	2,184	19.6%
Tucows Domains Inc.	1,037	9.3%
PDR Ltd. d/b/a PublicDomainRegistry.com	953	8.6%
eNom, Inc.	758	6.8%
FASTDOMAIN, INC.	347	3.1%
Registrar of Domain Names REG.RU, LLC	233	2.1%
Wild West Domains, LLC (GoDaddy)	219	2.0%
LAUNCHPAD.COM, INC.	182	1.6%
NameCheap Inc.	351	3.2%
NetRegistry	215	1.9%
others	4,656	41.8%
TOTAL	11,135	

How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking how many phishing sites are protected by HTTPs. HTTPS is used to secure communications by encrypting the data exchanged between a person's browser and the web site he or she is visiting. HTTPS is especially used by Web sites that offer online sales or password-protected accounts. Studying HTTP on phishing sites provides insight into how phishers are fooling Internet users by turning an Internet security feature against them. PhishLabs provides managed security services that help organizations protect against phishing attacks targeting their employees and their customers.

At the end of 2016, less than five percent of phishing sites were found on HTTPS infrastructure. By the second quarter of 2018, however, more than a third of phishing attacks were hosted on Web sites that had HTTPS and SSL certificates:



There are two primary reasons why phishers are increasingly hosting their malicious content this way:

1) More HTTPS Web sites = more HTTPS phishing sites. As more Web sites obtain SSL certificates, the number of potential HTTPS Web sites available for compromise increases. According to Let's Encrypt, two-thirds of Web sites loaded by Firefox at the end of 2017 used HTTPS, compared to 45 percent at the end of 2016.

2) Phishers are taking advantage of unclear security messaging. A significant number of HTTPS phish are hosted on domains that are registered by the phishers themselves.

Without an SSL certificate, the phishing page would still function as intended. But in these cases the phisher has obtained a valid SSL certificate. So why would a phisher take that extra step to create an HTTPS page when it is not actually needed? The answer is because phishers believe that the "HTTPS" designation makes a phishing site seem more legitimate to potential victims and, thus, more likely to lead to a successful outcome. And unfortunately, they're right. The general public's misunderstanding of the meaning of the HTTPS designation and the confusing labeling of HTTPS Web sites within browsers are the primary drivers of why they have quickly become a popular preference of phishers to host phishing sites.

Phishing and Identity Theft Techniques in Brazil

APWG member company Axur is located in Brazil and concentrates on protecting companies and their users in Brazil from Internet-based threats. Axur especially monitors attacks against banks, technology firms, airlines, and online marketplaces located in the country. Axur's data shows how criminals are perpetrating identity theft in South America's largest economy, and shows how these incidents are both a local and international problems.

In Q1 2018 Axur observed more than 17,600 fraud nexuses that targeted Brazilian companies and individuals:

Type	Description	Jan	Feb	Mar	Total 1Q2018
Phishing	Phishing	325	467	1,024	**1,816**
Malware	Malware distribution URLs	98	92	67	**257**
Paid Search Phishing	Paid ads with phishing on Google and Bing	6	8	32	**46**
Malicious proxy servers	Malicious proxy servers	12	1	13	**26**
Redirect	Redirection URLs, leading to phishing or malware	75	137	138	**350**
Social Media Scams	Scams on social media platforms (FB, Instagram, LinkedIn, YouTube, blogs, etc.)	1,442	1,245	1,522	**4,209**
Scam Web sites	Scams on Web sites in general	3,057	3,351	2,653	**9,061**
Mobile App Scam	Apps with unauthorized brand use in official stores (iTunes + GooglePlay) as well as .apk files in Web sites .	1,220	180	440	**1,840**
Total		**6,235**	**45,481**	**5,889**	**17,605**

The Q1 2018 totals were slightly above the Q4 2017 total of 16,559. Web site scams rose from 6,293 if Q4 2017 to 9,061 in 1Q 2018, while mobile app scams fell from 3,184 in 4Q 2017 to 1,840 in 1Q 2018.

But text messages are still a viable way for phishers to lure in unwary phone users. "Criminals keep using short text messages (SMS) to send phishing URLs to victims.," said Eduardo Schultze, CSIRT Coordinator at Axur. "As a global trend we also see in Brazil, phishing websites using SSL/HTTPs certificates have become a thing here and it's growing every day."

Most incidents were on Facebook, and hosted in the United States, followed by ASNs in Brazil and Ireland:

Country of hosting	Jan	Feb	March	Total 1Q2018
United States	3,871	3,415	3,667	**10,953**
Brazil	657	1,360	737	**2,754**
Ireland	698	496	796	**1,990**
Canada	180	194	161	**535**
Germany	97	116	119	**332**
Portugal	109	76	97	**282**
Italy	33	79	76	**188**
Czech Republic	39	34	46	**119**
Netherlands	45	29	43	**117**
Other (32 countries)	156	103	151	**410**
	5,885	**5,902**	**5,893**	**17,680**

Of the incidents detected by Axur, the incidents were found on the following platforms or (hosting) service providers:

Incidents per ISP	Jan	Feb	Mar	Total 1Q2018
Facebook Ireland Ltd	1,980	1,540	20,42	**5,562**
Cloudflare	880	476	551	**1,907**
Locaweb Serviços de Internet S/A	288	929	316	**1,533**

Google	436	523	359	**1,318**
Amazon.com	398	349	284	**1,031**
Websitewelcome.com	107	194	340	**641**
OVH Hosting	177	198	158	**533**
Fastly	129	106	70	**305**
IPV6 Internet Ltda	56	125	53	**234**
Others (408 ISPs)	1,501	1,426	1,689	**4616**
	5,952	**5,866**	**5,862**	**17,680**

APWG Phishing Activity Trends Report Contributors

Axur works to identify and fight the threats in the cyberspace that interfere with the interests of companies, governments, and individuals

iThreat provides risk data, intelligence tools, and analysis to help its clients protect their intellectual & Internet properties.

MarkMonitor, a global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PhishLabs provides 24/7 managed security services that help organizations protect against phishing attacks targeting their employees and customers.

RiskIQ is a digital threat management company enabling organizations to discover, understand and mitigate known, unknown, and malicious exposure across all digital channels

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, online 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.

APWG maintains it public website, <http://www.antiphishing.org>; the website of the STOP. THINK. CONNECT. Messaging Convention <http://www.stopthinkconnect.org> and the APWG's research website <http://www.ecrimeresearch.org>. These are resources about the problem of phishing and Internet frauds– and resources for countering these threats. The APWG, a 501(c)6 tax-exempted corporation, had its first meeting 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.

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 +1.404.434.7282 or foy@apwg.org. For media inquiries related to the company-content of this report, please contact APWG Secretary General Peter Cassidy at +1.617.669.1123; Stefanie Ellis at Stefanie.ellis@markmonitor.com; Eduardo Schultze of Axur at +55 51 3012-2987, eduardo.schultze@axur.com; Stacy Shelley of PhishLabs,at 1.843.329.7824, stacy@phishlabs.com' Kari Walker of RiskIQ at +1.703.928.9996, Kari@KariWalkerPR.com, +1.703.928.9996. **Analysis and editing by Greg Aaron, iThreat Cyber Group.**