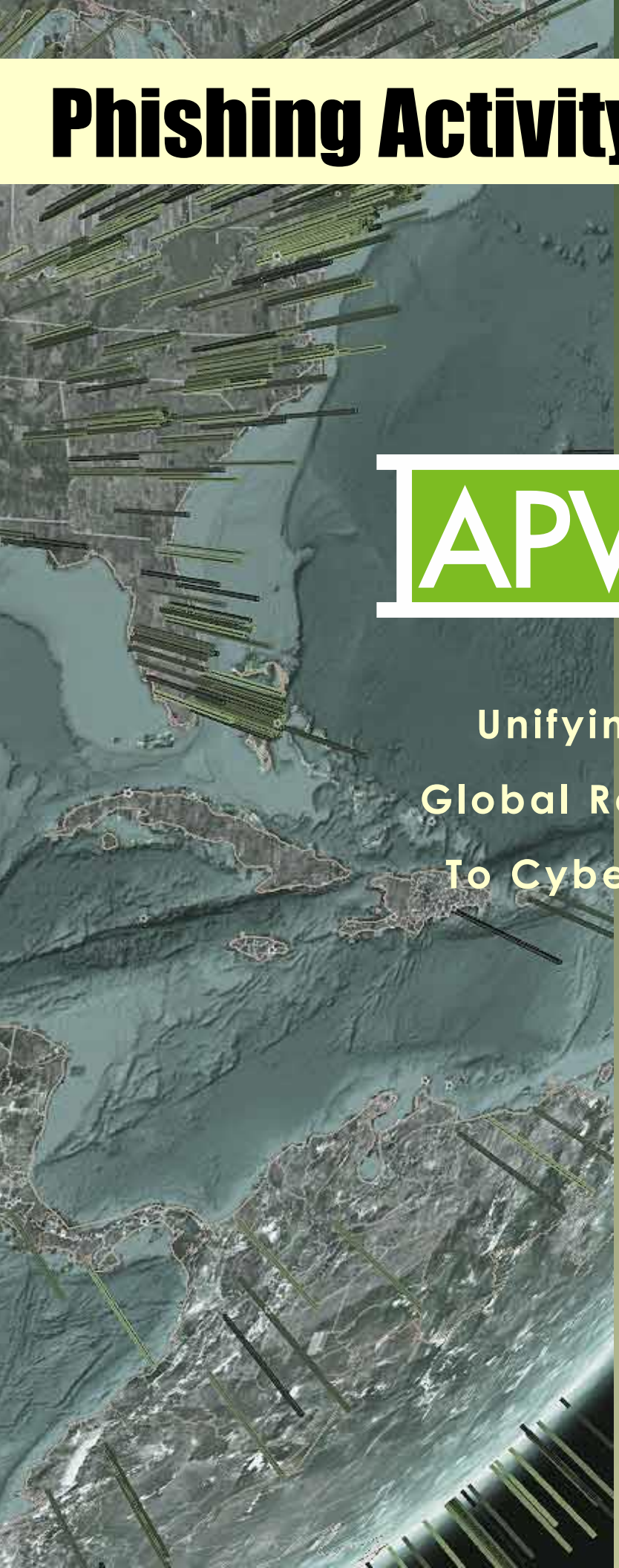
Phishing Activity Trends Report



2nd Quarter 2021

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2021

Published 22 September 2021

Phishing Report Scope

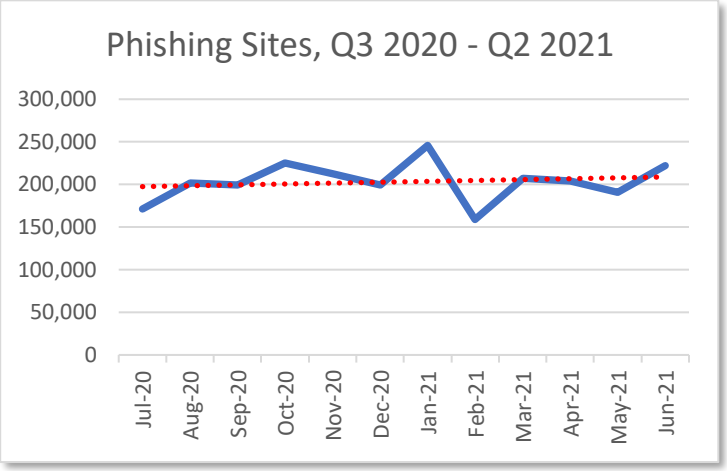
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org.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



Phishing remained at elevated levels in Q2 2021 and cybercrime gangs focus on cryptocurrency companies

Phishing Activity Trends Summary

- After doubling in 2020, the amount of phishing has remained at a steady but high level. APWG saw 222,127 attacks in June 2021, which was the third-worst month in APWG's reporting history. [pp. 3-4]
- The financial institution and social media sectors were the most frequently victimized by phishing in this quarter. Phishing against cryptocurrency targets, such as cryptocurrency exchanges and wallet providers, shot from 2 percent of all attacks in Q1 to 7.5 percent in Q2. [p. 5]
- Business e-mail compromise scams are becoming increasingly costly for victims. The average wire transfer request in BEC attacks increased to $106,000, up from $48,000 over the last year. [p. 6]
- The number of brands being attacked has risen during 2021. [p. 4]

Statistical Highlights for the 2nd 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:

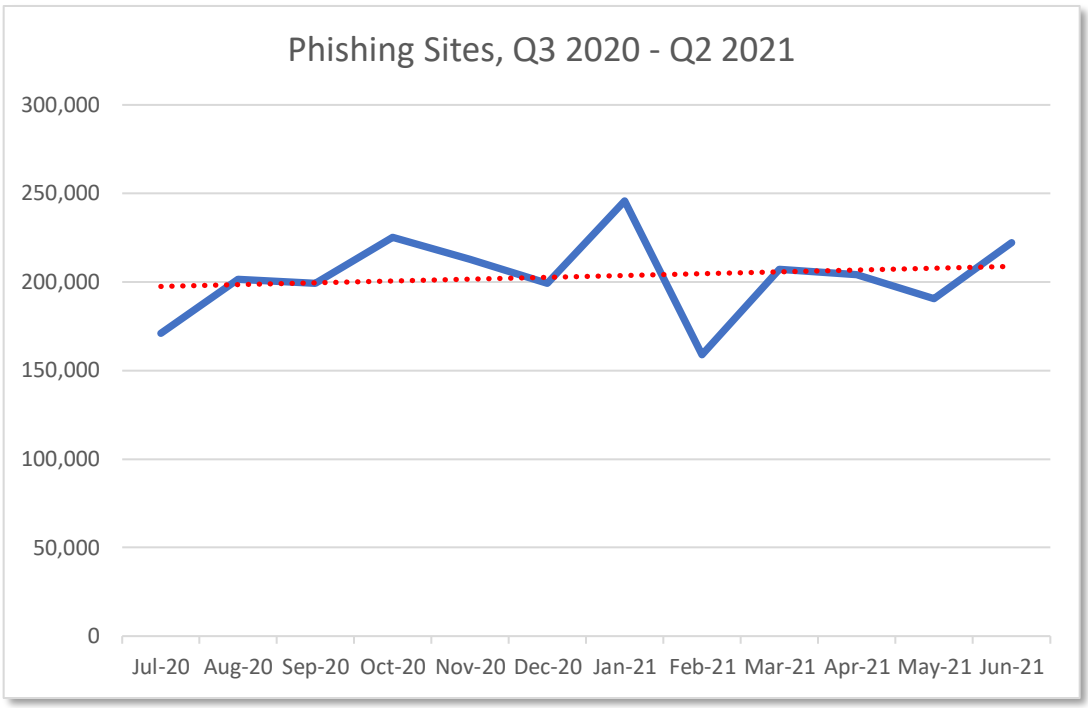
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique base URLs of phishing sites found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to 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.

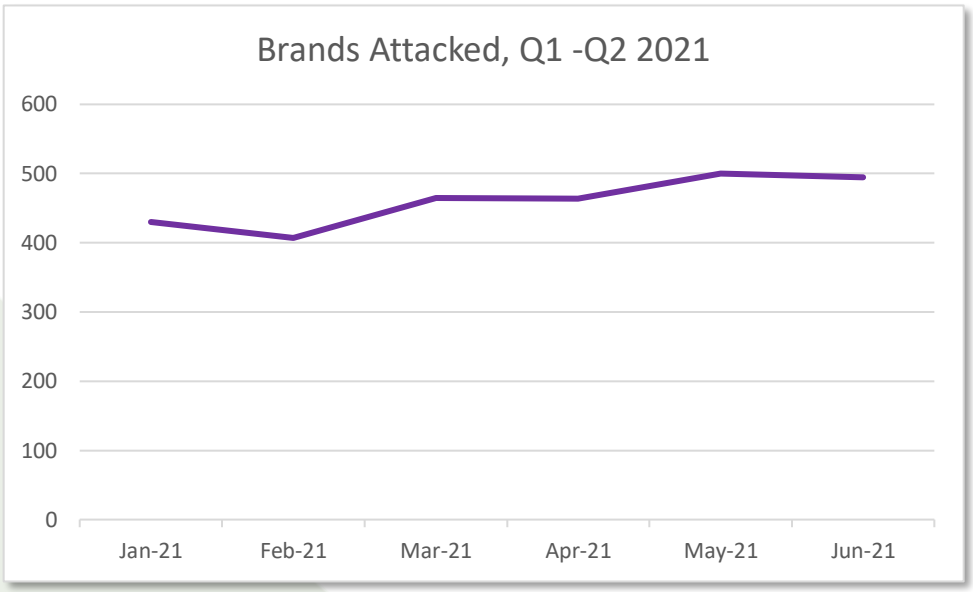
- The APWG also counts the **number of brands attacked** by examining the phishing reports submitted into the APWG eCrime Exchange, and normalizing the spellings of brand names.

	April	May	June
Number of unique phishing Web sites detected	204,050	190,762	222,127
Unique phishing email subjects	11,400	9,239	9,669
Number of brands targeted by phishing campaigns	464	500	495

The number of phishing attacks over the last year has remained fairly steady, but is roughly twice was it was from mid-2019 into mid-2020. APWG saw 222,127 attacks in June 2021, which was the third-worst month in APWG's reporting history.

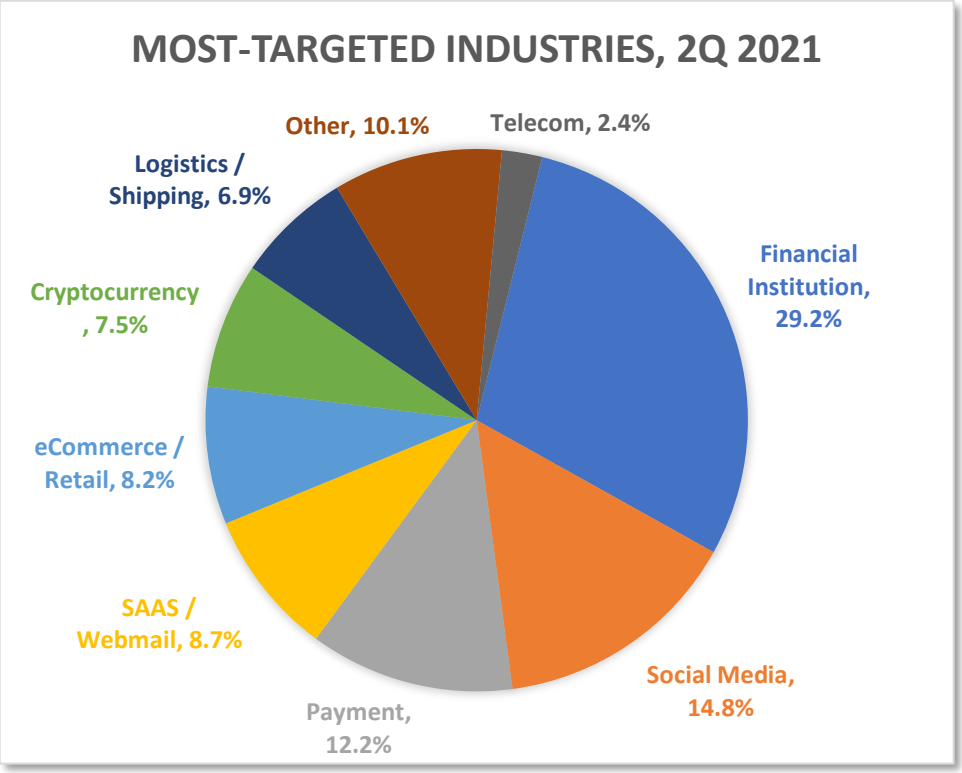


The number of Unique Subjects has dipped as more submitted emails have had duplicative subject lines. The number of brands attacked each month has trended upwards, with a high of 500 in May 2021:



Most-Targeted Industry Sectors – 2nd Quarter 2021

In the second quarter of 2021, APWG founding member OpSec Security found that phishing attacks against financial institutions were the still most prevalent, moving to 29.2 percent of all attacks, up from 22.5 percent of all attacks in 4Q2020. Phishing against cryptocurrency targets — such as cryptocurrency exchanges and wallet providers — rocketed from 2 percent of all attacks in Q1 to 7.5 percent in Q2.

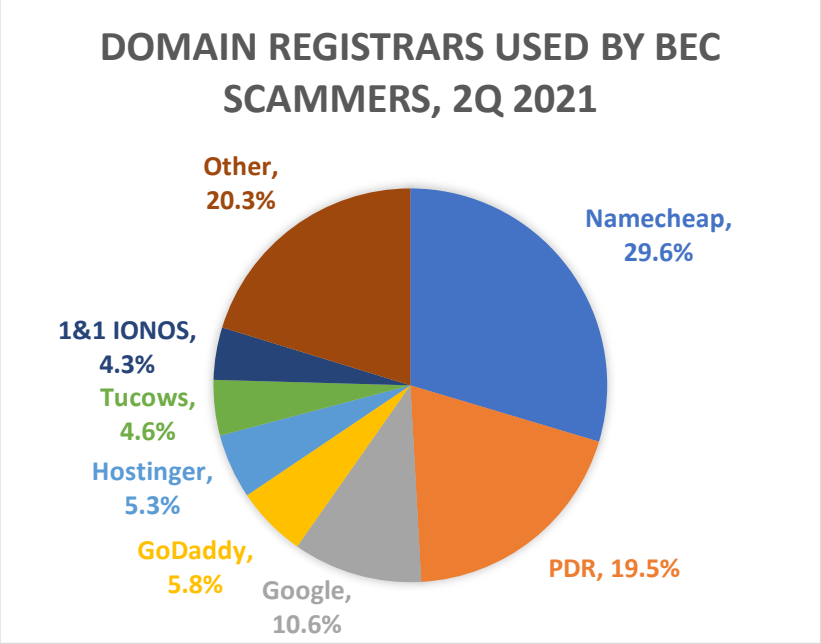


"We observed growth in expansion of crypto-business related attacks," noted Stefanie Wood Ellis, Director, Product Management at OpSec Security. "OpSec continues to observe increases in vishing and/or smishing related phishing. *Vishing* is phishing advertised via voice messages, and *smishing* is phishing advertised in SMS messages. Smishing is becoming more common for organizations that are primarily mobile app-driven. OpSec also detected about a 30 percent increase in overall phishing volume in Q2 versus Q1."

OpSec Security offers world-class brand protection solutions.

Business e-Mail Compromise (BEC), 2nd Quarter 2021

APWG member Agari by HelpSystems 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 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 the average amount requested in wire transfer BEC attacks in Q2 2021 was $106,000, up from $75,000 in Q4 2020. This increase was caused by both a rise in high-dollar transfer requests (20 percent of attacks requested more than $100,000 in Q2 compared to just 10 percent in Q1), as well as a decrease in lower-dollar requests.

Over the past year, Agari has observed a complete resurgence in the payroll diversion BEC attacks. In July 2020, only 3 percent of all BEC attacks that month targeted direct deposit charges. But in Q2 2021, 24 percent of all BEC attacks tried to divert employee payroll deposits. In May 2021, the percentage of payroll diversion BEC attacks surpassed wire transfer BEC attacks for the first time since September 2019.

Agari found also that in Q2 2021, scammers requested funds in the form of gift cards in 47 percent of BEC attacks, down from 60 percent in Q4 2020 and 71 percent in Q3 2020. The other 19 percent of attacks involved direct bank transfer requests.

eBay, iTunes, and Amazon gift cards were the most commonly requested gift cards in BEC attacks, and constituted 60 percent of gift card requests. BEC actors request gift cards because they can exchange them for cryptocurrency at cryptocurrency exchanges. Cybercriminals also like 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 that BEC actors use to move money.

Agari found that domain name registrars Namecheap and Public Domain Registry (PDR) continue be the primary registrars used by cybercriminals to register the domain names they use in BEC attacks. (39 percent of the total were at NameCheap, and 26 percent were at PDR.) Since Q4 202, these two registrars have represented a majority of maliciously registered domains.

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 2,447 confirmed phishing URLs reported to APWG in Q2 2021. RiskIQ found that they were hosted on 1,327 unique second-level domains (and 60 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 50.7 percent of the domain names in the world as of the beginning of Q2 2021, and represented 64 percent of the phishing domains in the sample set. There were 854 legacy gTLD domains in the sample set. Most of those were in .COM, which had 767 domains in the set.
- The new generic top-level domains (nTLDs), such as .XYZ and .ICU, were released after 2011. The nTLDs represented about 6.3 percent of the domains in the world, and were almost 9 percent of the domains in the sample set (117 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 27 percent of the domains in the Q3 sample set (354 domains).

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

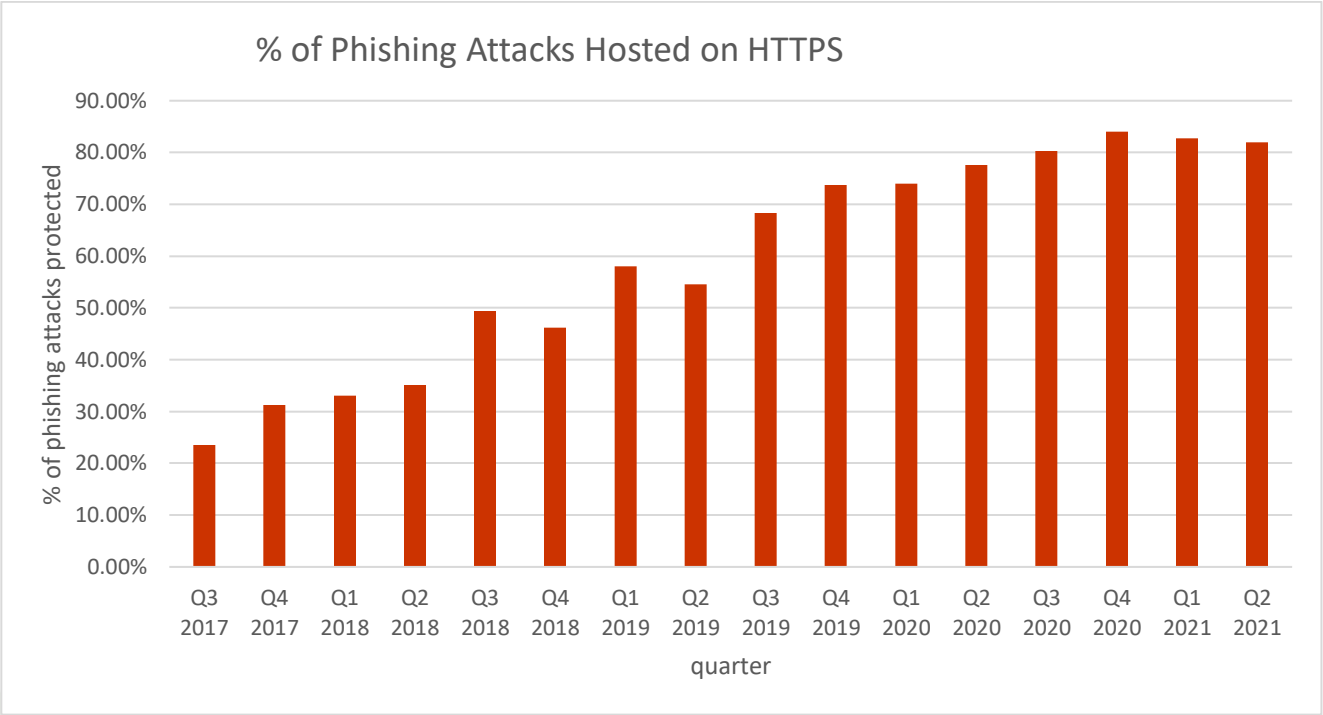
Rank	TLD	Category	# of Unique Domains in Sample Set (1Q 2021)
1	.COM	gTLD	767
2	.XYZ	nTLD	42
3	.UK	ccTLD	41
4	.NET	gTLD	40
5	.ME	ccTLD	34
6	.ORG	gTLD	34
7	.TK	ccTLD	30
8	.ML	ccTLD	23
8	.AU	ccTLD	19
10	.CF	ccTLD	19

In related news, in Q2, RiskIQ profiled a bulletproof hosting provider, Media Land LLC, run by cyber threat mogul Alexander Volosovik, and illuminated Volosovik's fast-flux techniques meant to evade detection. RiskIQ's research team shined new light on Agent Tesla, a popular "malware-as-a-service" remote access Trojan (RAT) used to steal information, such as credentials and keystrokes. RiskIQ found that Russia's APT29, which the US government associated with Russia's Foreign Intelligence Service, is actively serving malware previously used in espionage campaigns targeting COVID-19 research.

"In Q2, President Biden signed an executive order to modernize U.S. cybersecurity defenses. This presents great opportunity to foster and advance security and resiliency, and strengthen public-private partnerships," said Jonathan Matkowsky of RiskIQ.

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.



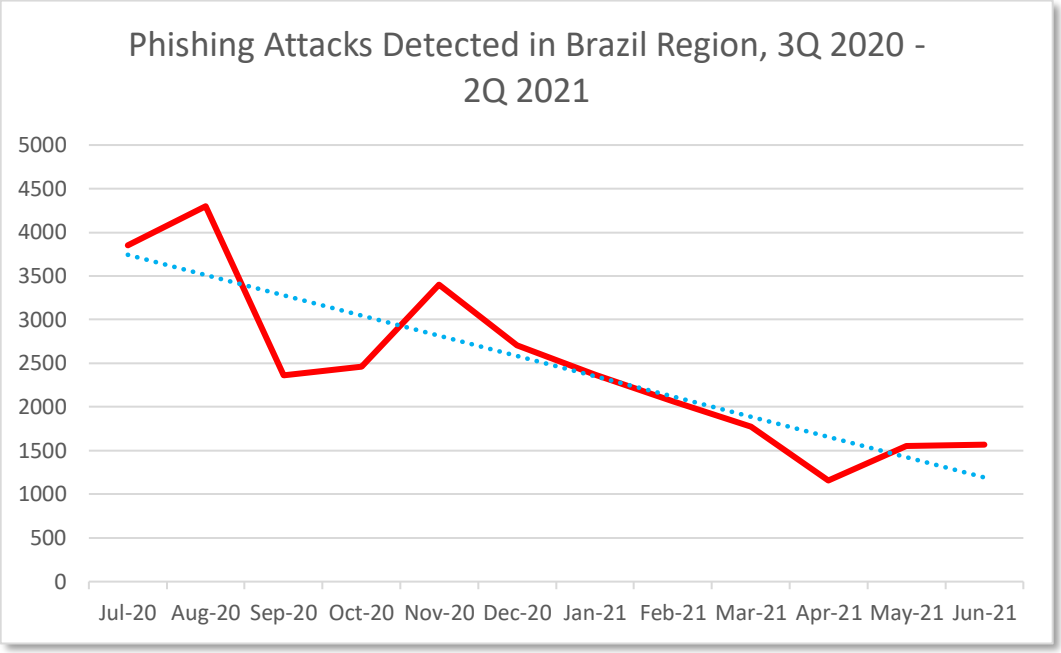
John LaCour, CTO of PhishLabs, analyzed the number of phishing sites using TLS certificates. According to LaCour, "After peaking in late 2020, the percentage of phishing sites protected by SSL dropped to 82 percent in 2Q 2021."

PhishLabs also collected data about the type of certificate used, and found 90 percent of the certificates used in phishing were the mostly free DV (Domain Validated) certs such as those issued by Cpanel and Let's Encrypt. LaCour notes that these provide the weakest form of certificate validation, requiring no authentication of the user — only the domain name being used. LaCour noted, "PhishLabs also found two hacked web sites using EV or Extended Validated certificates. While we did not find any EV certificates issued to attackers, we found two phishing sites installed on hacked web servers using EV certificates."

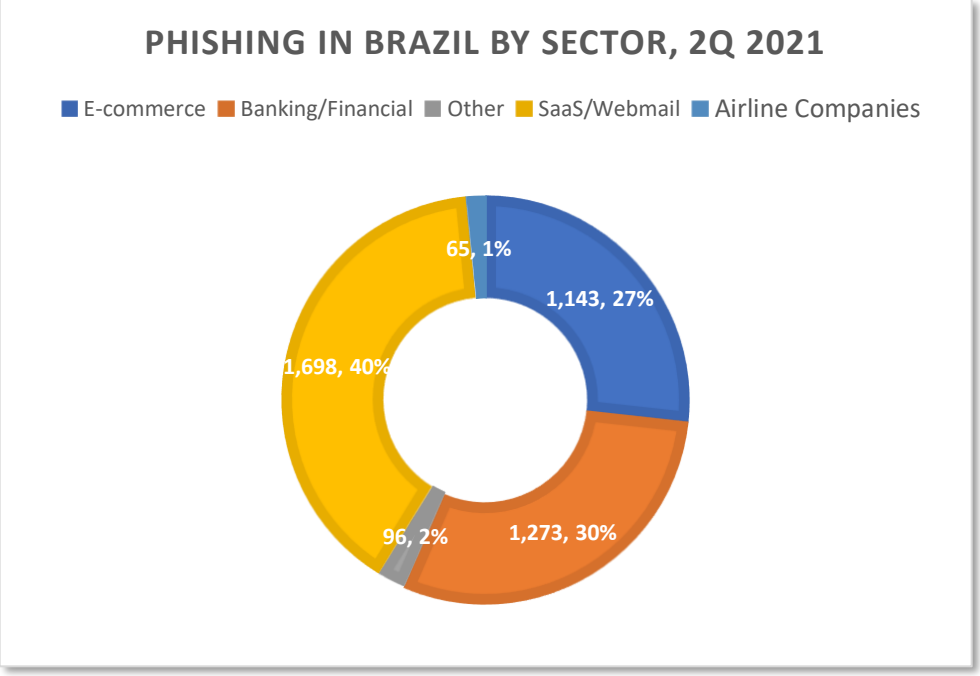
Online Criminal Activity in Brazil

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 show how criminals are perpetrating identity theft in South America's largest economy, and show 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 Q2 2021, Axur's systems identified 4,275 attacks, down from 6,209 in Q1:



In Q2, phishing against SaaS and Webmail companies became more prominent, accounting for 40 percent of all attacks. Phishing against e-commerce companies fell back to 27 percent of all attacks, down from 45 percent is Q1 2021:



Among the regional attacks it recorded in Q2, Axur found that 70 percent of the phishing sites were protected using HTTPS. This compared to a rate of 82 percent worldwide (see page 9).

APWG Phishing Activity Trends Report Contributors

Agari by HelpSystems protects organizations against phishing, business email compromise (BEC) scams, and 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 Security 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 Wood Ellis at OpSec Security (sellis@opsecsecurityonline.com); Angela Tuzzo of Agari by HelpSystems (atuzzo@mrb-pr.com); 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**