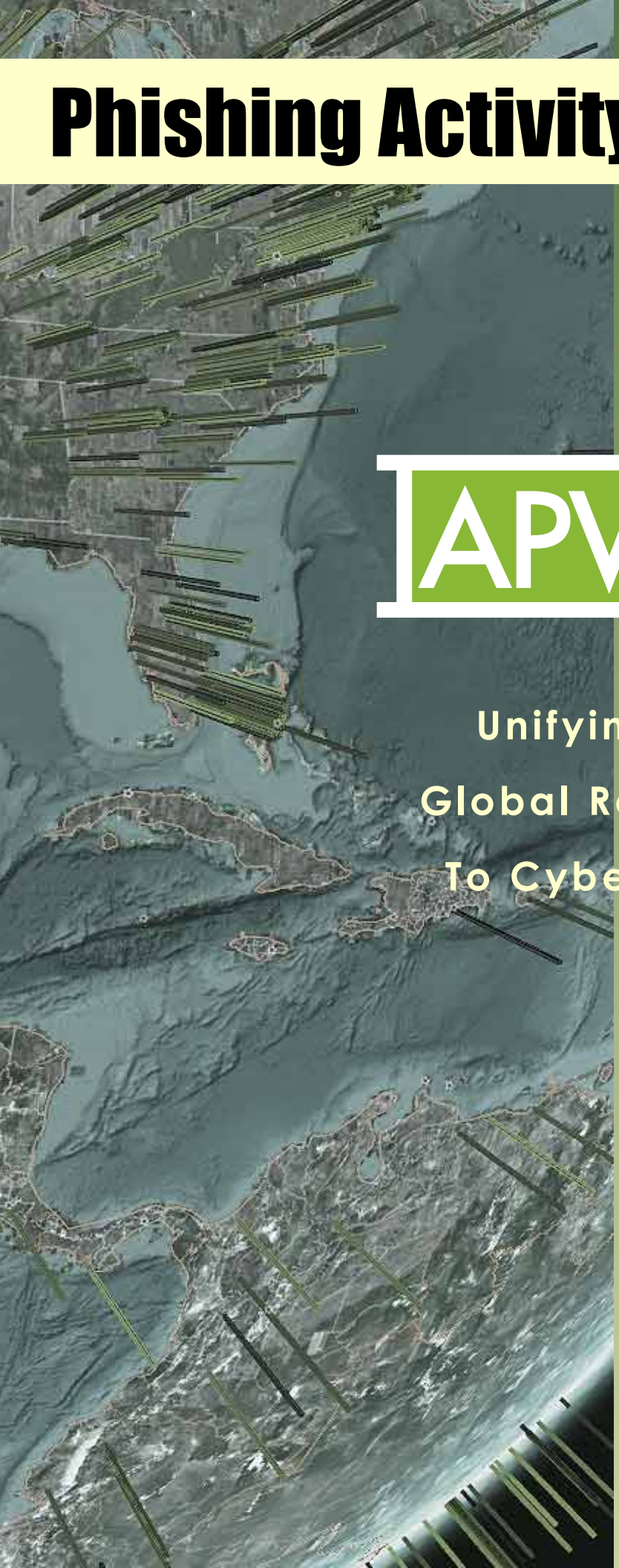
Phishing Activity Trends Report



2nd Quarter 2019

APWG

Unifying the
Global Response
To Cybercrime

Activity April-June 2019

Published September 12, 2019

Phishing Report Scope

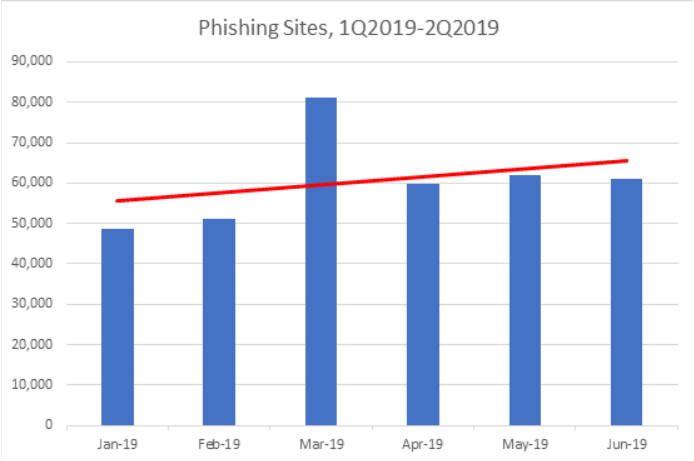
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of other methods of identity theft by drawing from the research of our member companies.

Phishing Defined

Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto computers to steal credentials directly, often using systems to intercept consumers' account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Phishing Attacks Up, Especially Against SaaS and Webmail Services



2nd Quarter 2019 Summary

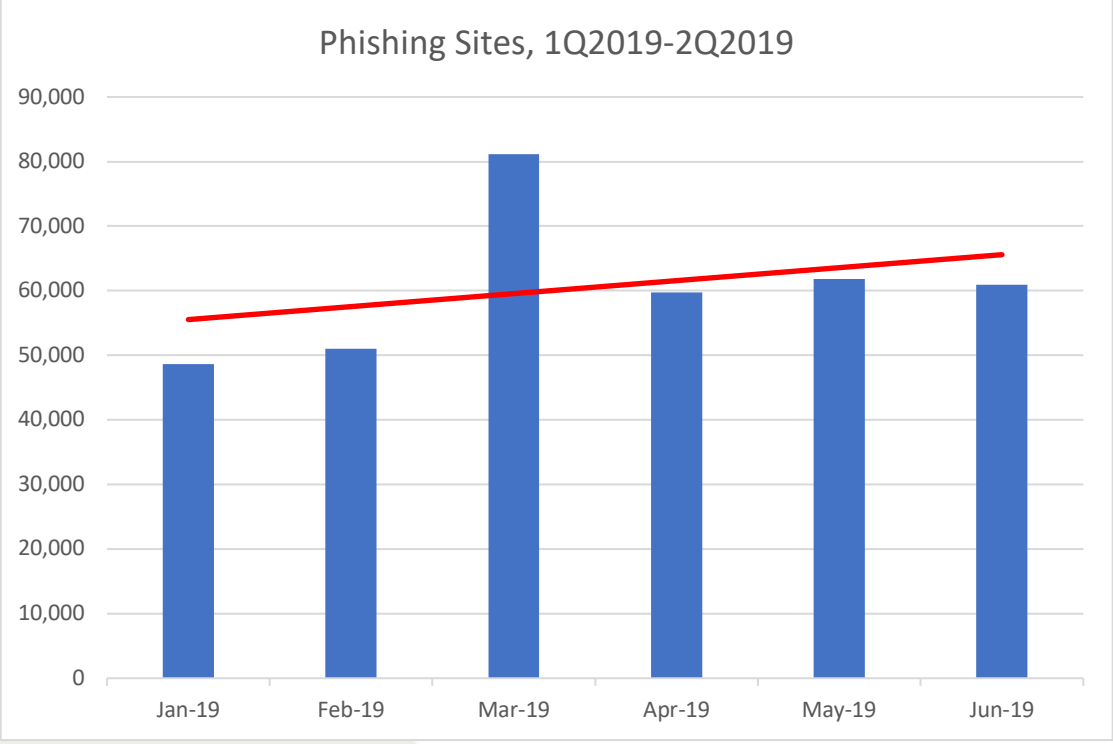
- The number of phishing attacks rose in the second quarter of 2019, eclipsing the number seen in the first quarter of 2019, and far above the amount recorded in the second half of 2018. [pp. 3-4]
- Employees should beware of requests for gift cards and payroll account changes. Gift cards were requested in 65% of business email compromise (BEC) attacks. About 20% of BEC attacks requested payroll diversions, and 15% requested direct bank transfers. The average bogus bank transfer request was for $64,717. [pp.6-9]
- Phishing that targeted Software-as-a-Service (SaaS) and webmail services continued to be biggest category of phishing. [p. 5]
- Certain top-level domains had more prevalent levels of phishing in them, while others avoided phishing. [p. 9]
- Criminals in South America used holiday shopping to take advantage of consumers. [p. 12]

Statistical Highlights for 2nd Quarter 2019

	April	May	June
Number of unique phishing Web sites detected	59,756	61,820	60,889
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	37,054	40,177	34,932
Number of brands targeted by phishing campaigns	341	308	289

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 2Q was 182,465, up slightly from the 180,768 seen in 1Q2019, and up notably from the 138,328 seen in 4Q 2018 and the 151,014 seen in 3Q 2018.



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.

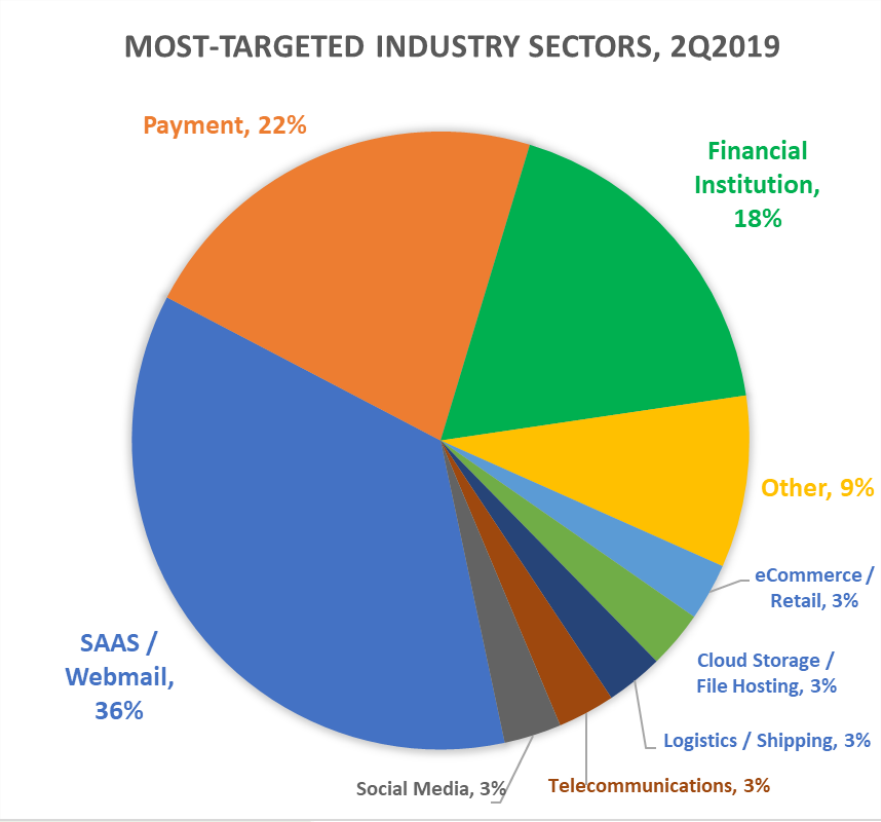
The number of unique phishing reports submitted to APWG during 1Q 2019 was 112,163, virtually the same as the 112,393 seen in 1Q. These were phishing emails submitted to APWG by the general public, and excludes phishing URLs reported by APWG members directly into APWG's eCrime eXchange.

Most-Targeted Industry Sectors – 2nd Quarter 2019

In 2Q 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: "There is an increased diversity of targets in the financial industry than in either SAAS/Webmail or Payment Services, where attacks are heavily focused on less than a dozen organizations. There was an increased diversity of targets in the financial industry, however."

Attacks against cloud storage and file hosting sites remained less popular, down from 11.3 percent of all attacks in Q1 2018 to just 3 percent in 2Q 2019. Attacks against the cryptocurrency, gaming, government, and healthcare sectors were negligible during 2Q. This is a shift from past years, when attacks against certain gaming platforms and Bitcoin-related sites were frequent occurrences.

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, 2nd 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, such as a wire transfer to a bank account controlled by the criminal. Sometimes the attacks may also involve malware. 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.

These scams target both large and small companies and organizations, and BEC attacks have caused aggregate losses in the billions of dollars. Agari examined thousands of attempted BEC attacks observed during Q2 to assemble its data set. Agari counts BEC as any response-based spear phishing attack that involves the impersonation of a trusted individual (company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive materials. Agari protects organizations against phishing, business email compromise (BEC) scams, and other advanced email threats.

Agari documented gift cards were requested in 65 percent of BEC attacks during the second quarter of 2019. Some 20 percent of attacks requested payroll diversions; 15 percent requested direct bank transfers.

According to Crane Hassold, Agari's Senior Director of Threat Research, "The most frequent cash out method sought by BEC attackers is, by a long shot, gift cards. During the second quarter of 2019, nearly two-thirds of all BEC attacks observed by the Agari Cyber Intelligence Division (ACID) requested that the target purchase gift cards and send them to the attacker. Because they are more anonymous, less reversible, and do not require the use of a mule intermediary, gift cards have quickly emerged as the most popular cash out option for scammers over the past year."

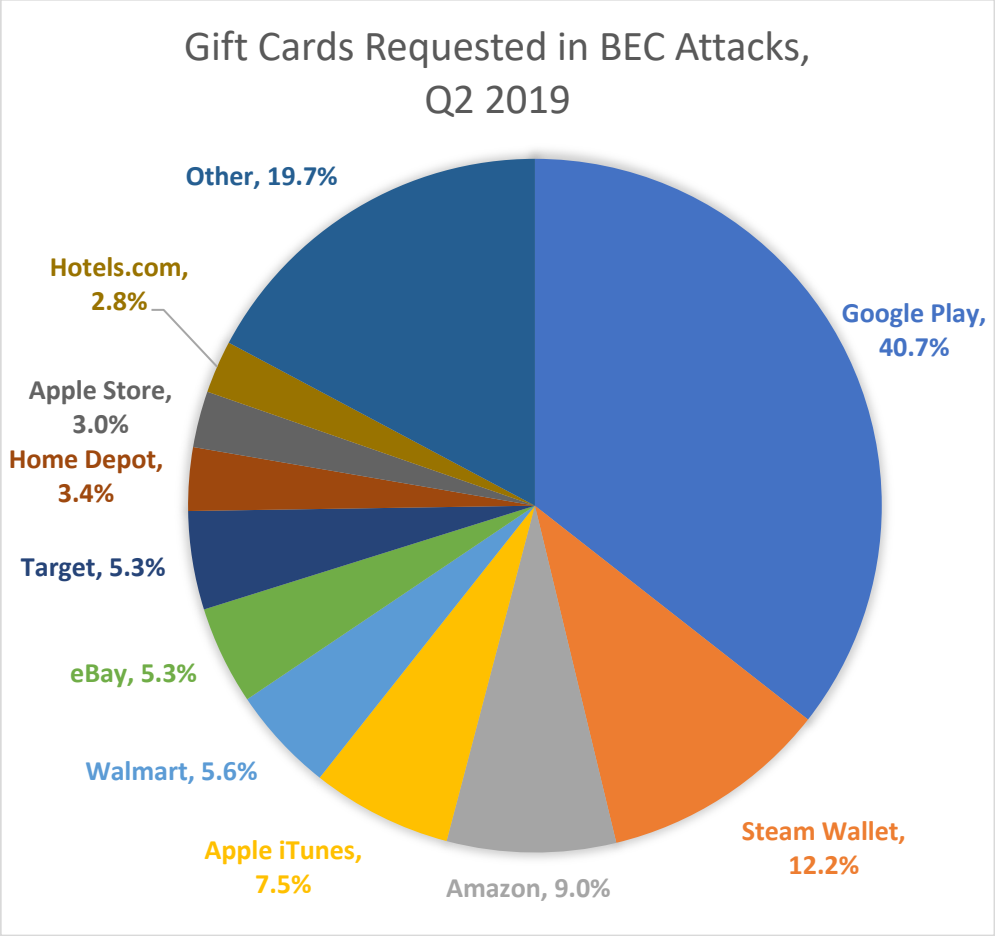
Although gift cards afford obvious benefits to BEC scammers, one of the biggest downsides is that the amount of money that an attacker can make in each gift card BEC attack is significantly less than with a wire transfer. During the second quarter, the average amount of gift cards requested by a BEC actor was just over $1,500. For wire transfer BEC attacks, the average amount requested was nearly $65,000:

.

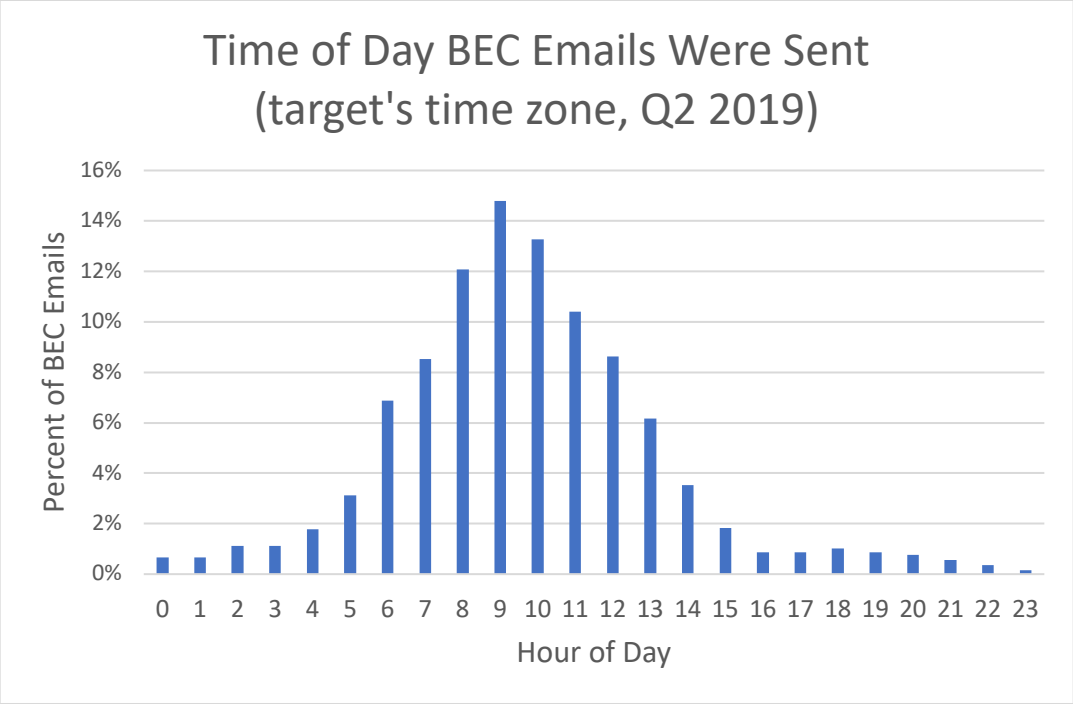
	Average	Median	Min	Max
Wire transfer requests	$64,717	$31,350	$5,000	$950,000
Gift card requests	$1,562	$1,000	$200	$6,000

Hassold added: "While there is a massive discrepancy in the amount of money that can be made per attack between these two cash-out methods, the continuous increase in the frequency of gift card BEC scams indicates that the return for these attacks outweighs the downsides."

By far, the most common gift card requested by BEC scammers was for Google Play, Google's online app store (41%). That was followed by gaming site Steam Wallet (12%), Amazon (9%), and Apple iTunes with (8%).



BEC criminals were careful to send their emails when the victims were starting their work days and could take action. Half of all BEC attacks were sent between 8:00am and 12:00pm (in the victim's time zone). Almost 90 percent of attacks were sent between 5:00am and 3:00pm (in the victim's time zone). And 97 percent were sent between Monday and Friday, avoiding weekends when victims were off of work.



Where do phishers get the tools needed to perpetrate these smaller-scale but highly targeted attacks? Sometimes, from other phishing scams. Criminals get email account usernames and passwords from traditional, mass phishing attacks. Indeed, BEC may be behind the surge in attacks against webmail and SaaS accounts. (See "Most-targeted Industry Sectors," above.) Some criminals perpetrate traditional phishing to fuel their own BEC spear phishing. Others visit online underground criminal forums and purchase credentials gathered from traditional phishing attacks, which they then use to pull off tailored spear phishing attacks and compromises.

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 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.

RiskIQ analyzed 7,633 confirmed phishing URLs reported to APWG in Q2 2019. RiskIQ found that they were hosted on 5,203 unique second-level domains (and 78 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 49% of the domain names in the world as of the beginning of Q2, and represented 64% 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 2,812 domains in the set.
- The new generic top-level domains (nTLDs), such as .ONLINE and .XYZ, were released after 2011. At the beginning of Q2, the nTLDs represented 6.5 percent of the domains in the world, and were 7 percent of the domains in the sample set. There were 356 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% of the domains in the world as of the beginning of Q2, but were only 29 percent of the domains in the sample set. There were 1,531 ccTLD domains in the sample set. ccTLD Internationalized domain names were included as part of this category; there was one of those.

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 (2Q 2019)
1	.COM / Legacy	2,812
2	.NET / Legacy	208
3	.BR / ccTLD (Brazil)	146
4	.ORG / Legacy	145
5	.UK / ccTLD (United Kingdom)	137
6	.TOP / nTLD	120
7	.INFO / Legacy	119
8	.IN / ccTLD (India)	105
9	.AU / ccTLD (Australia)	80

10	.XYZ / nTLD	63
11	.ICU / nTLD	59
12	.CL / ccTLD (Chile)	47
13	.GA / ccTLD (Gabon)	47
14	.ML / ccTLD (Mali)	43
15	.CF / ccTLD (Central African Republic)	41
16	.CO / ccTLD (Colombia)	41
17	.RU / ccTLD (Russian Federation)	38
18	.PL / ccTLD (Poland)	37
19	.ID / ccTLD (Indonesia)	36
20	.IT / ccTLD (Italy)	36

Several of the ccTLDs above -- .GA, .CF, and .ML—are "repurposed" ccTLDs where management rights have been granted to a third party that offers domain registration is free, so it is no surprise that these ccTLDs fall in the top 20.

.XYZ represented about 9 percent of all the nTLD domain names registered in the world as of the end of last quarter. But .XYZ had about 17% of the reported nTLDs domains used for phishing in the sample set. Although .ONLINE represented only 5 percent of the registered nTLD domains in the world, more than triple that percentage (~18%) of the nTLD domains in the sample were on .ONLINE second-level domains. In contrast: .SITE represented 4.5 percent of the registered nTLD domains in the world and .CLUB represented 4.7 percent, but neither .SITE nor .CLUB contained even close to 1 percent of the reported nTLD domains used for phishing.

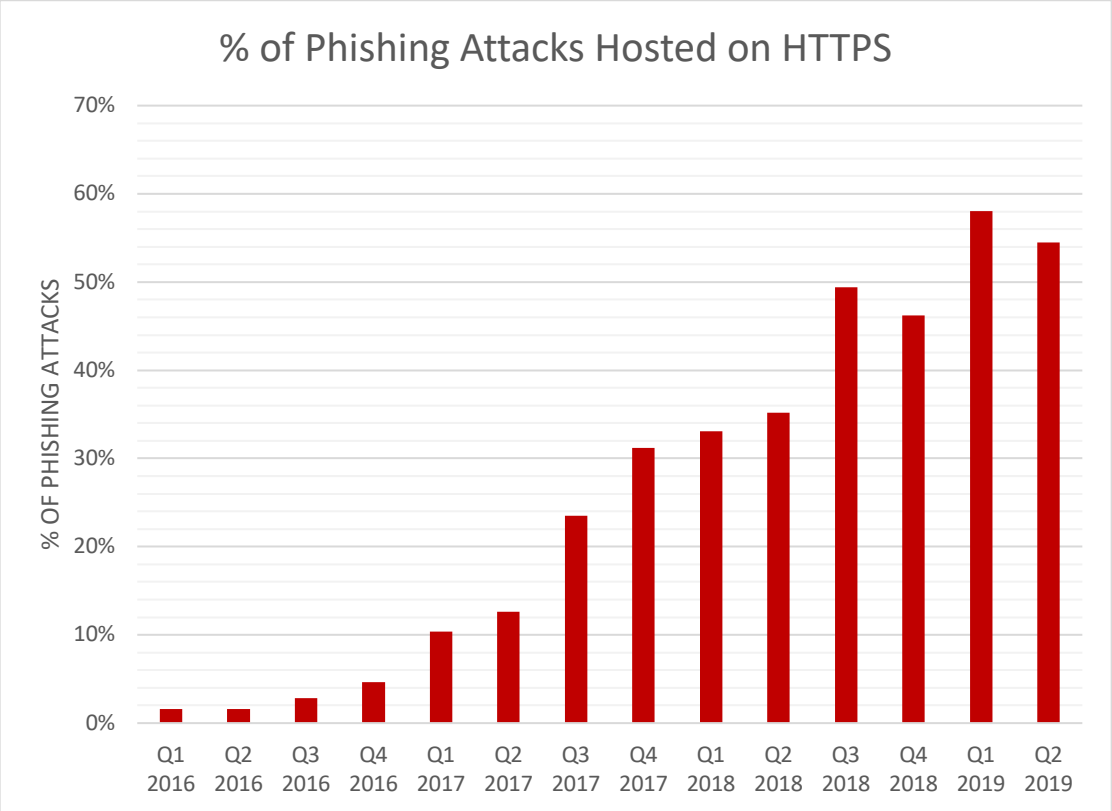
.TOP was 12.9 percent of all the nTLDs in the world as of the end of last quarter, but had only 2.3 percent of the reported phishing nTLDs in the sample set. However, more than half of the phishing domains in .TOP appeared to be randomly generated combinations of four lower-case letters and digits. It is generally understood that criminals using such algorithms in furtherance of their harmful cyber operations rely, in part, on both speed and low or free registration costs to have adequate malicious domain resources available. "It may reasonably be inferred that registrar platforms with APIs to manage and register domain names and SSL certs in bulk, and at the lowest possible cost across extensions in real-time, may be more susceptible to this kind of attempted abuse, said RiskIQ cyber advisor Jonathan Matkowsky. "Such API-driven platforms can also be used legitimately, such as by domain resellers. Part of mitigation may include raising awareness, so that those registrars whose infrastructures are being used to acquire resources in bulk for harmful cyber operations can more fully evaluate whether their anti-abuse safeguards are reasonably appropriate for this increased risk."

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.

"More than half – 55 percent – of phishing attacks detected in the second quarter of 2019 were using SSL. It is clear that users can't use SSL to know if a site is safe or not," said John LaCour, CTO of PhishLabs.

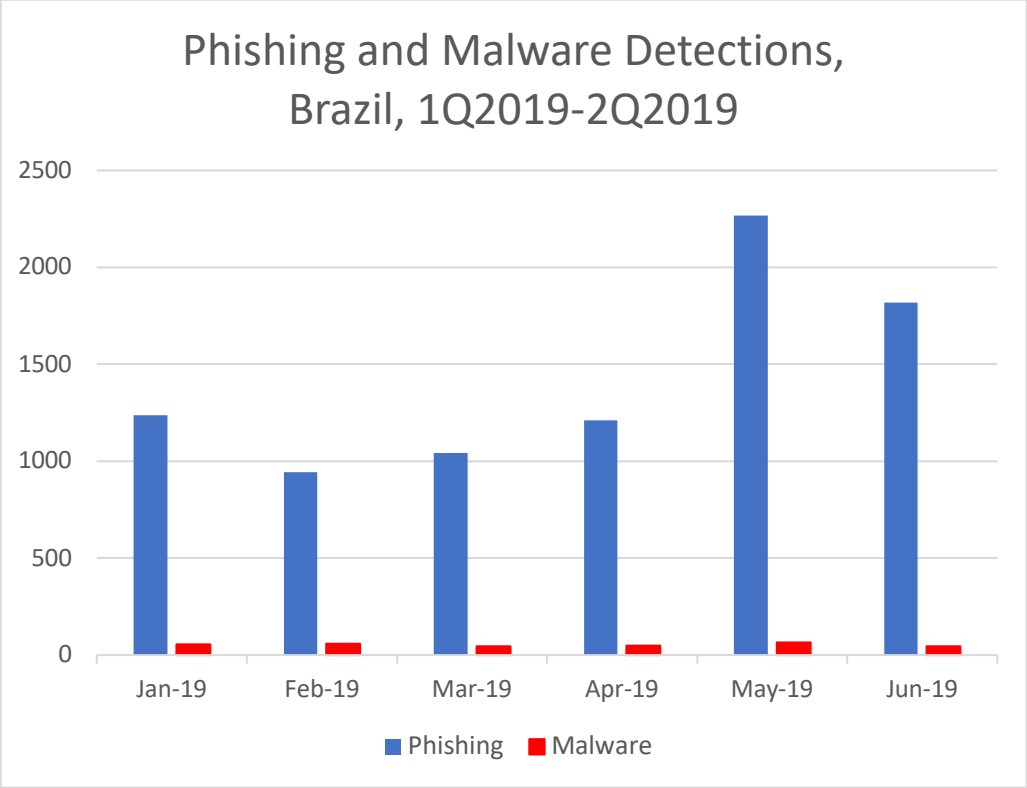
The Extended Validation SSL Certificate (EV SSL) is the most rigorous form of SSL certificate on the market, and proves the legal identity of the cert/site owner. Currently the Google Chrome, Mozilla Firefox, and Apple Safari web browsers show the verified legal identity of an EV cert owner in the browser user interface, either before or instead of the domain name. But in August 2019 Google and Mozilla announced that they plan to remove this distinction in the near future, which may effectively kill the use of EV certs. APWG will keep an eye on this development.



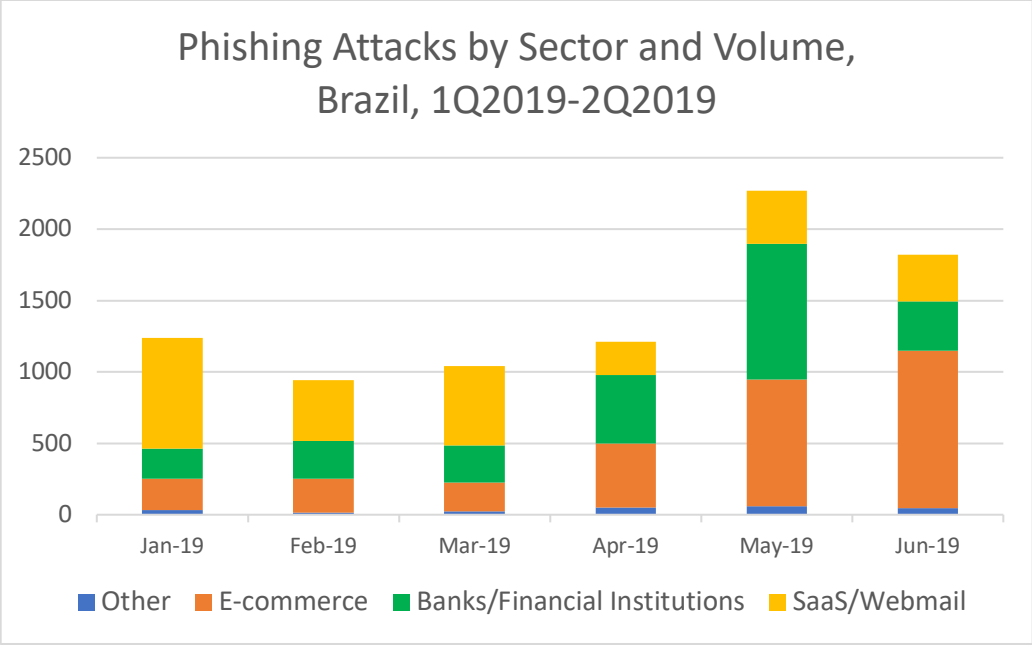
Online Criminal Activity in Brazil

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.

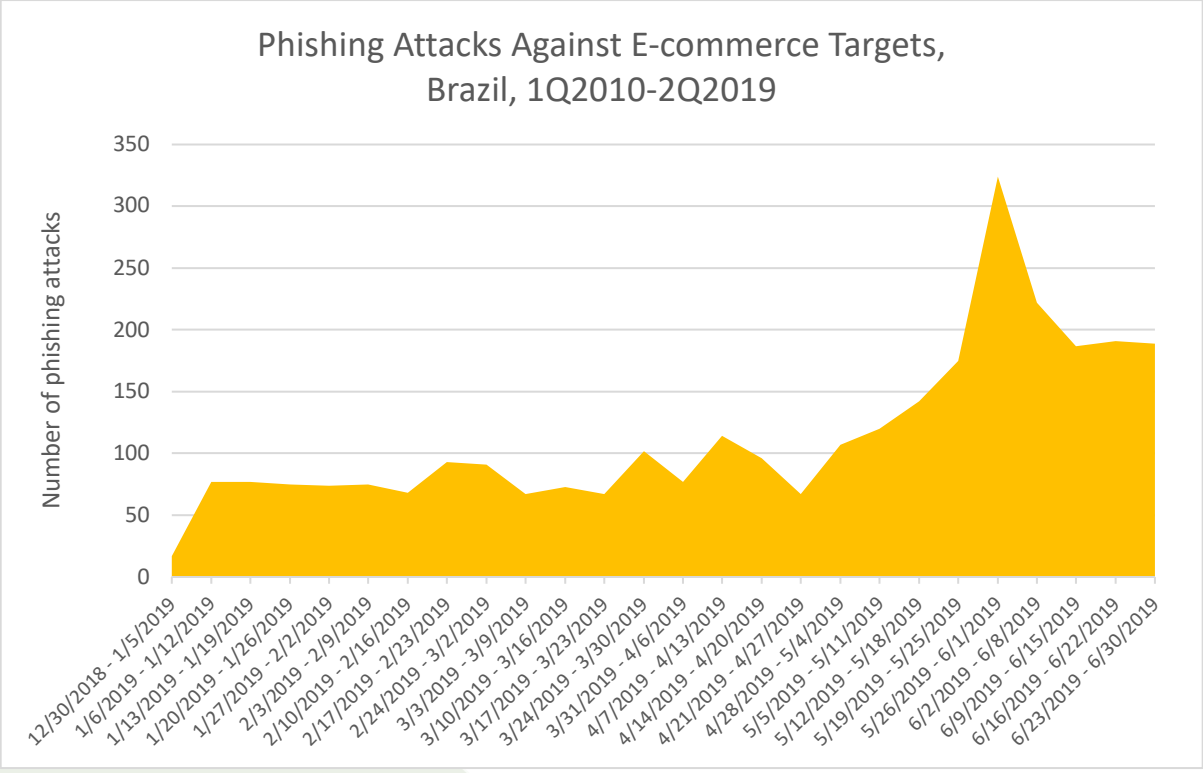
In the second quarter of 2019, Axur observed 5,297 cases of phishing – up 64 percent from the 3,220 that Axur observed in Q1. Specifically, these were attacks against Brazilian brands or against foreign services that are available in Portuguese in Brazil.



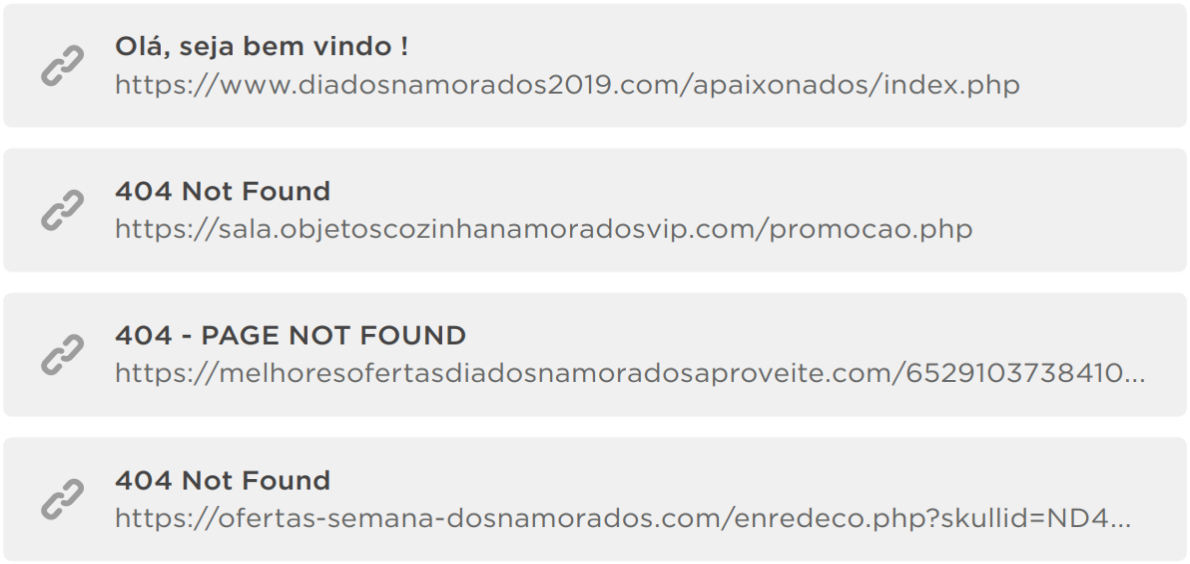
In the first quarter, the SaaS (Software as a Service) and Webmail sector was the main target of phishing attacks in Brazil, as it was also globally. However, in the second quarter in Brazil, phishing cases that were targeted to e-commerce, banks and financial institutions were the most frequent. Frauds affecting those sectors accounted for the jump in the number of phishing attacks:



Phishing attacks that targeted online retail trended upward sharply between May and June:



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. Many of the *Dia dos Namorados* attacks used maliciously registered domain names that named the holiday:



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

iThreat provides risk data, intelligence tools, and analysis to help clients protect their intellectual & Internet properties.

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

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 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, iThreat Cyber Group, www.ithreat.com