Phishing Activity Trends Report

1st Quarter 2019

APWG

Unifying the
Global Response
To Cybercrime

Activity January-March 2019

Published May 15, 2019

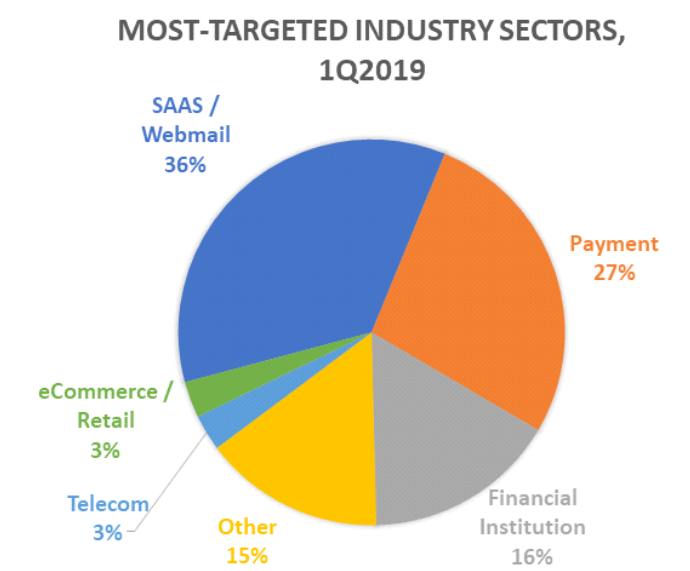
Phishing Report Scope

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 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).

Phishing of SaaS and Webmail Brands Surpasses Payment Brands for First Time



1st Quarter 2019 Phishing Activity Trends Summary

- Phishing that targeted Software-as-a-Service (SaaS) and webmail services became the biggest category of phishing. At 36 percent of all phishing attacks, it eclipsed phishing against the payment services category for the first time. [p. 5]
- The total number of phishing sites detected by APWG in the first quarter of 2019 was up notably over the third and fourth quarters of 2018. [p. 4]
- The number of phishing attacks hosted on Web sites that have HTTPS and SSL certificates reached a new high. [p. 6]
- In Brazil, mobile phishing rose, and phishers also attacked SaaS providers. Cybercriminals also deployed malware that targeted multiple banks at a time. [p. 7]

Table of Contents

Statistical Highlights for 1st Quarter 2019

	January	February	March
Number of unique phishing Web sites detected	48,663	50,983	81,122
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	34,630	35,364	42,399
Number of brands targeted by phishing campaigns	327	288	330

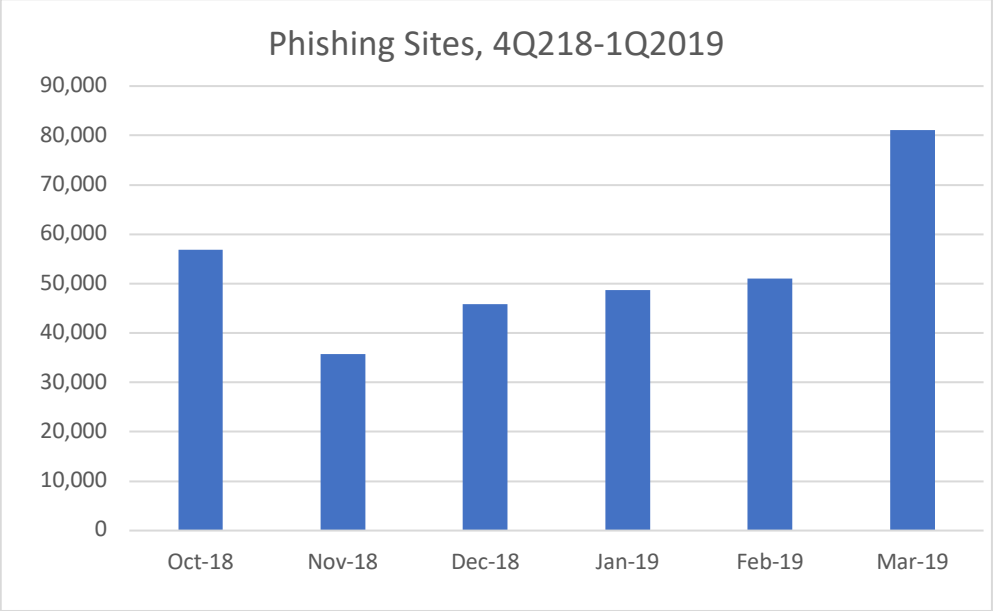
The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports.

The APWG 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 report phishing URLs into APWG. The contributing members also track a variety of additional metrics and data sets in order to track the fast-paced nature of cybercrime.

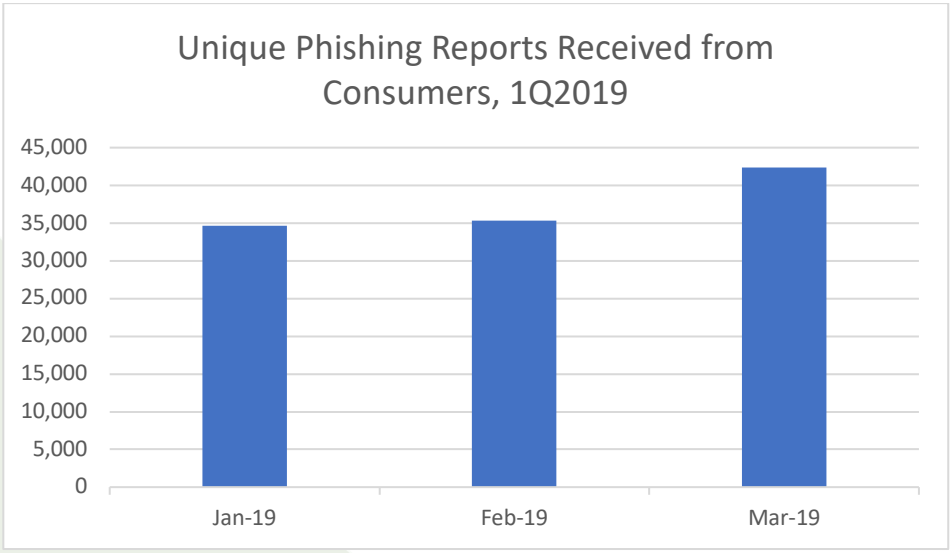
APWG also tracks and reports the number of unique phishing reports (email campaigns) it receives from consumers. An e-mail campaign is a unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report e-mails as those found in a given month that have the same email subject line.

Phishing Site and Phishing E-mail Trends – 1st Quarter 2019

The total number of phishing sites detected by APWG in 1Q was 180,768. That was up notably from the 138,328 seen in 4Q 2018, and from the 151,014 seen in 3Q 2018.



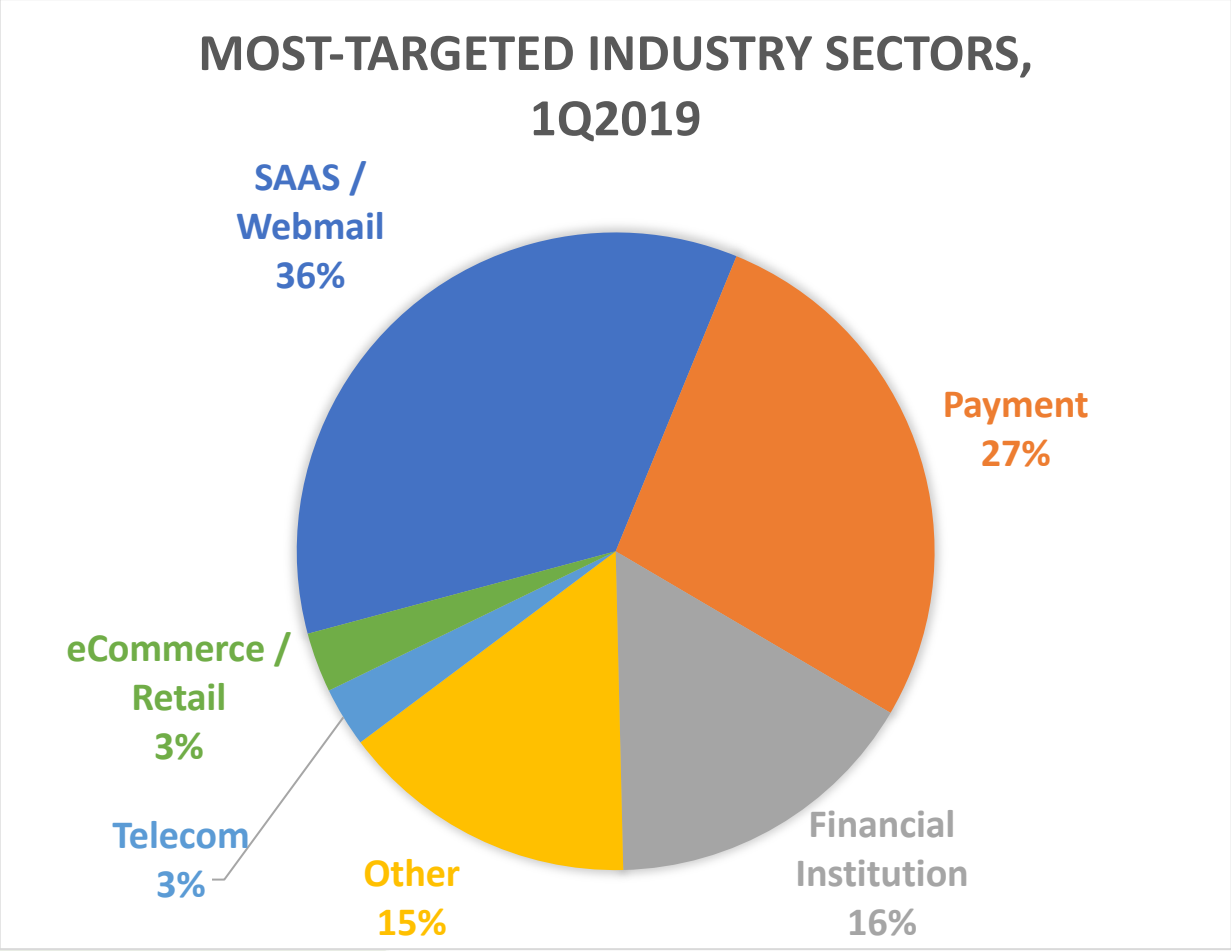
The number of unique phishing reports submitted to APWG during 1Q 2019 was 112,393. These were phishing emails submitted to APWG, and exclude phishing URLs reported by APWG members directly into APWG's eCrime eXchange.



Most-Targeted Industry Sectors – 4th Quarter 2018

In 1Q 2019, APWG member MarkMonitor saw phishing that targeted Software-as-a-Service (SaaS) and webmail services jump to 36 percent of all phishing attacks. That's up significantly from 30 percent in 4Q 2018 and 20.1 percent in 3Q 2018. Phishing against the SaaS and webmail category became the biggest category of phishing, eclipsing phishing against the payment services category for the first time.

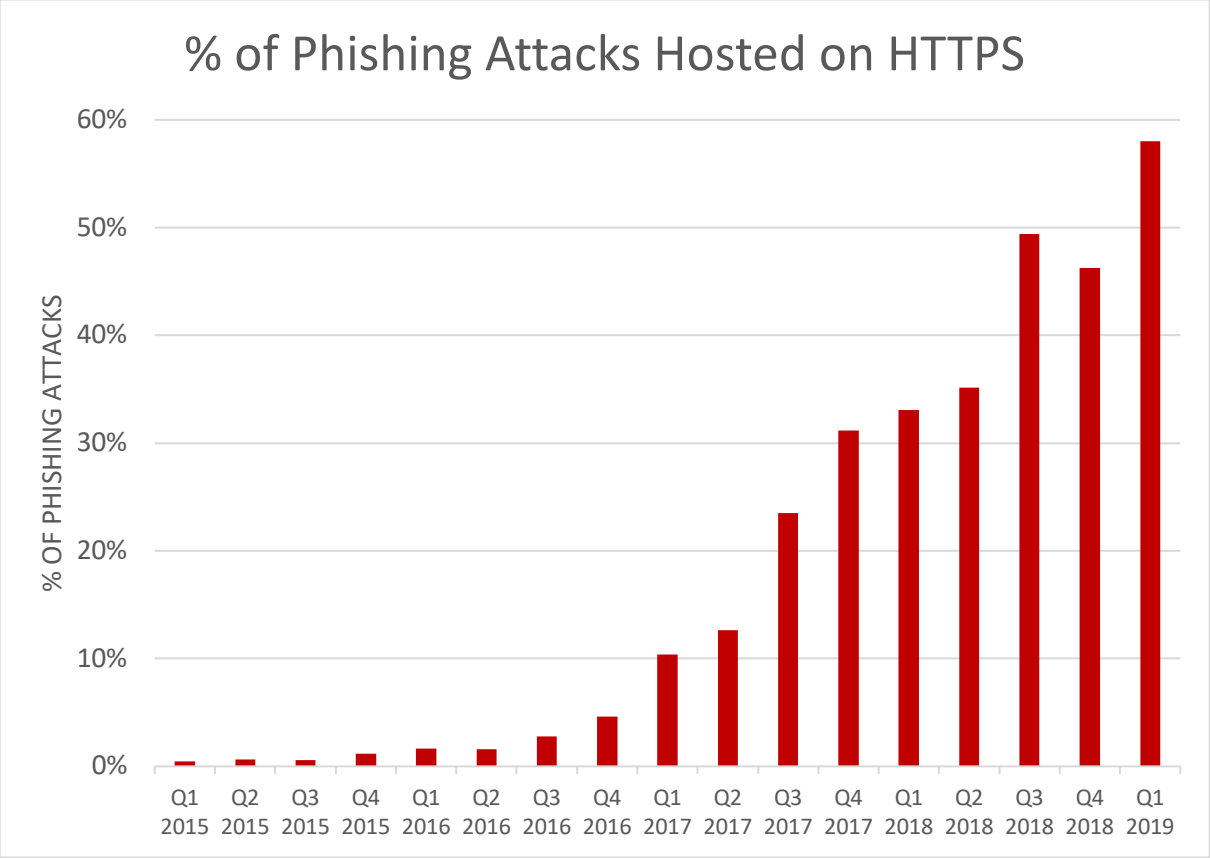
Attacks against cloud storage and file hosting sites continued to drop, decreasing from 11.3 percent of all attacks in Q1 2018 to just 2 percent in 1Q 2019. Founding APWG member MarkMonitor is an online brand protection organization, securing intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.



How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking the numbers of phishing sites 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 (typically by using the HTTPS protocol's lock icon in the browser address bar to assure users that the domain itself is 'safe'). PhishLabs provides managed security services that help organizations protect against phishing attacks targeting their employees and their customers.

"In Q1 2019, 58 percent of phishing sites were using SSL certificates, a significant increase from the prior quarter where 46 percent were using certificates," said John LaCour, CTO of PhishLabs. "There are two reasons we see more. Attackers can easily create free DV (Domain Validated) certificates, and more web sites are using SSL in general. More web sites are using SSL because browser warning users when SSL is not used. And most phishing is hosted on hacked, legitimate sites."

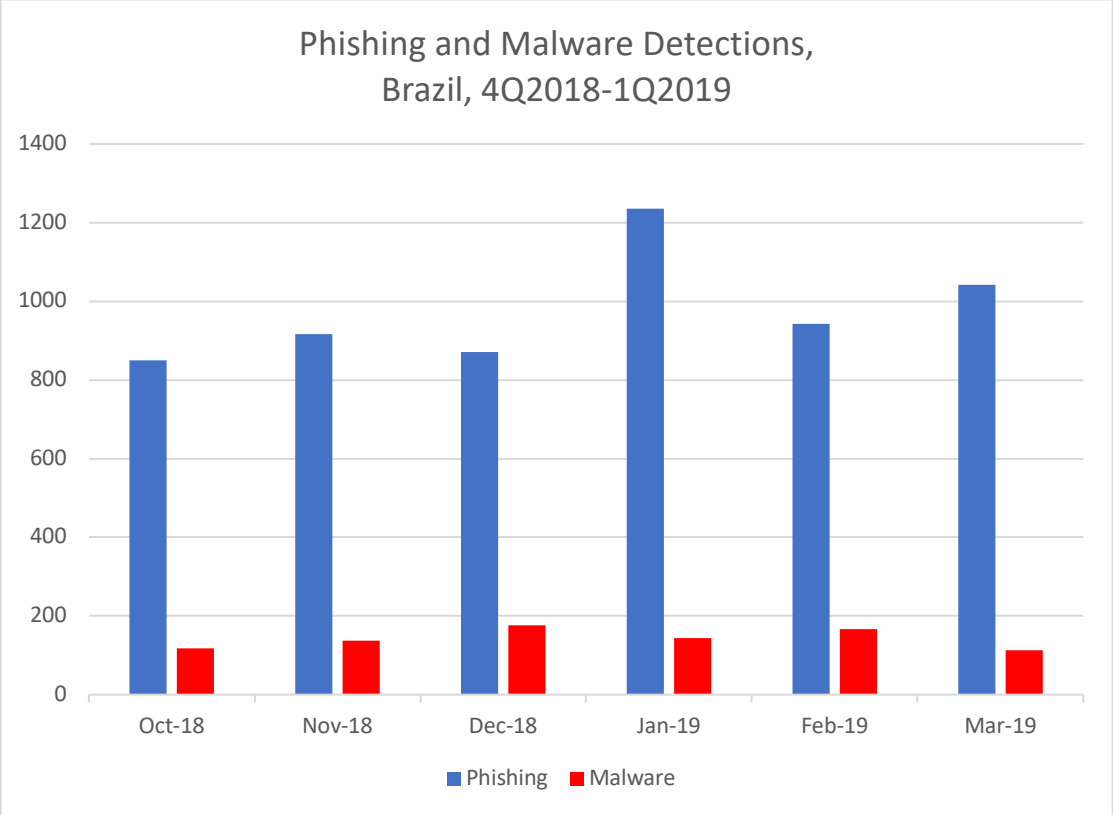


Online Criminal Activity in Brazil

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.

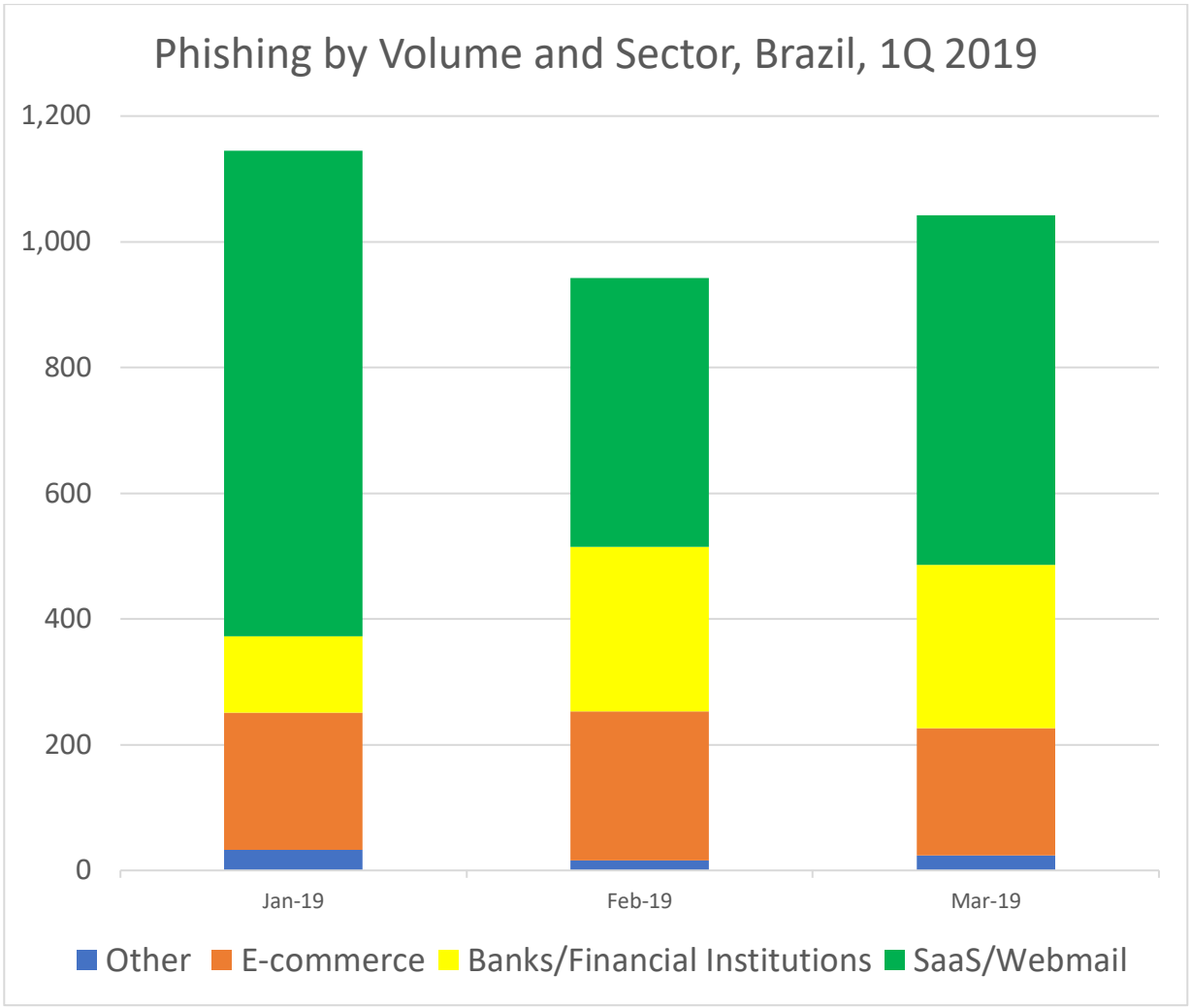
In the first quarter of 2019, Axur observed 3,220 cases of phishing and 180 cases of malware. Specifically, these were attacks against Brazilian brands or against foreign services that are available in Portuguese in Brazil.

In Brazil, the amount of phishing -- especially mobile phishing -- increased in the first quarter of 2019:



Each kind of malware identified during this period, on average, aimed to affect up to thirteen Brazilian financial institutions and their customers. The largest number of targets found in a single malware device was nineteen.

The phishing that Axur tracked in Brazil was often directed against SaaS and webmail targets:



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.**