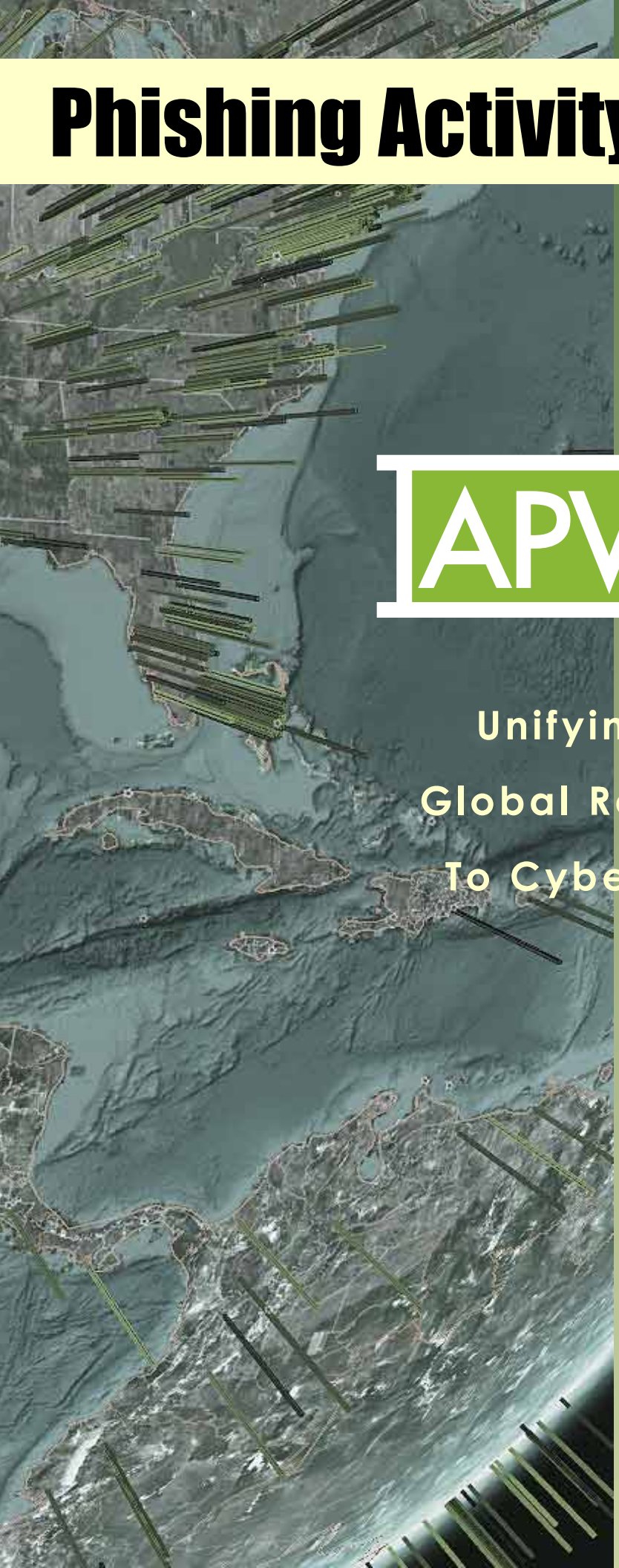
Phishing Activity Trends Report



3rd Quarter 2019

APWG

Unifying the
Global Response
To Cybercrime

Activity July-September 2019

Published November 4, 2019

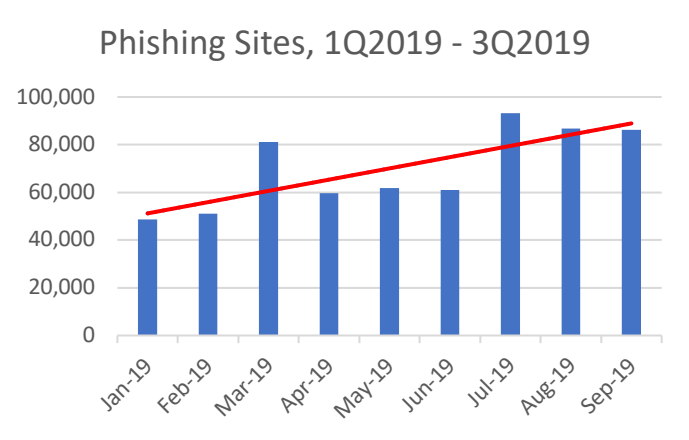
Phishing Report Scope

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.

Phishing Attacks Reach Highest Level in Three Years



3rd Quarter 2019 Phishing Activity Trends Summary

- The number of phishing attacks rose in the third quarter of 2019, to a high level not seen since late 2016. [pp. 3-4]
- Forty percent of Business Email Compromise (BEC) attacks use domain names registered by the criminals, a strategy used to fool unwary victims. [p. 8]
- More than two-thirds of all phishing sites used SSL protection. This was the highest percentage since tracking began in early 2015, and is a clear indicator that users can't rely on SSL alone to understand whether a site is safe or not. [p.10]
- Phishing that targeted webmail and Software-as-a-Service (SaaS) users continued to be biggest category of phishing. [p. 5]
- Phishing also rocketed upwards in South America. [p. 11]

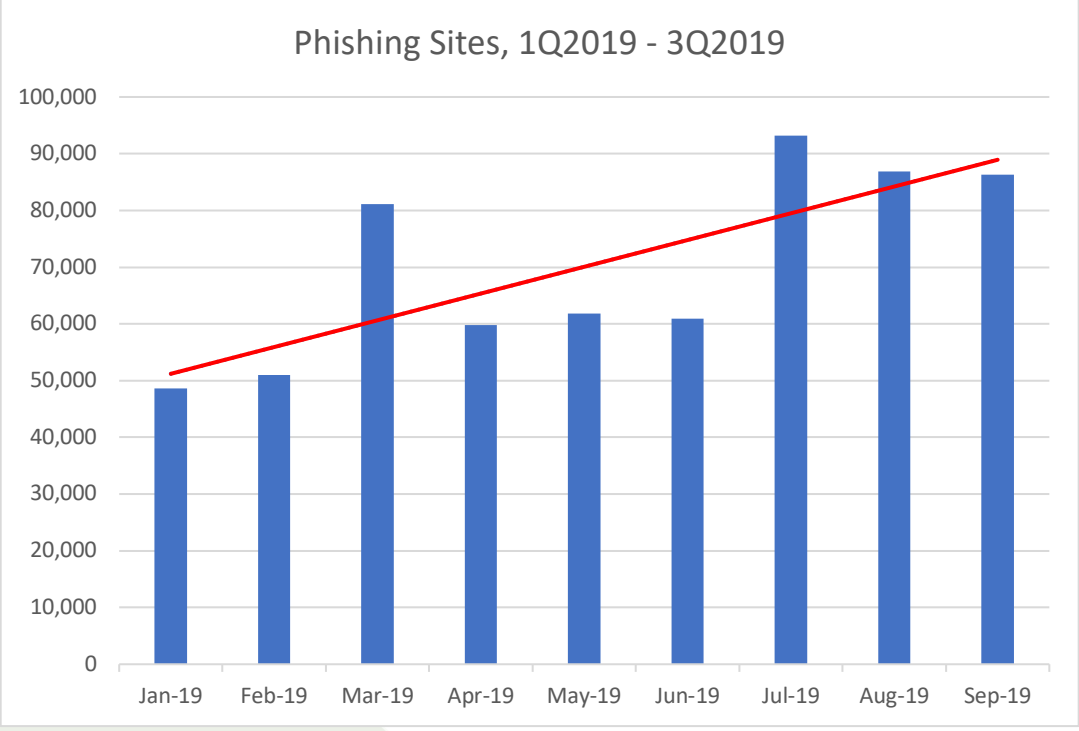
Table of Contents

Statistical Highlights for 3rd Quarter 2019

	July	August	September
Number of unique phishing Web sites detected	93,194	86,908	86,276
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	35,530	40,457	42,273
Number of brands targeted by phishing campaigns	444	414	425

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 by APWG in the third quarter of 2019 was 266,387. This was up 46 percent from the 182,465 seen in Q2, and almost double the 138,328 seen in Q4 2018.



"This is the worst period for phishing that the APWG has seen in three years, since the fourth quarter of 2016," said Greg Aaron, APWG Senior Research Fellow and President of Illumintel Inc. The APWG recorded 277,693 attacks in the fourth quarter of 2016.

In addition to the increase in phishing volume, the number of brands that were attacked by phishers in Q3 was also up notably. APWG contributor MarkMonitor saw attacks against more than 400 different brands (companies) per month in Q3, versus an average of 313 per month in Q2.

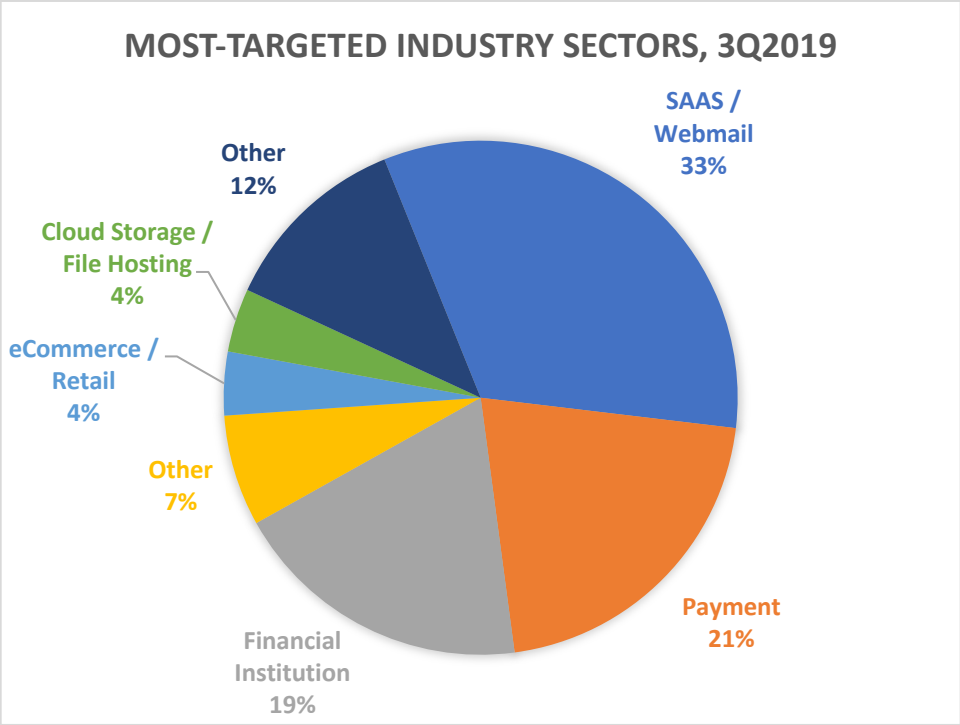
The APWG also tracks the number of unique phishing reports (email campaigns) it receives from consumers and the general public. An e-mail campaign is a unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts 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 3Q 2019 was 122,359, up from 112,163 in Q2. These were phishing emails submitted to APWG by the general public, and excludes phishing URLs reported by APWG members directly into APWG's eCrime eXchange.

Most-Targeted Industry Sectors – 3rd Quarter 2019

In the third quarter of 2019, APWG member MarkMonitor observed that SaaS and webmail sites remained the biggest targets of phishing. Phishers continue to harvest credentials to those kinds of sites, using them to perpetrate business e-mail compromises (BEC) and to penetrate corporate SaaS accounts. Stefanie Wood Ellis, Anti-Fraud Product & Marketing Manager at MarkMonitor, noted: "The top targeted industries are largely consistent with previous quarters."

Attacks against cloud storage and file hosting sites remained less popular, and attacks against the cryptocurrency, gaming, insurance, energy, government, and healthcare sectors were negligible during the third quarter.

Founding APWG member MarkMonitor is an online brand protection organization, securing intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.

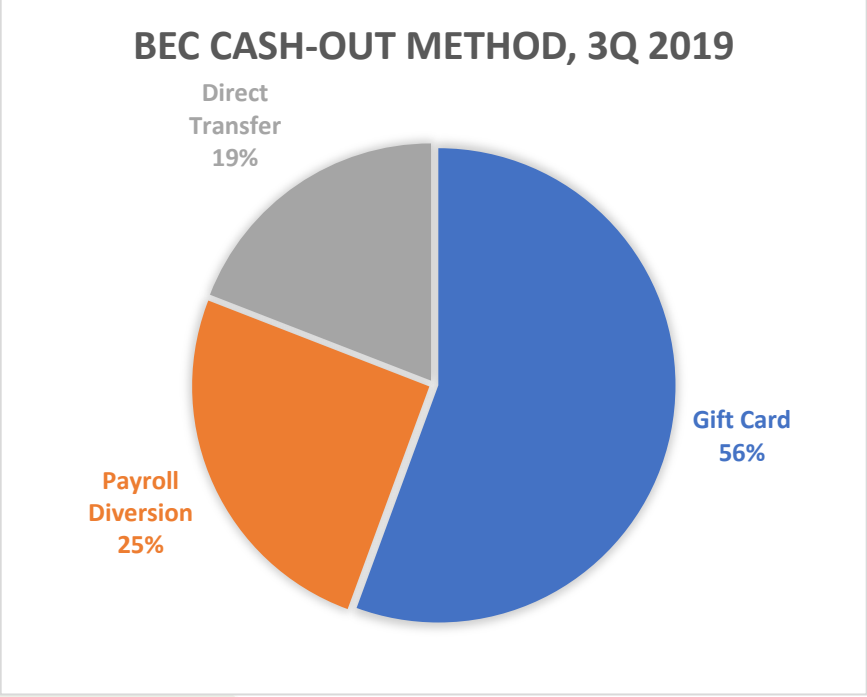


Business e-Mail Compromise, 3rd Quarter 2019

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 observed during Q3 to assemble its data set. 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 documented that scammers requested funds in the form of gift cards in 56 percent of BEC attacks during the third quarter of 2019, down from 65 percent in Q2. About 25 percent of attacks requested payroll diversions, and 19 percent requested direct bank transfers.



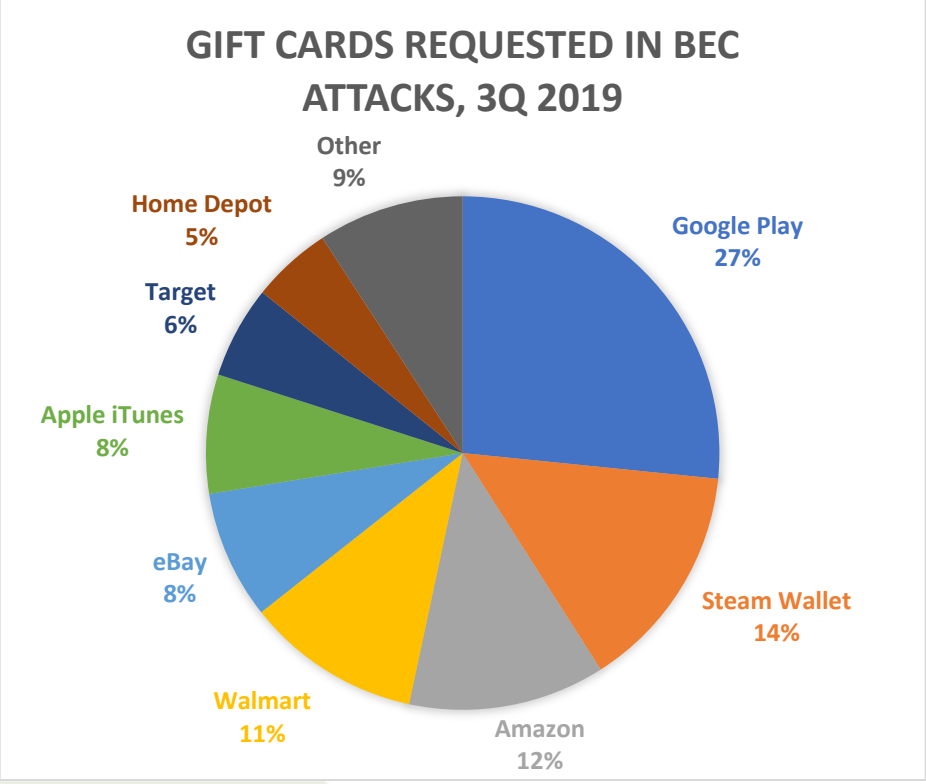
According to Crane Hassold, Agari's Senior Director of Threat Research, "Because they are more anonymous, less reversible, and do not require the help of a mule intermediary, gift cards have emerged as the most popular cash-out option for scammers."

The amount of money that an attacker can make by getting gift cards is significantly less than with a wire transfer. During Q3, the average amount of gift cards requested by a BEC actor was more than $1,500. But for wire transfer BEC attacks, the average amount requested in Q3 was over $52,000:

.

	Average	Median	Min	Max
Wire transfer requests	$52,325	$24,958	$2,530	$850,790
Gift card requests	$1,571	$1,000	$200	$8,000

By far, the most common gift card requested by BEC scammers was for Google Play, Google's online app store (27%, down from 41% in Q2). That was followed by gaming site Steam Wallet (14%) and Amazon (12%):



The share of BEC attacks sent from an account linked to a domain registered by a scammer increased slightly, from 33 percent in Q2 to 40 percent in Q3. These domains are often variations of a trusted, existing company name, meant to fool unwary victims. Free webmail accounts were used to send 54 percent of BEC attacks in Q3, but that dropped slightly from 62 percent in Q2.

Tuesday remained the most common day for BEC attacks to be sent. Almost half of BEC attacks were sent on a Monday or Tuesday, and 97 percent of attacks were sent between Monday and Friday.

The "Silent Starling" Gang

Agari has been monitoring a criminal gang it calls by the code-name *Silent Starling*. Silent Starling is comprised of three main threat actors, and has found success in compromising the email accounts of its victims. Once it breaks into a victim's email account, the members patiently gather information for weeks or months. The group consistently targets suppliers and vendors in their initial attacks, using phishing emails to encourage employees to divulge passwords, which can then be used to access the email account. Once this information is available, Silent Starling sets up a forwarding rule so the group receives copies of all emails into the account.

To read more about this criminal enterprise and its techniques, visit:
https://www.agari.com/email-security-blog/silent-starling-vendor-email-compromise/

Use of Domain Names for Phishing

APWG member RiskIQ provides ongoing analysis of where phishing is happening in the domain name system. RiskIQ analyzed 3,133 confirmed phishing URLs reported to APWG in Q3 2019. RiskIQ found that they were hosted on 1,959 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 in open, deep and dark web, mobile, and social digital channels to proactively protect organizations, brands, people, and data.

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 49% of the domain names in the world as of the beginning of Q3, and represented 65 percent percent of the phishing domains in the sample set. There were 3,316 legacy gTLDs in the sample set. Most of those were in .COM, which had 1,088 domains in the set.

- The new generic top-level domains (nTLDs), such as .WORK and .ICU, were released after 2011. At the beginning of Q2, the nTLDs represented about 6 percent of the domains in the world, and were about 7 percent of the domains in the sample set. There were 137 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 45 percent of the domains in the world as of the beginning of Q2, but were only 89 percent of the domains in the sample set of 543 ccTLD domains.

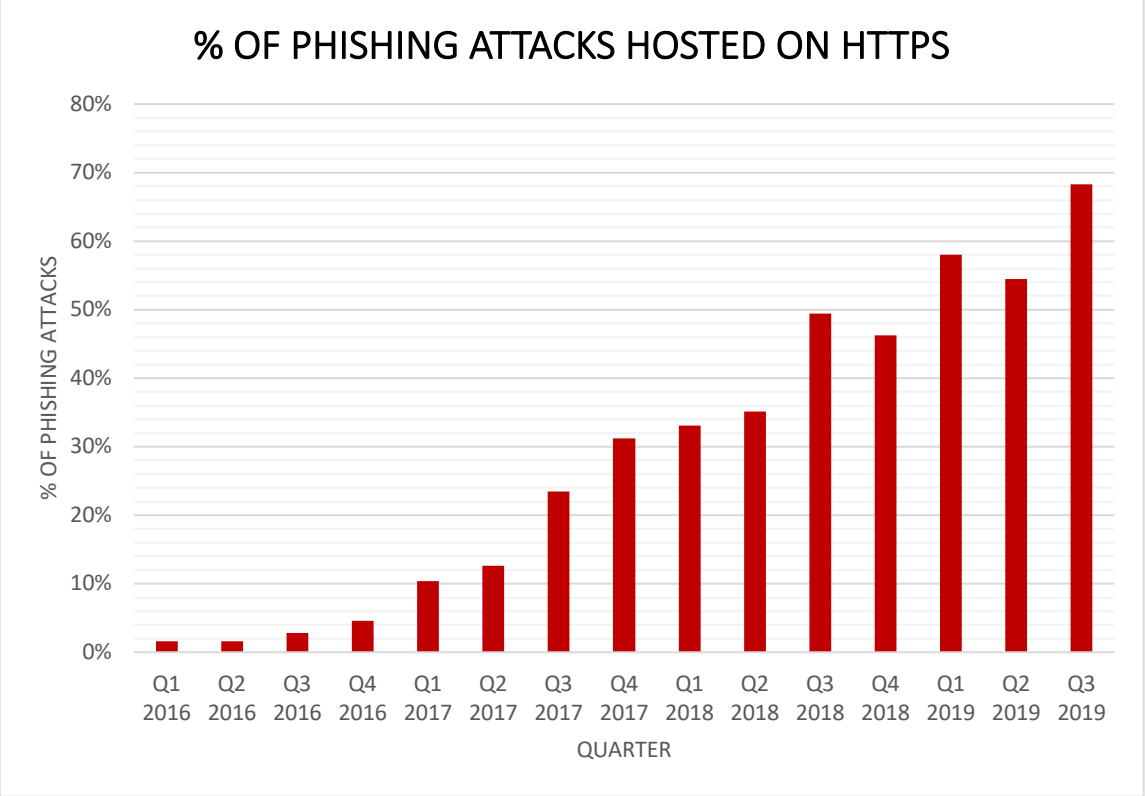
The chart below shows the TLDs that had the most unique second-level domains used for phishing. "No particular TLD stands out this quarter as having a disproportionate number of unique domains in the sample set," sais Jonathan Matkowsky, a cyber advisor at RiskIQ.

Rank	TLD / Category	# of Unique Domains in Sample Set (3Q 2019)
1	.COM / Legacy	1,088
2	.ORG / Legacy	80
3	.NET / Legacy	76
4	.BR / ccTLD (Brazil)	55
5	.GA / ccTLD (Gabon)	31
6	.INFO / Legacy	30
7	.ML / ccTLD (Mali)	27
8	.IN / ccTLD (India)	26
9	.ID / ccTLD (Indonesia)	24
9	.ICU / nTLD	24
10	.TOP / nTLD	23
10	.RU / ccTLD (Russian Federation)	23
10	.AU / ccTLD (Australia)	23
11	.XYZ / nTLD	22
11	.UK / ccTLD (United Kingdom)	22
12	.TK / ccTLD (Tokelau)	21
13	.ONLINE / nTLD	16
13	.FR / ccTLD (France)	16
14	.CF / ccTLD (Central African Rep.)	14
15	.PL / ccTLD (Poland)	13
15	.CO / ccTLD (Columbia)	13

Several of the ccTLDs above -- .GA, .ML, .TK, and .CF—are "repurposed" ccTLDs where management rights have been granted to a third party that offers domain registrations for free.

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.

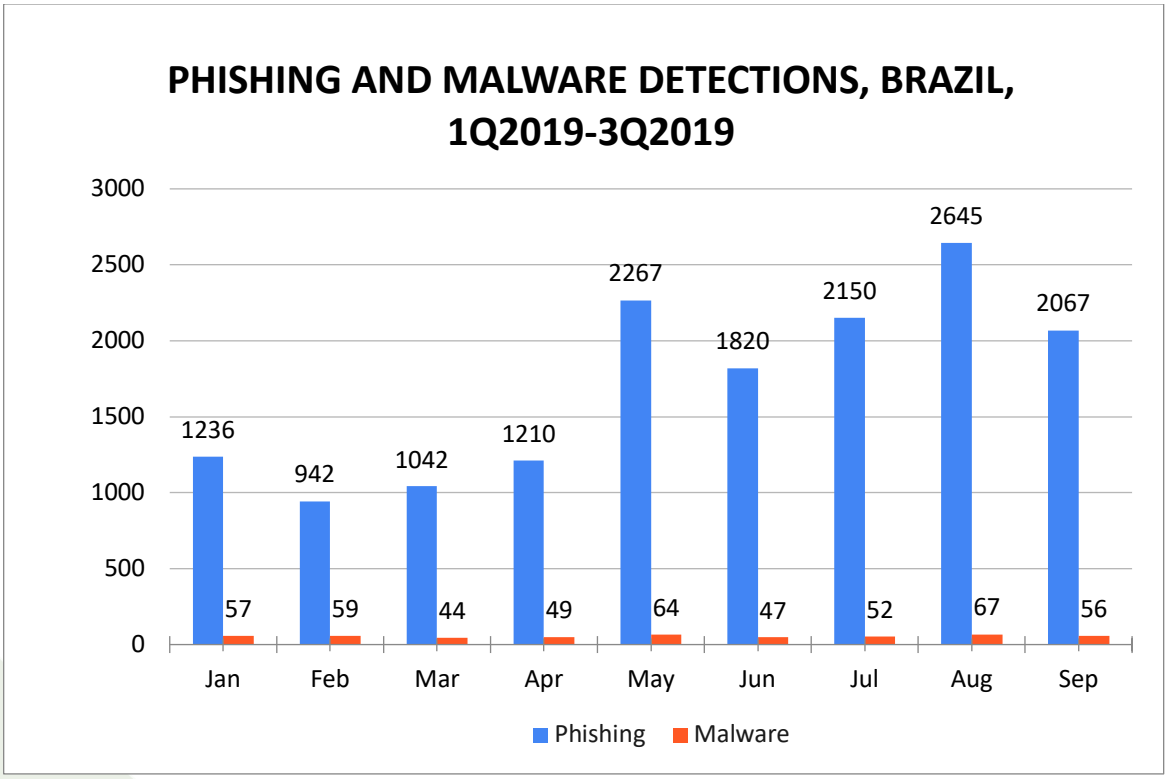


"In Q3 2019, more than two-thirds of all phishing sites - 68 percent - were using SSL. This was up from 54 percent the prior quarter," said John LaCour, PhishLabs Founder and CTO. "This is the highest number of phishing sites using SSL since we began tracking it in early 2015, and a clear indicator that users can't rely on SSL alone to indicate whether or not a site is safe."

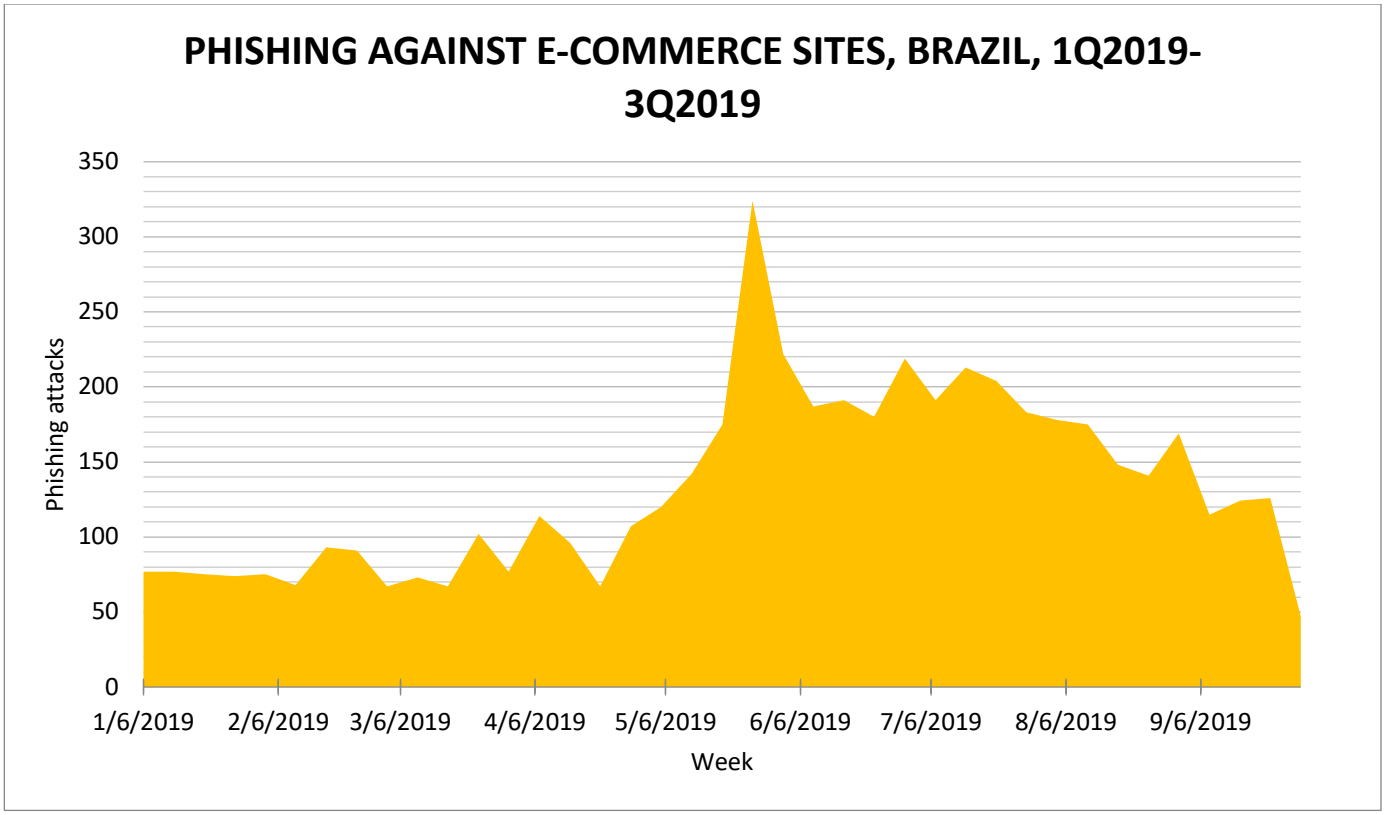
Online Criminal Activity in Brazil

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 third quarter of 2019, Axur observed 6,862 phishing attacks. That was up significantly from the 5,297 cases Axur observed in Q2, and more than *double* the 3,220 that Axur observed in Q1. Specifically, these were attacks against Brazilian brands - or against foreign services available in Portuguese in Brazil.



Thru the first three quarters of 2019, Axur saw that attacks against SaaS (Software as a Service) and Webmail services were most prevalent, confirming the global trend. The number of phishing attacks against e-commerce sites jumped in Q2 and then receded by the end of Q3:



That peak coincided with holidays such as Mother's Day (May 12) and *Dia dos Namorados,* a holiday similar to Valentine's Day celebrated on June 12. But there was no spike in phishing associated with Father's Day in Brazil (Dia dos Pais) on August 11th. Sorry, phishers—no neckties and cologne for you.

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.

MarkMonitor™

MarkMonitor, a global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

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 Markmonitor (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**