Phishing Activity Trends Report

4th Quarter 2019

APWG

Unifying the

Global Response

To Cybercrime

Activity October-December 2019

Published February 24, 2020

Phishing Report Scope

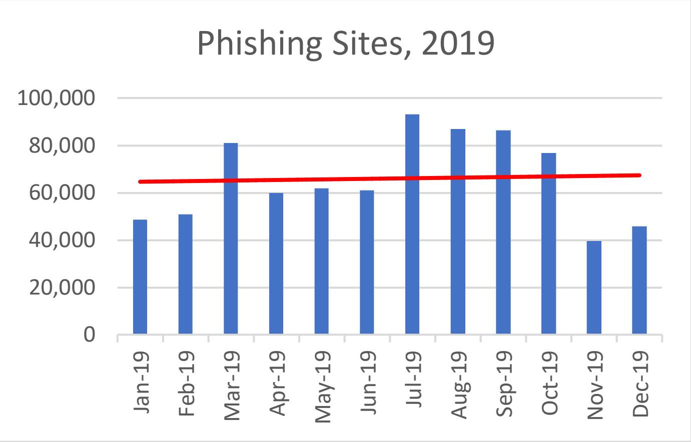
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG measures the evolution, proliferation, and propagation of identity theft methods by drawing from the research of our member companies and industry experts.

Phishing Defined

Phishing is a crime employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and email messages. These are designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant malware onto computers to steal credentials directly, often using systems that intercept consumers' account user names and passwords or misdirect consumers to counterfeit Web sites.

Table of Contents

The Year in Phishing: 2019 Ended with Ups and Downs



4th Quarter 2019 Phishing Activity Trends Summary

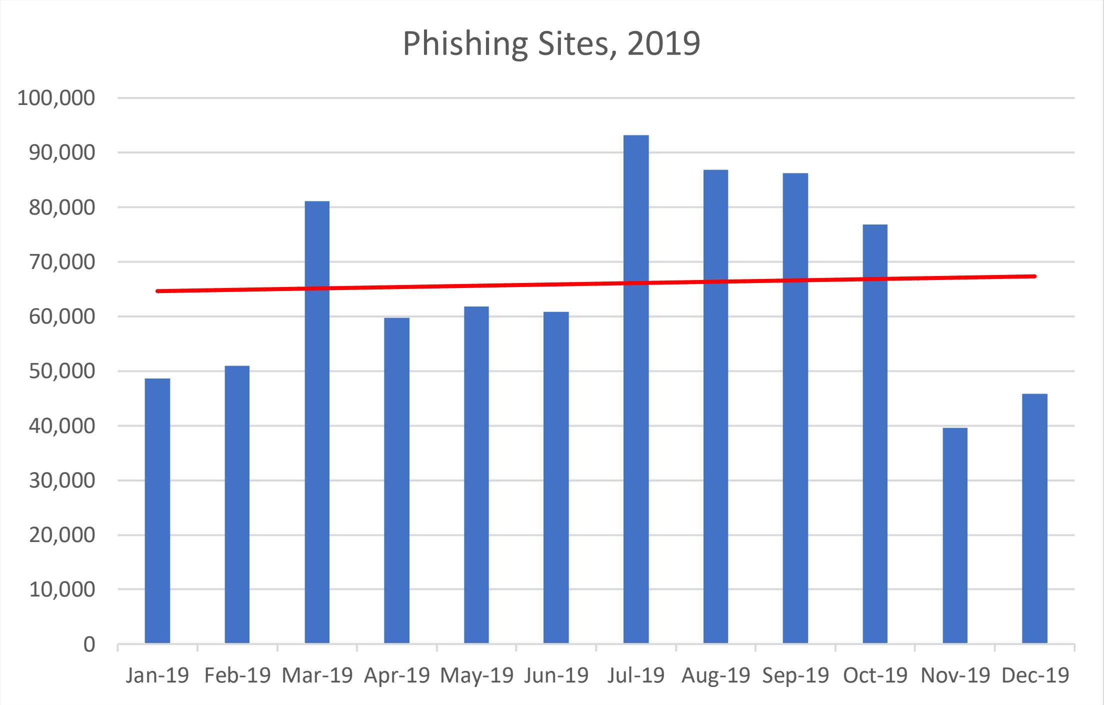
- The number of phishing attacks worldwide receded in the fourth quarter of 2019, reverting closer to the mean. [pp. 3-4]
- During 2019, the number phishing incidents in Brazil increased by 232 percent. [pp. 9-10]
- Phishing that targeted webmail and Software-as-a-Service (SaaS) users continued to be biggest category of phishing. [p. 5]
- Criminals perpetrating Business Email Compromise (BEC) attacks used gift cards to cash out during the holiday shopping season. [pp. 6-7]
- Almost three-quarters of all phishing sites now use SSL protection, highest recorded since early 2015, and an indicator that users can't rely on SSL alone to understand whether a site is safe or not. [p.11]
- The use of gTLD domain names for phishing occurs at a greater frequency than for ccTLDs. [p.9]

Statistical Highlights for 4th Quarter 2019

	October	November	December
Number of unique phishing Web sites detected	76,804	39,580	45,771
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	45,057	42,424	45,072
Number of brands targeted by phishing campaigns	333	325	341

APWG's contributing members report phishing URLs into APWG, and study the ever-evolving nature and techniques of cybercrime. The APWG tracks the number of unique phishing Web sites, a primary measure of phishing across the globe. This is 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.)

The total number of phishing sites detected by APWG in the fourth quarter was 162,155. This was down from the 266,387 seen in Q3 and the 182,465 seen in Q2, and up from the 138,328 seen in Q4 2018.



Statistical Highlights for 4th Quarter 2019

"The year 2019 turned out to be a roller-coaster ride for phishing," said Greg Aaron, APWG Senior Research Fellow and President of Illumintel Inc. "July though October was the worst period for phishing that the APWG had seen in three years, and then phishing levels settled back down to more normal levels."

The number of unique domain names used for phishing dropped at a lower rate, from 13,597 in October, to 15,261 in November, and to 12,260 in December.

The APWG also tracks the number of unique phishing reports (email campaigns) it receives from consumers and the general public. 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).

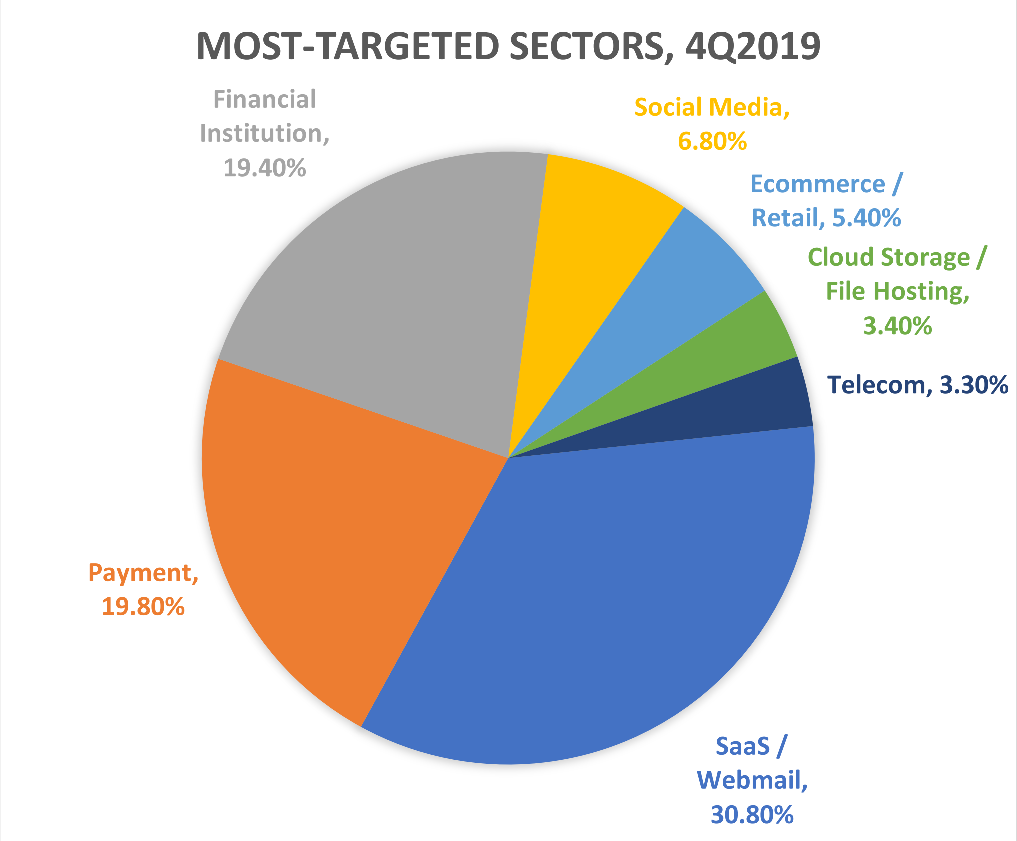
APWG counts unique phishing report e-mails as those found in a given month that have the same email subject line. The number of these unique phishing reports submitted to APWG during 4Q was 132,553, up from 122,359 in Q3 and 112,163 in Q2. These were phishing emails submitted to APWG by the general public, and excludes phishing URLs reported by APWG members directly into APWG's eCrime eXchange.

Most-Targeted Industry Sectors – 4th Quarter 2019

In the fourth quarter of 2019, APWG member OpSec Security found that SaaS and webmail sites remained the most frequent targets of phishing. Phishers continue to harvest credentials to those kinds of sites, using them to perpetrate business e-mail compromises (BEC) and to penetrate corporate SaaS accounts. Stefanie Wood Ellis, Anti-Fraud Product & Marketing Manager at OpSec Security, noted: "Phishing against Social Media targets grew every quarter of the year, doubling over the course of 2019."

Attacks against cloud storage and file hosting sites remained less popular. Attacks against the cryptocurrency, logistics/shipping, gaming, insurance, energy, government, and healthcare sectors were negligible during Q4, each at less than 1 percent of all phishing attacks detected.

OpSec Security (formerly known as MarkMonitor) is a founding APWG member and an online brand protection organization, securing intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.

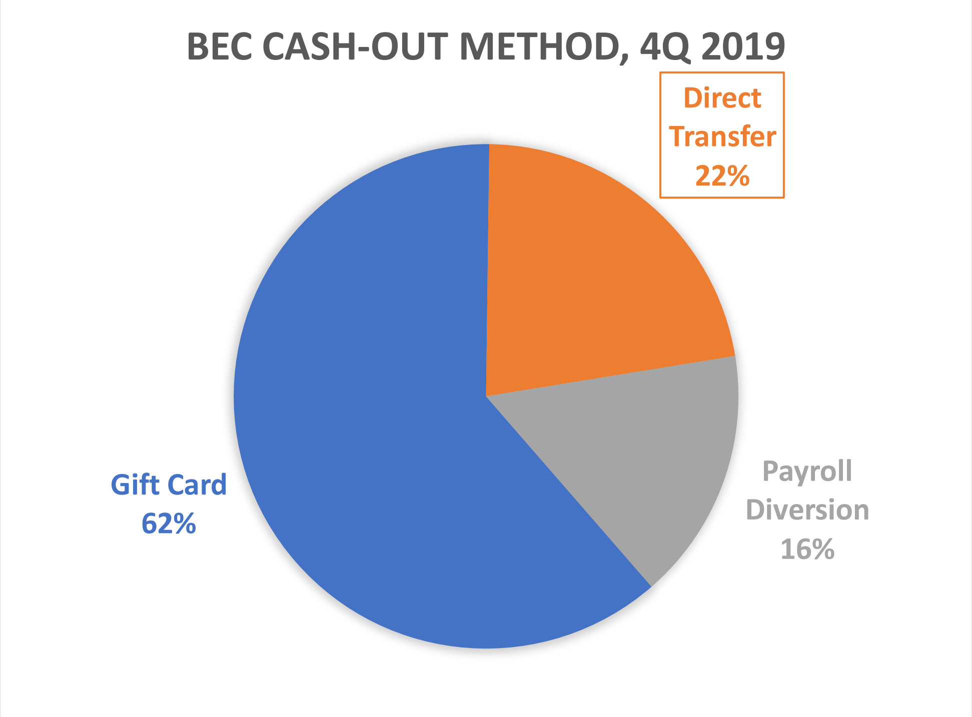


Business e-Mail Compromise, 4th Quarter 2019

APWG member Agari tracks the identity theft technique known as "business e-mail compromise" or BEC. In a BEC attack, a scammer targets employees who have access to company finances, usually by sending them email from fake or compromised email accounts (a "spear phishing" attack). The scammer impersonates a company employee or other trusted party, and tries to trick the employee into sending money. The attacker may prepare by spending weeks inside the organization's network and accounts, studying the organization's vendors, billing system, and even the CEO's style of communication. BEC attacks have caused aggregate losses in the billions of dollars, at large and small companies.

Agari examined thousands of attempted BEC attacks observed during Q4 to assemble its data set. Agari counts BEC as any response-based spear phishing attack that involves the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive materials. Agari protects organizations against phishing, BEC scams, and other advanced email threats.

Agari documented that scammers requested funds in the form of gift cards in 62 percent of BEC attacks, up from 56 percent during the third quarter of 2019, and down from 65 percent in Q2. About 16 percent of attacks requested payroll diversions, down from 25 percent in Q3. Some 22 percent of BEC attacks involved requests for direct bank transfers.

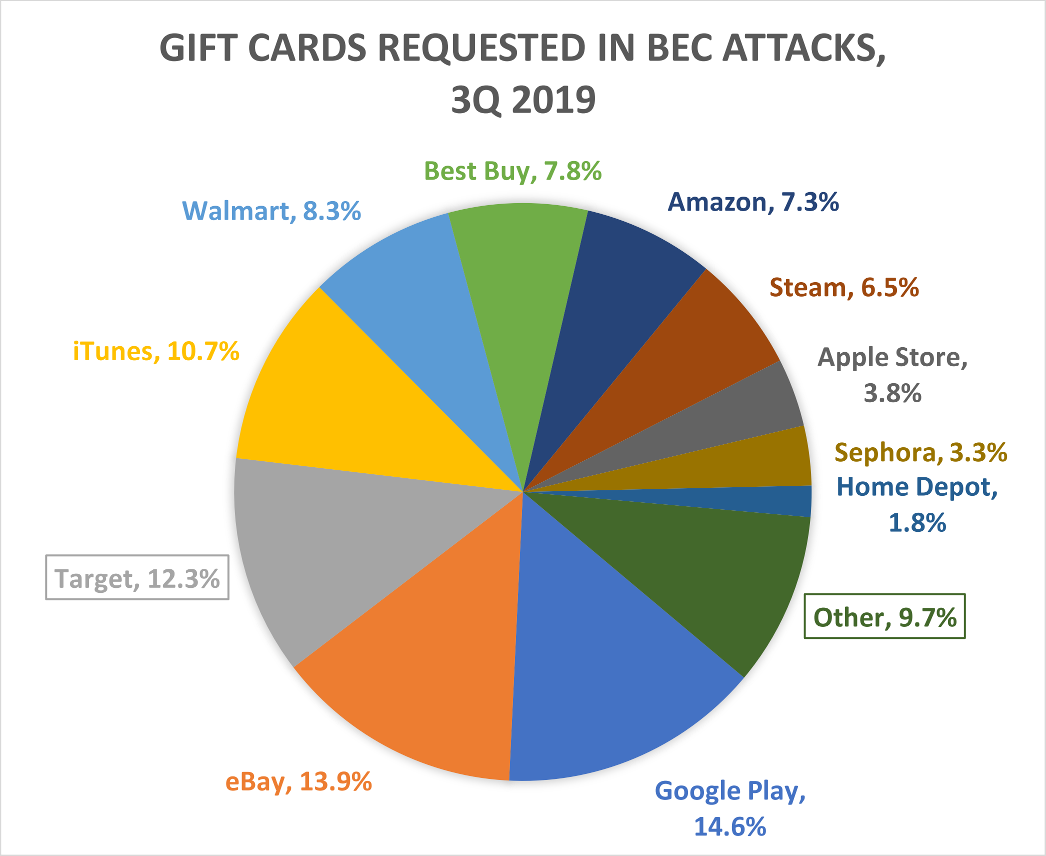


Business e-Mail Compromise, 4th Quarter 2019

The amount of money that an attacker can make by getting gift cards is significantly less than with a wire transfer. During Q4, the average amount of gift cards requested by a BEC actor was more than $1,600. But for wire transfer BEC attacks, the average amount requested in Q4 was over $55,000:

	Average	Median	Min	Max
Wire transfer requests	$55,395	$28,350	$2,550	$680,456
Gift card requests	$1,627	$1,200	$150	$10,000

According to Crane Hassold, Agari's Senior Director of Threat Research, "One of the really notable things we saw during the Q4 was a change in the types of gift cards requested. Google Play was still the most-requested gift card, but decreased from 27 percent to 15 percent of requests. We saw increases in requests for gift cards for eBay, Target, Best Buy, and Sephora. The increase could be due to the fact that all of these companies sell physical goods, and the attacks took place during the holiday season. It may indicate that scammers are looking to launder money by using the cards to buy physical goods that they can then sell, rather than putting the money into online cryptocurrency exchanges, which is also a popular laundering option."

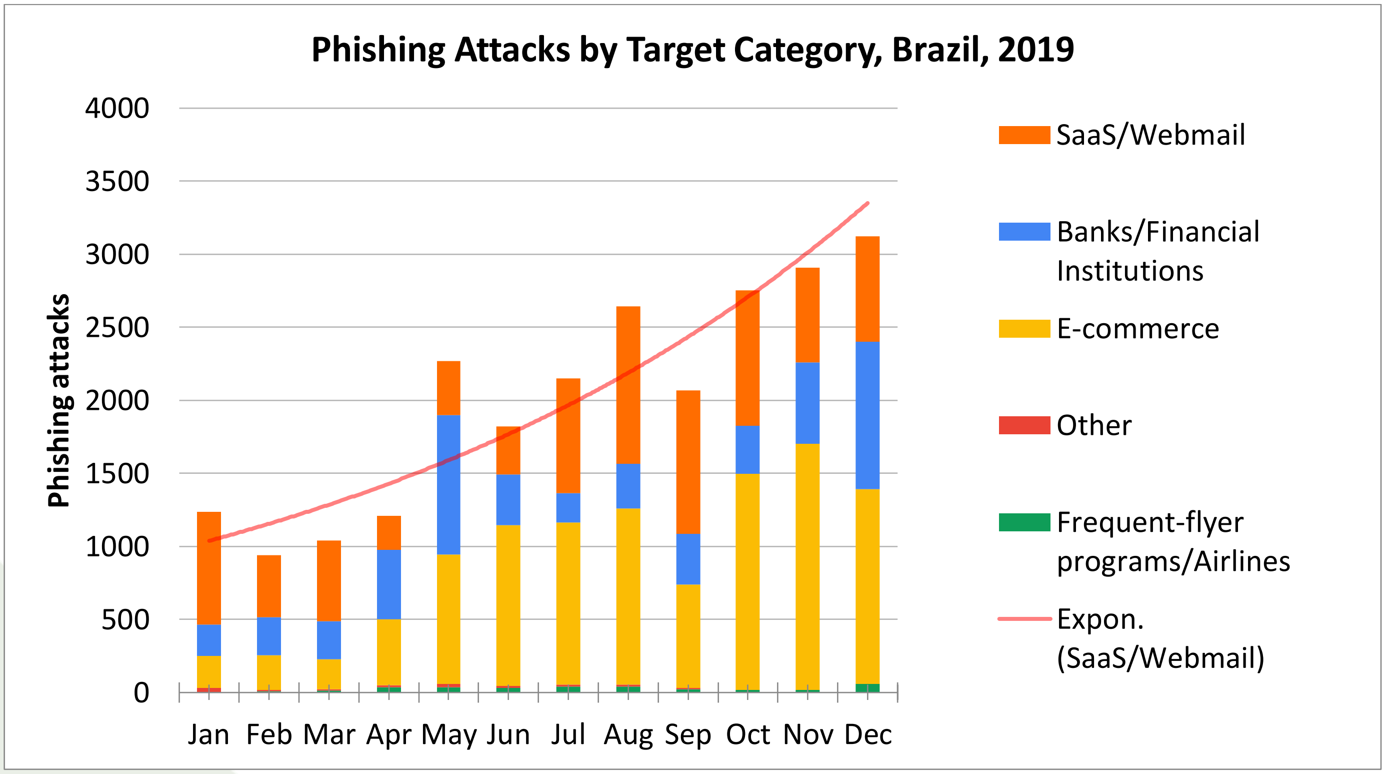


Overall, BEC attackers used Gmail accounts 20 percent of the time. By type of mail account, attackers used webmail accounts 57 percent of the time (Gmail being 35 percent of those), standard email accounts on other domains 39 percent of the time, and clearly compromised (hacked) email accounts about 4 percent of the time.

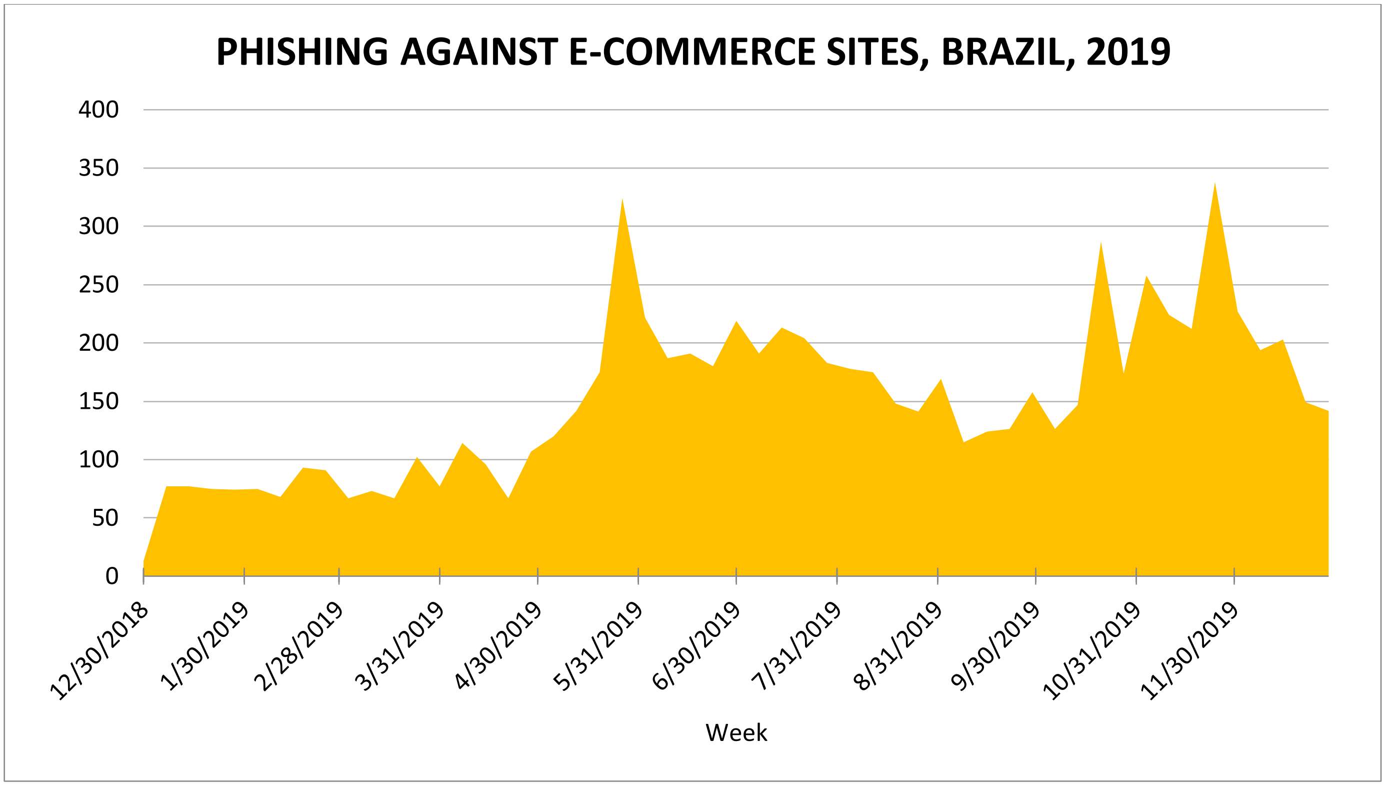
Online Criminal Activity in Brazil

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 the fourth quarter of 2019, Axur observed 8,872 phishing attacks. That was up significantly from the 6,862 cases Axur detected in Q3, the 5,297 cases in Q2, and the 3,220 in Q1. Specifically, these were attacks against Brazilian brands or against foreign services that are available in Portuguese in Brazil.



From February to December 2019, the monthly totals of phishing incidents in Brazil increased a disturbing 232%:



The peak came in November, with 1,685 unique phishing cases in Brazil. This is the highest number of the year and it came mainly from scams around the Black Friday shopping holiday. Historically, criminals in Brazil have increased the frequency of their attacks near the end-of-year holidays, targeting the financial sector to steal data. Similarly, 13th salary payments in Brazil (happening between November and December) are bank transitions that might attract attacks.

Use of Domain Names for Phishing

APWG member RiskIQ provides ongoing analysis of where phishing is happening in the domain name system. RiskIQ analyzed 2,149 confirmed phishing URLs reported to APWG in Q4 2019. RiskIQ found that they were hosted on 1,328 unique second-level domains. RiskIQ provides digital risk protection by illuminating risk associated with an organization's digital presence.

There are three types of top-level domains (TLDs) for purposes of this report:

- "Legacy" generic TLDs, which existed before 2011. These include .COM, .ORG, and TLDs such as .ASIA and .BIZ. They represented 49% of the domain names in the world as of the beginning of Q4, and represented 65% percent of the phishing domains in the sample set. There were 865 legacy gTLDs in the sample set. Most of those were in .COM.
- The new generic top-level domains (nTLDs), such as .WORK and .ICU, were released after 2011. At the beginning of Q4, the nTLDs represented about 7% of the domains in the world, and were about 7% of the domains in the sample set. There were 88 nTLD domains in the sample set.
- The country code domains (ccTLDs), such as .UK for the United Kingdom and .MX for Mexico. ccTLDs were about 45% of the domains in the world as of the beginning of Q4, but were only 28% of the domains in the sample set. There were 375 ccTLD domains in the sample set.

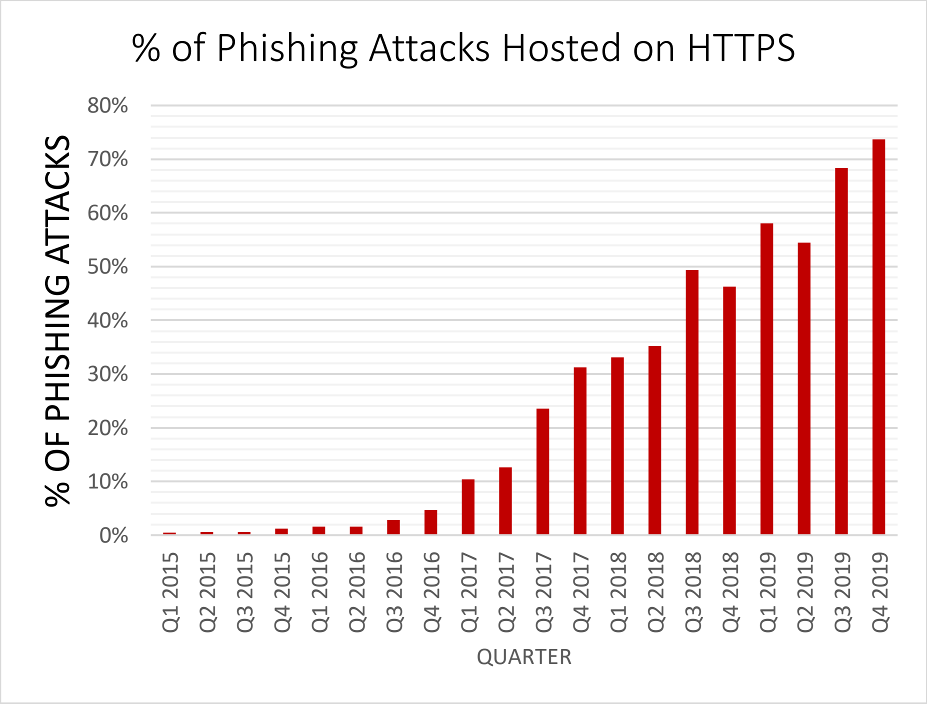
The chart below shows the TLDs that had the most unique second-level domains used for phishing.

Rank	TLD	Category	# of Unique Domains in Sample Set (4Q 2019)
1	.COM	generic	727
2	.ORG	generic	50
3	.BR	ccTLD	46
4	.NET	generic	43
5	.INFO	generic	33
6	.UK	ccTLD	29
7	.RU	ccTLD	24
8	.IN	ccTLD	23
9	.XYZ	nTLD	18
10	.ML	ccTLD	15
11	.AU	ccTLD	14
12	.TOP	nTLD	13
12	.KR	ccTLD	13
13	.ZA	ccTLD	12
14	.CF	ccTLD	10
14	.TK	ccTLD	10
14	.VN	ccTLD	10
15	.MX	ccTLD	9

"Over 80 unique domains or IP addresses in the sample set used for phishing targeted multiple companies and their brands," said Jonathan Matkowsky, a cyber advisor at RiskIQ. "The bulk of them were not on free hosting accounts, but either on maliciously registered domains used exclusively for phishing, or on compromised sites—but relatively speaking, that is still a small percentage of the sample set. This may just be a result of what is being detected and reported."

How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking how many phishing sites are protected by the HTTPS 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 important on 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.



In Q3 2019, 68 percent of sites used for phishing were using SSL. "But by the end of 2019, 74% of all phishing sites were using TLS/SSL," observed John LaCour, Founder and CTO of PhishLabs. "Attackers are using free certificates on phishing sites that they create, and are abusing the encryption already installed on hacked web sites."

APWG Phishing Activity Trends Report Contributors

AGARI

Agari protects organizations against phishing, business email compromise (BEC) scams, and other advanced email threats.

///AXUR

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

ILLUMINTEL

Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.

OpSec ONLINE

OpSec Online™ (formerly founding APWG member MarkMonitor®), offers world class brand protection solutions.

PHISHLABS

PhishLabs provides managed threat intelligence and mitigation services that protect brands, customers, and the enterprise from digital risks.

RISKIQ

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 (foy@apwg.org, +1.404.434.728). For media inquiries related to the company-content of this report, please contact APWG Secretary General Peter Cassidy (pcassidy@apwg.org, +1.617.669.1123); Stefanie Ellis at OpSec Security (Stefanie.ellis@markmonitor.com); Jean Creech of Agari (jcreech@agari.com, +1.650.627.7667); Eduardo Schultze of Axur (eduardo.schultze@axur.com,+55 51 3012-2987); Stacy Shelley of PhishLabs (stacy@phishlabs.com, +1.843.329.7824); Kari Walker of RiskIQ (Kari@KariWalkerPR.com, +1.703.928.9996). **Analysis and editing by Greg Aaron, Illumintel Inc., www.illumintel.com**