Phishing Activity Trends Report

2nd Quarter 2020

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2020

Published 27 August 2020

Phishing Report Scope

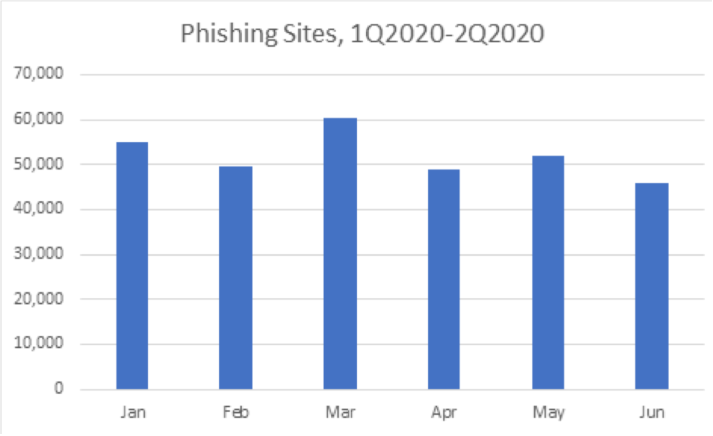
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org.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

Cybercrime Gangs Attempting and Achieving Heists of Increasing Scale



Phishing Activity Trends Summary

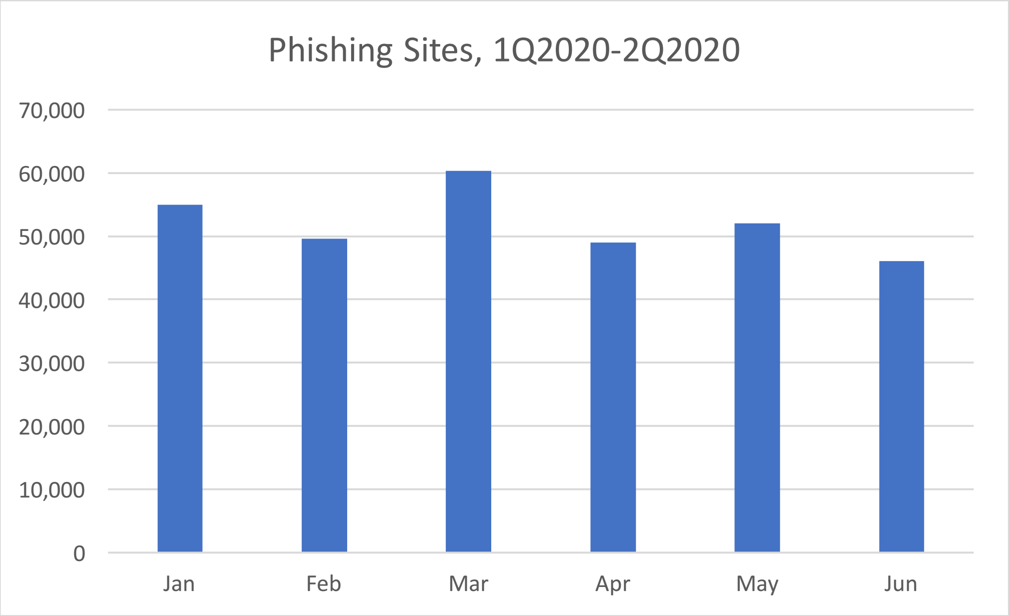
- The average wire transfer loss from Business Email Compromise (BEC) attacks is increasing: The average wire transfer attempt in the second quarter of 2020 was $80,183, up notably from $54,000 in the first quarter. A Russian BEC operation has been targeting companies for an average of $1.27 million. [pp. 6-8]
- The number of phishing sites detected in the second quarter of 2020 was 146,994, down from the 165,772 observed in the first quarter. [p. 3]
- Phishing that targeted webmail and Software-as-a-Service (SaaS) users continued to be biggest category of phishing. Attacks targeting the Social Media sector increased in Q2 about 20 percent over Q1, primarily driven by targeted attacks against Facebook and WhatsApp. [p. 5]
- 78 percent of all phishing sites now use SSL protection. [p. 11]
- After an explosion in 2019 and into early 2020, phishing in Brazil dropped back slightly. When phishers there registered domains names for their attacks, most of those domains did not contain names of the target companies, or a compelling catchword designed to fool people. [p. 9]

Statistical Highlights for 2nd Quarter 2020

	April	M ay	June
Number of unique phishing Web sites detected	48,951	52,007	46,036
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	43,282	39,908	44,497
Number of brands targeted by phishing campaigns	364	352	363

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 second quarter of 2020 was 146,994. That was down 11 percent from the 165,772 in Q1 2020.

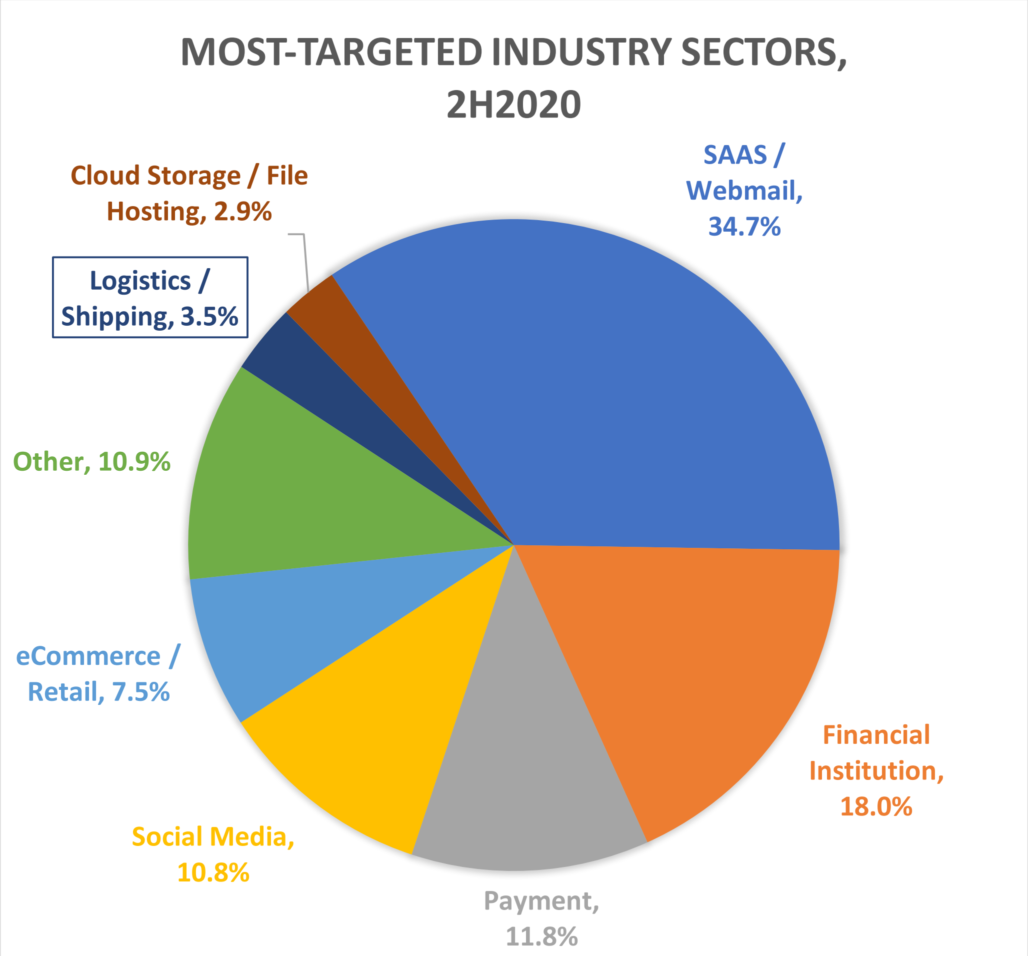


The APWG also tracks the number of unique phishing reports (email campaigns) it receives from consumers and the general public. An e-mail campaign is a unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts 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 2Q2020 was 127,787. The numbers are generally comparable to previous quarters: 139,685 in 1Q2020, 132,553 in 4Q2019, 122,359 in 3Q2019, and 112,163 in 2Q2019. These were phishing emails submitted to APWG, and the total does not count phishing URLs reported by APWG members directly into APWG's eCrime Exchange.

Most-Targeted Industry Sectors – 2nd Quarter 2020

In the second quarter of 2020, APWG member OpSec Security found that SaaS and webmail sites remained the biggest targets of phishing, with more than 35% of all attacks. "In Q2 we detected a slightly higher concentration of attacks on the top targeted industries, with specific increases over Q1 in SAAS/Webmail and Social Media targets," noted Stefanie Wood Ellis, Anti-Fraud Product & Marketing Manager at OpSec Online. "Attacks targeting the Social Media sector increased in Q2 about 20 percent over Q1, primarily driven by targeted attacks against Facebook and WhatsApp."

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



Business e-Mail Compromise (BEC), 2nd 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.

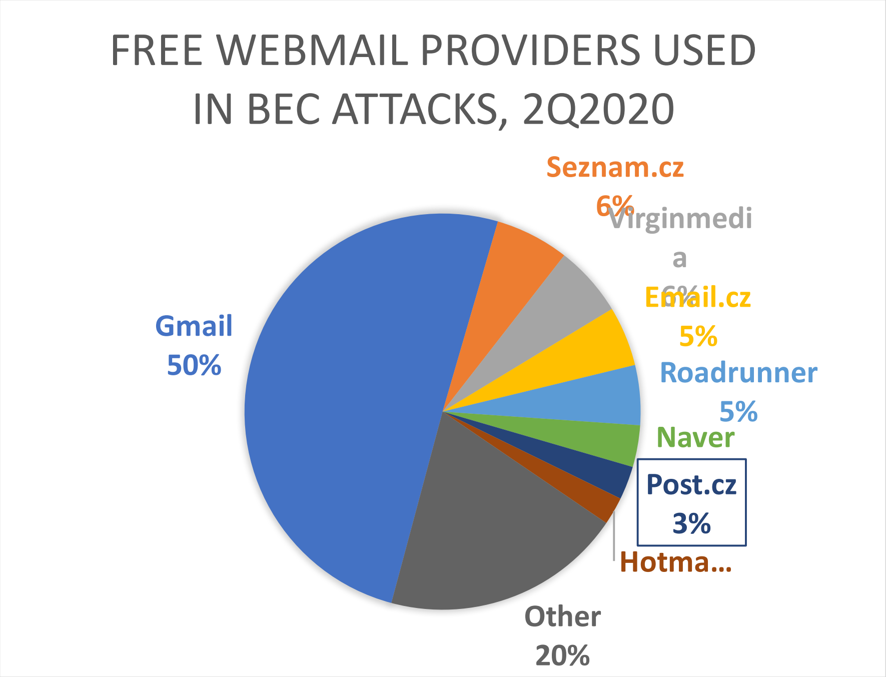
Agari examined thousands of attempted BEC attacks it observed during Q2. Agari counts BEC as any response-based spear phishing attack that involves the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive materials. 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. About 16 percent of attacks requested payroll diversions, down from 25 percent in 3Q2019. 18 percent requested direct bank transfers.

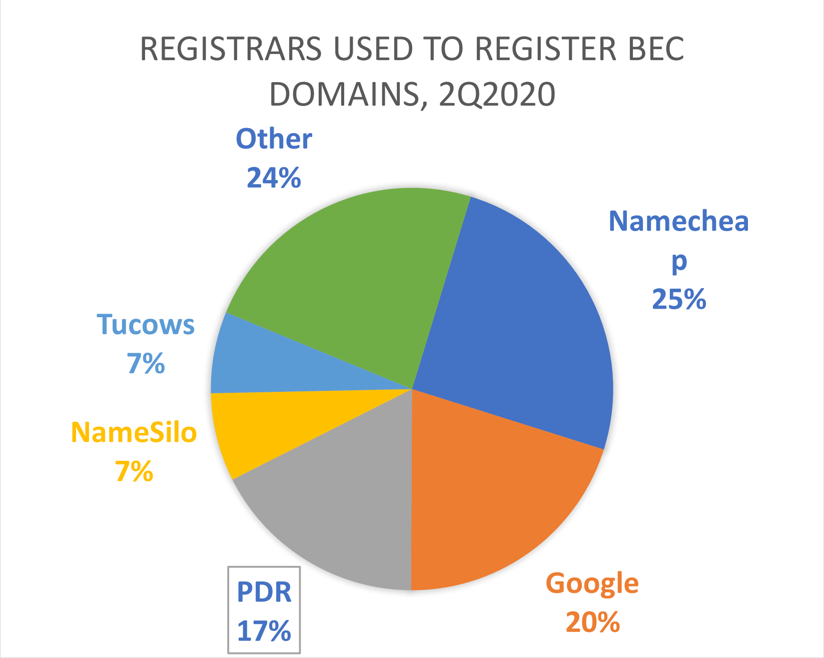
The amount of money that an attacker can make by getting gift cards is significantly less than he can get with a wire transfer. During the second quarter of 2020, the average amount of gift cards requested by BEC attackers was $1,213, down from $1,453 in the first quarter of 2020. Scam attempts around 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, Apple iTunes, and Steam Wallet made up 70 percent of gift card requests in the second quarter.

On the other hand, BEC attacks that ask for wire transfers are pursuing much larger amounts. The average BEC wire transfer attempt requested in the second quarter of 2020 was for $80,183, up notably from $54,000 in the first quarter.

About 72 percent of BEC attacks in Q2 were sent from free webmail accounts, up from 61 percent in Q1. Half of all BEC attacks sent from free webmail providers used Gmail. Notably, BEC attackers used several services in the Czech Republic, including Seznam.cz, Email.cz, and Post.cz:



Nearly a quarter (24%) of BEC attacks in 2Q202 were sent from email accounts hosted on domains registered by scammers. More than three quarters (76%) of those domains were registered at just five domain registrars: Namecheap (25%), Google (20%), Public Domain Registry (PDR) (17%), NameSilo (7%), and Tucows (7%).

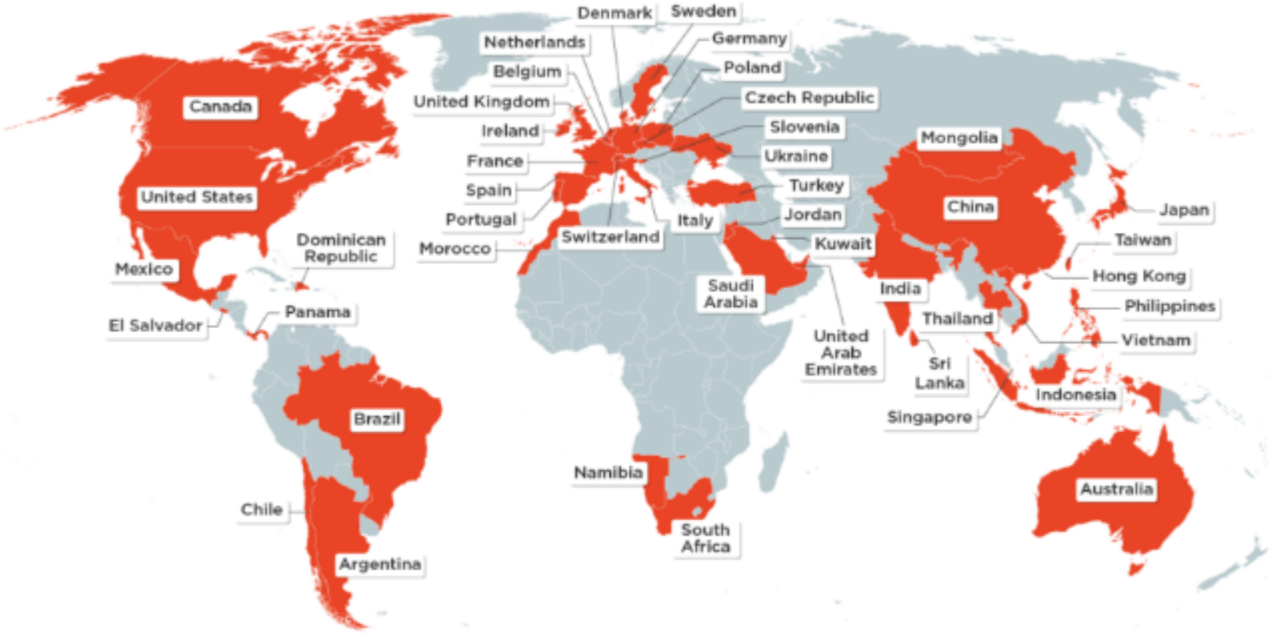


According to Crane Hassold, Agari's Senior Director of Threat Research, Russian cybercriminals have been using BEC attacks recently. Agari has given the code-name "Cosmic Lynx" to the first documented Russian BEC group, which is one of the most important BEC groups outside of West Africa, where many BEC attacks are launched. "We were expecting that Russian cybercriminals would move into the world of BEC because the return on investment for basic social engineering attacks is much higher than launching more sophisticated (and more expensive) malware-based attacks," said Hassold.

Agari has observed more than 200 BEC campaigns linked to Cosmic Lynx since July 2019, which have targeted individuals in 46 countries on six continents. Cosmic Lynx attacks large multinational organizations, many of which are Fortune 500 and Global 2000 companies. Cosmic Lynx employs a dual impersonation scheme. The pretext of their attacks is that the target organization is preparing to close an acquisition with an Asian company as part of a corporate expansion.

First Cosmic Lynx impersonate a company's CEO, asking the target employee to work with "external legal counsel" to coordinate the payments needed to close the acquisition. Then Cosmic Lynx hijacks the identity of a legitimate attorney at a UK-based law firm, whose supposed job it is to facilitate the transaction. The final stage of a Cosmic Lynx BEC attack is getting the target to send payments to mule accounts controlled by the group.

The average amount requested by Cosmic Lynx in its attacks is an astounding $1.27 million.

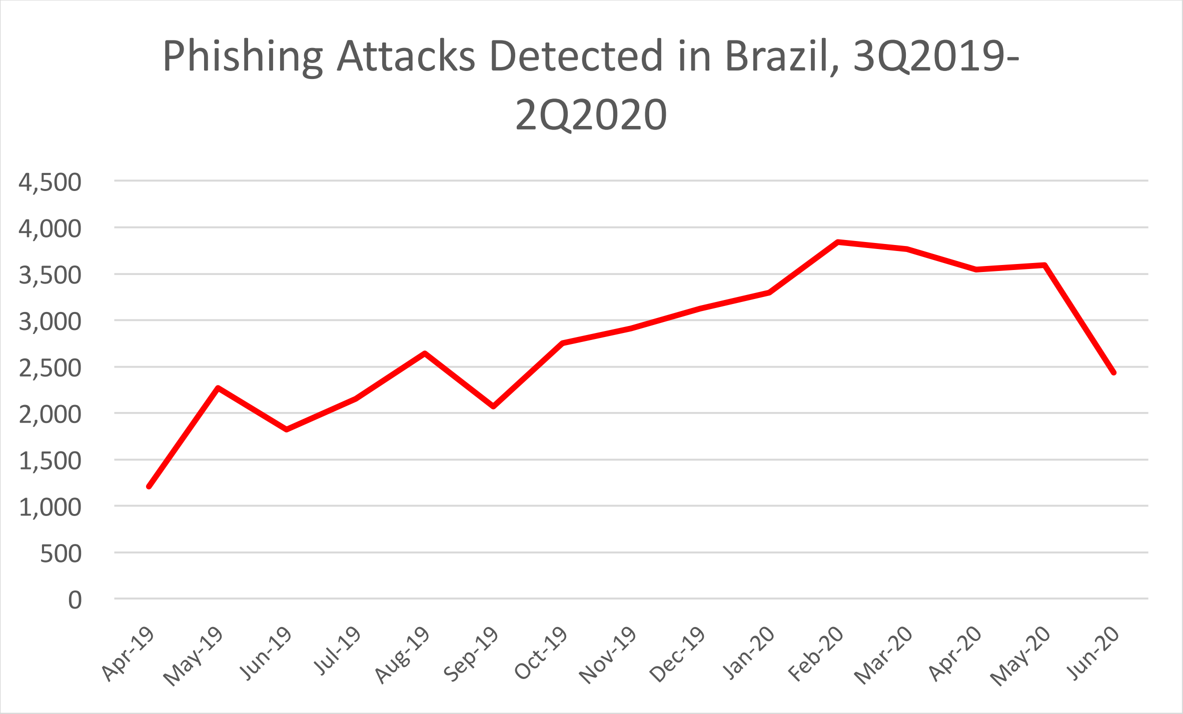


Above: the locations of Cosmic Lynx targets

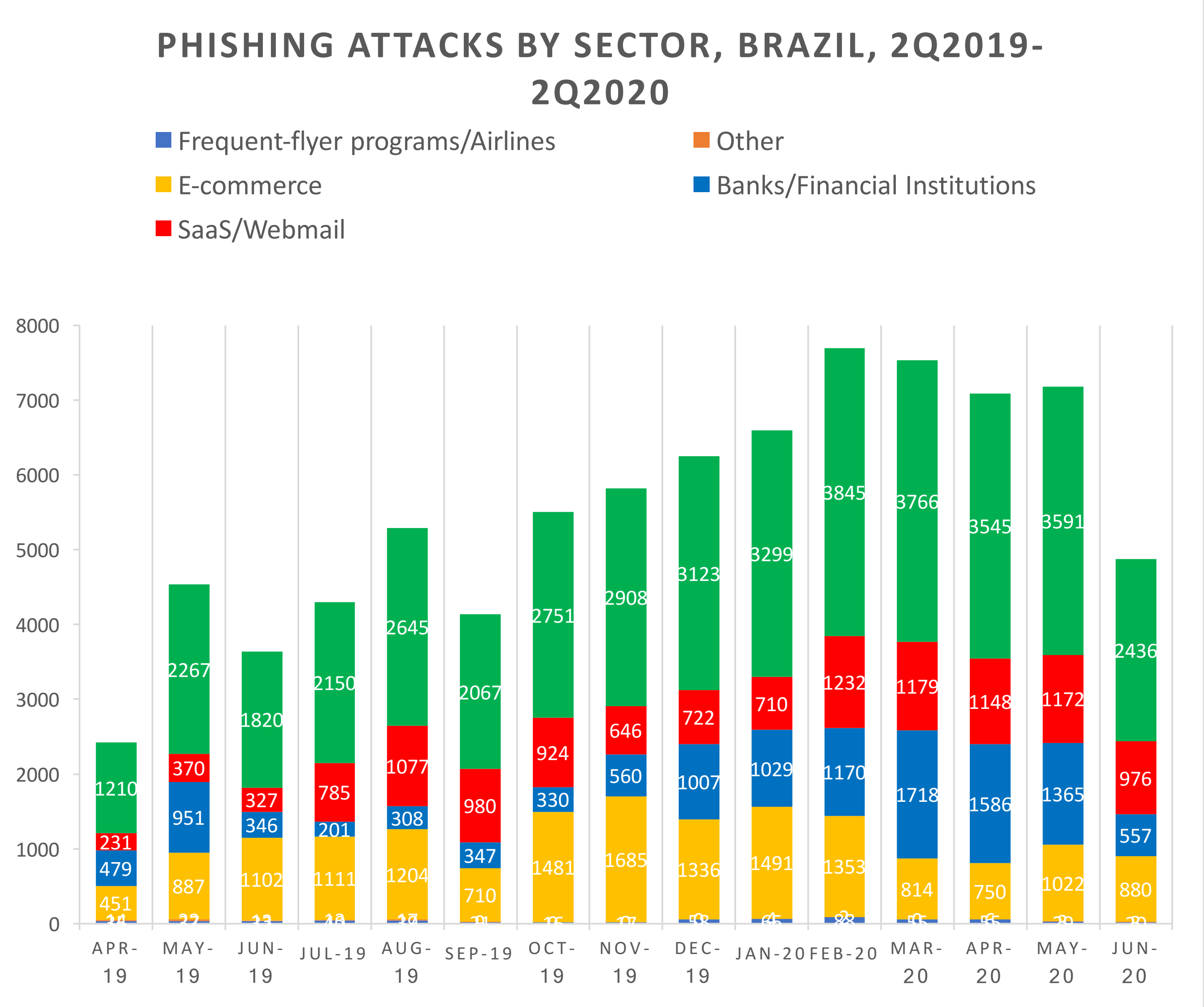
Online Criminal Activity in Brazil

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 second quarter of 2020, Axur observed 9,572 unique phishng cases in Brazil, down from 10,910 in the first quarter, but far above the 8,782 seen in the fourth quarter of 2019, the 52,97 in Q2 of 2019, and the 3,220 cases from 1Q2019. In other parts of the world, phishing did not leap so dramatically during the same time period.



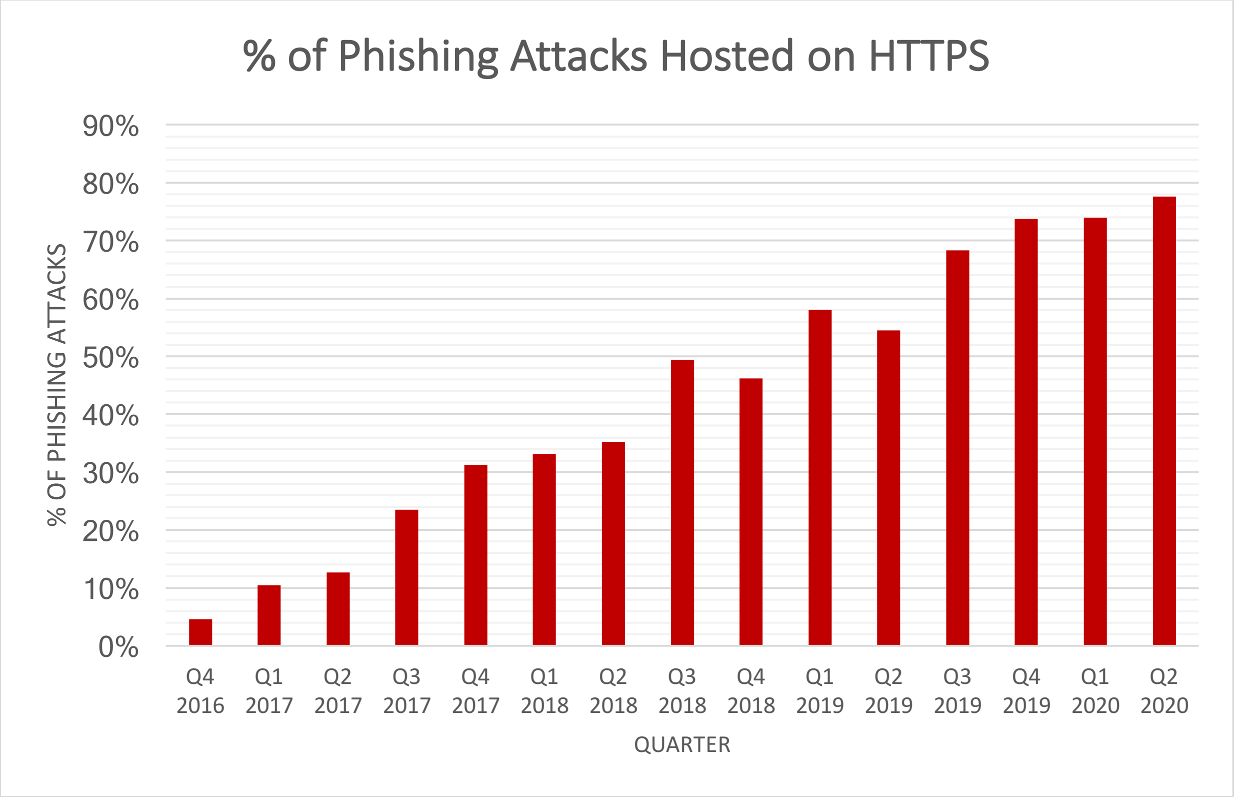
The decrease in cases of digital fraud in June 2020 was most evident the banking and financial sector, as shown below. This dip also occurred between May and June of 2019. Even so, the banking and financial sector is still the primary target of phishing attacks in Brazil.



When phishers registered domains names for their attacks, Axur found that 58 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 shows phishers trying to avoid detection, because telltale words in domain names are easier for defenders to find.

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.



"The number of phishing sites using TLS continues to increase," said John LaCour, Founder and CTO of Digital Risk Protection company PhishLabs. "Most web sites—good and bad—now use TLS. Phishers are hacking into legitimate web sites and placing their phishing files on those compromised sites."

In the second quarter of 2020, the percentage of phishing sites using SSL/TLS certificates increased slightly to 77.6 percent, up from 74 percent the prior quarter. 36.2 percent of all certificates seen in phishing attacks during the quarter were issued by the certificate authority Let's Encrypt, which issues free certificates.

“The vast majority of certificates used in phishing attacks — 91 percent — are Domain Validated (“DV”) certificates,” noted LaCour. “Interestingly, we found 27 web sites that were using Extended Validation (“EV”) certificates.” This use of Extended Validation certificates is a serious business. The point of an Extended Validation certificate is that they require verification of the requesting entity's legal identity before the certificate is issued. In the sites detected, hackers didn’t manage to get EV certificates themselves – they hacked web sites that already had them.

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**