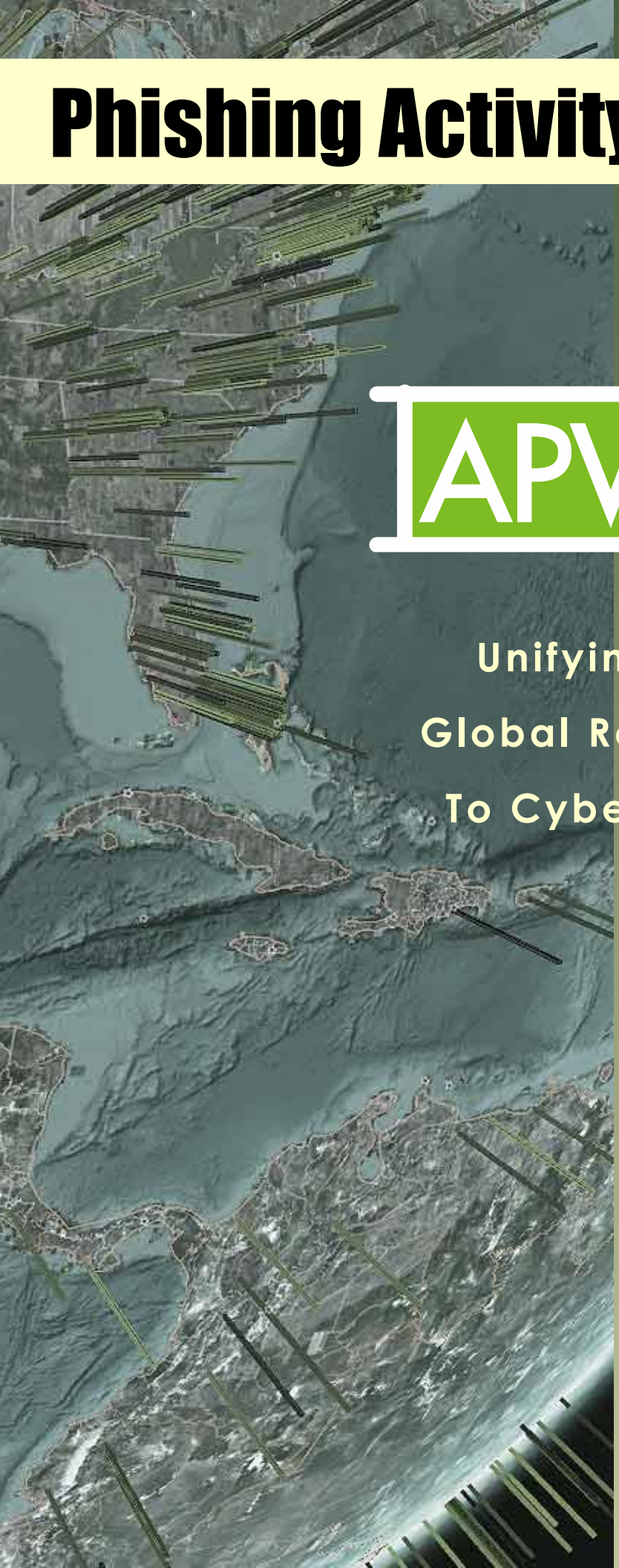
Phishing Activity Trends Report



1st Half 2017

APWG

Unifying the
Global Response
To Cybercrime

January – June 2017

Published October 17, 2017

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 crimeware 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 websites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

APWG Sees a Steady Stream of Phishing Attacks in First Half of 2017

The APWG saw a constant stream of phishing reports and confirmed attack sites in the first half of 2017. [pp. 3-4]

This Report's Phishing Activity Trends Highlights

- Several hundred companies are being targeted regularly, at least every few weeks, while a smaller number of companies are attacked intermittently. Over time a few companies fall off the lists completely, to be replaced by new and up-and-coming targets of opportunity. [p. 6]
- Phishing attacks occurred most frequently in the Payment, Financial, and Webmail sectors. [p. 7]
- There has been an increase in the number of phishing attacks using free hosting providers or website builders. [pp. 6-7]
- In the new gTLDs and in ccTLDs, much of the phishing activity was concentrated in a small number of domains. [pp. 9-10]
- Of malware incidents documented Brazil, many were spread via Facebook, and half were hosted in the United States. A few pharming incidents were documented. [pp. 11-12]

Table of Contents

Methodology and Instrumented Data Sets

The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG tracks and reports the number of unique phishing reports (email campaigns) it receives. 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 subject line in the e-mail.

The APWG also tracks the number of unique phishing websites. A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same attack destination. The number of unique attacks is usually determined by examining the URLs of the phishing sites, finding common subdirectory and URL paths, and sifting out variations. This de-duplication process is accomplished slightly differently by different industry observers who attempt to count phishing attacks, and can lead to varying attack numbers depending upon one's algorithm. For example beginning in January 2017, MarkMonitor revised its attack-counting methodology, which yielded lower attack numbers than previously.

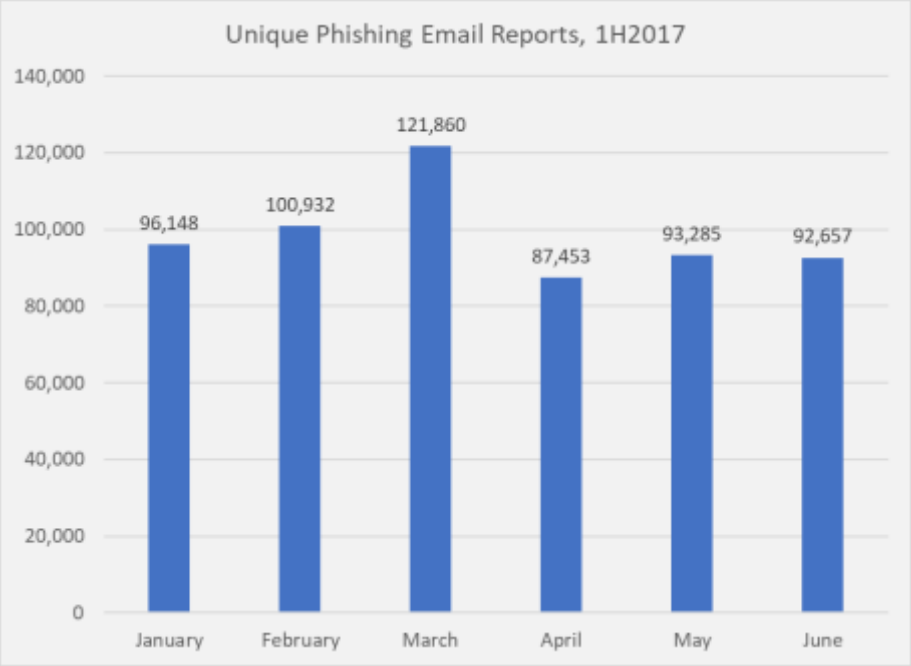
APWG additionally tracks the top-level domains used in phishing attacks, and what brands are attached (victim companies).

Statistical Highlights for 1st Half 2017

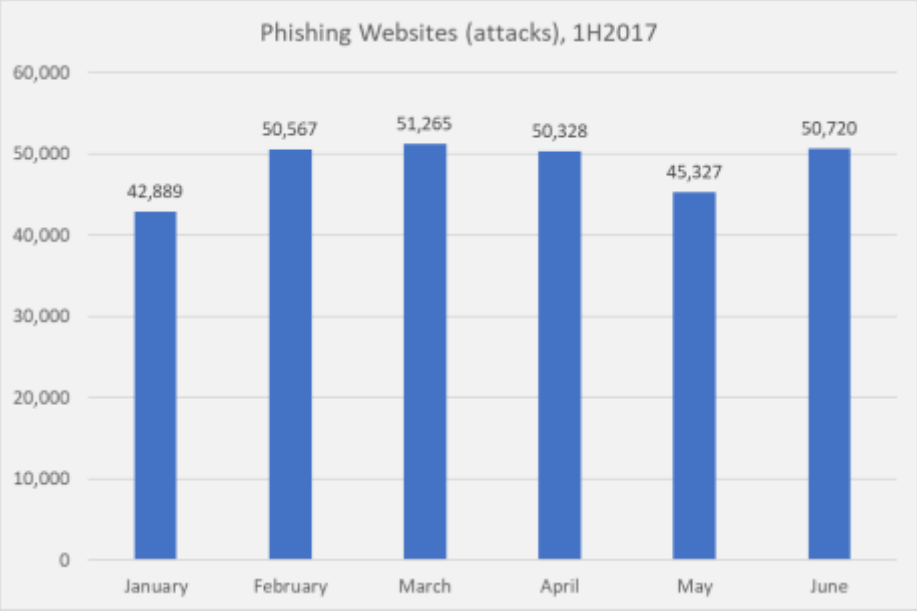
	January	February	March	April	May	June
Number of unique phishing websites detected	42,889	50,567	51,265	50,328	45,327	50,720
Number of unique phishing e-mail reports (campaigns)	96,148	100,932	121,860	87,453	93,285	92,657
Number of brands targeted by phishing campaigns	424	423	444	460	457	452
Number of domain names used in attacks	13,977	15,877	17,397	21,652	21,373	18,404

Phishing E-mail Campaigns and Phishing Site Trends – 2nd Quarter 2017

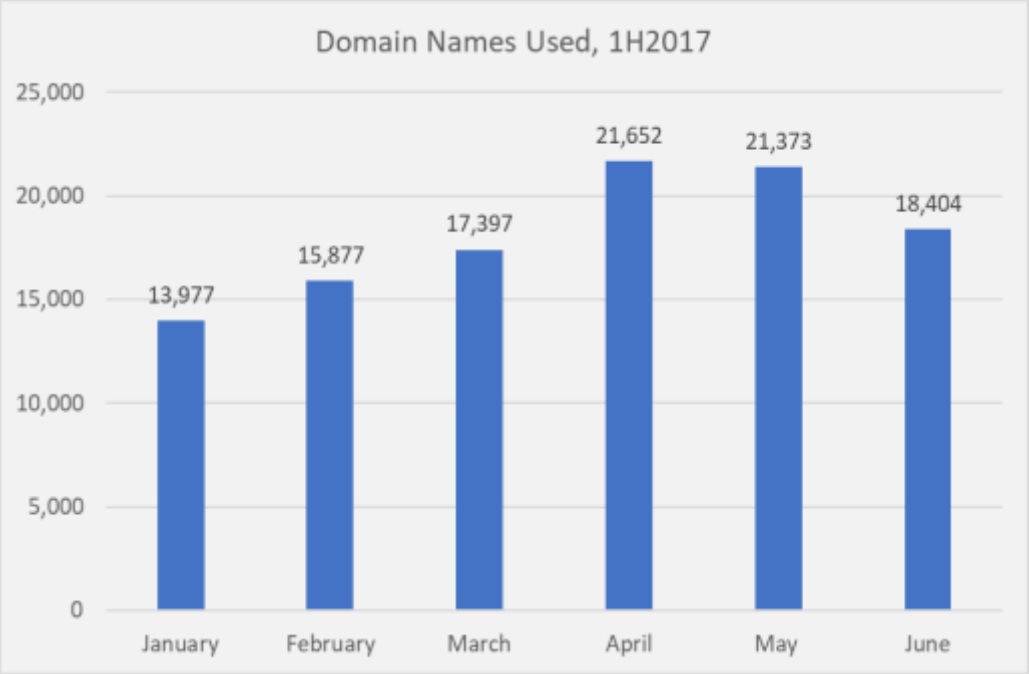
The number of unique phishing email reports (campaigns) was largely consistent from month to month, except for a 21 percent spike in March 2017:



APWG contributor MarkMonitor oberseved that the number of attacks per month was steady in the first half of 2017:

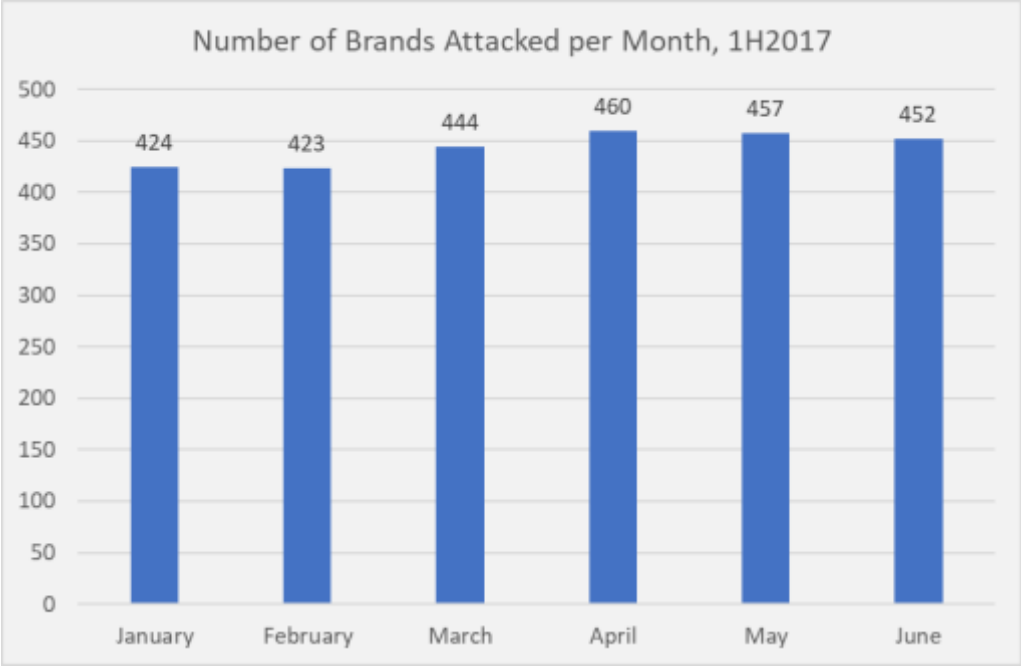


Separately, APWG contributor PhishLabs examined the confirmed phishing URLs that it oberved and counted how many unique domain names were used in the attacks. PhishLabs provides managed security services that help organizations protect against phishing attacks targeting their employees and their customers. PhishLabs found that the number of domain names used fluctuated from month to month as various phishers used different methods to create and mail out phishing URLs:



Brands and Providers Targeted by Phishing Attacks – 1st Half 2017

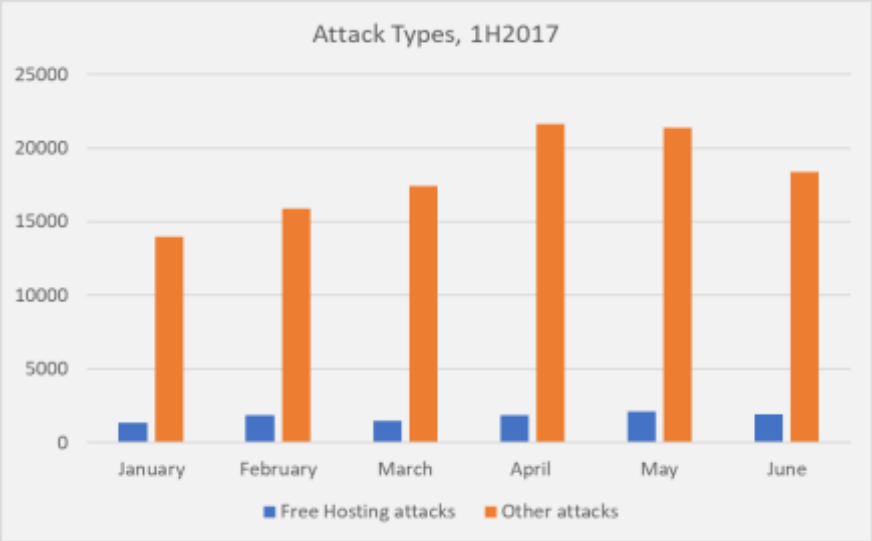
PhishLabs also tracked which brands were targeted by phishers. The number remained steady from month to month. In the second quarter, from April to June, PhishLabs saw a total 640 different, unique brands targets by phishers. This continues a years-long trend in which a few hundred companies are attacked regularly, from every few weeks to every day, while a smaller number of companies are attacked intermittently. Over time a few companies fall off the lists completely, to be replaced by new and up-and-coming targets of opportunity.



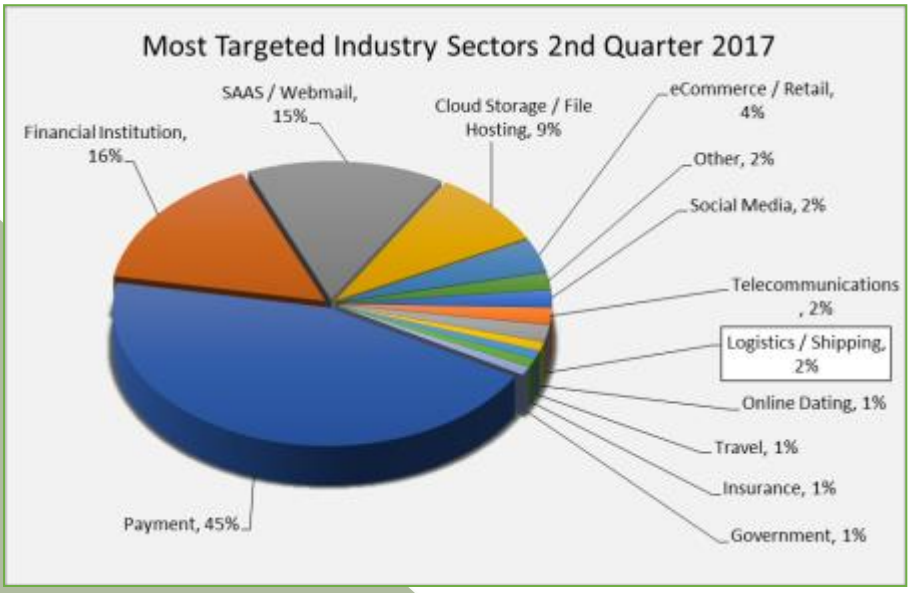
PhishLabs also examined what resources phishers chose to use. Crane Hassold, Manager of Threat Intelligence at PhishLabs noted, "There has been an increase in the number of phishing attacks using free hosting providers or website builders. These free hosts are not only easy and cheap to use, but they also allow threat actors to create subdomains spoofing a targeted brand, resulting in a more legitimate-looking phishing site. Free hosts also afford phishers additional anonymity, because these services do not make registrant information easily available. Some of the more common free hosts used by phishing threat actors include 000WEBHOST.COM, MYJINO.COM, and FREEAVAILABLEDOMAINS.COM."

As observed by PhishLabs, there were 10,544 attacks using free hosts in the first half of 2017:

	January	February	March	April	May	June
Free Hosting attacks	1,323	1,855	1,499	1,839	2,099	1,939
Other attacks	13,977	15,877	17,397	21,652	21,373	18,404



APWG contributor MarkMonitor examined the industry sectors in which it observed phishing in the second quarter. There were upticks in incidents targeting Financial Institutions, Logistics & Shipping, and Cloud Storage companies:

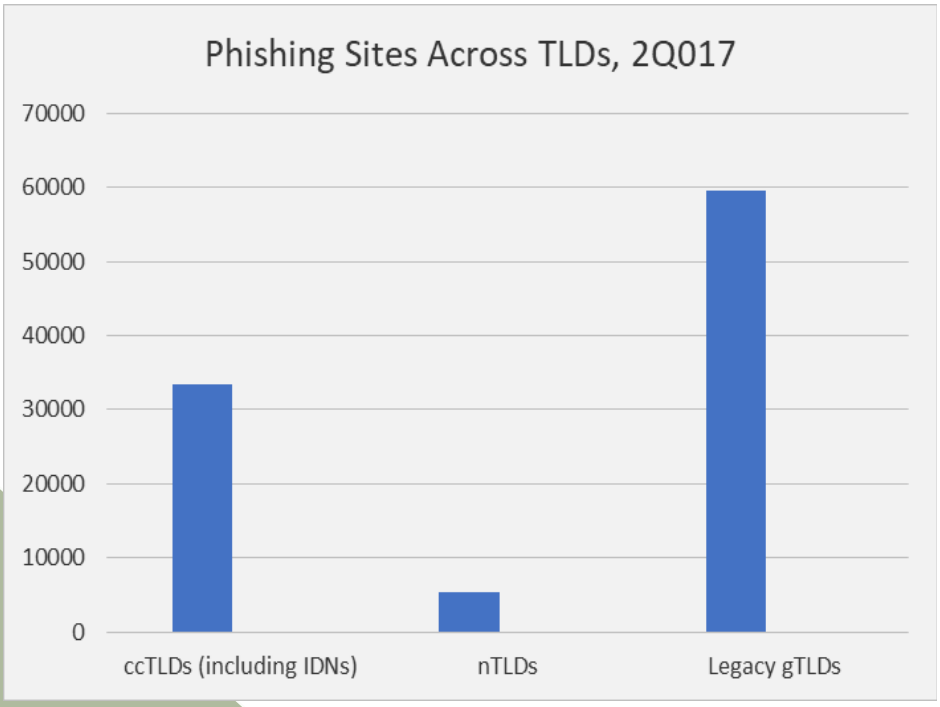


Use of Domain Names for Phishing

APWG contributor RiskIQ examined the thousands of phishing attack URLs that were submitted to the APWG's data repository in the second quarter 2017. RiskIQ monitors for code-level threats, malware, phishing, social media attacks, and fraud to protect corporate customers. RiskIQ analyzed the unique phishing URLs found, and determined which top-level domains (TLDs) the attacks were in. (Excluded in this data set's categorization schema are attacks mounted on IP addresses rather than domains; IP-based attacks were slightly over 1 percent of the total.) Some domains hosted phishing attacks that targeted multiple brands, or targeted the same brand with separate attacks taking place on the same domain (e.g., using multiple directories). Redirect services like goo.gl and bit.ly are included in the analysis.

The "ccTLD" category includes country-code top-level domains (ccTLDs), including internationalized (IDN) TLDs. The "legacy gTLDs" are the older generic domains such as .COM and .ORG that were introduced before 2013. The "new gTLDs (or "nTLDs") were introduced from 2013 to the present, and include domains such as .SCIENCE, .TOP, and .XYZ. This category includes TLDs that have registration restrictions, including ".brand TLDs" such as .HYUNDAI and .HERMES. Like any others, domains in these TLDs can be compromised (hacked) by phishers.

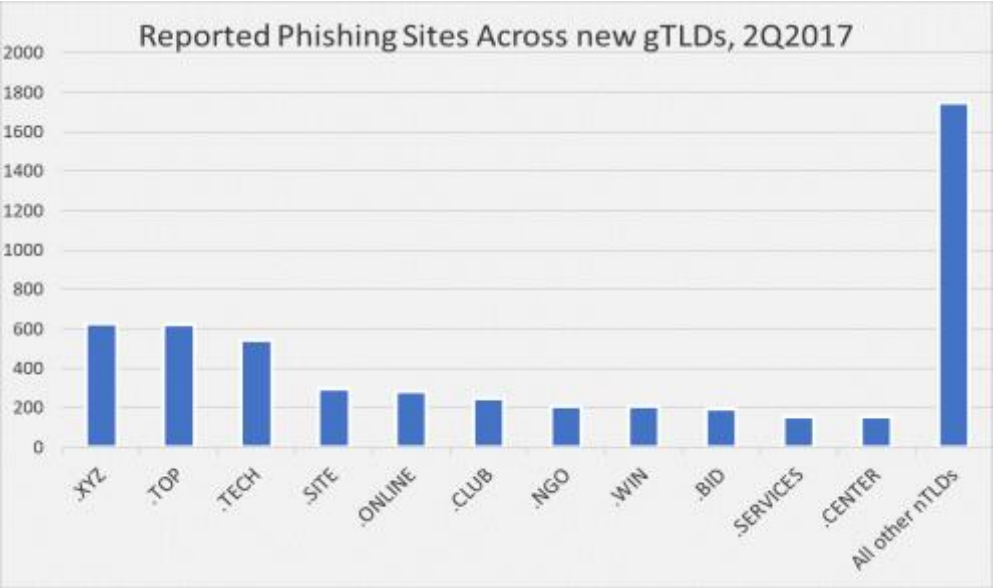
RiskIQ observed that 34 percent of the phishing sites reported to APWG during the second quarter of 2017 were hosted within ccTLDs. Legacy gTLDs accounted for 61 percent of phishing sites, and nTLDs hosted 5 percent of phishing sites.



RiskIQ then took a closer look at the ccTLDs, where RiskIQ observed 28,164 phishing attacks. About 18 percent of all phishing attacks in ccTLDs were concentrated at a set of TLDs that are under common control. They are operated by a Netherlands-based company called Freenom, which offers free domain registrations in these repurposed ccTLDs: .TK, .ML, .GA, .CF, and .GQ. The other ccTLDs below are each managed by different operators:

UK (.UK) is one of the largest ccTLDs, but had a lower volume of phishing than would be expected. Brazil (.BR) continues to have a significantly larger volume of phishing compared to other ccTLDs. However, NIC.BR, the registry operator, has a security and incident response (CERT.BR) team that performs incident handling and is actively engaged in security training and awareness. Phishing in .IN, the ccTLD of India, remains a problem. India does have incident and vulnerability reporting mechanisms through its Indian Computer Emergency Response Team. Phishing in .KE, the TLD of Kenya, also remains high.

In the new gTLDs, significant phishing activity clustered in a small number of domains:



.TECH had a higher concentration of phishing sites than would be expected, considering the number of domains in the TLD. RiskIQ's investigation found that this was because a hosting provider in the Russian Federation was allowing its customers to create sub-domains on the hosting provider's domain name. This offered miscreants the opportunity to target multiple brands across a variety of industries.

Phishing and Identity Theft Techniques in Brazil

APWG research contributor 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 2017, Axur observed nearly 8,0000 fraud nexuses that targeted Brazilian companies and individuals:

Type	Description	April	May	June	Total
Malware C&C	Malware command and control servers	72	73	5	**150**
Malware	Malware distribution URLs	174	63	57	**294**
PAC	Proxy Auto Configuration files that setup the user's browser to access fraudulent websites	2	0	8	**10**
Paid Search Phishing	Paid ads with phishing in Google and Bing	1	2	0	**3**
Pharming	Rogue DNS	3	2	10	**15**
Phishing	Phishing	76	158	189	**423**
Malicious proxy servers	Malicious proxy servers	4	0	3	**7**
Redirect	Redirection URLs	135	43	45	**223**
Social Media Scams	Scams on social media platforms (FB, Instagram, LinkedIn, Youtube, blogs, etc.)	1,047	1,259	841	**3,147**
Scam Web sites	Scams on websites in general	499	1,015	1,177	**2,691**
Mobile App Scam	Apps with unauthorized brand use in official stores (iTunes + Google Play) as well as .apk files in websites.	426	268	333	**1027**
Total		**2,439**	**2,883**	**2,668**	**7,990**

"In the second quarter of 2017, we detected 150 C&Cs (malware command and control servers) , 294 malware distribution sites, and 15 pharming incidents," said Fabio Ramos, CEO of Axur. "On average, each malware targeted three companies, and each pharming incident targeted two targets. The maximum number of targets for a single piece of malware was 23, while one pharming attack targeted six companies. The targeted companies were usually from the financial sector: banks and credit card companies."

Of the 7,990 incidents reported, many were spread via Facebook. Half were hosted in the United States, followed by Brazil, as identified by ASN (autonomous system number, or network):

Country\month	April	May	June	Total
United States	1,,313	1444	1,269	**4,026**
Brazil	631	393	475	**1,499**
Ireland	315	311	221	**847**
Canada	43	36	78	**157**
Germany	25	38	41	**104**
France	33	35	4	**72**
Czech Republic	7	19	18	**44**
Argentina	30	1	1	**32**
Netherlands	2	7	11	**20**
Virgin Islands, British	10	4	5	**19**
Others	30	595	545	**1170**
Total	**2,439**	**2,883**	**2,668**	**7,990**

When targeting Brazilians, the fraudsters often block access to the fraud from IP addresses outside of Brazil. The goal is make it more difficult for response teams at the ISPs (most of which are outside of Brazil) from viewing the active fraud. They sometimes also block the IPs of the target company (a bank, for instance) so the victim company's security team will think the fraud is offline. The IP filters are usually set up through the .htaccess file, inserting rules that allow traffic only from Brazilian IP ranges.

Type of incident, Q2 2017	No IP Filter	IP Filtered	Total	% per type
Malware C&C	150		150	**0%**
Malware	226	68	294	**23%**
PAC	9	1	10	**10%**
Paid Search Phishing	3		3	**0%**
Pharming	15		15	**0%**
Phishing	315	108	423	**26%**
Malicious Proxy Server	7		7	**0%**
Redirect	169	54	223	**24%**
Social Media Scams	3171		3171	**0%**
Scam Website	3694		3694	**0%**
Total	**7759**	**231**	**7990**	**3%**

APWG Phishing Activity Trends Report Contributors

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 its 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 24/7 managed security services that help organizations protect against phishing attacks targeting their employees and customers.

RiskIQ is a digital threat management company enabling organizations to discover, understand and mitigate known, unknown, and malicious exposure across all digital channels

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 at +1.404.434.7282 or foy@apwg.org. For media inquiries related to the company-content of this report, please contact APWG Secretary General Peter Cassidy at +1.617.669.1123; Stefanie Ellis at Stefanie.ellis@markmonitor.com; Fabricio Pessôa of Axur at +55.51.30122987, fabricio.pessoa@axur.com; Stacy Shelley of PhishLabs,at 1.843.329.7824, stacy@phishlabs.com.

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, 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, was founded by Tumbleweed Communications, financial services institutions and e-commerce providers. APWG's first meeting was 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.

Analysis by Greg Aaron, iThreat Cyber Group; editing by Ronnie Manning, Mynt Public Relations.