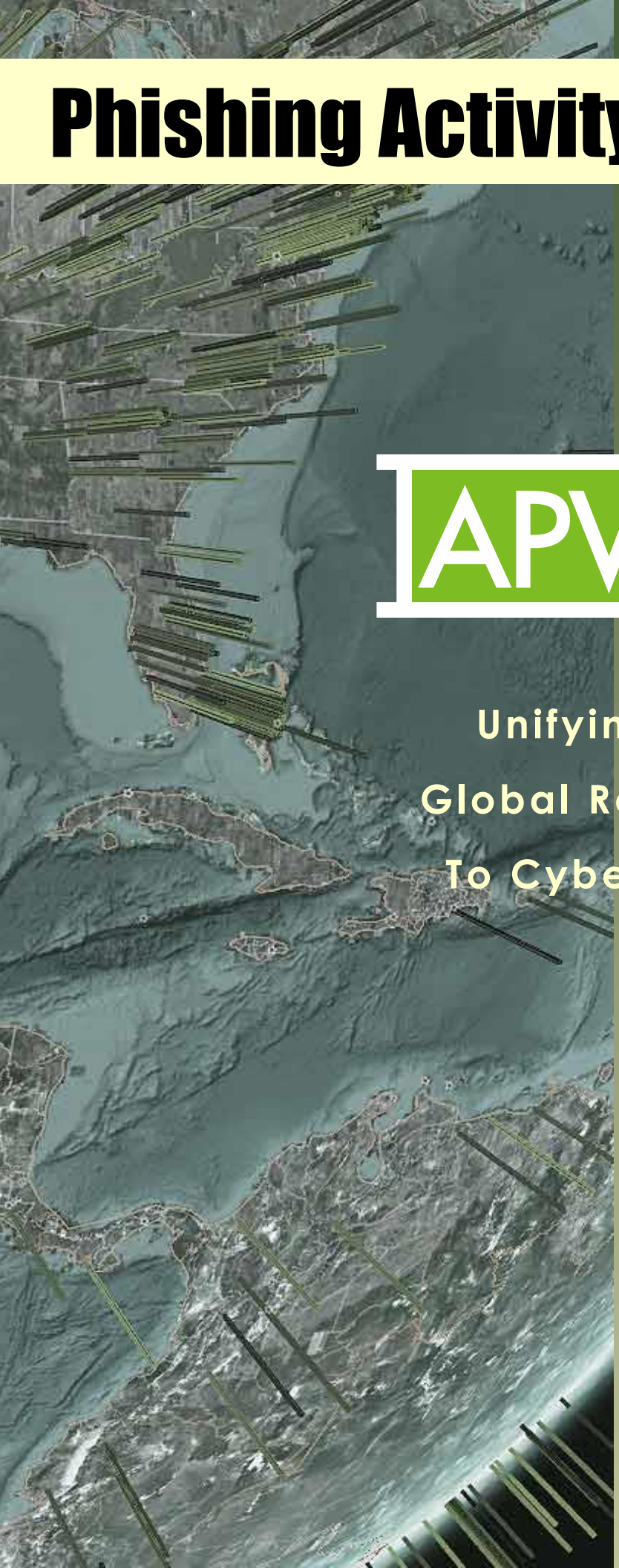
Phishing Activity Trends Report



1st Quarter 2021

APWG

Unifying the
Global Response
To Cybercrime

Activity January-March 2021

Published 8 June 2021

Phishing Report Scope

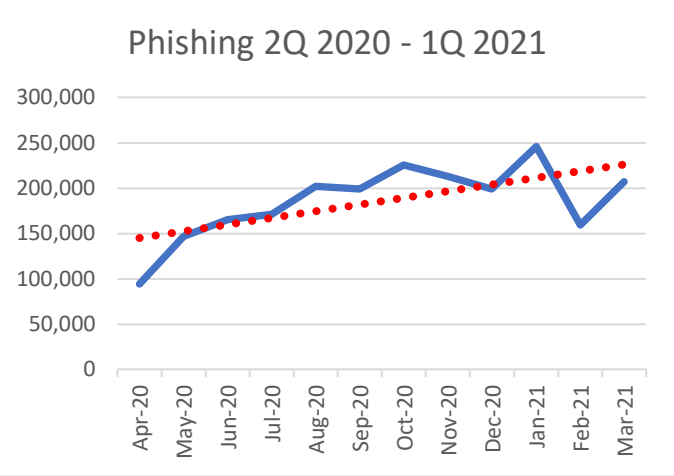
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. 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 Remains at Historic Highs; January 2021 Smashes All Records



Phishing Activity Trends Summary

- After doubling in 2020, the amount of phishing declined during the first quarter of 2021. However, January 2021 was a high in the APWG's records, with an unprecendented 245,771 attacks in one month. [pp. 3-4]
- Business e-mail compromise scams are becoming more costly with average wire transfer requests in BEC attacks increasing to $85,000, up from $48,000 in Q3 2020. [pp. 6-7]
- The financial institution, webmail, and social media sectors were the most frequently victimized by phishing in this quarter. [p. 5]
- The use of HTTPS encryption on phishing sites stalled at 83 percent, after rising steadily for years. [p. 8]
- Phishers continue to use certain domain name registrars to obtain domains for their schemes. [pp. 7, 10-11]

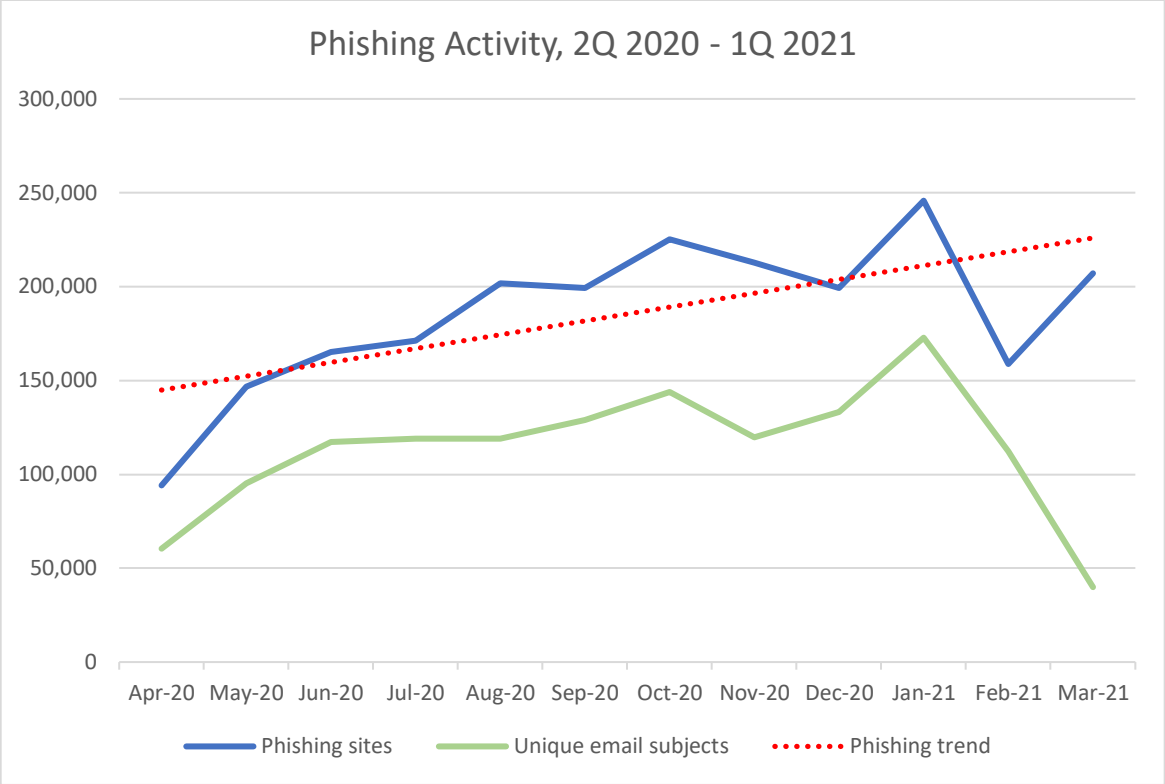
Statistical Highlights for the 1st Quarter 2021

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.
- **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 can be 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.

	January	February	March
Number of unique phishing Web sites detected	245,771	158,898	207,208
Unique phishing email subjects	172,793	112,369	39,918
Number of brands targeted by phishing campaigns	430	407	465

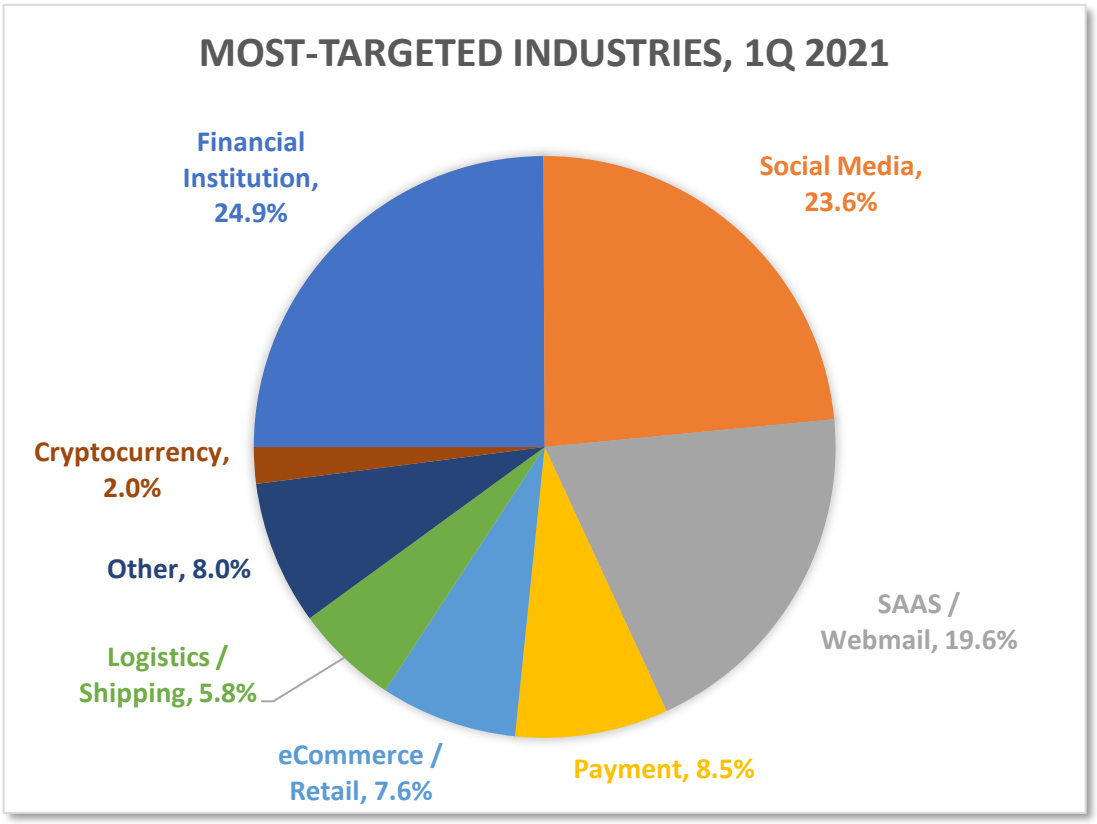


The number of phishing attacks observed by the APWG and its contributing members doubled over the course of 2020. Attacks then peaked in January 2021, with an all-time high of 245,771 new phishing sites appearing in that month alone. The number of attacks then declined in February and March, offering some hope for online consumers. Still, March suffered more than 200,00 attacks, and was the fourth-worst month in APWG's reporting history.

The number of Unique Subjects dipped in March 2021, since the phishing emails reported to APWG that month had an unusual number of duplicative subject lines. The number of brands attacked each month in Q1 also dipped from Q4, when more than 500 brands were attacked every month.

Most-Targeted Industry Sectors – 1st Quarter 2021

In the first quarter of 2021, APWG founding member OpSec Security found that phishing attacks against financial institutions were the still most prevalent, moving from 22.5 percent of all attacks in 4Q2020 to 24.9 percent in 1Q 2021. Attacks against social media sites moved into second place, up from 11.8 percent of all attacks in 4Q 2020 to 23.6 percent in 1Q 2021. Phishing against cryptocurrency targets broke 2 per for the first time. OpSec Online offers world-class brand protection solutions.



Vishing is phishing advertised via voice messages, and *smishing* is phishing advertised in SMS messages. "Vishing and smishing incidents are on the rise across organizations in a variety of industries, but the reported volume growth doesn't yet rival traditional phishing," noted Stefanie Wood Ellis, Senior Product Manager at founding APWG member OpSec Online. "Vishing and smishing volume is likely larger than reported, as both methods rely on the consumers to report the incidents." In contrast, phishing advertised via email can be more easily caught by security providers, such as anti-spam and anti-phishing companies.

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 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 the average amount requested in wire transfer BEC attacks increased 14 percent from $75,000 in Q4 2020 to $85,000 in Q1 2021. This increase is primarily attributed to a continued resurgence in BEC campaigns from Cosmic Lynx, a sophisticated Russian-based BEC group, as well as mergers-and-acquisitions themed campaigns that have requested larger payments from BEC targets.

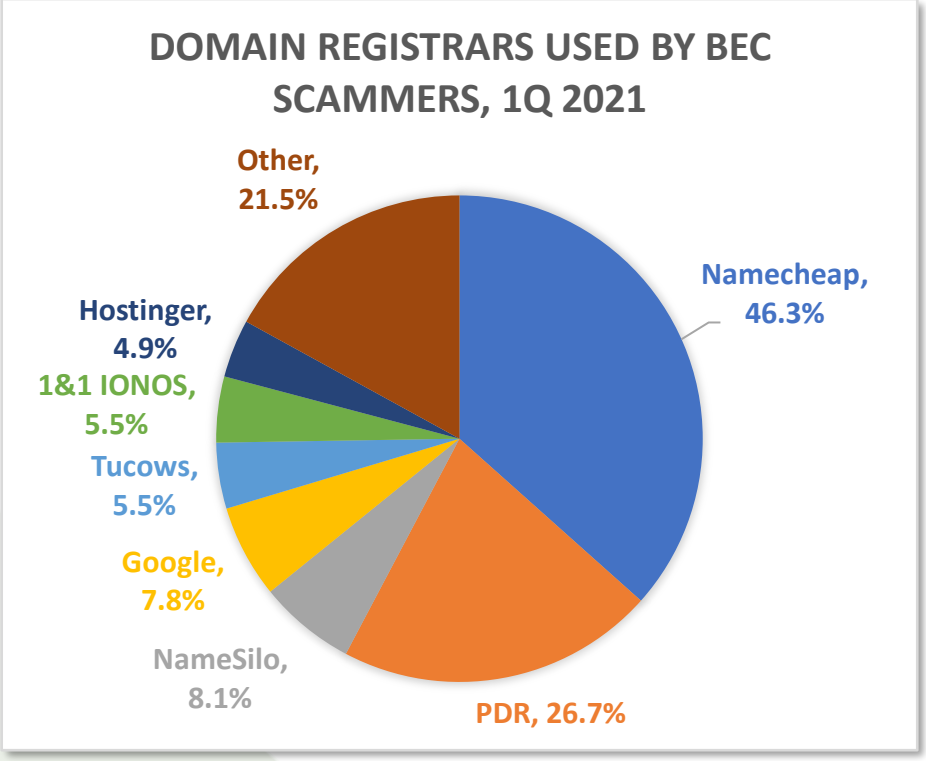
Agari found also that in Q1 2021, scammers requested funds in the form of gift cards in 54 percent of BEC attacks, down from 60 percent in Q 4 2020 and 71 percent in Q3 2020. The other 46 percent of requests involved bank transfer, payroll diversion, and "financial aging requests." In a financial aging request, the scammer impersonates an executive and requests that someone in the target company send him a report that contain details about outstanding payments owed by the company's customers, and the accompanying customer contact details. While aging report BEC attacks have been around for more than a year, their volume was minimal until Q1 2021, when more than 10 percent of all BEC attacks involved aging report requests.

"While a majority of aging report requests have previously been attributed to a group we call Ancient Tortoise, the growing number of BEC attacks coming from actors using markedly different tactics indicates that these attacks are becoming more widely adopted in the BEC ecosystem," said Crane Hassold, Senior Director of Threat Research at Agari. "Aging report BEC attacks compromise information from one organization in order to target that organization's customers, similar to Vendor Email Compromise (VEC) attacks. Unlike VEC attacks, however, they do not involve the actual compromise of an employee's email account. Instead, the attacker impersonates a company's executive and simply requests a copy of a recent aging report from their accounting department, which contains a list of all unpaid customer accounts, as well as the names and email addresses of the primary customer contacts. Once an attacker has received an aging report from a victim, he will then target the victim's customers requesting that they pay their overdue invoices to a new bank account controlled by the scammer."

eBay, Google Play, iTunes, and Amazon remained the most commonly-requested branded gift cards in BEC attacks; however, Agari observed a notable increase in attacks requesting American Express, Visa, and OneVanilla gift cards, a trend that started in late 2020.

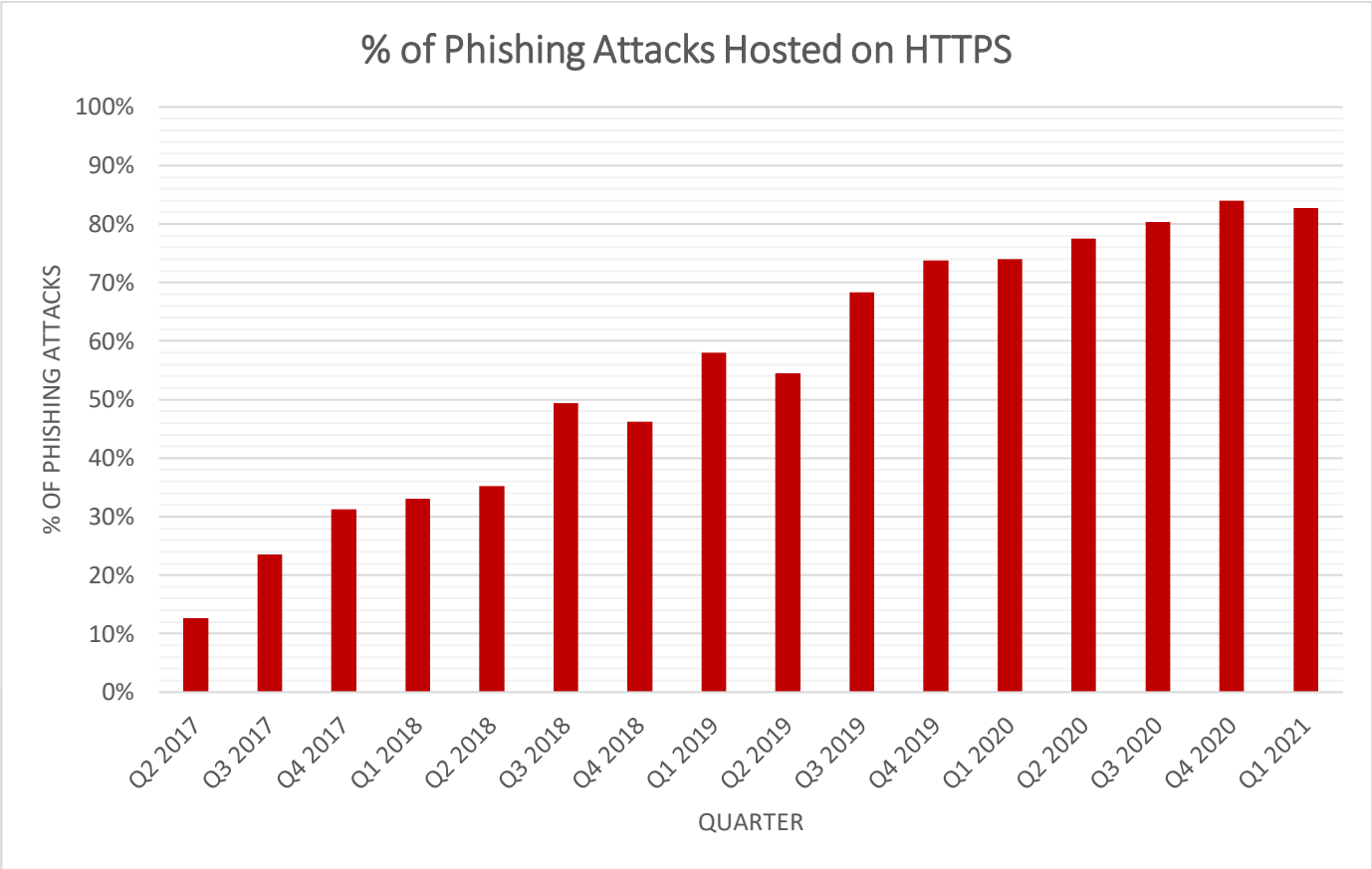
"Twenty percent of all gift card BEC attacks requested one of these three types of cards," noted Hassold. "While we know BEC actors request gift cards because they can exchange then for cryptocurrency at cryptocurrency exchanges, it is possible that this shift may indicate cybercriminals are moving to types of gift cards that are more versatile and can be used to purchase a variety of different things. Additionally, these cards can also be loaded into other accounts, like CashApp, which has emerged as a primary application BEC actors use to move money."

Namecheap and Public Domain Registry (PDR) continue be the primary registrars used by cybercriminals to register the domain names they use in BEC attacks. Agari noted that nearly three-quarters of maliciously registered domains — 73 percent — used in BEC attacks were registered at one of these two registrars. This is an increase from 55 percent in Q4 2020, and from 43% in Q3 2020.



How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking the proportion of phishing sites that 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 first quarter of 2021 was the first quarter in which we did not see an increase in the number of phishing sites using SSL. The percentage has leveled off at about 83 percent for two quarters in a row."

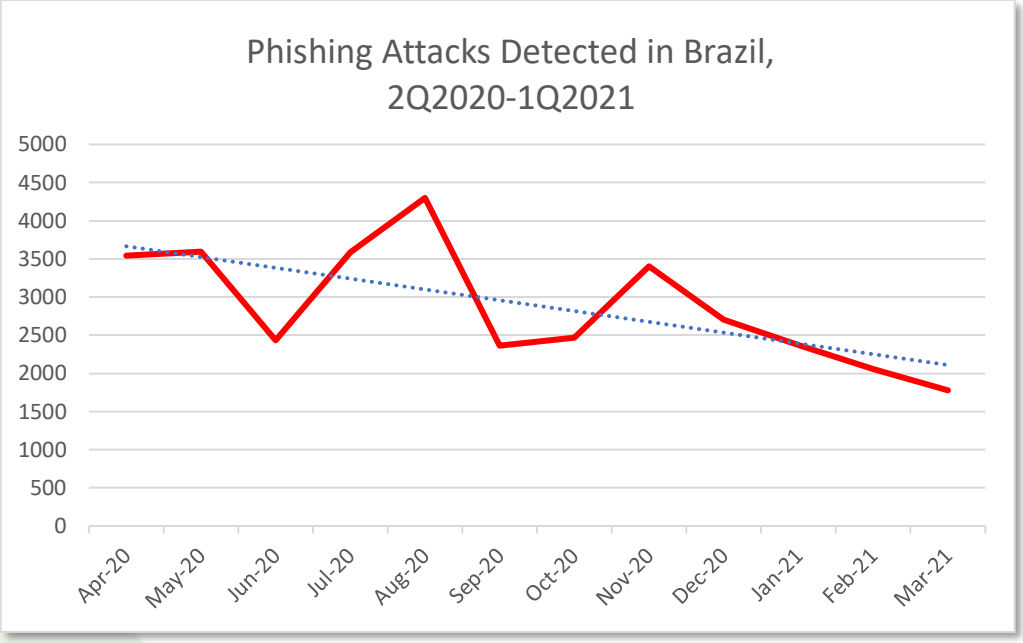
LaCour also analyzed the type of certificates used. In Q1 2021, 94.5 percent of certificates used in phishing were "Domain Valid" or "DV" certificates. "DV certificates are commonly granted for free by providers

such as Let's Encrypt and cPanel, and provide the weakest form of certificate validation, requiring no authentication of the user – only the domain name being used," noted LaCour. PhishLabs only found 11 phishing sites that had Extended Validation (EV) certificates installed. Those sites were all legitimate sites that had been hacked, rather than sites built by attackers who had somehow acquired EV certificates.

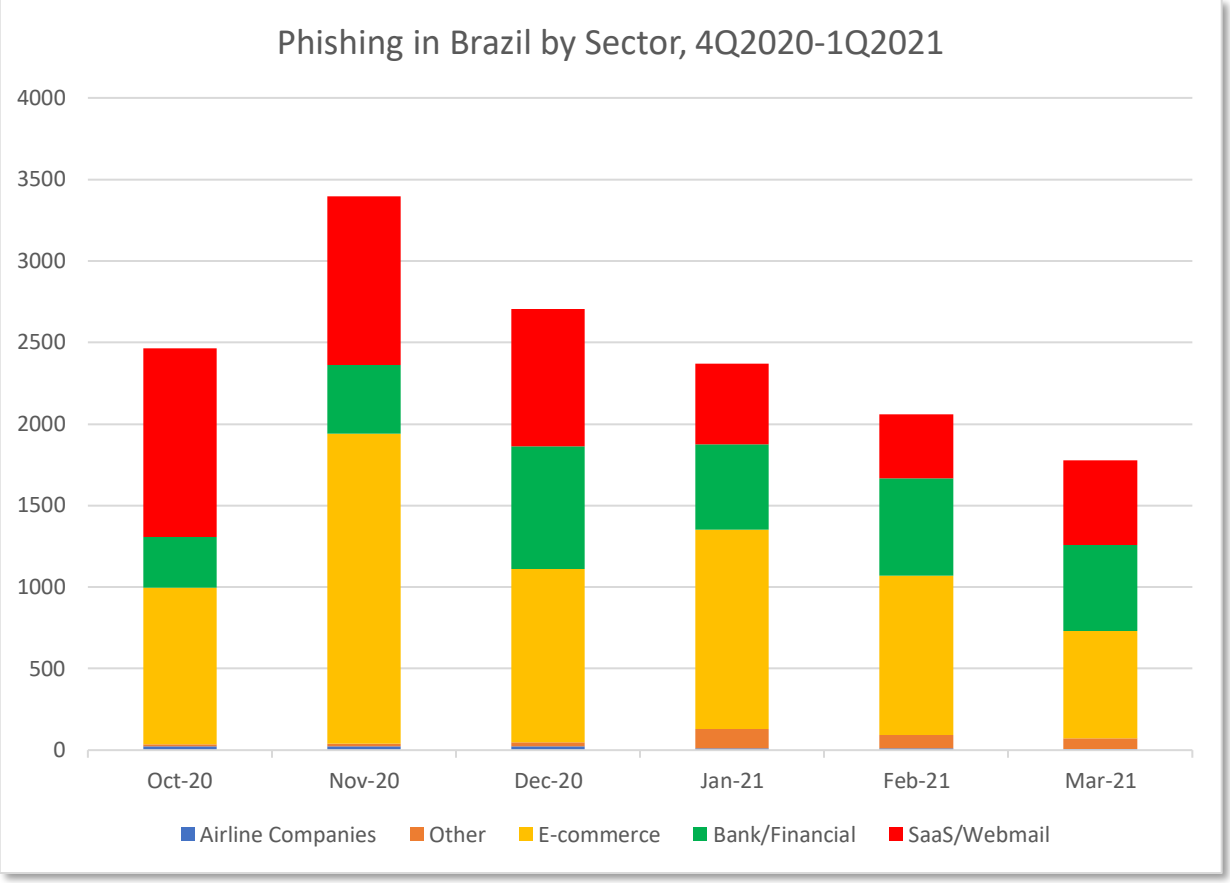
Online Criminal Activity in Brazil

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 Q1 2021, Axur's systems identified 6,209 phishing attacks. This data is encouraging, as it represents a decline from the third and fourth quarters of 2020:



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



Among the attacks in Q1, Axur found that only 56% of the sites were protected using HTTPS. This compared to a rate of 83 percent worldwide (see page 8).

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, their brands, and their customers.

RiskIQ analyzed 3,054 confirmed phishing URLs reported to APWG in Q1 2021. RiskIQ found that they were hosted on 2,134 unique second-level domains (and 35 were hosted on unique IP addresses, without domain names).

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, but represented 77.6% percent of the phishing domains in the sample set. There were 1,656 legacy gTLDs in the sample set. Most of those were in .COM, which had 1,535 domains in the set.
- The new generic top-level domains (nTLDs), such as .XYZ and .ICU, were released after 2011. The nTLDs represented about 8 percent of the domains in the world, and were about 8 percent of the domains in the sample set (173 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, but were only 14 percent of the domains in the Q3 sample set (305 domains).

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

Rank	TLD	Category	# of Unique Domains in Sample Set (1Q 2021)
1	.COM	gTLD	1,535
2	.UK	ccTLD	77
3	.ORG	gTLD	55
4	.NET	gTLD	46
5	.XYZ	nTLD	43
6	.LIVE	nTLD	28
7	.BR	ccTLD	24
8	.LINK	nTLD	24
8	.INFO	gTLD	18
10	.ME	ccTLD	18

In related news, RiskIQ took a closer look at the infrastructure and criminal enterprise behind LogoKit, a simple, modularized, and adaptable phish kit running on at least hundreds of domains. The resulting investigation illuminated a massive phishing ecosystem and thriving crimeware economy driven by a high demand for simple, effective phishing tools.

Magecart phishing attacks skyrocketed, and in one period RiskIQ detected new attacks every few minutes. The Magecart threat actors use digital skimmers to intercept and exfiltrate credit card information from online purchases to either use or sell on the dark web.

Android apps containing the Cerberus and Anubis banking trojans were more extensive than previously believed. These campaigns, dubbed "Turkey Dog," attempt to lull Turkish speakers into installing the trojans by either masquerading as part of the Turkish government by promising cash payments of

thousands of Turkish lira, or promising a free Internet package to stay safe at home during the pandemic. The remote access trojans (RATs) can exploit SMS to circumvent two-factor authentication, as well as record audio, perform full-screen overlays to present a false login page for harvesting banking credentials, and install additional software.

"As the global pandemic is not yet behind us, we must maintain and encourage vigilance against scammers that will continue to try and illegally profit by abusing the public's interest in vaccination," said Jonathan Matkowsky, Vice-President of Digital Risk at RiskIQ.

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); Seth Knox of Agari (sknox@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); Holly Hitchcock of RiskIQ (holly@frontlines.io). **Analysis and editing by Greg Aaron, Illumintel Inc., www.illumintel.com**