Phishing Activity Trends Report

3rd Quarter 2020

APWG

Unifying the
Global Response
To Cybercrime

Activity July-September 2020

Published 24, November 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 usernames and passwords or misdirect consumers to counterfeit Web sites.

Phishing Attacks Rise in the Third Quarter of 2020

Phishing Activity Trends Summary

- The number of phishing attacks has grown since March 2020. [pp. 3-4]
- The average amount requested during wire transfer BEC attacks was $48,000 in Q3. [p. 6]
- Phishing targeting webmail and Software-as-a-Service (SaaS) endures as the largest phishing category, with 31.4 percent of all attacks. [p. 5]
- Most phishing campaigns are animated by a small number of registrars, domain registries, and hosting providers - providers with wherewithal to mitigate phishing better. [pp. 9-10]
- Eighty percent of phishing sites have SSL encryption enabled to fool victims, more than general SSL deployment – at just 66.8 percent of websites. [p. 8]
- In Brazil, phishers are avoiding using domains names that may attract attention to their schemes. Some 63 percent of domains did not contain names of the target companies, or a compelling catchword designed to fool people. [p. 11]

Table of Contents

Statistical Highlights for 3rd Quarter 2020

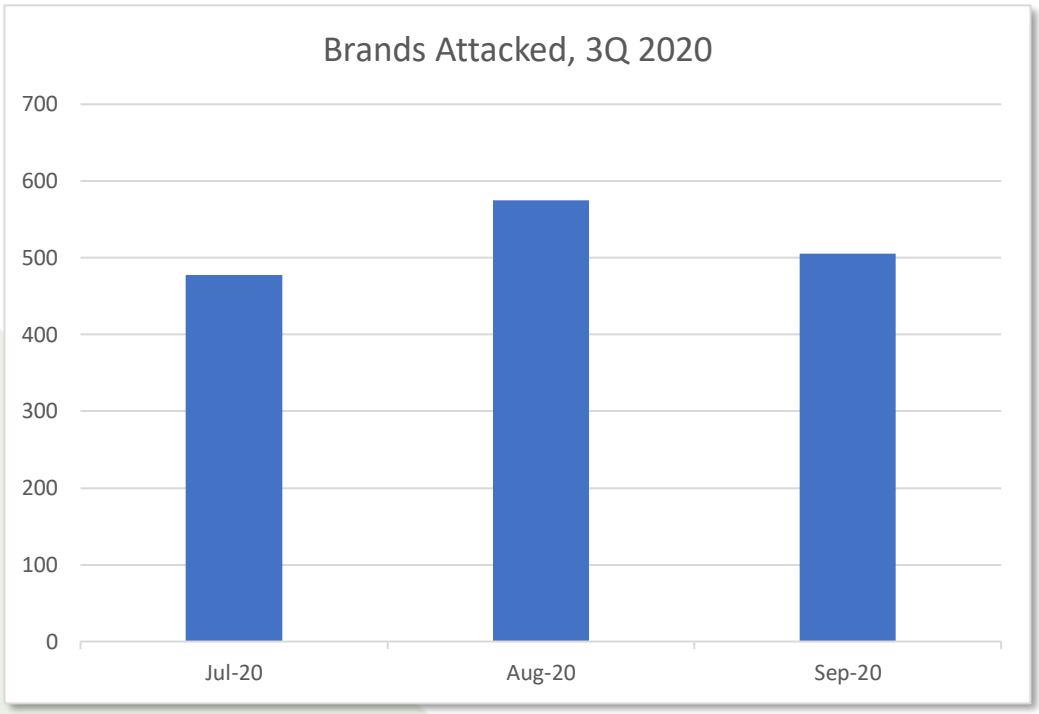
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. With this report, the APWG has refined the methodologies it uses to report phishing. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing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

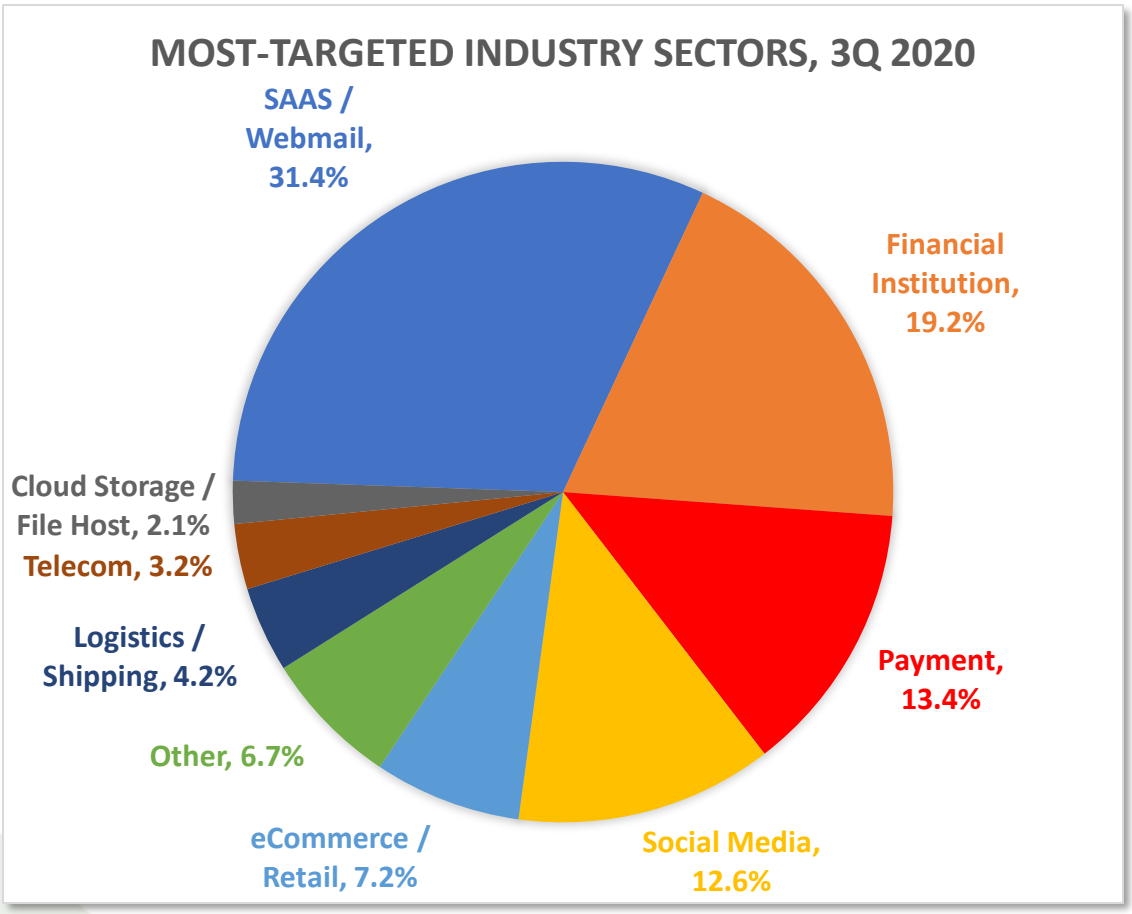
	July	August	September
Number of unique phishing Web sites detected	171,040	201,591	199,133
Unique phishing email subjects	119,181	119,180	128,926
Number of brands targeted by phishing campaigns	478	575	505


Phishing Activity, 3Q 2019 to 3Q 2020
250,000
200,000
150,000
100,000
50,000
0
Aug-19
Sep-19
Oct-19
Nov-19
Dec-19
Jan-20
Feb-20
Mar-20
Apr-20
May-20
Jun-20
Jul-20
Aug-20
Sep-20
Phishing sites
Unique email subjects


Brands Attacked, 3Q 2020
700
600
500
400
300
200
100
0
Jul-20
Aug-20
Sep-20

Most-Targeted Industry Sectors – 3rd Quarter 2020

In the third quarter of 2020, APWG member OpSec Security found that SaaS and webmail sites remained the most frequent targets of phishing, with 31.4 percent of all attacks, down from 35 percent in Q2. Phishing against social media companies crept up from 10.8 to 12.6 percent, noted Stefanie Wood Ellis, Anti-Fraud Product & Marketing Manager at founding APWG member OpSec Online. OpSec Online offers world-class brand protection solutions.



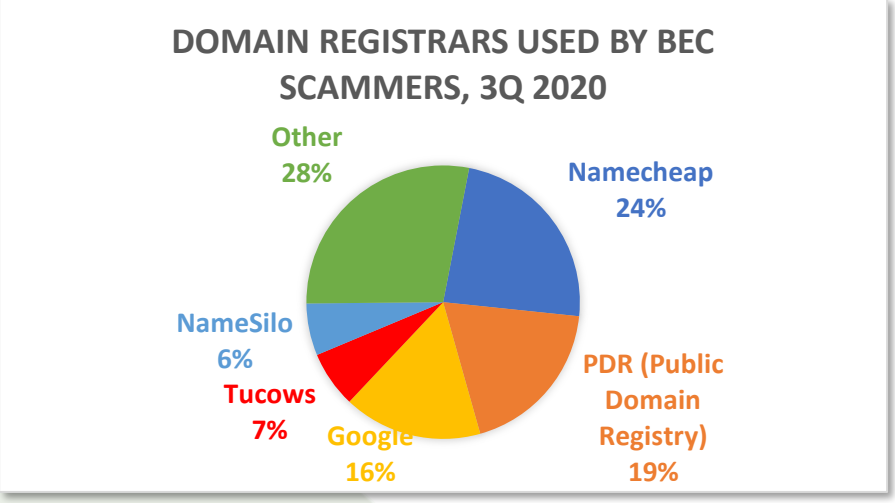
Business e-Mail Compromise (BEC), 3rd Quarter 2020

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 Q3. 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 Q3, scammers requested funds in the form of gift cards in 71 percent of BEC attacks. In 6 percent of attacks they requested payroll diversions, down from 25 percent in Q3 2019. In 14 percent they requested direct bank transfers.

During Q3 2020, the average amount of gift cards requested by BEC attackers was $1,205. 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 72 percent of the gift card requests in Q3. On the other hand, the average amount requested in wire transfer BEC attacks was $48,000 in Q3, down from $80,000 in Q2 and $54,000 in Q1.

About 16.3 percent of BEC attacks involved domain names registered by the scammers, domains that they used to send email to their intended victims. Most of these were registered at just five registrars: Namecheap, Public Domain Registry, Google, Tucows and NameSilo.



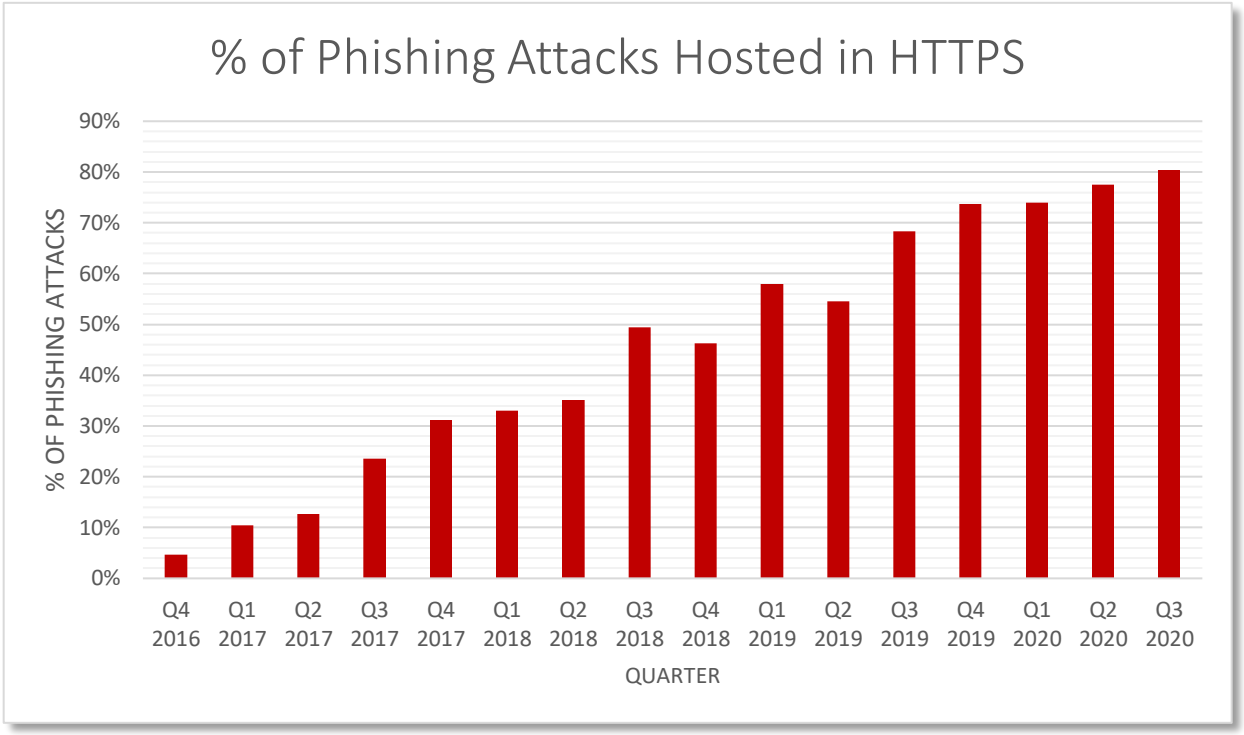
About 81 percent of BEC attacks in Q3 were sent from free webmail accounts, rising from 71 percent in Q2 and 61 percent in Q1. About 69 percent all BEC attacks sent from free webmail providers used Gmail accounts. The next-most-popular webmail provider was Cox, with 7.3 percent.

In a new study, Agari identified BEC criminals operating out of 50 countries. Agari believes that half of these scammers were located in Nigeria, a traditional epicenter of social engineering scams. A quarter of the BEC scammers were based in the United States. During the study Agari collected more than 2,900 mule accounts located in 39 countries, through which scammers intended to receive more than $64 million in stolen funds from BEC victims.

Above: global locations of BEC criminals, summer 2020

How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs tracks numbers of phishing sites 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.



"Now, 80 percent of phishing sites have SSL encryption enabled – which surprisingly is even higher than web sites in general," said John LaCour, CTO of PhishLabs. (According to a Q-Source survey, as of October 2020, only 66.8 percent of web sites used SSL by default.)

"Not surprisingly, most SSL certificates used by phishers were Domain-Validated ("DV"), which is the weakest form of certificate validation," said LaCour. PhishLabs looked at 53,189 certificates used on phishing sites, and found that 91.3 percent were DV), while 8.6 percent were OV (organization Validation) certs, and just 0.1% were Extended Validation (EV).

Another key finding is that in Q3, 40 percent of all SSL certificates used by phishers were issued by a certificate authority that offers free certificates: Let's Encrypt.

Use of Domain Names for Phishing

APWG member RiskIQ provides ongoing analysis of where phishing is happening in the domain name system. RiskIQ analyzed 2,019 confirmed phishing URLs reported to the APWG's eCrime Exchange in Q3 2020. RiskIQ found that they were hosted on 1,274 unique second-level domains (and 15 were hosted on unique IP addresses, without domains). 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.

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 Q3, and represented 68 percent of the phishing domains in the sample set (858 domains). Most of those were in .COM, which had 740 domains in the set.
- The new generic top-level domains (nTLDs), such as .WORK and .ICU, were released after 2011. At the beginning of Q9, the nTLDs represented about 8 percent of the domains in the world, and were about 8 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 Q3, but were only 23 percent of the domains in the Q3 sample set (295 domains). About 8 percent of the ccTLDs in the sample set were in .BR, whereas .BR represented only 3 percent (4.3 million) of ccTLD domains in the world as of the beginning of Q3.

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

Rank	TLD	Category	# of Unique Domains in Sample Set (3Q 2020)
1	.com	gTLD	740
2	.org	gTLD	46
3	.net	gTLD	40
4	xyz	nTLD	30
5	.info	gTLD	28
6	.br	ccTLD	24
6	.in	ccTLD	24
6	.tk	ccTLD	24

RiskIQ also analyzed a sampling of 13,567 confirmed phishing URLs on 1,565 unique domain names used for phishing during Q3 to attack the financial sector, as reported to the applicable hosting provider.

RiskIQ then scanned the same unique domains for analysis on November 2, 2020. Eleven of the unique domains that were reported for takedown during Q3 were still hosting the same phishing pages as of November 2, 2020. "Hosting providers appear to be more proactive compared to the beginning of the year, since almost 1.5 percent of unique phishing domains in Q1 were still active when scanned in Q2, whereas now less than 1 percent of the sample set were still active as of November that were reported in Q3. Also, as compared to Q1 where close to 47 percent of active domains in the sample set still being used for phishing after being reported originated from Endurance, the situation has improved as none of the active domains reported in Q3 that were still hosting phishing in November originated from Endurance," says Jonathan Matkowsky of RiskIQ's Incident Investigation & Intelligence (*i3*) group.

RiskIQ continues to enable the cybersecurity community through a COVID-19 Internet Intelligence Gateway, which includes a free submission and lookup service that uses RiskIQ's web crawling infrastructure to find and analyze malicious URLs related to COVID-themed malware and scams. In Q3, RiskIQ explained how ransomware threat actors are using new infrastructure to capitalize on both the pandemic and the U.S. election. The findings show the traffic funnel—from fake news sites to "subscription traps" comes together for ill-gotten gain through shadowy operations at the expense of unwitting Internet users.

In a separate research project published in October, APWG members at Interisle Consulting Group studied more than 122,000 phishing sites discovered in May through July 2020. The study found that:

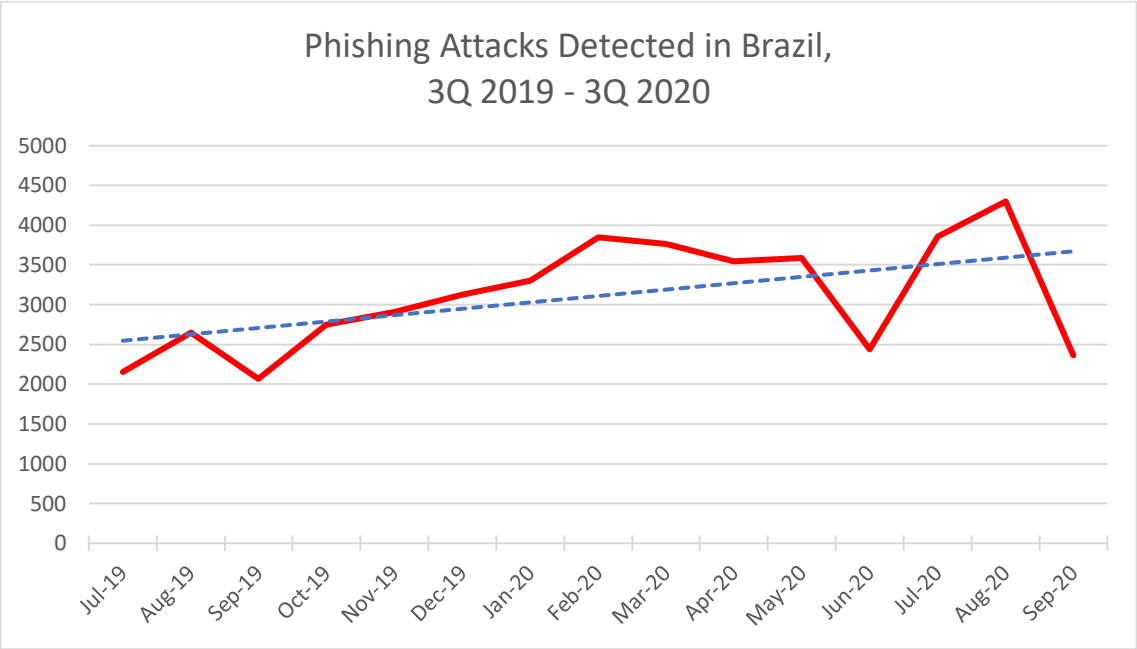
- Most phishing is concentrated at small numbers of domain registrars, domain registries, and hosting providers.
- Phishers themselves registered about 60 percent of the domain names on which phishing occurs.
- About 65 percent of maliciously registered domain names are used for phishing within five days of registration.
- The new top-level domains introduced since 2014 account for 9 percent of all registered domain names, but 18 percent of the domain names used for phishing.

"Domain name registrars and registry operators can prevent and mitigate large amounts of phishing by finding and suspending maliciously registered domains," said Greg Aaron, APWG Senior Research Follow, and one of the co-authors of the Interisle report. "Many anti-abuse programs focus on mitigation — taking steps to stop a phishing attack once it is underway. That's a reactive stance, and by the time a mitigation effort gets underway, the phishing has already taken place. In some places, these reactive programs are allowing constant cycles of new phishing, leading to no overall improvement of Internet safety."

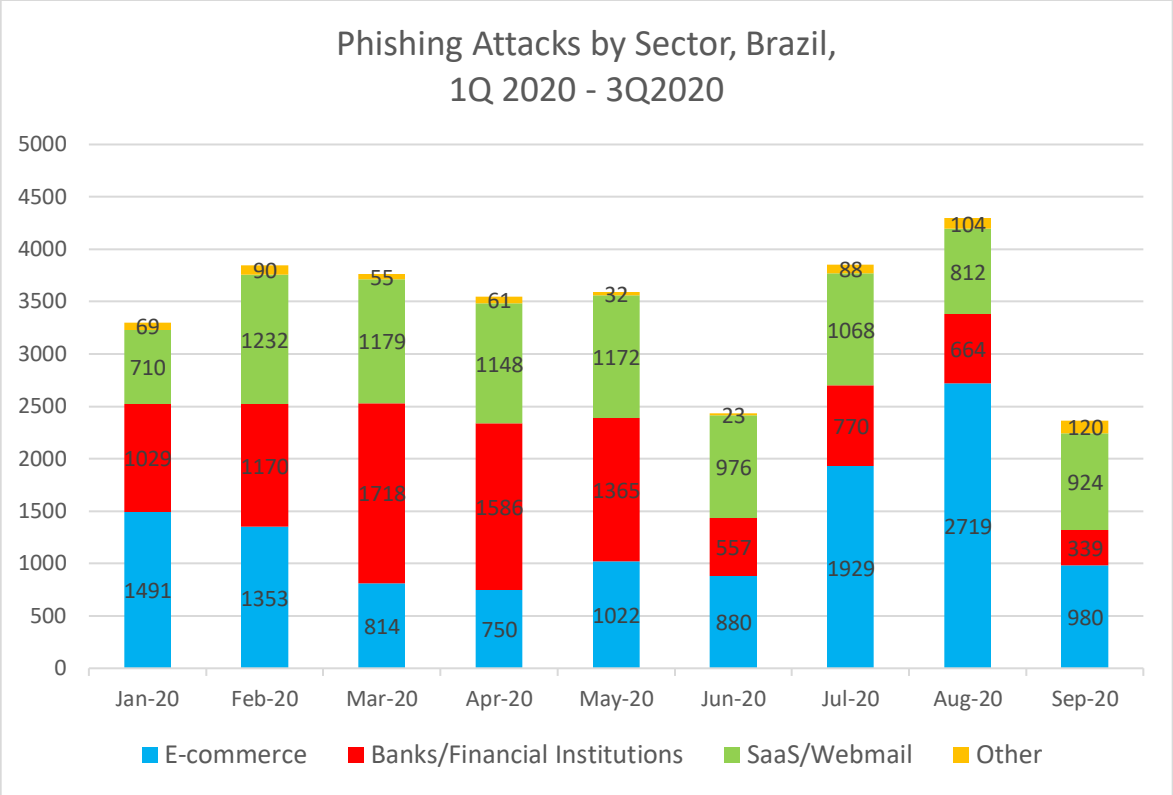
Online Criminal Activity in Brazil

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.

In the third quarter of 2020, Axur observed 10,517 unique phishing cases in Brazil, up from 9,572 in Q2 and 10,910 in Q1. The trend has been upward for the last fifteen months:



The decrease in cases of digital fraud in June 2020 was most evident the banking and financial sector, as shown below. This dip also occurred between May and June of 2019. Even so, the banking and financial sector is still the primary target of phishing attacks in Brazil.



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.

APWG Phishing Activity Trends Report Contributors

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

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

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

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

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

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**