Phishing Activity Trends Report

1st Quarter 2020

plus

COVID-19

coverage

APWG

Unifying the
Global Response
To Cybercrime

Activity January-March 2020

Published 11 May 2020

Phishing Report Scope

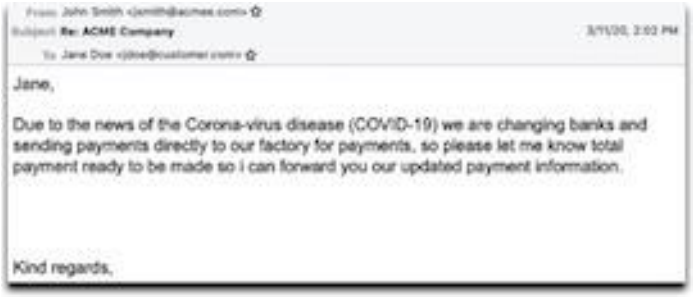
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org.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

Cyber Gangs Leverage COVID-19 to Accelerate Cybercrime Mutation



From: John Smith <jsmith@acmee.com>
Subject: Re: ACME Company 3/11/20, 2:02 PM
To: Jane Doe <jdoe@customer.com>

Jane,

Due to the news of the Corona-virus disease (COVID-19) we are changing banks and sending payments directly to our factory for payments, so please let me know total payment ready to be made so i can forward you our updated payment information.

Kind regards,

Phishing Activity Trends Summary

- Beginning in mid-March, cybercriminals launched a variety of COVID-19 themed phishing and malware attacks against workers, healthcare facilities, and the recently unemployed. [pp. 3-6]
- The number of phishing sites detected in the first quarter of 2020 was 165,772, up from the 162,155 observed in the fourth quarter of 2019. [p. 7]
- Phishing that targeted webmail and Software-as-a-Service (SaaS) users continued to be biggest category of phishing. [p. 8]
- Criminals perpetrating Business Email Compromise (BEC) attacks prefer gift cards to cash out, but one criminal attempted a wire transfer scam for $976,522. [pp. 9-10]
- 75 percent of all phishing sites now use SSL protection. [p. 11]
- Some phishing reported to large hosting providers can stay unmitigated for months. [pp. 12-13]
- Phishing in Brazil was up 24 percent during Q1. Brazil has seen an outsized growth in phishing over the last year. [p. 11]

Cybercrime During the COVID-19 Pandemic

Disasters have always been an opportunity for criminals—they have crafted attacks to take advantage of hurricanes, recessions, and other difficult times, promoting fake charitable giving opportunities and non-existent products. The COVID-19 pandemic of 2020 is unfortunately the latest example. Below the APWG looks at four ways in which cybercriminals have taken advantage of the pandemic to deploy ever more sophisticated scenarios to lure their prey.

Zoom Users Become Targets

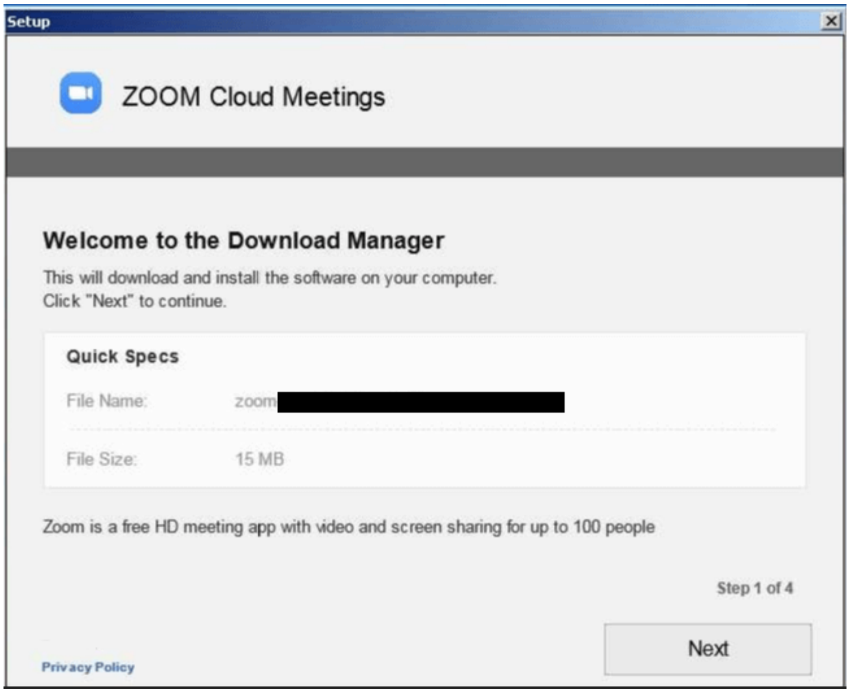
In March 2020, the APWG received just eight reports to its eCrime eXchange of phishing attacks against videoconference service Zoom's brand and its users. But in April, APWG received reports of 1,054 attacks against Zoom.

Some of the attacks were phishing attacks, in which phishers emailed out fake Zoom video-conferencing meeting notifications. These took victims to Web pages set up by the phishers, designed to steal Zoom account usernames and passwords from unwary users. Phishers can use these credentials to log in to corporate video conferencing accounts, and can try the harvested passwords on other sites and services.

Other attacks offered Internet users the opportunity to download the Zoom client. But instead, these delivered malware files. This download was an example:

Zoom is a video-conferencing and chat application, and it was popular with businesses before the pandmeic. But Zoom usage exploded in March 2020 as companies sent their employees to work from home and schools switched to distance learning.

According to Zoom, its user base doubled from 100 million to 200 million daily meeting participants in the short time between December 2019 and the end of March 2020.



ZOOM Cloud Meetings

Welcome to the Download Manager

This will download and install the software on your computer.
Click "Next" to continue.

Quick Specs

File Name: zoom[redacted]

File Size: 15 MB

Zoom is a free HD meeting app with video and screen sharing for up to 100 people

Step 1 of 4

APWG member companies submit phishing reports into the APWG's e-Crime Exchange (eCX), where other members can see the data and use it to protect Internet users around the world. The data shows how phishers have targeted an Internet service that has become essential during the pandemic: Zoom.

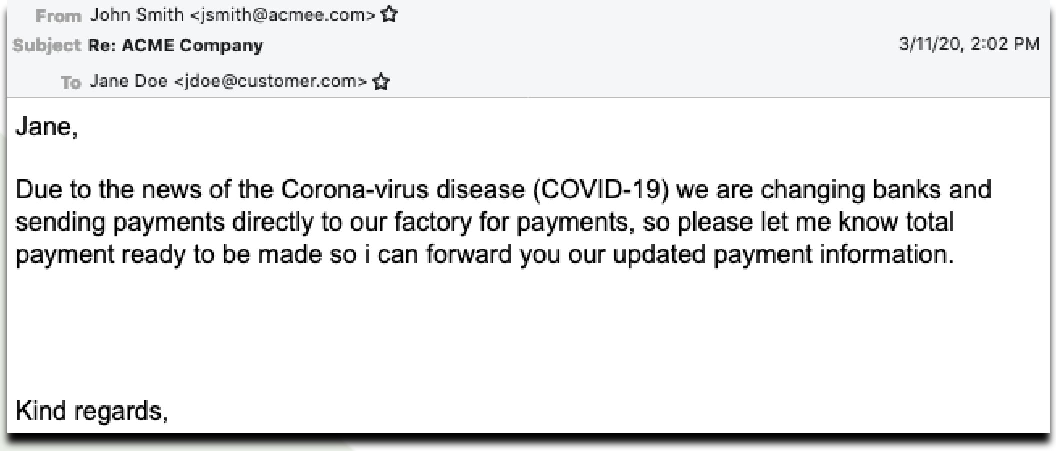
The attacks reported to APWG eCX were not Zoom's fault – as any popular service tends to attract malefactors. (And other video-conferencing providers such as Skype and Cisco Webex were also attacked.) But these and other attack vectors did require Zoom to upgrade its security in a variety of ways to secure a rapidly expanding base of everyday users.

Criminals Use Covid-19 in Business Email Compromise Attacks

APWG member and *Trends* contributor Agari has also been tracking COVID-19 phishing attacks. "Our data indicates that COVID-19 phishing attacks started spiking the week of March 8. That was the same time that COVID-19 started to spike as a topic of general public interest according to Google Trends," said Crane Hassold, Senior Director of Threat Research at Agari.

Agari identified what may have been the first documented use of the pandemic as a lure in a "Business Email Compromise" or BEC attack. In a BEC attack, a scammer targets employees who have access to company finances, usually by sending them email from a fake or compromised email account (a "spear phishing" attack). The scammer impersonates a company employee or other trusted party, and tries to trick the employee into sending money.

On March 11, a criminal group that Agari calls "Ancient Tortoise" reached out to a company and posed as one of the company's real suppliers. The criminal requested that the company pay past-due invoices, and used the coronavirus as a pretext to provide new payment details to the victim. The criminal explained that the outbreak had forced the supplier to change the bank it was using to receive payments. The new account turned out to be in Hong Kong, from which the criminal could retrieve funds via money mules.



From John Smith <jsmith@acmee.com> ☆
Subject Re: ACME Company 3/11/20, 2:02 PM
To Jane Doe <jdoe@customer.com> ☆

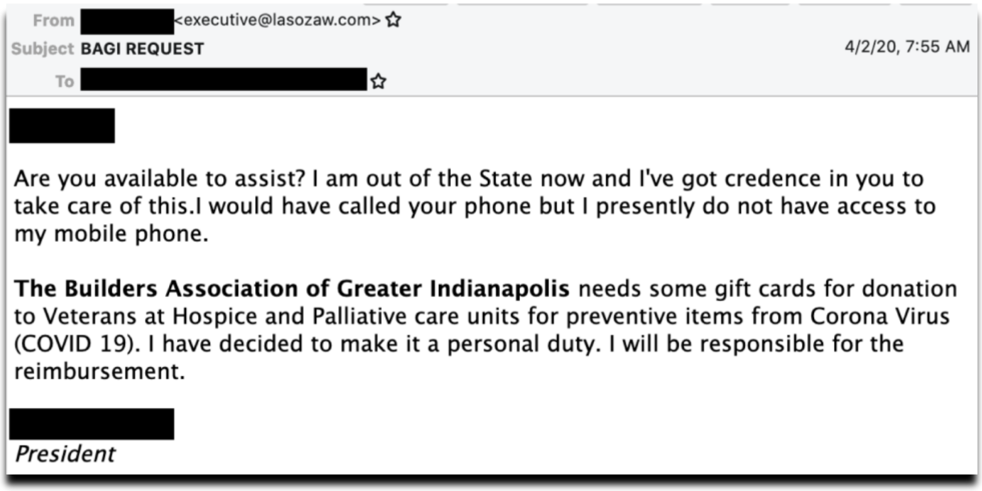
Jane,

Due to the news of the Corona-virus disease (COVID-19) we are changing banks and sending payments directly to our factory for payments, so please let me know total payment ready to be made so i can forward you our updated payment information.

Kind regards,

Above: the attacker used a look-alike domain to spoof the target company.
Note: Names and domains used have been changed above to protect the victim.

In a different attack, a criminal asked a potential victim to send gift cards that would supposedly be given to sick miltary veterans:



From [redacted] <executive@lasozaw.com> ☆
Subject **BAGI REQUEST**
4/2/20, 7:55 AM
To [redacted] ☆

[redacted]

Are you available to assist? I am out of the State now and I've got credence in you to take care of this.I would have called your phone but I presently do not have access to my mobile phone.

The Builders Association of Greater Indianapolis needs some gift cards for donation to Veterans at Hospice and Palliative care units for preventive items from Corona Virus (COVID 19). I have decided to make it a personal duty. I will be responsible for the reimbursement.

[redacted]
President

This is yet another example of how cybercriminals exploit global trends for their own ends.

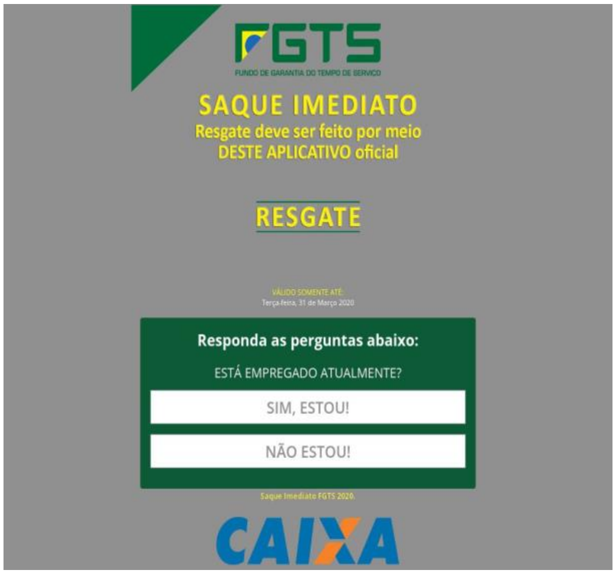
Criminals Attack Healthcare Facilities During the Pandemic

On March 26, i3 reported that ransomware attacks on healthcare facilities were up 35 percent, versus similar attacks from 2016 through 2019. Healthcare providers must prevent disruptions to patient care, and criminals saw them as targets that would likely pay ransom. RiskIQ found that 70 percent of the healthcare attacks it analyzed were directed at healthcare facilities with fewer than 500 employees. It appears that attackers targeted smaller direct-patient care facilities because they might have smaller security budgets.

On March 9, APWG member and *Trends* contributor RiskIQ put its Incident Investigation & Intelligence (*i*3) analyst team on the COVID-19 problem. The i3 team began collecting disparate kinds of data into comprehensive daily updates to help raise the situational awareness of security teams around the world. In mid-March, i3 predicted that threat actors would begin using ransomware against companies and organization in healthcare and related fields. By March 19, cybercriminals were spreading malware by adding text from COVID-19 news stories in attempts to bypass security software that uses artificial intelligence and machine learning to detect malware.

COVID-19 Fraud: A Worldwide Problem

Cybercriminals have adopted a variety of tactics during the pandemic, some of which vary by region. In Brazil, APWG member and *Trends* contributor Axur found a fake site disseminated via the WhatsApp instant messaging application. It created a network of "shares," resulting in a massive dissemination of the fake ads on mobile devices. The ad claimed to be an official registration for the immediate withdrawal of money from the Brazilian government's Severance Indemnity Fund *(Fundo de Garantia do Tempo de Serviço—FGTS)*. This is the government unemployment fund, of interest to workers laid off during the pandemic. This fraud used the generic name: *auxiliocorona.online*.



SAQUE IMEDIATO
Resgate deve ser feito por meio
DESTE APLICATIVO oficial

VÁLIDO SOMENTE ATÉ:
Terça-feira, 31 de Março 2020

Responda as perguntas abaixo:

ESTÁ EMPREGADO ATUALMENTE?

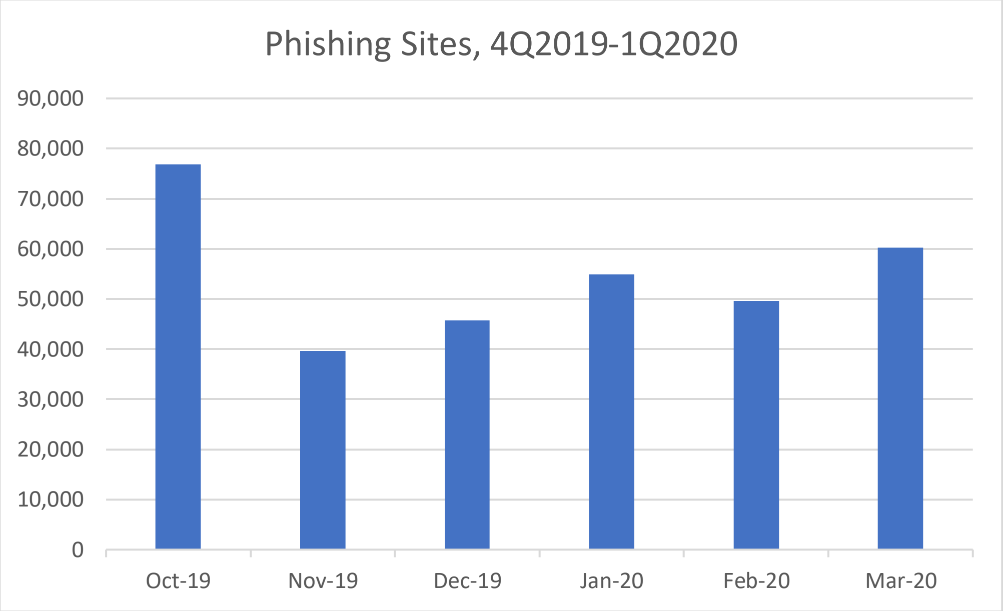
Saque Imediato FGTS 2020.

Statistical Highlights for 1st Quarter 2020

	January	February	March
Number of unique phishing Web sites detected	54,926	49,560	60,286
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	52,407	43,270	44,008
Number of brands targeted by phishing campaigns	374	331	344

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.)

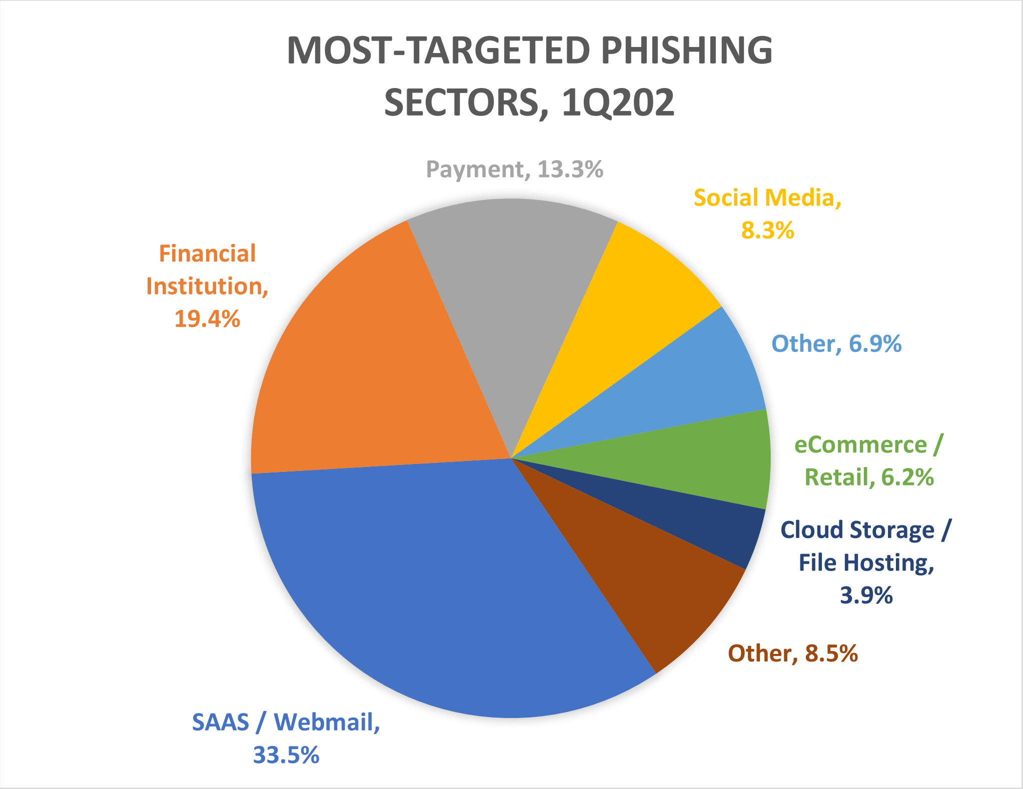
The total number of phishing sites detected in the first quarter of 2020 was 165,772. That was up slightly from the 162,155 in Q4 2019. The trend since November 2019 has been headed upward:



APWG also tracks the number of unique phishing reports (email campaigns) it receives from consumers and the general public through the reportphishing@apwg.org service. 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 1Q2020 was 139,685. This was up from 132,553 in 4Q2020, 122,359 in 3Q2020 and 112,163 in 2Q2020. These were phishing emails submitted to APWG, and does not count phishing URLs reported by APWG members directly into APWG's eCrime Exchange.

Most-Targeted Industry Sectors – 1st Quarter 2020

In the first quarter of 2020, APWG member OpSec Security found that SaaS and webmail sites remained the biggest targets of phishing, with 34 percent of all attacks. "In February we detected a dip in attacks against the payment sector," noted Stefanie Wood Ellis, Anti-Fraud Product & Marketing Manager at OpSec Online. "That dropped Payment-targeted phish to only 13 percent of all targets, when in the preceding four quarters the Payment sector had been 20 percent of all phishing." OpSec (a founding APWG member formerly known as MarkMonitor) offers world-class brand protection solutions.

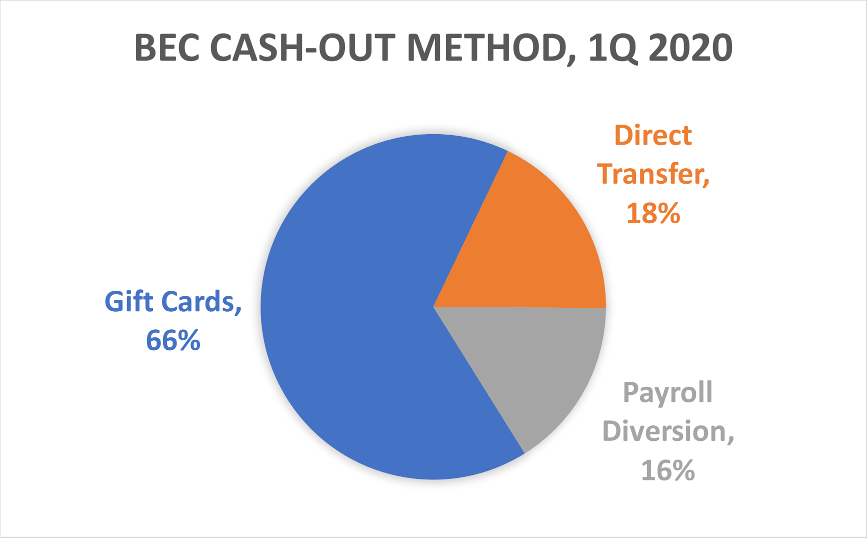


Business e-Mail Compromise (BEC), 1st Quarter 2020

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 it observed during Q1. 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 scammers requested funds in the form of gift cards in 66 percent of BEC attacks, up from 56 percent during the third quarter of 2019. About 16 percent of attacks requested payroll diversions, down from 25 percent in Q3. Some 18 percent requested direct bank transfers.



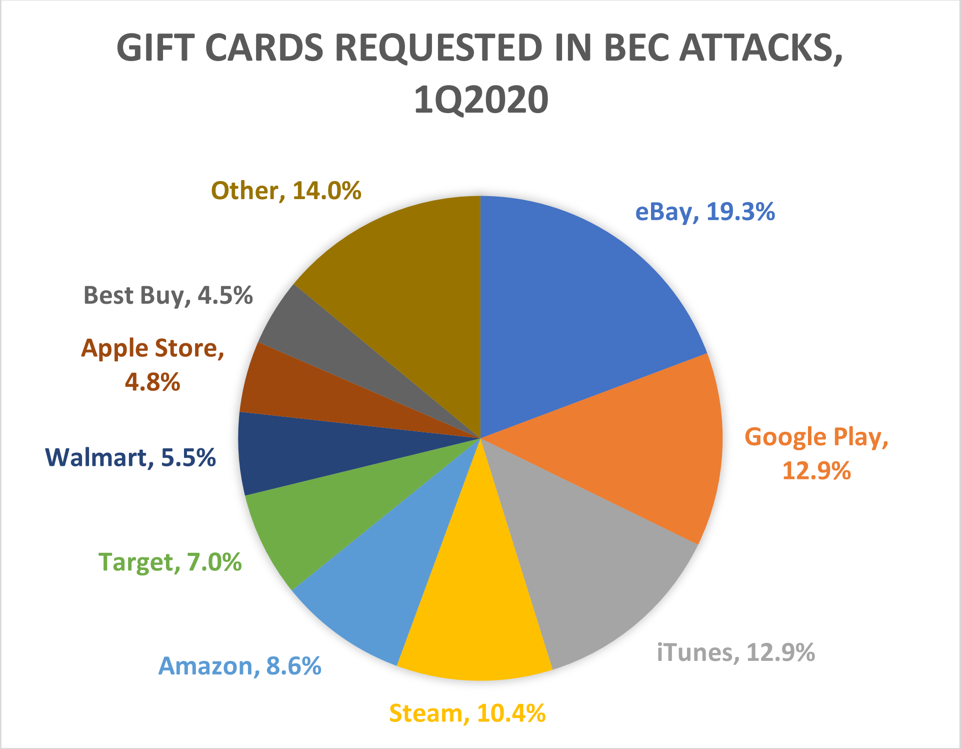
The amount of money that an attacker can make by getting gift cards is significantly less than he can get with a wire transfer. During the first quarter of 2020, the average amount of gift cards requested by a BEC attacker was $1,000. Scam attempts around this dollar amount may have a decent chance of 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.

On the other hand, BEC attacks that ask for wire transfers are after much larger amounts. The average BEC wire transfer attempt requested in Q1 was for over $54,000:

	Average	Median	Min	Max
Wire transfer requests	$54,006	$29,726	$800	$976,522
Gift card requests	$1,453	$1,000	$100	$15,000

Agari watched one criminal attempt a big score – a wire transfer request for $976,522. This was much larger than the biggest request that Agari observed in Q4, which was for $680,456.

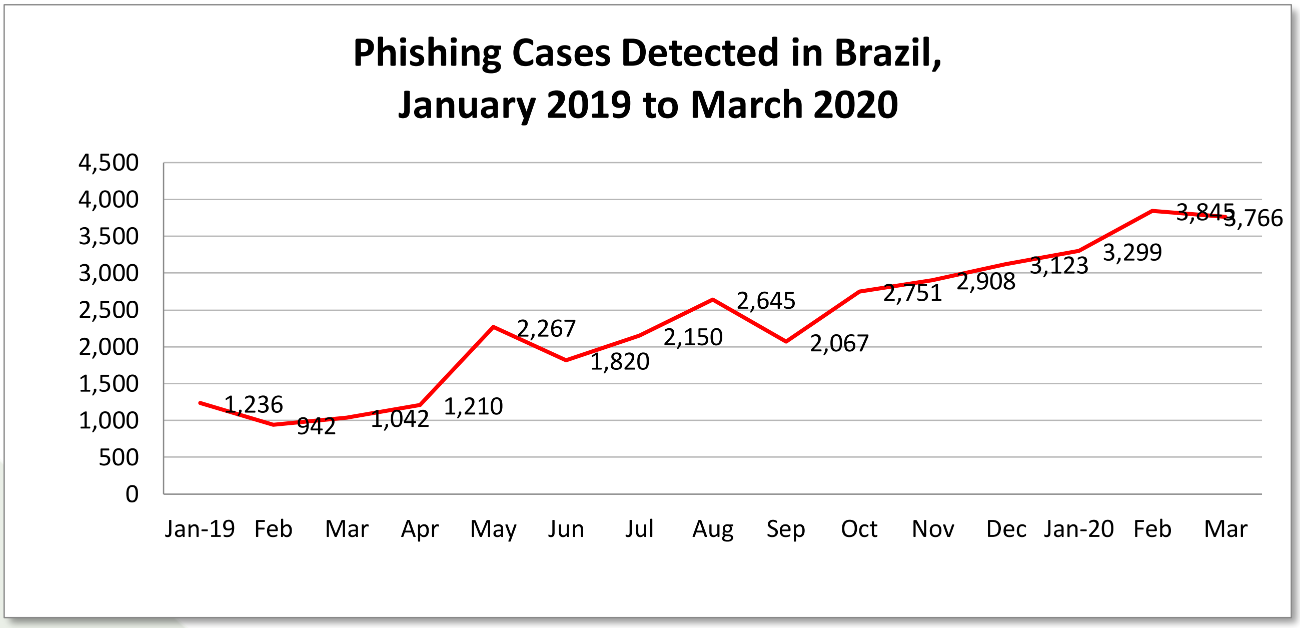
According to Crane Hassold, Agari's Senior Director of Threat Research, "In the first quarter of 2020, eBay overtook Google Play as the most popular type of gift card requested by BEC scammers. That signals a pretty significant shift since Google Play had been the predominant type of gift card requested in BEC attacks for more than a year." The increase could be due to the fact that eBay sells physical goods – as do other popular BEC card requests, such as Walmart, Target, Amazon, and Best Buy. It may indicate that scammers are looking to launder money by using the cards to buy physical goods that they can then sell.



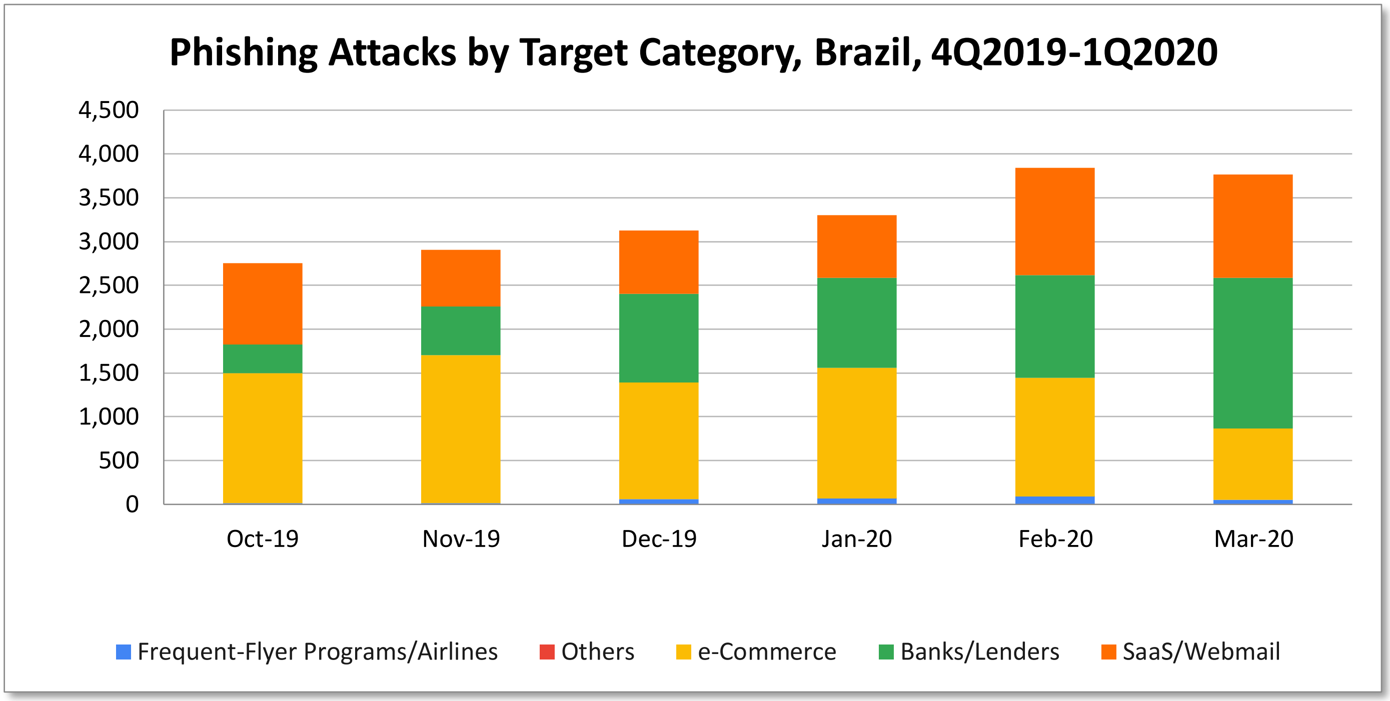
Online Criminal Activity in Brazil

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.

Between January 1 and March 31, 2020, Axur observed 10,910 cases of phishing. Specifically, these were attacks against Brazilian brands or against foreign services that are available in Portuguese in Brazil. That was an increase of 24 percent compared to the fourth quarter of 2019, when Axur detected 8,782 cases. And the 1Q 2020 numbers were a notable increase of 239 percent from the same period in 2019, when Axur observed 3,220 cases. In other parts of the world, phishing did not leap so dramatically during the same time period.


Phishing Cases Detected in Brazil, January 2019 to March 2020

From the last quarter of 2019 through the first quarter of 2020, Axur saw attacks increase against banks. For the first time in Brazil, banks and financial institutions were the sector most affected by phishing, accounting for some 40 percent of the quarterly total:



Attacks against e-commerce sites decreased, but still accounted for a third of attacks in 1Q 2020. Attacks against e-commerce sites are more prevalent in Brazil than elsewhere.

Use of Domain Names and Hosting for Phishing

APWG member RiskIQ provides ongoing analysis of where phishing is happening in the domain name system. RiskIQ analyzed 1,766 confirmed phishing URLs reported to APWG in Q1 2020. RiskIQ found that they were hosted on 983 unique second-level domains (and 19 were hosted on unique IP addresses, without 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 about 48 percent of the domain names in the world as of the beginning of 2020, and represented 65 percent of the phishing domains in the sample set. There were 640 legacy gTLDs in the sample set. Most of those were in .COM, which had 521 domains in the set.

- The new generic top-level domains (nTLDs), such as .WORK and .ICU, were released after 2011. At the beginning of Q1, the nTLDs represented about 8 percent of the domains in the world, and were about 8 percent of the domains in the sample set. There were 75 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 44% of the domains in the world as of the beginning of Q1, but were only 27 percent of the domains in the Q1 sample set. The .UK ccTLD maintains registration for 8 percent (13 million) of ccTLDs in the world, but represented 15 percent of the ccTLD domains in the phishing set. The chart below shows the TLDs that had the most unique second-level domains used for phishing.

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 (1Q 2020)
1	.com	gTLD	521
2	.net	gTLD	43
3	.org	gTLD	41
4	.uk	ccTLD	39
5	.info	ccTLD	29
5	.br	gTLD	29
6	.ru	ccTLD	15
7	.au	ccTLD	11
7	.live	nTLD	11
7	.me	ccTLD	11
8	.kr	ccTLD	10
9	.in	ccTLD	9
9	.xyz	nTLD	9
10	.cf	ccTLD	7
10	.ga	ccTLD	7

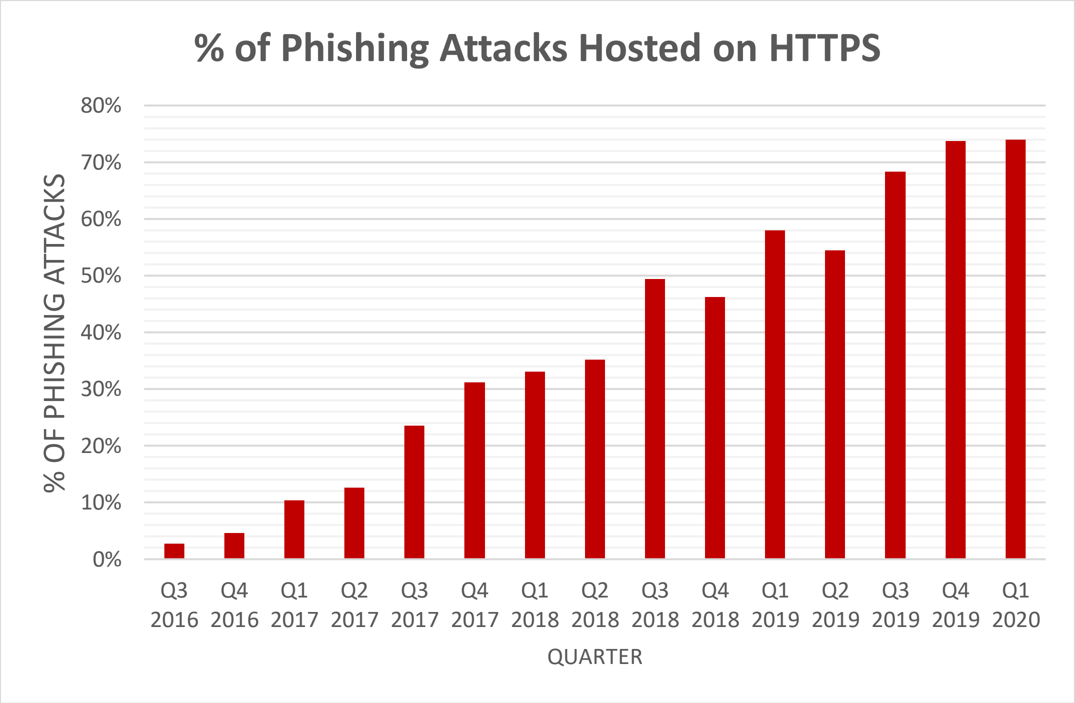
RiskIQ also analyzed a set of 3,041 unique domain names used for phishing during the period from January 1 through March 31; all hosted phishing that attacked companies in the financial sector. RiskIQ then scanned the same unique domains for analysis on May 3, 2020, more than a month after the last phishing report. As of May 3, 2020, 43 of the unique domains were still hosting phishing pages; all 43 had been reported by RiskIQ to the responsible hosting providers during Q1.

Some of these phishing attacks were re-activated, but most of the 43 had never been taken down by the hosting providers. Of the 43 domains still being used for phishing, almost half here hosted by Unified

Layer (AS46606), a hosting unit of Endurance International Group, one of the Internet's largest hosting providers. "The parent company, Endurance, was ultimately responsive to the concern, but we continue to monitor the situation," says Jonathan Matkowsky of RiskIQ's Incident Investigation & Intelligence (*i3*) group.

How Phishers Use Encryption to Fool Victims

APWG *Trends* 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 Q1 2020, a new high of 74 percent of sites used for phishing were protected with SSL. "The majority of phishing web sites continue to use SSL/TLS," said John LaCour, Founder and CTO, PhishLabs. "We hope that users have learned that SSL doesn't mean a site is legitimate. Virtually every web site—good and bad—now uses SSL." Phishers often mount phishing pages within legitimate sites that use SSL.

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**