Phishing Activity Trends Report

3rd Quarter 2018

APWG

Unifying the
Global Response
To Cybercrime

Activity July – September 2018

Published December 11, 2018

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 Web sites 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 Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Criminal Innovation Ramps Up With Phishing Attacks in 2018

After spiking in the spring, phishing has been taking place at steady pace—but phishers are using new techniques to carry out their attacks and to conceal them.

3rd Quarter 2018 Phishing Activity Trends Summary

- Phishing that targeted cloud storage and file hosting sites fell, while phishing against payment processors and banks remained high. [p. 5]
- Phishing remains most prevalent in the old, large gTLD .COM. But phishing is higher than normal in the new gTLDs and in repurposed ccTLDs. [pp. 6-7]
- Phishers are increasingly using web page redirects as a way of hiding their phishing sites from detection. [p. 4]
- Half of all phishing attacks are now hosted on Web sites that have HTTPS and SSL certificates. [p.6]
- In Brazil, phishers turned away from attacking e-commerce sites, and concentrated on attacking banks and their customers. [p.9]

Statistical Highlights for 3rd Quarter 2018

	July	August	September
Number of unique phishing Web sites detected	52,613	44,855	53,546
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	93,078	89,323	88,156
Number of brands targeted by phishing campaigns	231	260	286

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 Web sites. This is now 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.) APWG's contributing members also track a variety of additional metrics and data sets in order to track the fast-paces nature of cybercrime.

Phishing Site and Phishing E-mail Trends – 3rd Quarter 2018

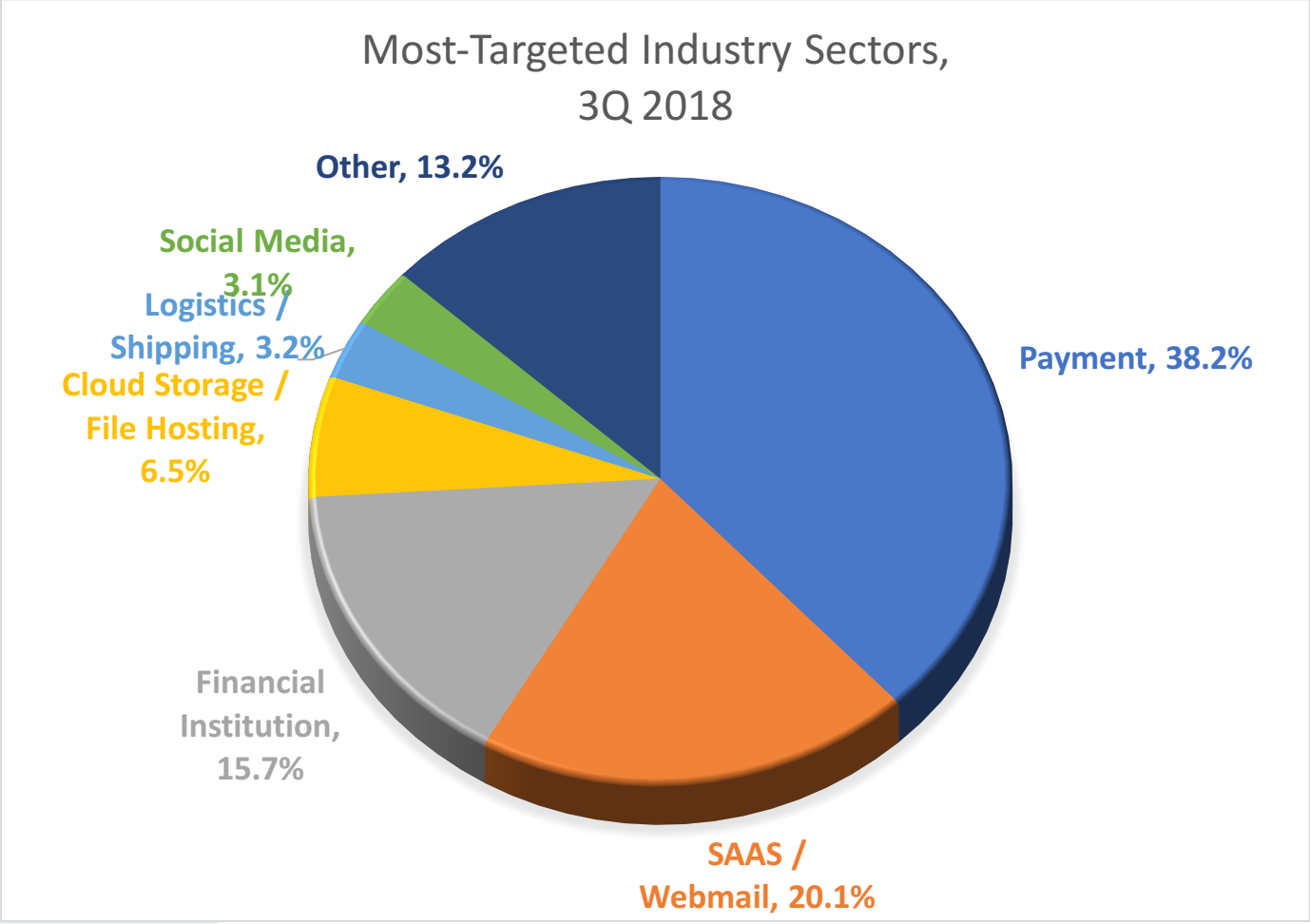
The total number of phish detected by APWG in Q3 2018 was 151,014. This was down from 233,040 in Q2 and 263,538 in Q1. There was an unusual rash of phishing in the spring of 2018, and the amount of phishing in Q3 was closer to the levels seen thru 2017.

"Detections were flat over the summer months, June through September" said Stefanie Ellis, Anti-Fraud Product Marketing Manager at MarkMonitor. "However, MarkMonitor is detecting an increase in the use of redirectors, placed both prior to the phishing site landing page and then following the submission of the credentials as well. This obfuscation technique is an effort by the phishers to hide the phishing URL – most notably from detection via web server log referrer field monitoring."

The number of unique phishing reports submitted to APWG during 2Q 2018 was 264,483, almost the same as the 262,704 seen in Q2 2018:

Most-Targeted Industry Sectors – 3rd Quarter 2018

APWG member MarkMonitor saw phishing that targeted cloud storage and file hosting sites dropped from 11.3 percent of all attacks in Q1 2018, to 9 percent in Q2, and down to 6.5 percent in Q3. In the meantime, payment processing firms remained the most-targeted companies, followed by the banking sector. 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.



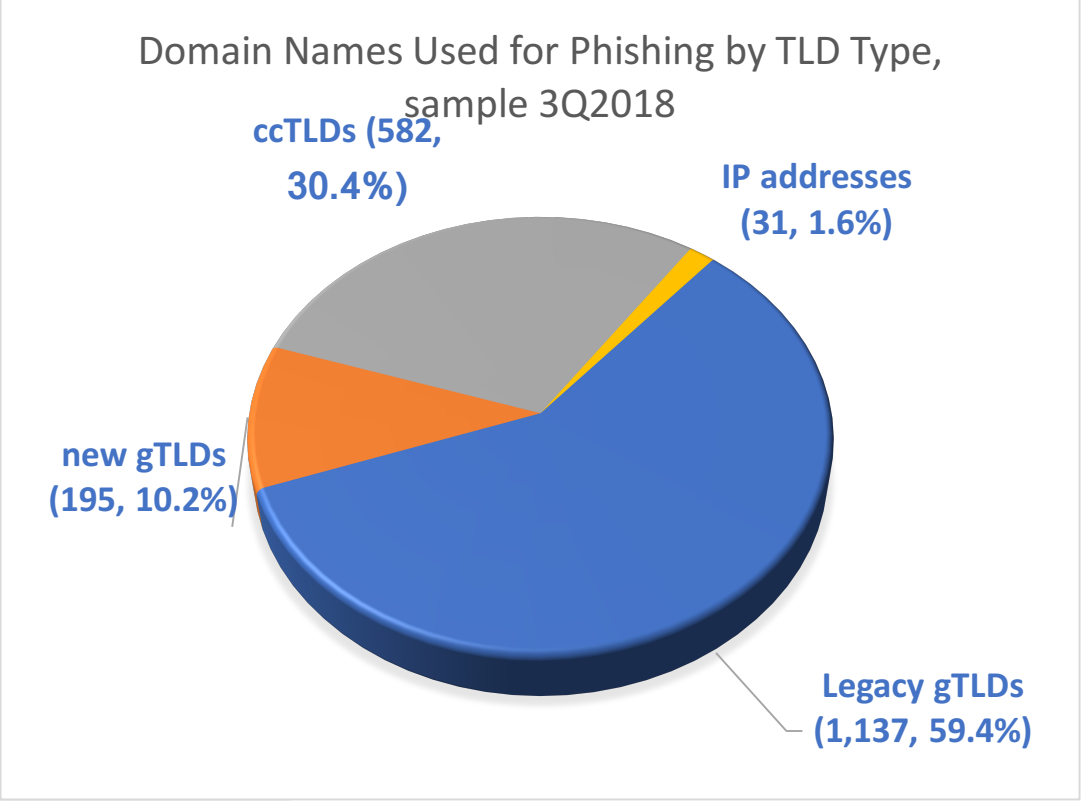
The 286 brands targeted in September 2018 was the most seen in a month since November 2017, but below the 325 brands targets in mid-2017.

Use of Domain Names for Phishing

APWG member RiskIQ monitors for code-level threats, malware, phishing, social media attacks, and fraud to protect corporate customers. RiskIQ analyzed a random sampling of 3,378 confirmed phishing URLs reported to APWG in Q3 2018, and found that they were hosted on 1,914 unique second-level domains (and 31 were hosted on IP addresses, without domains). Those domains were in 139 different top-level domains (TLDs).

There are three types of top-level domains:

- The legacy generic TLDs (such as .COM, .ORG, and .INFO, all released before 2008). They represent 49.9 percent of the domain names in the world, and represented 59.4 percent of the phishing domains in the sample set. Most of these were in .COM, which had 922 domains in the set. There were 12 legacy gTLDs in the sample set.
- The new generic top-level domains (nTLDs, such as .TOP and .ACCOUNTANT, all released after 2011). The nTLDs represent 7 percent of the domains in the world, and were 10.2 percent of the domains in the sample set. There were 43 nTLDs in the sample set.
- The country code domains (ccTLDs, such as .UK for the United Kingdom and .MX for Mexico). ccTLDs are 43.1 percent of the domains in the world, and were 30.4 percent of the domains in the sample set. There were 84 ccTLDs in the sample set.



Use of Domain Names for Phishing

The top 20 TLDs used were:

Rank	TLD	Type of TLD	Number of unique domains used for phishing in study set
1	.com	legacy gTLD	922
2	.org	legacy gTLD	80
3	.net	legacy gTLD	78
4	.pw	ccTLD (Palau)	53
5	.info	legacy gTLD	43
6	.br	ccTLD (Brazil)	41
7	.xyz	new gTLD	30
8	.ml	ccTLD (Mali)	28
9	.ru	ccTLD (Russia)	28
10	.in	ccTLD (India)	24
11	.tk	ccTLD (Tokelau)	24
12	.ga	ccTLD (Gabon)	23
13	.uk	ccTLD (United Kingdom)	23
14	.cf	ccTLD (Central African Republic)	22
15	.gq	ccTLD (Equatorial Guinea)	22
16	.au	ccTLD (Australia)	20
17	.top	new gTLD	20
18	.business	new gTLD	17
19	.agency	new gTLD	15
20	.co	ccTLD (Colombia)	15

Many of the ccTLD that have notable amounts of phishing in them are "repurposed" ccTLDs – domains where management rights have been granted to third parties who have then commercialized the TLDs. .TK, .ML, .GA, .CF, and .GQ are all operated by a Dutch company that offers domain names in those TLD for free, while .PW is operated by a company based in India.

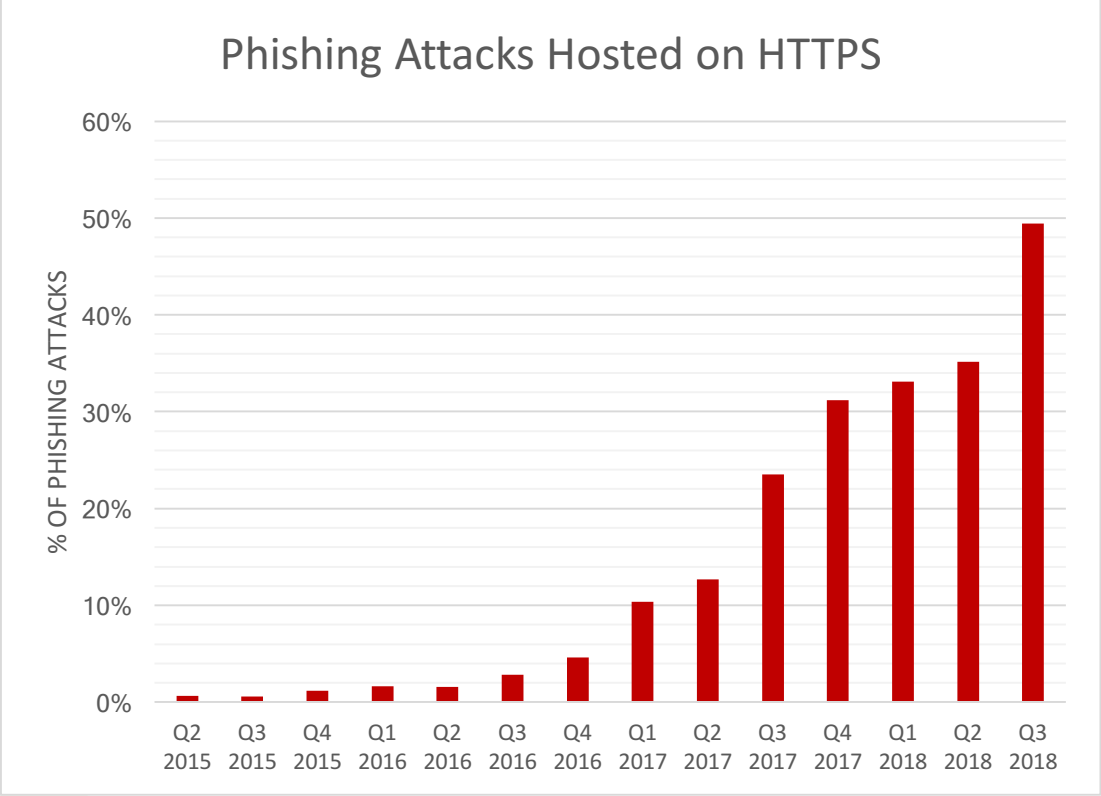
"Sometimes it is easy to discount the total volume of abuse in a TLD if the TLD has a large number of domains in it," said Jonathan Matkowsky of RiskIQ. "We assigned a weighted score against the total number of domains in each zone, looking at TLDs where there were at least five unique domain names used for phishing, as a way of understanding the size of the zone and the phishing prevalence in it. After discounting the number of unique hosts by the relative size of those zones, .TOP and .XYZ were still the new gTLDs that scored highest."

RiskIQ also analyzed unique third-level domains that targeted numerous brands on the same unique second-level domain. The domain 000WEBHOSTAPP.COM hosted phishing sites targeting at least 11 unique famous brands on more than 90 unique third-level domains. Hostinger International Ltd is a Cyprus private limited company known as "000webhost.com". A user can sign up for a free hosting account with Hostinger by becoming a user of 000webhost. Members can set up a free web hosting account from its control panel with instant activation. 5GBFREE.COM (associated with NETHOSTING.COM and FIBER.NET) hosted phishing sites targeting at least six unique brands on at least 10 unique third level domains. 5GBfree is an online free website hosting site.

How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking how many phishing sites are protected by HTTPs. 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.

At the end of 2016, less than five percent of phishing sites were found on HTTPS infrastructure. In the third quarter of 2018, PhishLabs saw the number of phishing web sites using SSL/TLS encryption increase to 49.4 percent, up from 35.2 percent in the second quarter:

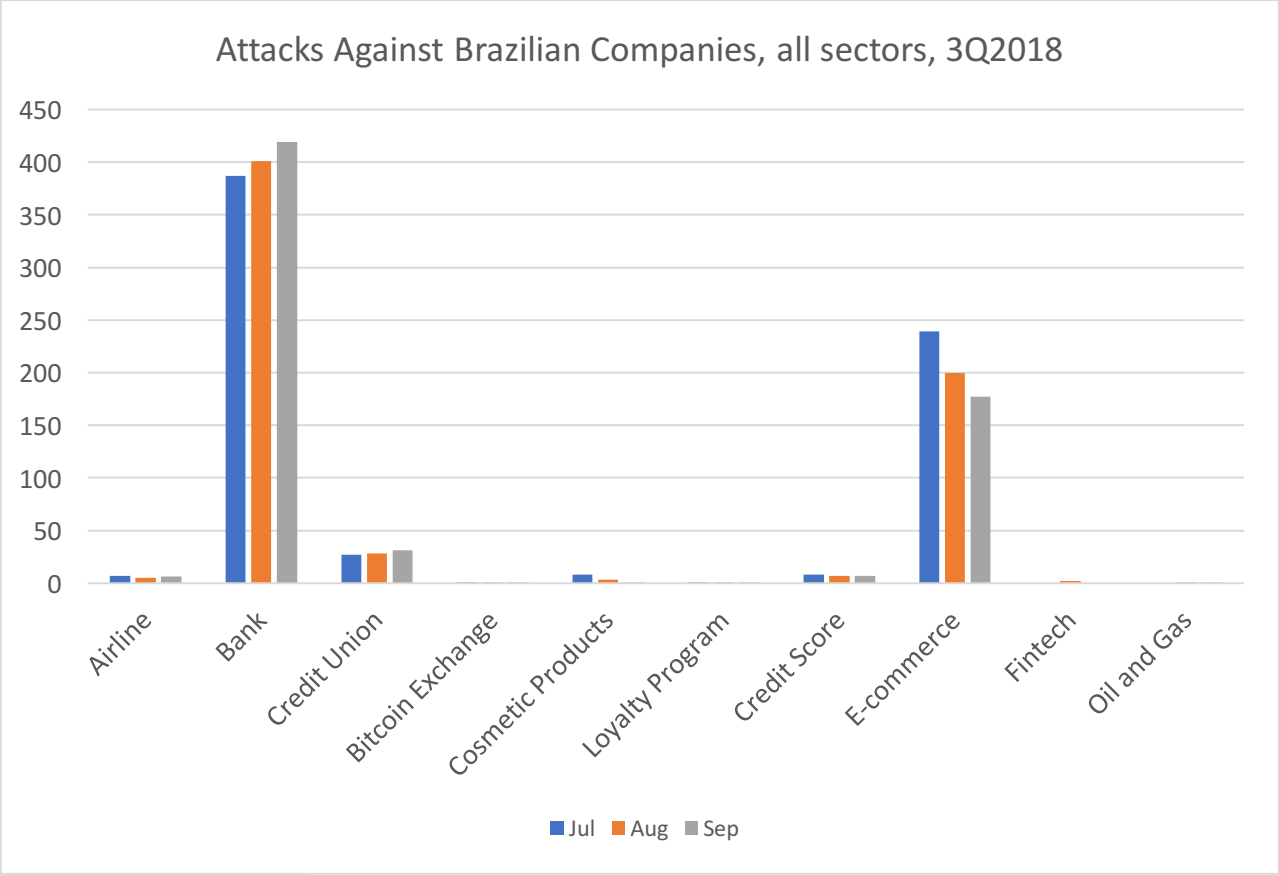


John LaCour, the Chief Technology Officer of PhishLabs, noted: "This is likely a result of attackers obtaining certificates for use on their own infrastructure, and in general, as more legitimate Web sites obtain SSL certificates, some of those will naturally become compromised by phishers." LaCour notes, "As of July 2018, the Google Chrome browser began to warn users that plain HTTP sites are 'not secure', and that will drive more web site owners to use HTTPS. So over time we expect that most phishing sites will use SSL certificates. Certificate authorities that offer free certificates will be increasingly abused by phishers in the future."

Phishing and Identity Theft Techniques 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.

Brazilian e-commerce websites are commonly used by criminals to purchase electronic products who use stolen credentials and credit cards, usually obtained through social engineering and phishing attacks. The Axur team observed that the number of phishing attacks against Brazilian e-commerce sites fell 53 percent from April to June after the FIFA World Cup, and continued to drop through the third quarter. In the meantime, attacks against Brazilian banks and credit unions inched up. Attacks against the other sectors were negligible. This regional phenomenon is different from the global distribution, where attacks against SAAS solution providers, cloud storage, and webmail providers made up more than 25 percent of phishing attacks.



Eduardo Schultze, CSIRT Coordinator at Axur, offered some insights about the autumn's activity. "In the second quarter of the year we saw notable phishing targeted bitcoin exchanges, but that is now gone. In the past, we had from eight to fifteen cases a month and in the third quarter is was just one or two." Schultze added: "Our Threat

Intelligence team has seen criminals selling ready-made phishing already hosted on some ISPs. You can buy the phishing kit and host it yourself or rent it already hosted from the criminal, with what they call 'anti-phishing protection.' This means that the setup will only be visible from Brazilian IPs, where the hosting provider itself cannot view the pages. And some of these phishing websites will only work for mobile devices. The criminal's ad says 'Phishing stays on the ISP for 30 days due to anti-phishing methods.' One of the preferred ISPs for this kind of phishing is Google Cloud. This kind of attack also comes hosted on generic domain names, with the brand name of the target appearing in a subdomain."

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

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 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; Eduardo Schultze of Axur at +55 51 3012-2987, eduardo.schultze@axur.com; Stacy Shelley of PhishLabs at 1.843.329.7824, stacy@phishlabs.com, Kari Walker of RiskIQ at +1.703.928.9996, Kari@KariWalkerPR.com, +1.703.928.9996. **Analysis and editing by Greg Aaron, iThreat Cyber Group.**