Phishing Activity Trends Report

3rd Quarter 2017

APWG

Unifying the
Global Response
To Cybercrime

July – September 2017

Published February 27, 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 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 Are Using HTTPS To Assure Users That Phishing Sites Are 'Safe'

Phishers are using HTTPS protection to fool victims into thinking that phishing sites are safe. [p. 5]

3rd Quarter 2017 Phishing Activity Trends Summary

- Phishing was found in more than 200 different top-level domains, with free domain services continuing to enable abuse. [p. 8]
- The number of unique phishing reports submitted to APWG during Q3 2017 was 296,208, nearly 23,000 more than the previous quarter. The number of unique phishing sites declined. [p. 4]
- Phishers are using HTTPS protection to fool victims into thinking phishing sites are safe. [p. 5]
- National Cybercrime Threat Profile: Brazil. [p. 9]
- In South America, phishing campaigns were aimed at companies who deal with cryptocurrencies. [p.10]
- APWG saw notable increases in phishing that targeted SAAS and webmail providers. [p. 12]
- The most-targed sector continued to be payment providers. [p. 12]

Statistical Highlights for 3rd Quarter 2017

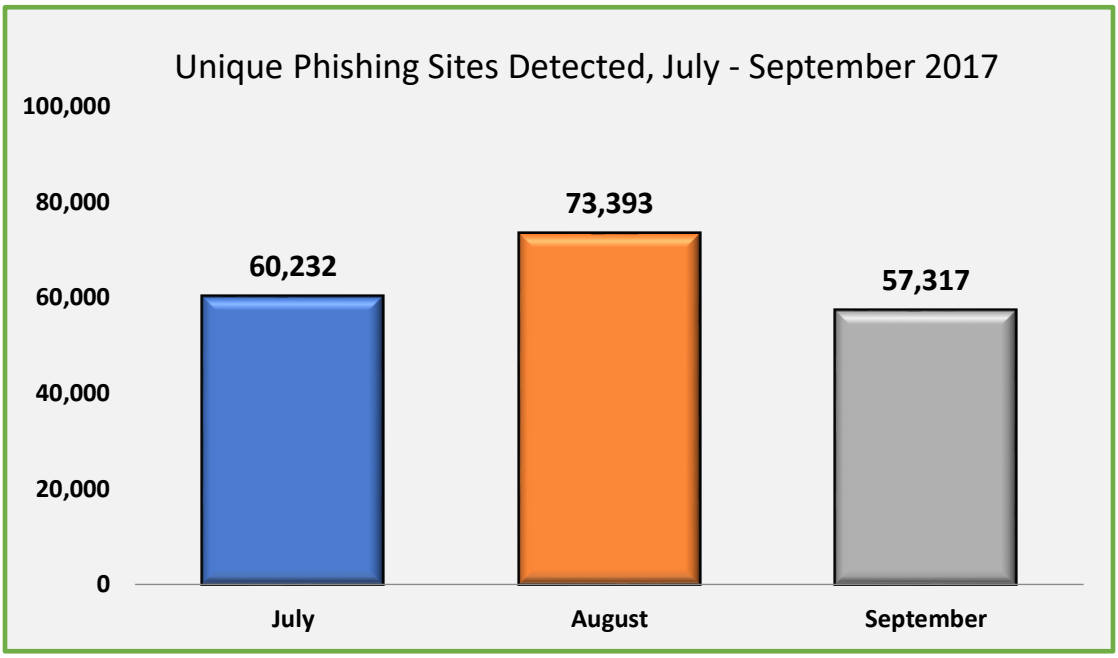
	July	August	September
Number of unique phishing websites detected	60,232	73,393	57,317
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	99,024	99,172	98,012
Number of brands targeted by phishing campaigns	277	313	325

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.

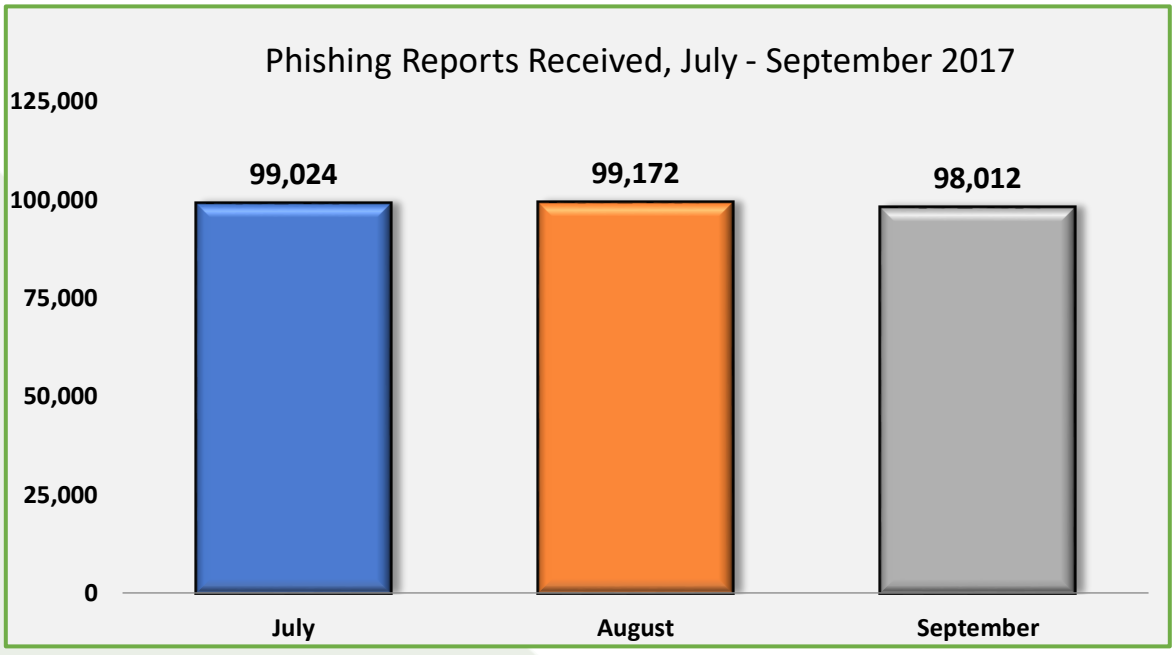
The APWG also tracks the number of unique phishing websites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLS, all leading to basically the same attack destination.) APWG's contributing members also track a variety of additional metrics and data sets in order to track the fast-paces nature of cybercrime.

Phishing E-mail Reports and Phishing Site Trends – 3rd Quarter 2017

The total number of phish detected in Q3 was 190,942, with the highest number occurring in August, which is normally one of the quietest months of the year. The number of sites detected was down from the second quarter.



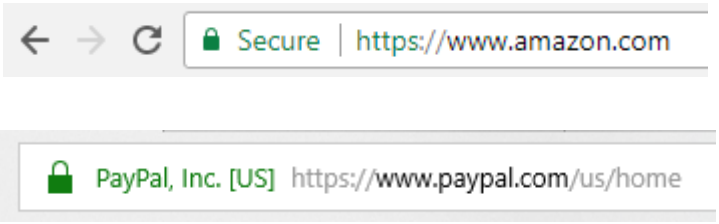
The number of unique phishing reports submitted to APWG during Q3 2017 was 296,208, nearly 23,000 more than the 273,395 reported in Q2, 2017. Volume remained consistent during the three-month period.



How Phishers Use Encryption to Fool Victims

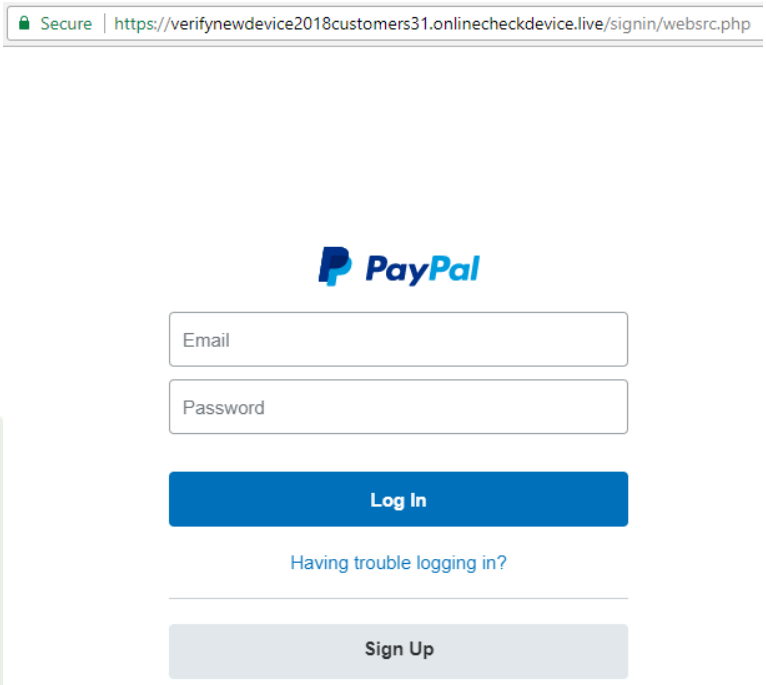
APWG contributor PhishLabs has been tracking how many phishing sites are protected by HTTPs. This provides insight into how phishers are fooling Internet users by turning an Internet security feature against them. PhishLabs provides managed security services that help organizations protect against phishing attacks targeting their employees and their customers.

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. In web browsers, HTTPS-protected sites are indicated with a padlock as a signal to the user:

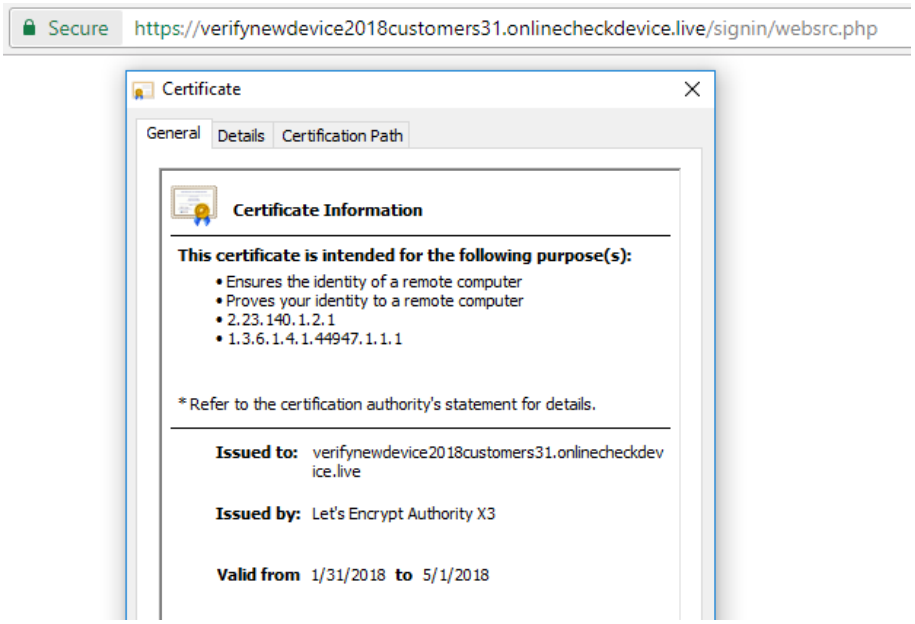


However, the mere presence of HTTPS does not indicate that the site is safe from phishing, and many Internet users do not know this. A phisher who has broken into the hosting of a web site and has installed a phishing page there has access to the transmitted data, such as passwords and credit card numbers. And phishers can set up their own HTTPS-protected sites, to lure users into a false sense of security.

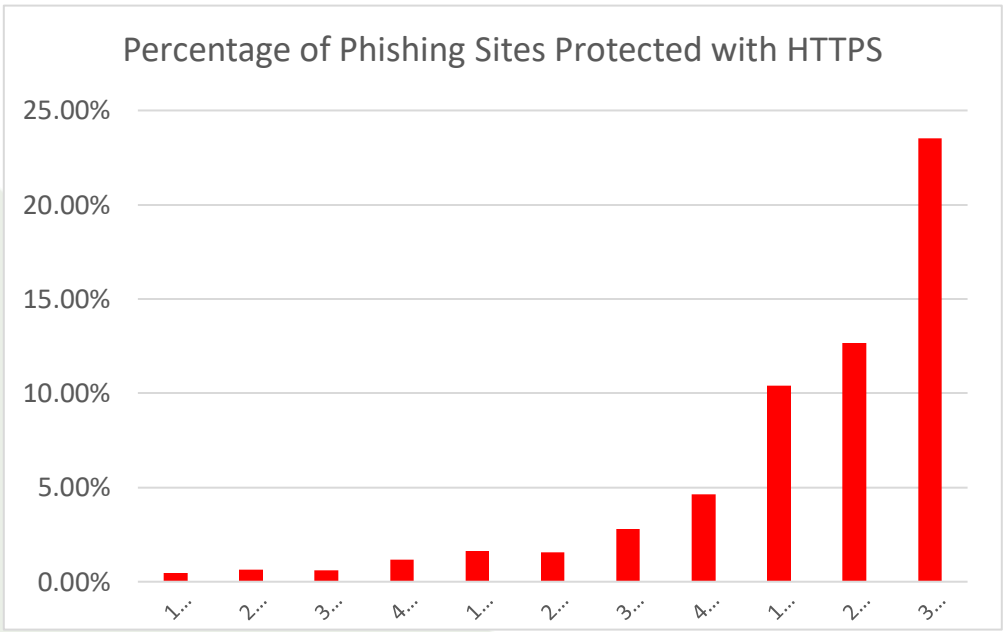
Below is an example on the domain onlinecheckdevice.live, which the phisher purchased on 31 January 2018, and then immediately used to launch this HTTPS-protected phishing site that mimics PayPal:



The phisher obtained the encryption certificate from Let's Encrypt, which provides free certificates via an easy-to-use, automated system:



PhishLabs examined 54,631 unique phishing sites (attacks) in the third quarter of 2017, and found that almost a quarter were protected by HTTPS:



Crane Hassold, Threat Intelligence Manager at PhishLabs, said, "Just a year before, less than three percent of phish were hosted on websites using SSL certificates," said. Hassold noted that some of the rise is due to generally increased deployment of HTTPS across the Internet. In the last two years especially, more companies have been encrypting their entire web sites, not just sensitive pages. Google has found that desktop users of its Chrome browser load more than half of the pages they view over HTTPS."[1]

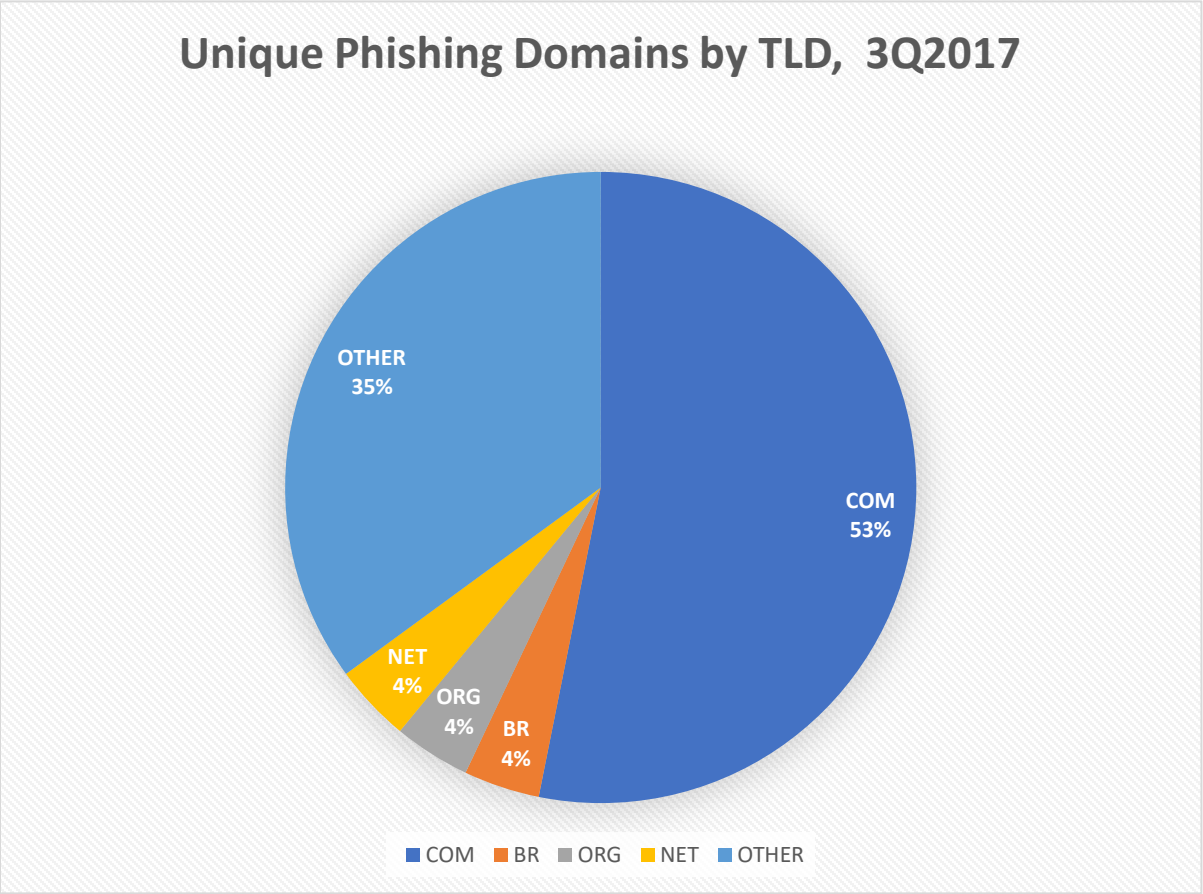
But phishers are actively tricking Internet users with the HTTPS ploy. Hassold noted: "An analysis of third-quarter 2017 HTTPS phishing attacks against two of the most phished brands indicates that nearly *three-quarters* of HTTPS phishing sites targeting them were hosted on maliciously-registered domains rather than compromised web sites. That's substantially higher than the overall HTTPS global usage rate."

[1] https://transparencyreport.google.com/https/overview

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 Q3, 2017. The study set contained 8,835 unique domain names and 106 unique IP addresses (URLs that did not contains a domain name).

Fifty-three percent of the unique phishing domain names were on .COM. The .COM top level domain represented about 40 percent of the registered domain names worldwide in Q3. Another 12 percent of the unique phishing domains were spread out evenly between .BR, .NET, and .ORG. The remaining 35 percent were distributed across hundreds of other TLDs. About 3 percent were spread across 66 new gTLDs.



"Free infrastructure continues to enable abuse," said Jonathan Matkowsky, Vice President of IP and Brand Security at RiskIQ. "For example, within the new gTLDs, while .TECH had relatively very few unique second level domains used in phishing attacks, 21 percent of phishing sites across the new gTLDs were on .TECH primarily because a Russian hosting company in Saint Petersburg offers temporary free hosting on its own .TECH domain so that customers can test sites prior to registering second-level domains. Criminals will continue to take advantage of such free infrastructure."

National Cybercrime Threat Profile: Phishing and Identity Theft Techniques in Brazil

APWG member company Axur, which is located in Brazil, concentrates on protecting companies and their users in Brazil from Internet-based threats, with a focus on 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 Q3 2017 Axur observed nearly 6,500 fraud nexuses that targeted Brazilian companies and individuals:

Type	Description	July	Aug	Sept	Total
Malware C&C	Malware command and control servers	1	4	10	**15**
Malware	Malware distribution URLs	239	192	87	**518**
PAC	Proxy auto-configuration files that setup the user's browser to access fraudulent websites	1	0	0	**1**
Paid Search Phishing	Paid ads with phishing in Google and Bing	0	1	0	**1**
Pharming	Rogue DNS	17	13	0	**30**
Phishing	Phishing	209	137	84	**430**
Malicious proxy servers	Malicious proxy servers	48	7	3	**58**
Redirect	Redirection URLs	59	401	51	**511**
Social Media Scams	Scams on social media platforms (FB, instagram, LinkedIn, Youtube, blogs, etc.)	982	545	382	**1909**
Scam Web sites	Scams on websites in general	459	1239	864	**2562**
Mobile App Scam	Apps with unauthorized brand use in official stores (iTunes + GooglePlay) as well as .apk files in websites.	85	68	243	**396**
Total		**2100**	**2607**	**1724**	**6431**

"In the 3rd quarter of 2017, we detected 15 C&Cs, 518 malwares, and 30 pharming attacks," said Fabio Ramos, CEO of Axur. "On average, each malware targeted two companies and each pharming attack three targets. The maximum number of targets in a single malware was 11, while on pharming attack targeted four companies. The targeted companies are usually from the financial sector: banks and credit card companies. We have seen lots of new phishing campaigns aimed at companies who deal with cryptocurrencies. We believe that as cryptocurrencies become even more popular and increase in market value such cases will be more frequent. Startup fintechs in general also seem to be a new target for our region."

With 6,431 incidents reported, most of incidents were on Facebook, and hosted in the United States, followed by ASNs in Ireland:

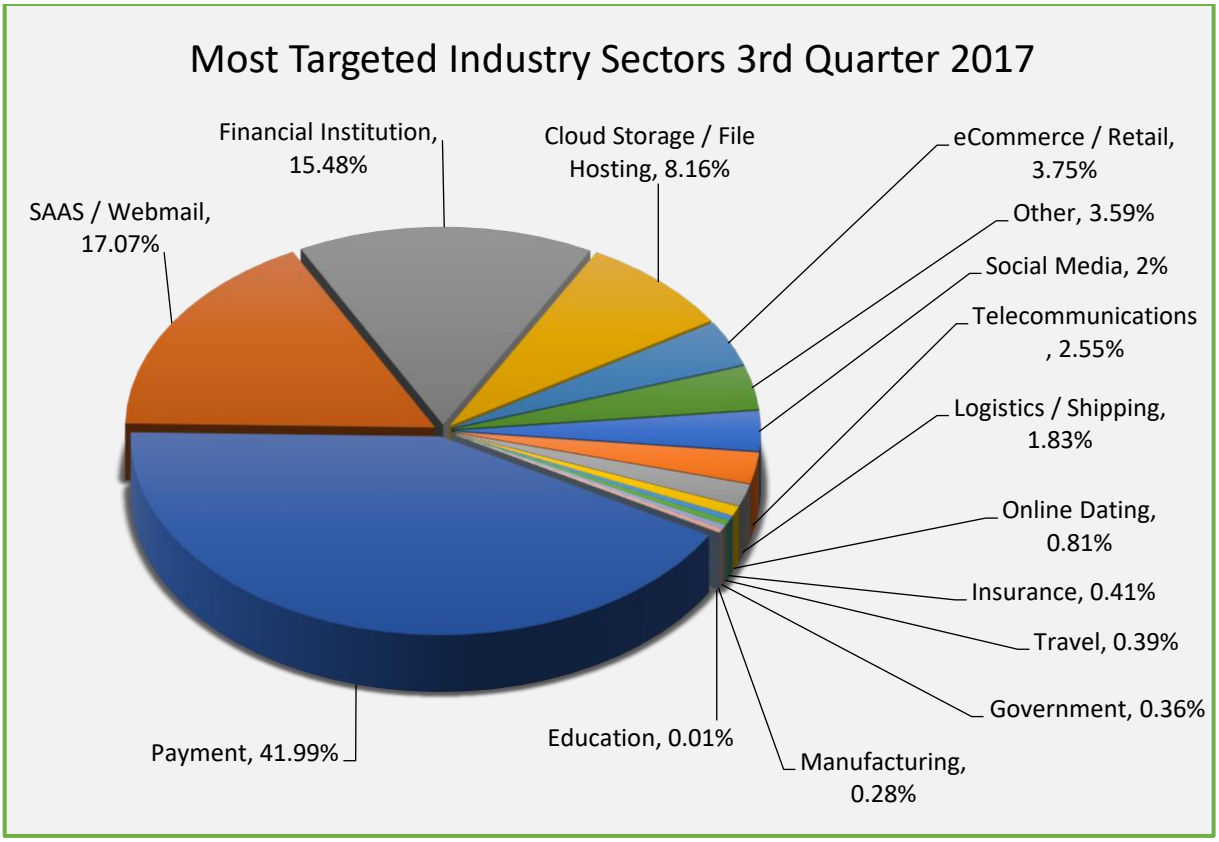
Country of hosting	July	Aug	Sept	Total
United States	1,392	1,686	1,082	**4,160**
Ireland	375	208	165	**748**
Brazil	148	239	175	**562**
France	19	60	87	**166**
Germany	21	68	57	**146**
Canada	44	68	33	**145**
Switzerland	0	77	8	**85**
Netherlands	12	34	22	**68**
United Kingdom	11	21	30	**62**
Czech Republic	19	25	13	**57**
Others (35 countries)	59	121	52	**232**
Total	**2,100**	**2,607**	**1,724**	**6,431**

Fraudsters block access to the fraud from non-Brazilian IPs. The goal is to prevent (or make it more difficult for) the response team at the ISP from viewing the active fraud, especially when the frauds are hosted on ISPs in other countries (not Brazil). They 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.

Type of incident\Q3 2017	No IP Filter	IP Filtered	Total	% per type
Malware C&C	15	0	15	**0%**
Malware	275	243	518	**47%**
PAC	396	0	396	**0%**
Paid Search Phishing	0	1	1	**100%**
Pharming	1	0	1	**0%**
Phishing	30	0	30	**0%**
Malicious Proxy Server	280	150	430	**35%**
Redirect	58	0	58	**0%**
Social Media Scams	275	236	511	**46%**
Scam Website	1909	0	1909	**0%**
Total	2562	0	2562	**0%**

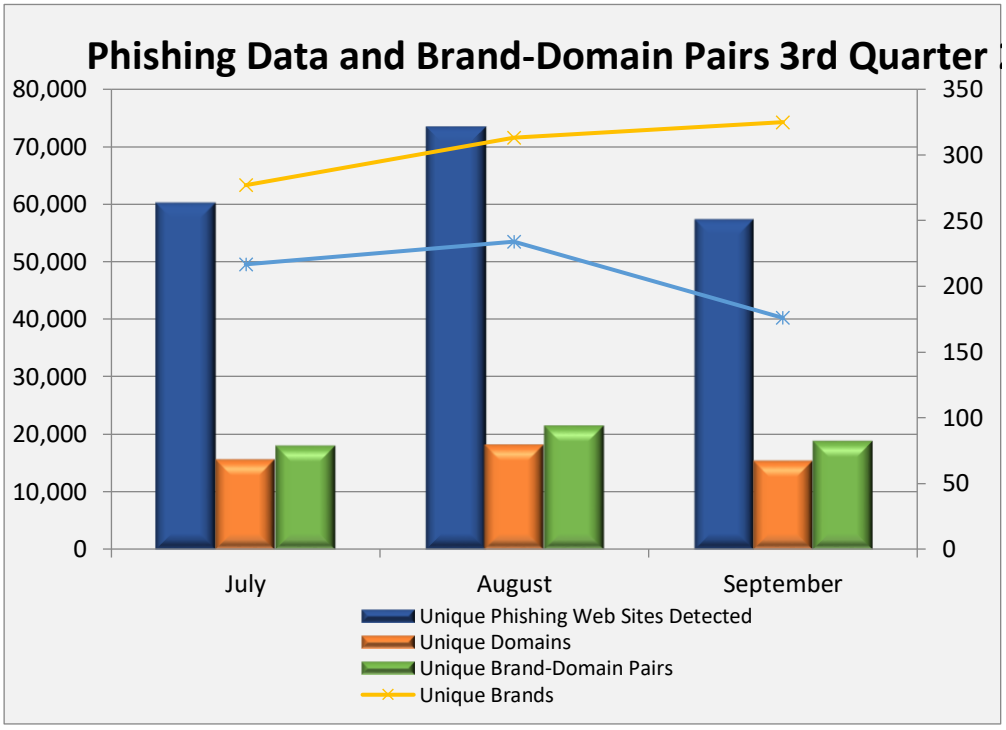
Most-Targeted Industry Sectors – 3rd Quarter 2017

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.



Brand-Domain Pairs Measurement – 3rd Quarter 2017

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.



	July	August	September
Number of Unique Phishing Web Sites Detected	60,232	73,393	57,317
Unique Domains	15,567	18,145	15,356
Unique Brand-Domain Pairs	18,039	21,463	18,806
Unique Brands	277	313	325
URLs Per Brand	217	234	176

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