Phishing Activity Trends Report

4th Quarter 2020

APWG

Unifying the Global Response To Cybercrime

Activity October-December 2020

Published 9 February 2021

Phishing Report Scope

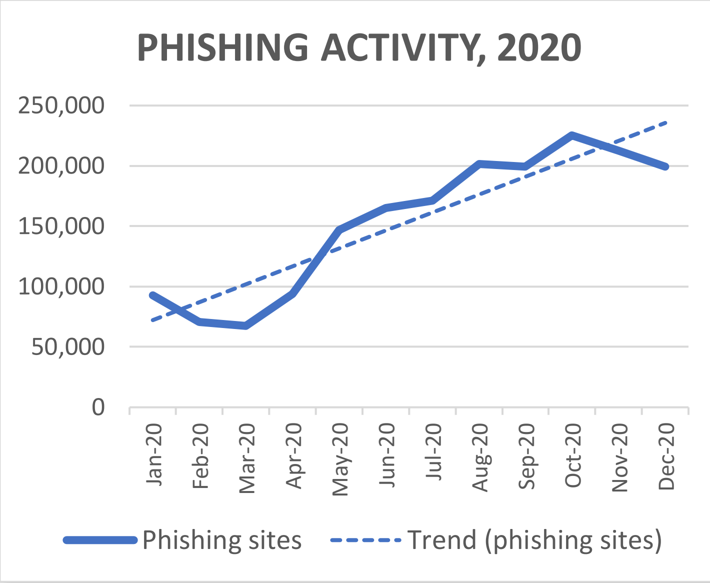
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. 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 usernames and passwords or misdirect consumers to counterfeit Web sites.

Table of Contents

Phishing Attacks Doubled in 2020 as October Shatters Monthly Records



Phishing Activity Trends Summary

- The number of phishing attacks observed by APWG and its members grew through 2020, doubling over the course of the year. [pp. 3-4, 8]
- Business e-mail compromise scams are becoming more costly for victims. The average wire transfer request in BEC attacks increased from $48,000 in Q3 to $75,000 in Q4. [p. 6]
- The financial institution, webmail, and SaaS site category was the one most frequently victimized by phishing in this quarter. [p. 5]
- Phishers are using an array of deception techniques to fool users. These include domain names chosen to avoid detection (pp. 7, 9 and 12), encryption designed to lull victims into a false sense of security (p. 11), and deceptive email addresses used to spoof trusted companies and business contacts (p. 7).

This edition of the Trends Report is dedicated to the memory of two friends of APWG:
Ben Butler of GoDaddy, and Yonathan Klijnsma of RiskIQ.

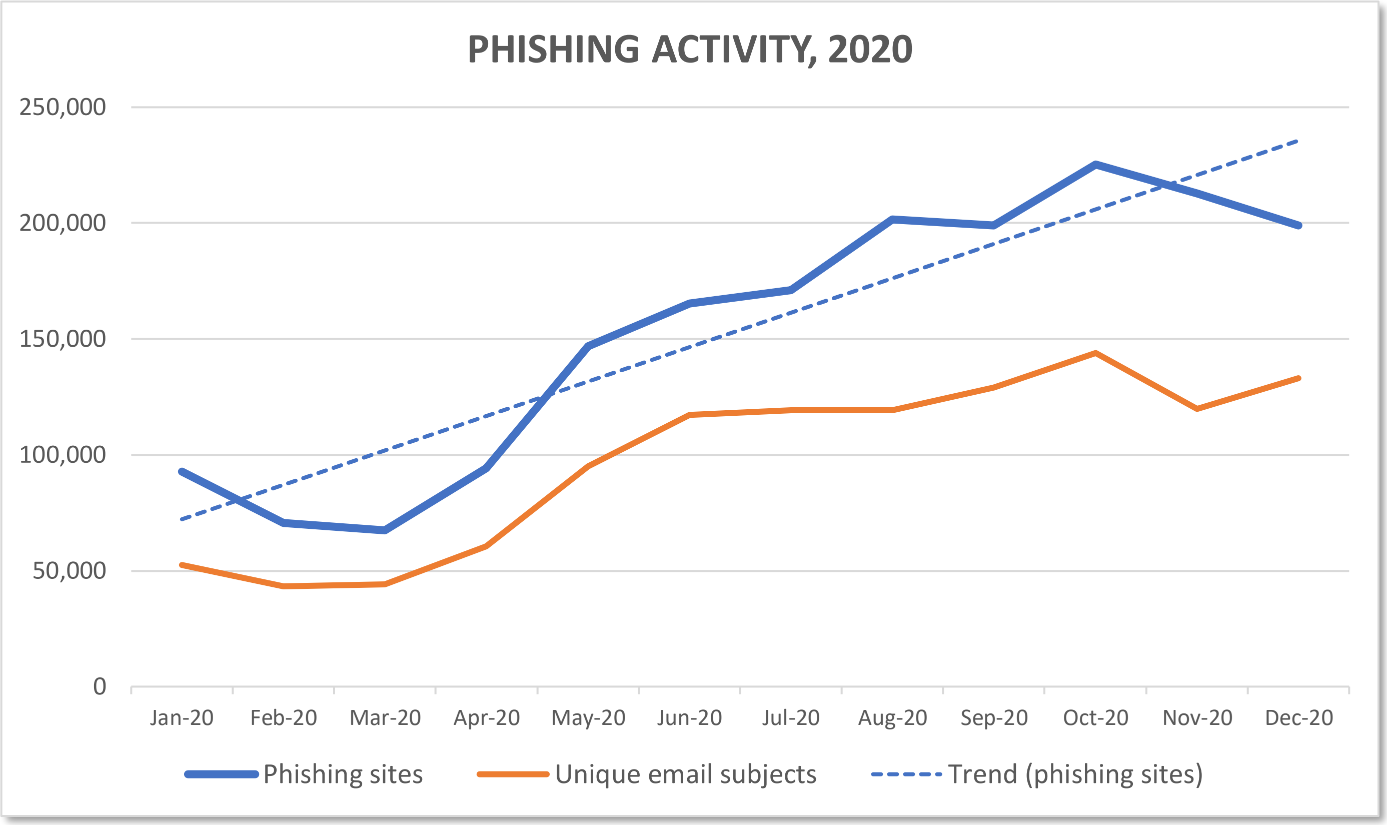
Statistical Highlights for the 4th Quarter 2020

APWG's contributing members study the ever-evolving nature and techniques of cybercrime. With this report, the APWG has refined the methodologies it uses to report phishing. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

The APWG tracks:

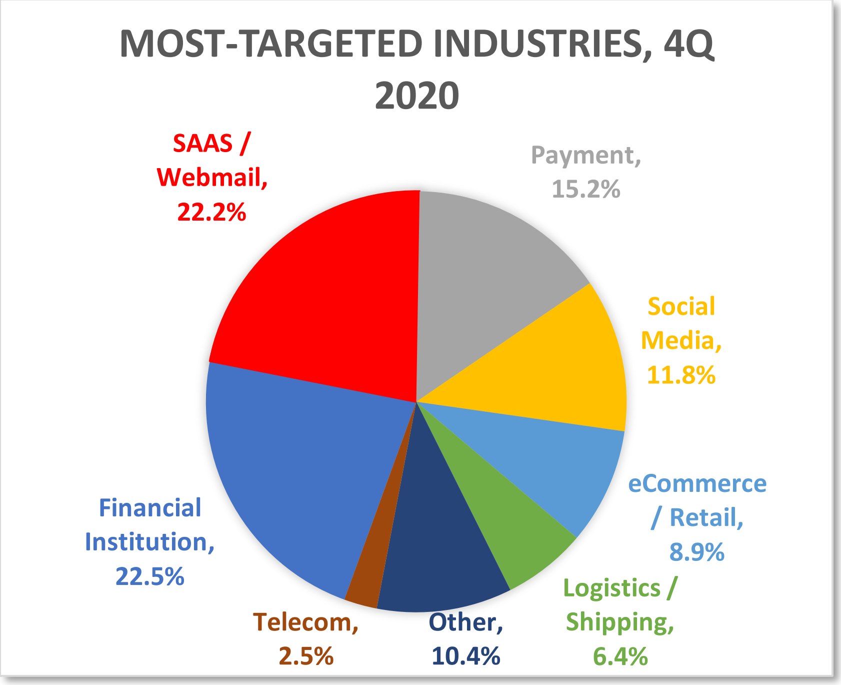
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique base URLs of phishing sites found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same *attack*, or destination.) APWG is measuring reported phishing sites on a more accurate basis accounting for how phishers have been constructing phishing URLs. Applied to our historic data going back a year, this counting reveals a climbing number of phishing attacks since March 2020.
- **Unique phishing e-mails subjects**. This counts email lures that have different email subject lines. Some phishing campaigns may use the same subject line but advertise different phishing sites. This metric is a general measure of the variety of phishing attacks, and a rough proxy for the amount of phishing taking place.
- The APWG also counts the **number of brands attacked** by examining the phishing reports submitted into the APWG eCrime Exchange, and normalizing the spellings of brand names.

	October	November	December
Number of unique phishing Web sites detected	225,304	212,878	199,120
Unique phishing email subjects	143,950	119,700	133,038
Number of brands targeted by phishing campaigns	532	505	515


PHISHING ACTIVITY, 2020
250,000
200,000
150,000
100,000
50,000
0
Jan-20
Feb-20
Mar-20
Apr-20
May-20
Jun-20
Jul-20
Aug-20
Sep-20
Oct-20
Nov-20
Dec-20
Phishing sites
Unique email subjects
Trend (phishing sites)

Most-Targeted Industry Sectors – 4th Quarter 2020

In the fourth quarter of 2020, APWG member OpSec Security found that phishing attacks against financial institutions were the most prevalent. Phishing against SaaS and webmail sites was down, from 31.4 percent of all attacks in Q3 2020 to 22.2 percent in Q4. Phishing against e-commerce sites ticked up, while attacks against social media companies dipped slightly from 12.6 percent to 11.8 percent of all attacks, even during the U.S. presidential election.



"Looking back at the entirety of 2020, the ten most-targeted organizations accounted for about 60 percent of the total phishing attacks detected throughout the year," noted Stefanie Wood Ellis, Anti-Fraud Product & Marketing Manager at founding APWG member OpSec Online. "They were primarily financial institutions, SAAS or webmail-based organizations, and payment providers. Social media services were targeted more frequently, with emphasis on messaging applications. Though the volume is still relatively low, we see cryptocurrency exchanges and related sites being targeted more frequently as well."

Stefanie Wood Ellis added: "Working with our customers over the course of 2020 and the COVID-19 pandemic, we've seen some shifts from traditional phishing to more elaborate trademark or copyright misuse scams. These include fake marketplaces where the victim loses the money they paid for goods, and their credentials are potentially compromised as well. Leading to further losses."

OpSec Online offers world-class brand protection solutions.

Business e-Mail Compromise (BEC), 4th Quarter 2020

APWG member Agari tracks the identity theft technique known as "business e-mail compromise" or BEC, which has caused aggregate losses in the billions of dollars, at large and small companies. In a BEC attack, a scammer impersonates a company employee or other trusted party, and tries to trick an employee into sending money, usually by sending the victim email from fake or compromised email accounts (a "spear phishing" attack). Agari examined thousands of BEC attacks attempted during Q4. 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.

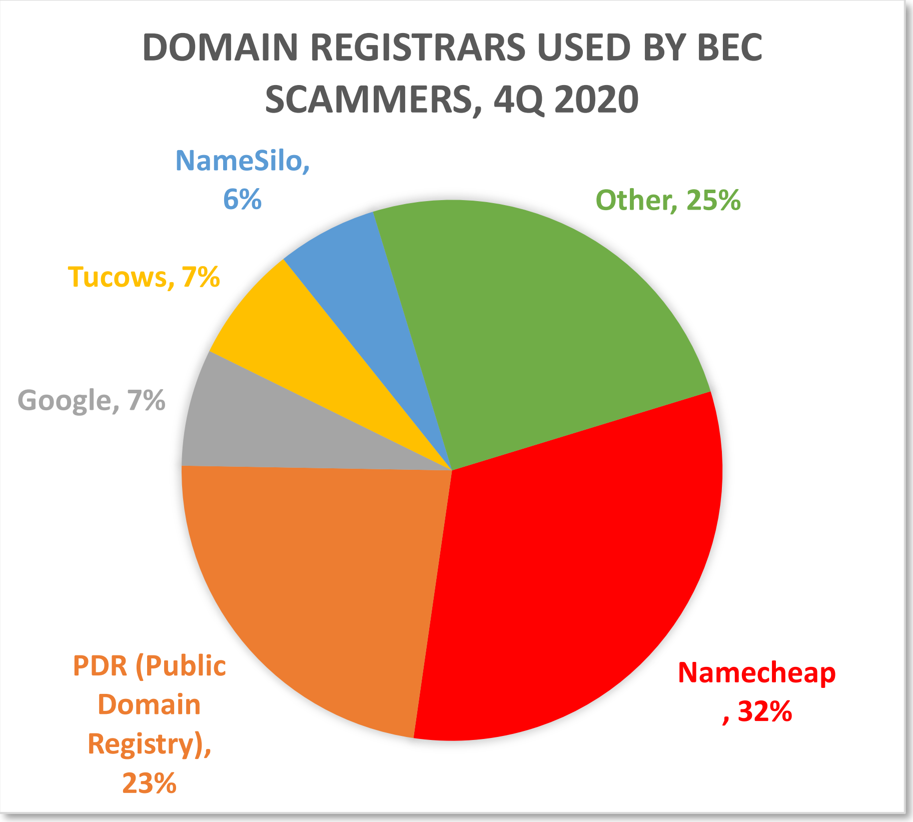
Agari found that in Q4, scammers requested funds in the form of gift cards in 60 percent of BEC attacks, down from 71 percent in Q3. In Q4, BEC attackers requested direct bank transfers in 22 percent of cases, up from 14 percent in Q3. There was also an increase in the number of attacks that requested payroll diversions, which grew to 13 percent in Q4 from 6 percent in Q3 to 13 percent in Q4. The remaining 5 percent of attacks asked for funds through other means.

The average amount requested in wire transfer BEC attacks increased from $48,000 in Q3 to $75,000 in Q4. This increase is primarily due to a resurgence in BEC campaigns from Cosmic Lynx, a sophisticated Russian-based BEC group, and the use of a new "pretext" scam that requested capital-call investment payments from targets. One wire transfer request in the fourth quarter was for a whopping $999,600.

During Q4, the average amount of gift cards requested by BEC attackers was $1,260, about the same as in Q3. Scam attempts around this dollar amount may have a decent chance of success, because they can be approved by multiple people in a medium-to-large company, and the amount is small enough to slip by some companies' financial controls. Gift cards for eBay, Google Play, Amazon, Apple iTunes, and Steam Wallet made up 69.2 percent of the gift card requests in Q4.

"We know that BEC criminals request gift cards that they can convert into online cryptocurrency," said Crane Hassold, Senior Director of Threat Research at Agari. "However, we also observed a notable increase in attacks requesting American Express, Visa, and OneVanilla gift cards, which cannot be converted at cryptocurrency exchanges. It is possible that this shift may indicate cybercriminals are moving to types of gift cards that are more "liquid" and can be used to purchase a variety of different things, rather than can be redeemed at only one location."

Namecheap and Public Domain Registry (PDR) continue be the primary registrars used by cybercriminals to register the domain names they use in BEC attacks. More than half of such maliciously registered domains (55%) used in BEC attacks were registered with one of these two registrars (up from 43% in Q3).

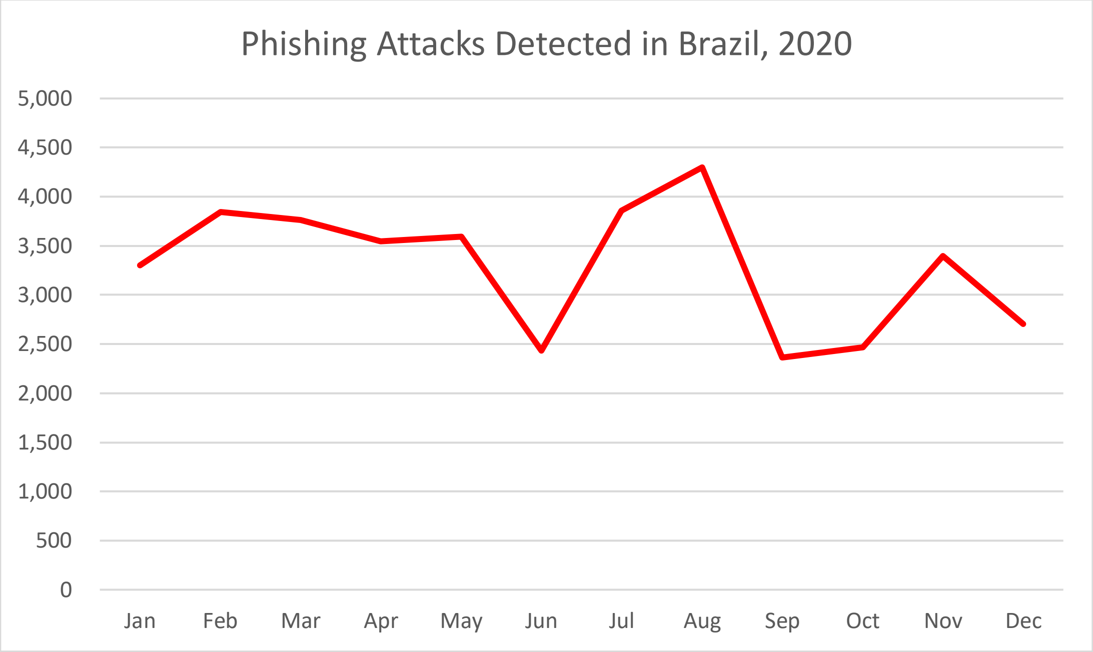


About 75 percent of BEC attacks in Q4 were sent from free webmail accounts, rising steadily from 61 percent in Q1. About 69 percent all BEC attacks sent from free webmail providers used Gmail accounts. Google's Gmail service continues the primary free webmail provider used by BEC actors to send attacks. Nearly two-thirds of BEC attacks using free webmail accounts used Gmail.

Online Criminal Activity in Brazil

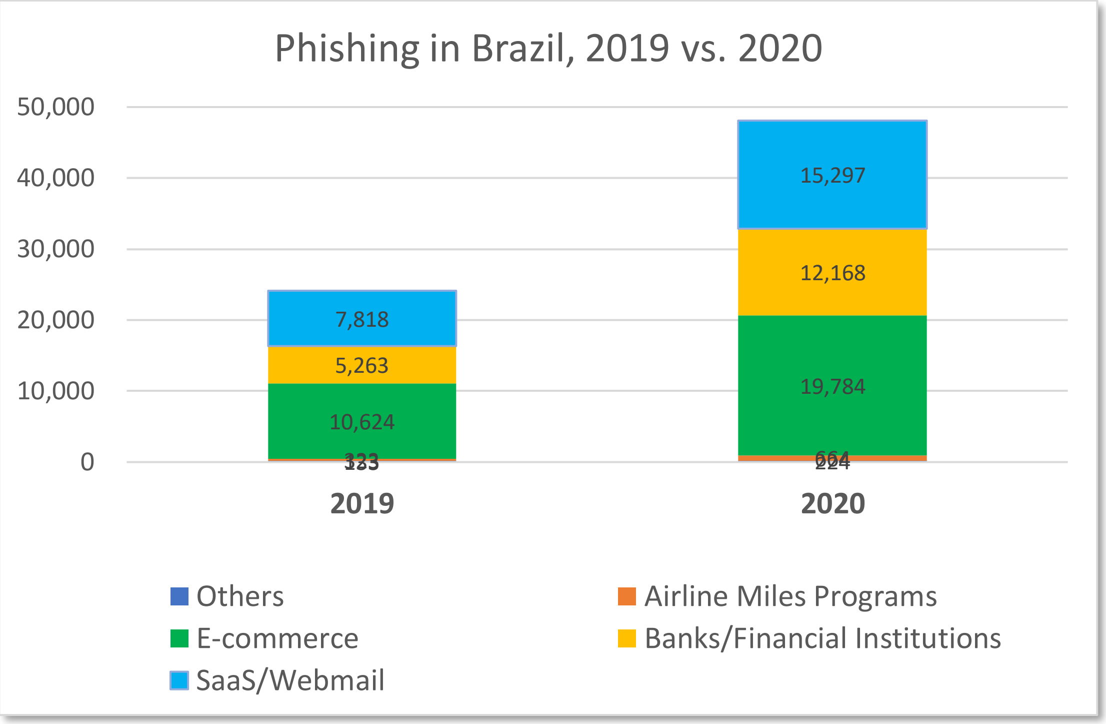
APWG member company Axur is located in Brazil and concentrates on protecting companies and their users in Brazil from Internet-based threats. Axur especially monitors attacks against banks, technology firms, airlines, and online marketplaces located in the country. Axur's data shows how criminals are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

In the final quarter of 2020, Axur's systems identified 8,569 cases of phishing. This data is actually encouraging, as it represents a decline of more than 18 percent compared to the 10,517 recorded in the third quarter of 2020.

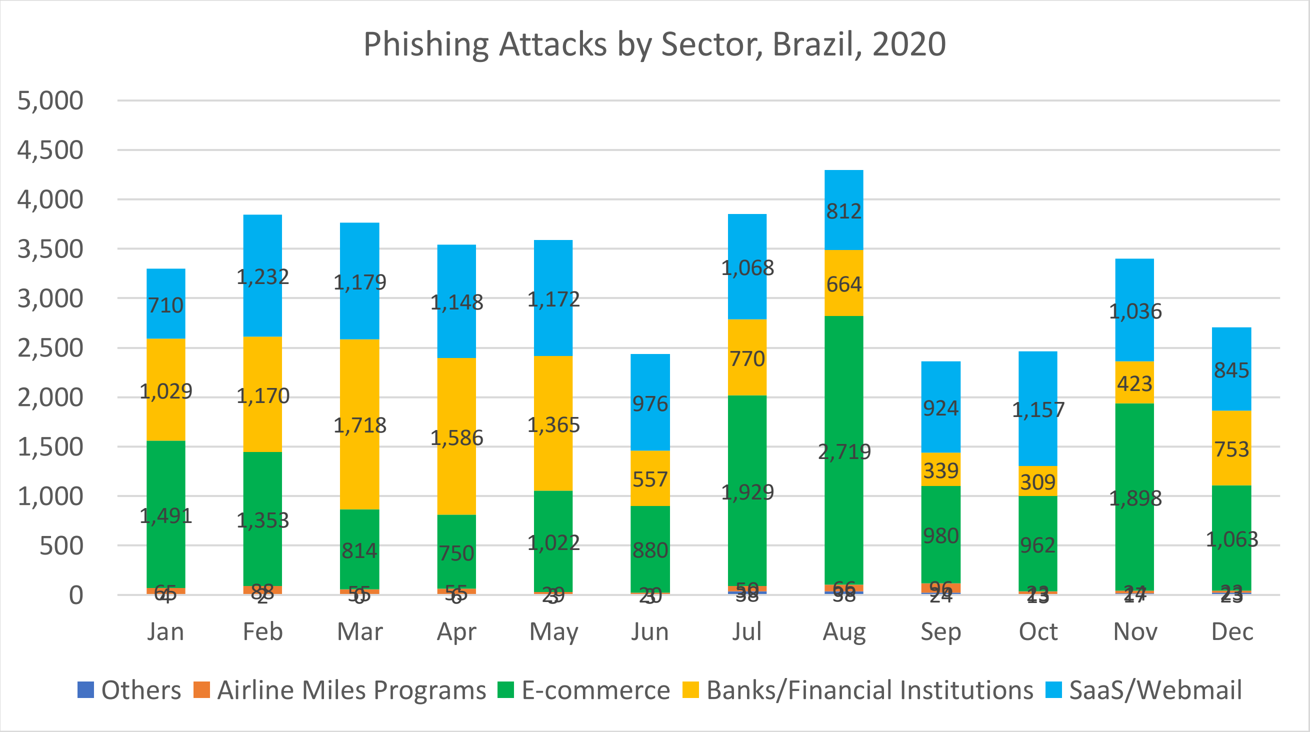


Despite the cumulative drop during the quarter, the Black Friday, shopping holiday on November 27 produced 3,398 phishing attacks, a nearly 17 percent increase over Black Friday 2019.

Unfortunately, Axur found that 2020 still produced much more phishing than occurred in 2019. Axur recorded 24,161 cases of phishing in 2019, and 48,137 in 2020 – a 99 percent increase year over year:



The fourth quarter's most significant increase in phishing in Brazil was in the e-commerce sector, suffering the most attacks, accounting for 45 percent of the quarterly volume of phishing:



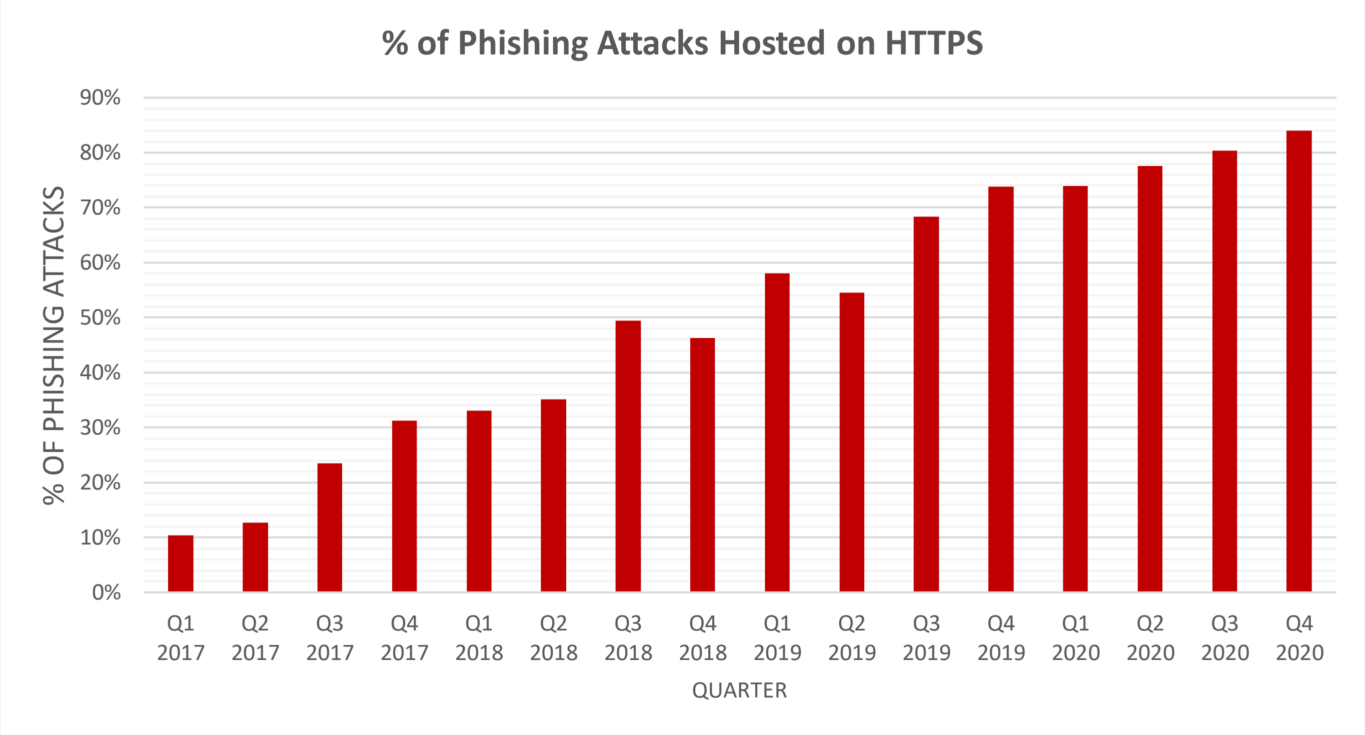
This may be explained by the reduction of sales in physical stores due to the COVID-19 pandemic.

When phishers registered domains names for their attacks, Axur found that 63 percent of those domains did not contain brand names (the names of the target companies), and did not contain a compelling catchword (like "accountupdate" or "sale") designed to fool consumers. This is up from 58 percent in Q2, and 33 percent in 2019. This shows phishers trying to avoid detection, because telltale words in domain names are easier for defenders to find.

In 2019, the cybercriminals' pattern of behavior was to use domain names that contained or imitated the names of real brands. Such attacks represented 67 percent of the samples collected by Axur. In the final quarter of 2019, however, the practice changed. In 2020, most domains used for phishing in Brazil used generic terms in their domain names, such as like "update," "enjoy" and "offers". By the end of 2020, 65 percent of domain names used for phishing in Brazil used a generic term.

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.



John LaCour, CTO of PhishLabs, analyzed the number of phishing sites using TLS certificates in the quarter. According to LaCour, "the number of phishing sites using SSL/TLS increased 3 percent quarter-over-quarter and 10 percent year-over-year to 84 percent. It is virtually the default setting for web sites to use TLS certificates now."

LaCour also analyzed the type of certificates used. In Q4 2020, 89 percent of certificates used in phishing were "Domain Valid" or "DV" certificates. "DV certificates are commonly provided for free, and provide the weakest form of certificate validation, requiring no authentication of the user – only the domain name being used," noted LaCour.

Use of Domain Names for Phishing

APWG member RiskIQ provides ongoing analysis of where phishing is happening in the domain name system. RiskIQ provides digital attack surface management, providing discovery, intelligence, and mitigation of threats associated with an organization's digital presence to protect businesses, brands, and customers. RiskIQ analyzed 6,153 unique phishing URLs that were reported to the APWG's eCrime Exchange in Q4 2020. RiskIQ found that they were hosted on 3,598 unique second-level domains (and 15 more were hosted on unique IP addresses, without domains).

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 about 48 percent of the domain names in the world as of the beginning of Q4, but represented 78 percent of the phishing domains in the sample set. There were 2,797 legacy gTLDs in the sample set. Most of those were in .COM, which had 2,575 domains in the set.
- The new generic top-level domains (nTLDs), such as .XYZ and .ICU, were released after 2011. At the beginning of Q4, the nTLDs represented about 8 percent of the domains in the world, and were about 7 percent of the domains in the sample set (105 domains).
- The country code domains (ccTLDs), such as .UK for the United Kingdom and .BR for Brazil. ccTLDs were about 43 percent of the domains in the world as of the beginning of Q6, but were only 15 percent of the domains in the Q3 sample set (546 domains).

The TLDs that had the most unique second-level domains used for phishing were:

Rank	TLD	Category	# of Unique Domains in Sample Set (4Q 2020)
1	.com	gTLD	2,575
2	.uk	ccTLD	218
3	.info	gTLD	85
4	.net	gTLD	81
5	.live	nTLD	71
6	.link	nTLD	58
7	.org	gTLD	55
8	.xyz	nTLD	36
8	.me	ccTLD	36
10	.br	ccTLD	33

RiskIQ analyzed a subset of the domain names in the sample set (89% of the domains, 3,197 of them) to see how recently they were registered as of January 31, 2021. A total of 2,457 of the domains in the subset were created within Q4 2020 or within the three preceding months), amounting to 77 percent of the subset. "It appears that most of the domain names used for phishing are not compromised infrastructure but are malicious domain name registrations created by the threat actors themselves, consistent with the *Phishing Landscape 2020* report published by Interisle Consulting Group," says Jonathan Matkowsky of RiskIQ's Incident Investigation and Intelligence (i3) team.

RiskIQ has also been tracking the emergence of *LogoKit*. This phishing tool changes the logos and text on a phishing page in real time, to adapt to targeted victims. Once a victim navigates to the phishing URL, LogoKit fetches a company logo from a third-party service. The victim's email address is also auto-filled into the email or username field on the phishing page, to give the targeted victims false confidence that they have previously logged into the site.

With the rapidly expanding attack surface during the pandemic, RiskIQ reported that many college and university students are being targeted with phishing attacks. These phishing campaigns resemble the campaign of a nation-state actor that used similar domain-shadowing and credential-harvesting techniques.

RiskIQ's CEO discussed the unprecedented impact of the SolarWinds breach and lessons to be learned from it. This breach had critical consequences and will be a primary focus of anyone with "security" in their job title for the coming months.

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**