Phishing Activity Trends Report

4th Quarter 2017

APWG

Unifying the
Global Response
To Cybercrime

Activity October – December 2017

Published May 15, 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

Cloud Storage and SaaS Increasingly Attacked by Phishers

In the fourth quarter of 2017, the APWG saw notable increases in phishing that targeted SaaS/webmail providers, as well as increased attacks on financial/banking targets and cloud storage and file-sharing sites. [p. 5]

4thy Quarter 2017 Phishing Activity Trends Summary

- Phishing decreased in the fourth quarter of 2018. Usually the holiday shopping season suffers an increase in phishing. [p. 4]
- The financial services industry has more companies being targeted by phishing than in any other industry sector. [p. 5]
- Phishers continue to fool Internet users into complacency by using HTTP protection on phishing sites. [p. 6]
- The APWG's observer in Brazil recorded triple-digit percentage increased in Interenet frauds, including phishing and social-media based scams. [p. 8]

Statistical Highlights for 4th Quarter 2017

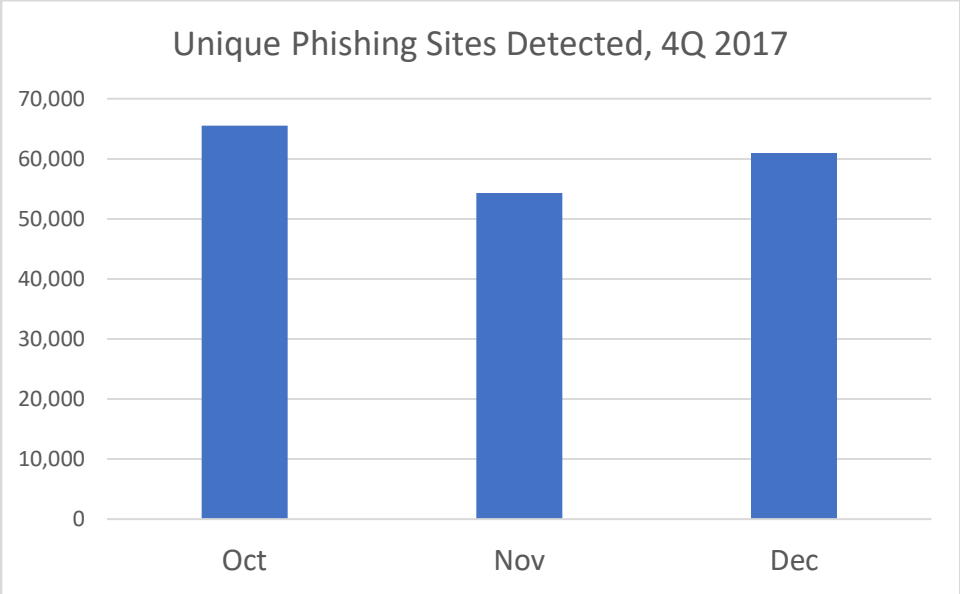
	October	November	December
Number of unique phishing Web sites detected	65,509	54,322	60,926
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	61,322	86,547	85,744
Number of brands targeted by phishing campaigns	348	323	268

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-paces nature of cybercrime.

Phishing Site and Phishing E-mail Trends – 4th Quarter 2017

The total number of phish detected in Q4 was 180,577, which included the holiday season, a traditionally high period of the year for phishing. That was down from 190,942 in 3Q 2017.

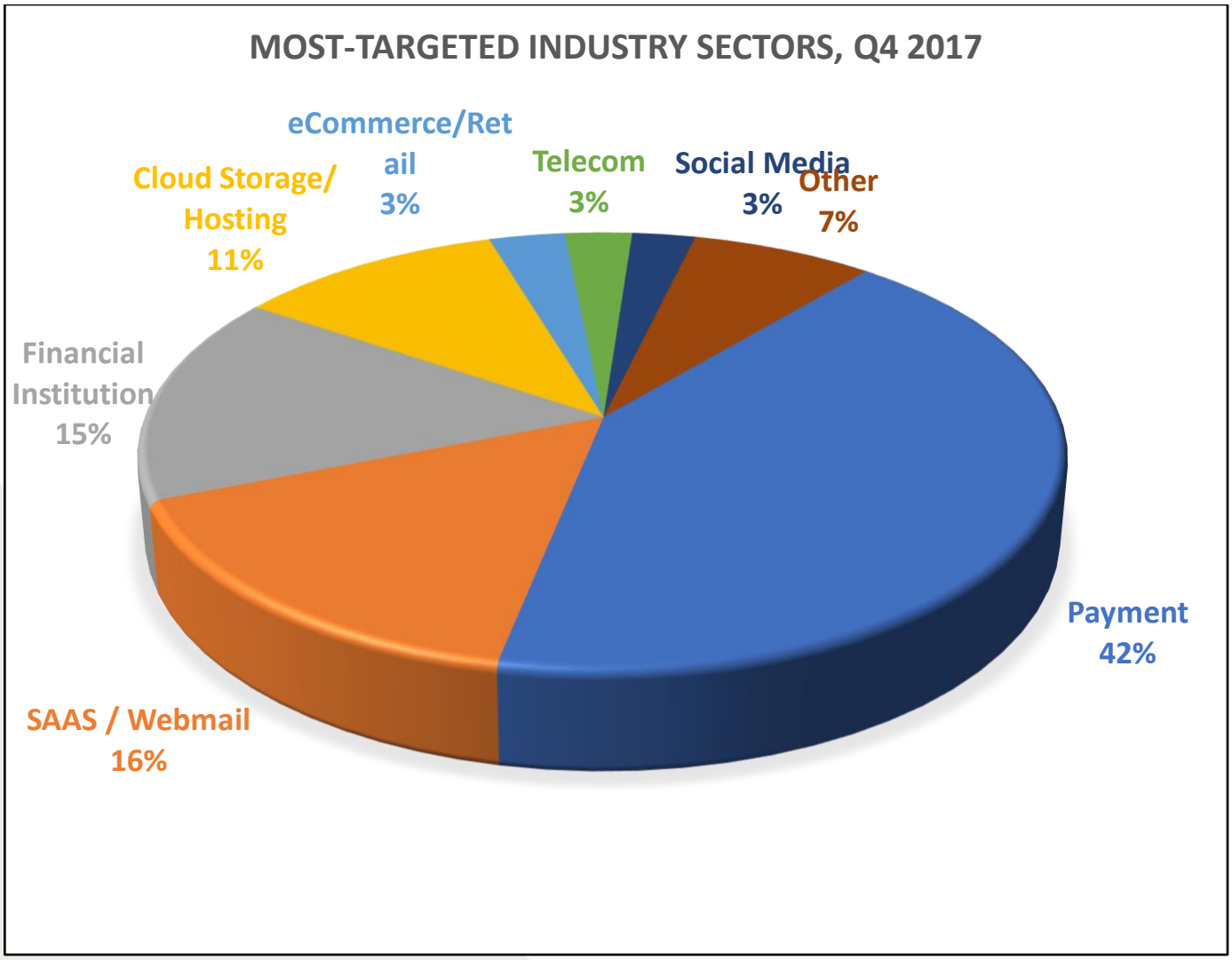


The number of unique phishing reports submitted to APWG during 4Q 2017 was 233,613. That was below the 3Q total of 296,208.

Most-Targeted Industry Sectors – 4th Quarter 2017

APWG member MarkMonitor saw notable increases in phishing that targeted SaaS/webmail providers, as well as increased attacks on financial/banking targets and file hosting/sharing sites. MarkMonitor is the online protection standard for organizations globally, securing intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.

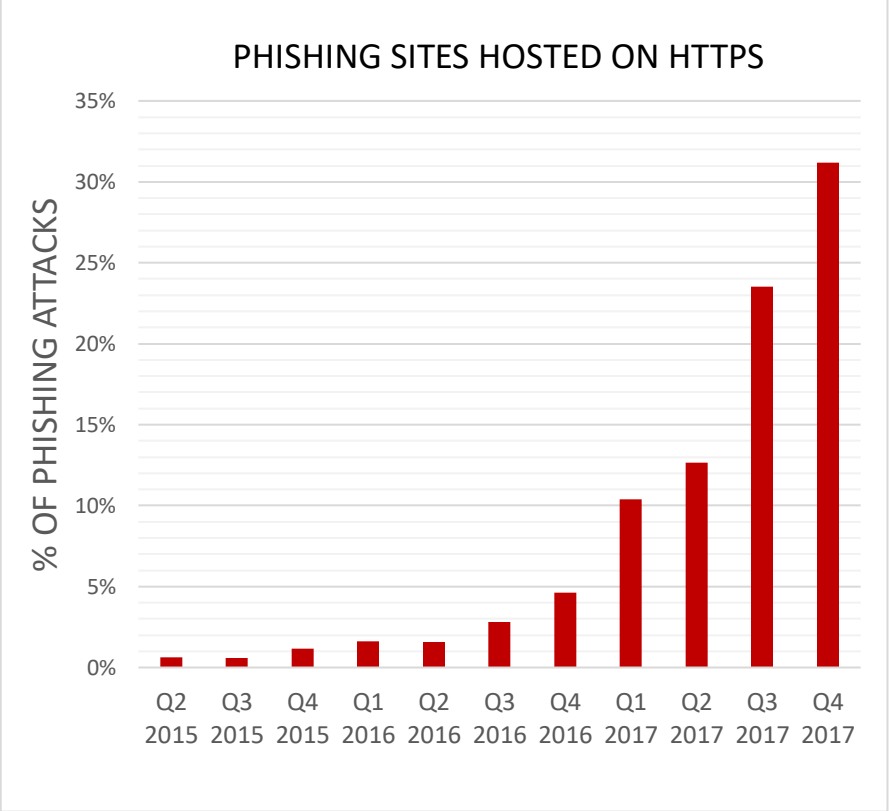
In Q4, MarkMonitor detected a steady growth in SaaS/Webmail and Cloud Storage/File Hosting targeted phishing, while phish volumes targeting financial institutions dropped slightly. While financial institutions are experiencing some reductions in volume individually, there are more financial institutions being targeted than in any other sector. MarkMonitor detected phishing attacks targeting 454 organizations in Q4, and 60 percent of those organizations were financial institutions. In contrast, 4 percent were payment providers, and 6 percent were SaaS/Webmail organizations.



How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking how many phishing sites are protected by the HTTPS content encryption protocol. 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 fourth quarter of 2017, however, *nearly a third* of phishing attacks were hosted on Web sites that had HTTPS and SSL certificates. Nearly 20 percent of all phishing sites observed in 2017 were found on HTTPS-protected domains.



So why are we seeing this significant shift in the way phishers are hosting their malicious content? There are two primary reasons:

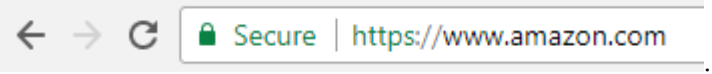
1) More HTTPS Web sites = more HTTPS phishing sites. As more Web sites obtain SSL certificates, the number of potential HTTPS Web sites available for compromise increases. According to Let's Encrypt, two-thirds of Web sites loaded by Firefox at the end of 2017 used HTTPS, compared to 45 percent at the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

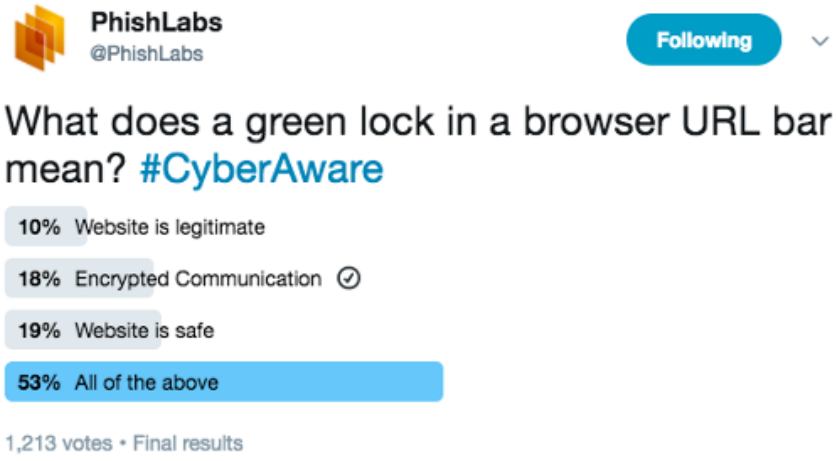
most phished brands indicates that nearly three-quarters of HTTPS phishing sites targeting them were hosted on maliciously-registered domains rather than compromised Web sites, which is substantially higher than the overall global rate. Based on APWG data from 2016, slightly less than half of all phishing sites were hosted on domains registered by a threat actor.

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.

In November 2017, PhishLabs conducted an informal poll to see how many people actually knew the meaning of the green padlock that is associated with HTTPS Web sites:



More than 80 percent of the respondents believed the green lock indicated that a website was either legitimate and/or safe — neither of which is true.



Adding to the confusion, browsers like Google Chrome label Web sites with SSL certificates as "Secure" in the URL bar. Another word for secure: safe.

The misunderstanding of the meaning of the HTTPS designation among the general public 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. Combined with the accelerated adoption of HTTPS among website owners globally, we can expect to see the number of HTTPS phishing sites to continue to grow rapidly.

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 Q4 2017 Axur observed more than 16,500 fraud nexuses that targeted Brazilian companies and individuals:

Type	Description	Oct	Nov	Dec	Total
Phishing	Phishing	460	645	526	1,631
Malware	Malware distribution URLs	1682	82	160	410
Paid Search Phishing	Paid ads with phishing on Google and Bing	16	6	5	25
Malicious proxy servers	Malicious proxy servers	13	5	1	19
Redirect	Redirection URLs, leading to phishing or malware	126	75	72	273
Social Media Scams	Scams on social media platforms (FB, Instagram, LinkedIn, YouTube, blogs, etc.)	1,990	1,122	1,612	4,724
Scam Web sites	Scams on Web sites in general	1,310	1,803	3,180	6,293
Mobile App Scam	Apps with unauthorized brand use in official stores (iTunes + GooglePlay) as well as .apk files in Web sites .	1,016	408	1,760	3,184
Total		**5,097**	**4,146**	**7,316**	**16,559**

Axur detected much more abuse in the fourth quarter of 2017 than in the third quarter:

- A 379% increase in phishing (430 in Q3 versus 1,631 in Q4)
- A 245% increase in scam Web sites (2,562 in Q3 versus 6,293 in Q4)
- A 247% increase in social media-based scams (1,909 in Q3 versus 4,724 in Q4)

"In the fourth quarter of 2017 we detected 410 malwares and 320 rogue DNS severs," said Fabio Ramos, CEO of Axur. "On average, each malware targeted ten companies and each rogue DNS targeted three companies. The targeted companies are usually from the financial sector, such as banks and credit card companies."

"In the quarter we also saw phishing targeting Bitcoin exchanges, something we have not seen in Brazil before. In December we detected the first phishing attacks that led people to malware that mined Monero/XMR when the victim was on the fake website."

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

Country of hosting	Oct	Nov	Dec	Total
United States	2,771	1,828	5,897	10,496
Ireland	797	418	1437	2,652
Brazil	404	397	968	1,769
Germany	96	92	325	513
Canada	129	75	273	477
Netherlands	26	47	67	140
Czech Republic	30	45	50	125
Portugal	29	21	43	93
United Kingdom	25	15	48	88
Other (39 countries)	151	127	248	526
Total	4458	3065	9356	16,879

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

Incidents per ISP	Oct	Nov	Dec	Total
Facebook (Ireland Ltd)	1,521	904	3,913	6,338
Google	301	223	963	1,487
Cloudflare	226	206	763	1,195
Amazon.com	161	182	699	1,042
Websitewelcome.com	93	86	293	472

Locaweb Serviços de Internet S/A	65	110	268	443
OVH Hosting	47	66	250	363
Universo Online S.A.	53	69	182	304
Hostinger International Limited	48	75	176	299
Other (443 ISPs)	768	1,024	3,144	4,936
Total	3,283	2,945	10,651	16,879

Axur also sees that fraudsters block access to phishing sites when visited from non-Brazilian IPs. This technique was used in 38 percent of phishing attacks (622 out of 1,631 times). The goal is to prevent (or make it more difficult for) the response team at the ISP or hosting provider from viewing the active fraud, especially when the frauds are hosted on ISPs in other countries (not Brazil). The fraudsters sometimes also block the IPs of the target company (a bank, for instance) so the company's security team will not see the fraud page, unless they access it from an IP that doesn't belong to the company's IP range. The IP filters are usually set up through the htaccess file, inserting rules that allow traffic only from Brazilian IP ranges.

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, 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, 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.

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; Fabricio Pessôa of Axur at +55.51.30122987, fabricio.pessoa@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.**