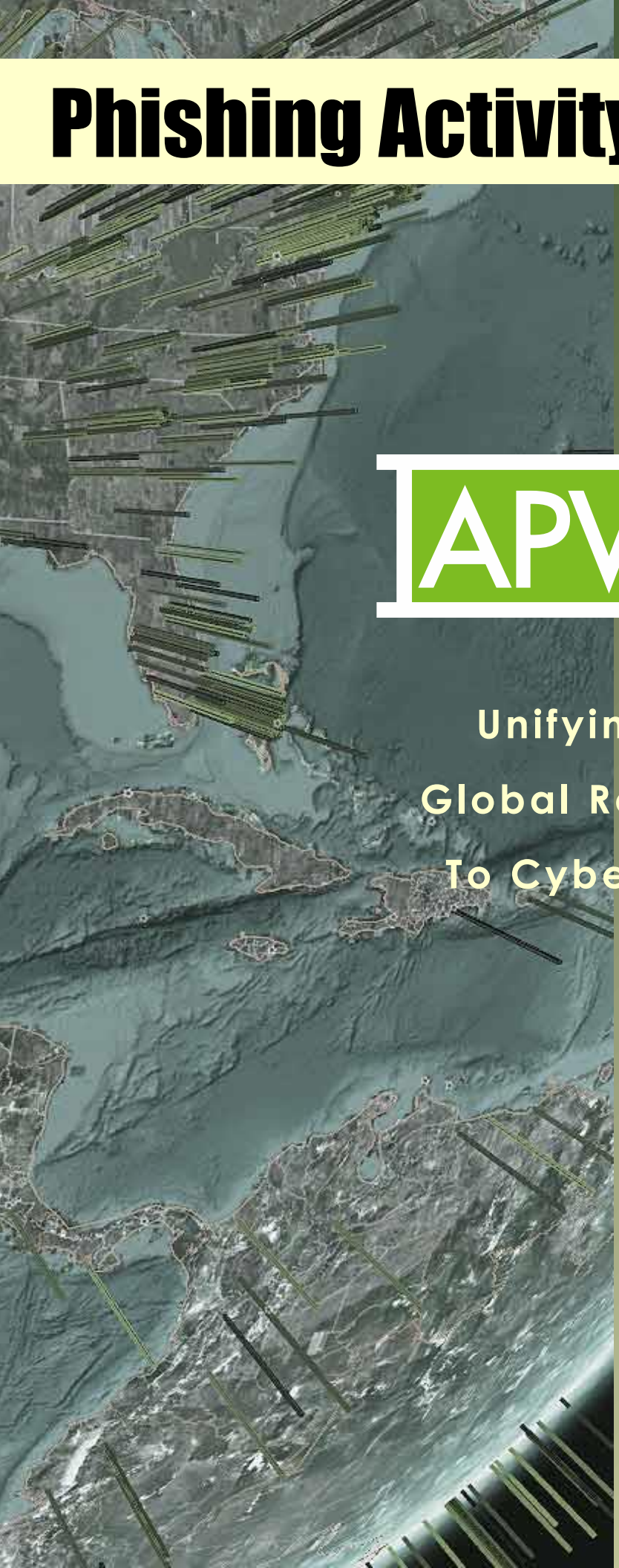
Phishing Activity Trends Report



3rd Quarter 2021

APWG

Unifying the
Global Response
To Cybercrime

Activity July-September 2021

Published 22 November 2021

Phishing Report Scope

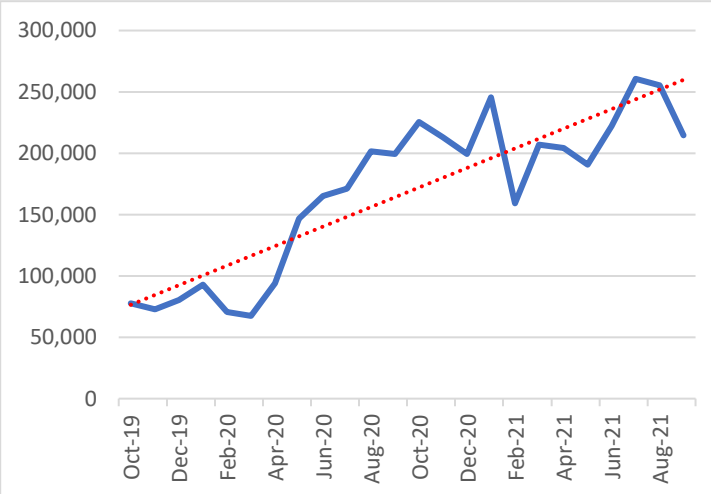
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. 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 usernames and passwords or misdirect consumers to counterfeit Web sites.

Table of Contents

Phishing Reaches Monthly Record in Q3; Attacks Doubled since Early 2020



Phishing Activity Trends Summary

- APWG saw 260,642 phishing attacks in July 2021, which was the highest monthly in APWG's reporting history. [pp. 3-4]
- The number of phishing attacks has doubled from early 2020. [pp. 3-4]
- The software-as-a-service and webmail sector was the most frequently victimized by phishing in the third quarter, with 29.1% of all attacks.
- Attacks against financial institutions and payment providers continued to be numerous, and were a combined 34.9% of all attacks.
- Phishing against cryptocurrency targets – cryptocurrency exchanges and wallet providers – settled at 5.6% of attacks. [p. 5]
- The number of brands being attacked has risen during 2021, from just over 400 per month to more than 700 in September. [p. 4]
- Phishing attacks in Brazil rose, from 4,275 in Q2 to 7,741 in Q3. [p. 7]

Statistical Highlights for the 3rd Quarter 2021

APWG's contributing members study the ever-evolving nature and techniques of cybercrime. With this report, the APWG has refined the methodologies it uses to report phishing. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

The APWG tracks:

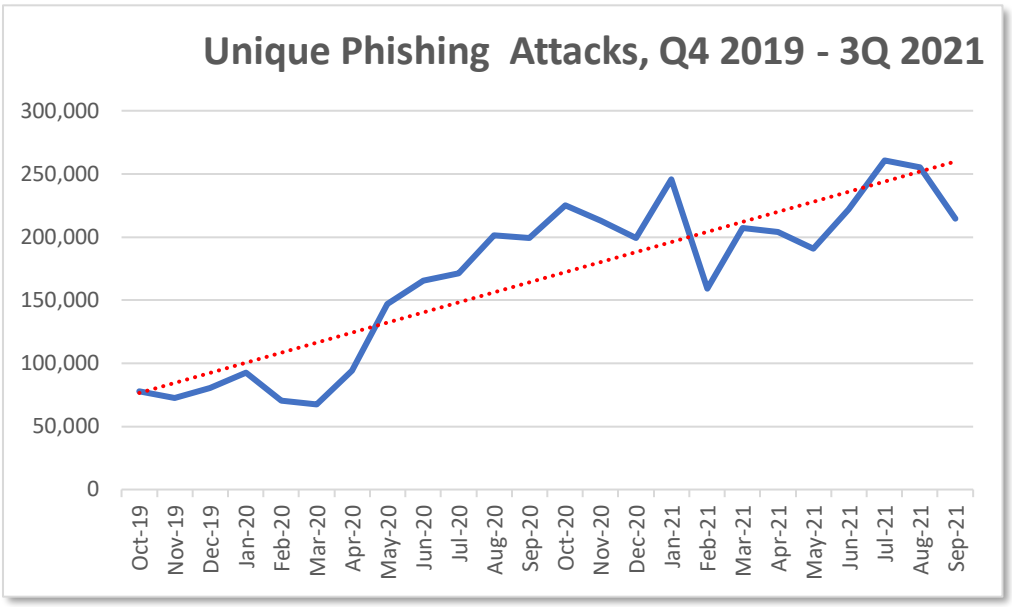
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique base URLs of phishing sites found in phishing emails reported to APWG. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same *attack*, or destination.) APWG is measuring reported phishing sites on a more accurate basis accounting for how phishers have been constructing phishing URLs.

- **Unique phishing e-mails subjects**. This counts email lures that have different email subject lines. Some phishing campaigns may use the same subject line but advertise different phishing sites. This metric is a general measure of the variety of phishing attacks, and can be a rough proxy for the amount of phishing taking place.

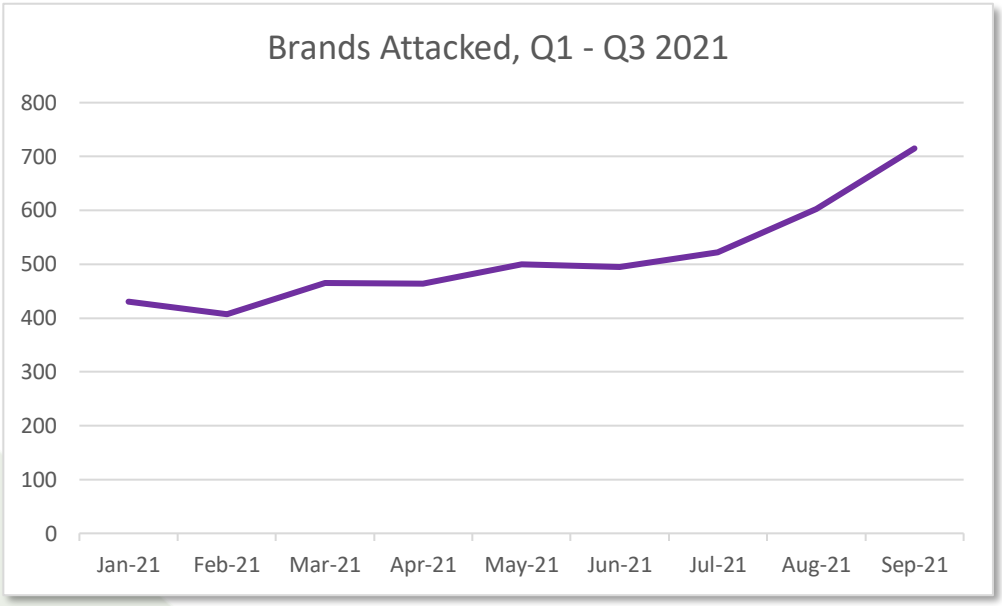
- The APWG also counts the **number of brands attacked** by examining the phishing reports submitted into the APWG eCrime Exchange, and normalizing the spellings of brand names.

	July	August	Sept.
Number of unique phishing Web sites (attacks) detected	260,642	255,385	214,345
Unique phishing email subjects	11,384	10,716	64,233
Number of brands targeted by phishing campaigns	522	603	715

The number of recent phishing attacks has more than doubled since early 2020, when APWG was observing between 68,000 and 94,000 attacks per month. APWG saw 260,642 attacks in July 2021, which was the highest monthly attack count recorded in APWG's reporting history.



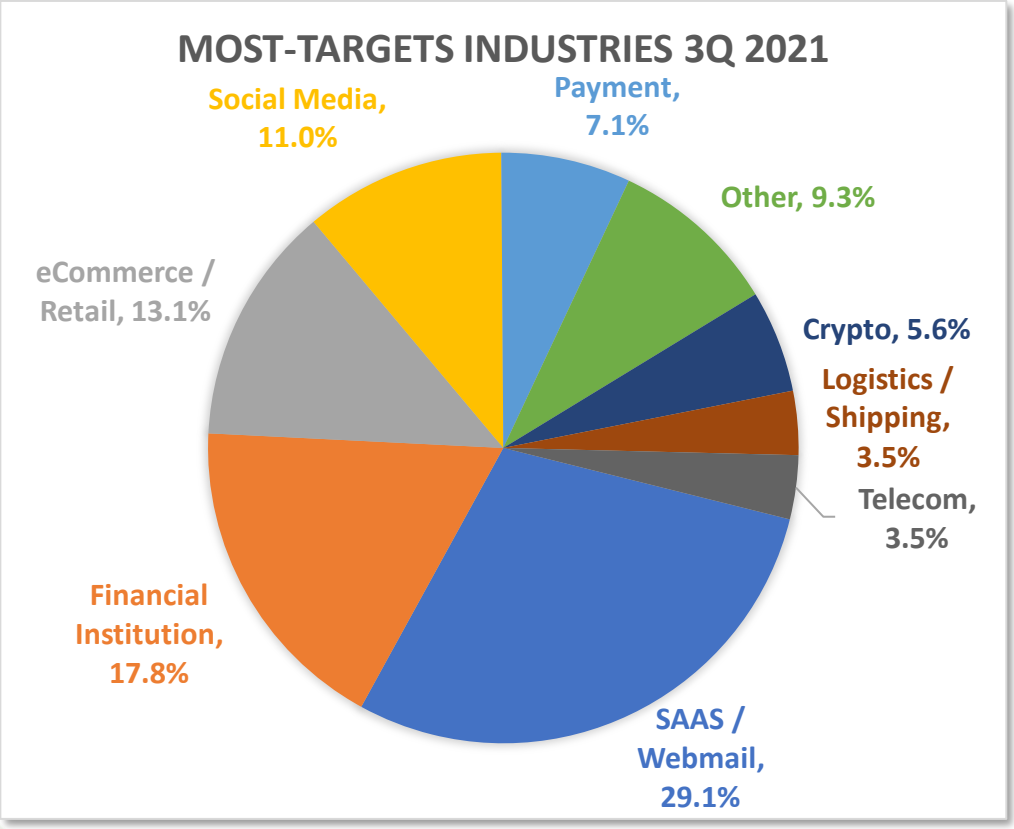
The number of Unique Subjects has dipped as more submitted emails have had duplicative subject lines.



The number of brands attacked each month has trended upwards, to a high of 715 in September 2021.

Most-Targeted Industry Sectors – 3rd Quarter 2021

In the third quarter of 2021, APWG founding member OpSec Security found that phishing attacks against webmail and software-as-a-service (SAAS) providers were most prevalent, exploding from just 8.7 percent of all attacks in Q2 2021 to 29.1 percent of all attacks in Q3. Attacks against financial institutions and payment providers continued to be numerous, and were a combined 34.9% of all attacks. Phishing against cryptocurrency targets – such as cryptocurrency exchanges and wallet providers – settled at 5.6 percent of attacks, after leaping from 2 percent of all attacks in Q1 to 7.5 percent in Q2. Social Media rounded out the top-targeted industries.



OpSesc also reported increased activity with smishing and vishing campaigns, especially targeting companies that are app-based, such as email and finance organizations. OpSec noted that its own monitoring found that Q3 represented a nearly 30 percent increase in total phishing over Q2, and that Q2 represented nearly a 30 percent increase over Q1.

OpSec Security offers world-class brand protection solutions.

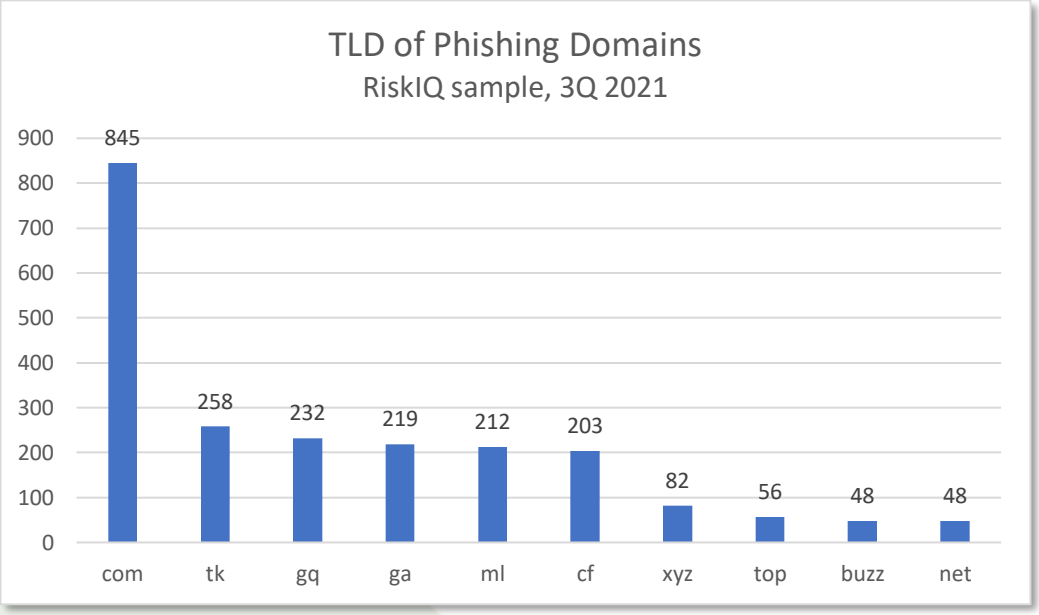
Use of Domain Names for Phishing

APWG member RiskIQ (now a Microsoft subsidiary) provides ongoing analysis of where phishing is happening in the domain name system. RiskIQ provides digital attack surface management, providing discovery, intelligence, and mitigation of threats associated with an organization's digital presence to protect businesses, brands, and customers.

RiskIQ analyzed 4,340 confirmed phishing URLs reported to APWG in Q3 2021. RiskIQ found that they were hosted on 2,649 unique second-level domains (and 18 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 about 51 percent of the domain names in the world as of the beginning of Q3 2021, and represented 37 percent of the phishing domains in the sample set. There were 993 legacy gTLD domains in the sample set. Most of those were in .COM, which had 845 domains in the set.
- The new generic top-level domains (nTLDs), such as .XYZ and .ICU, were released after 2011. The nTLDs represented about 6 percent of the domains in the world, but about 9 percent of the domains in the sample set (249 domains).
- The country code domains (ccTLDs), such as .UK for the United Kingdom and .BR for Brazil. ccTLDs were about 43 percent of the domains in the world, but were 53 percent of the domains in the Q3 sample set (1,407 domains).

The TLDs that had the most unique second-level domains used for phishing were:



The .TK, .GQ, .GA, .ML, and .CF ccTLDs are operated by Freenom, a company in the Netherlands that offers free domain name registrations in these TLDs.

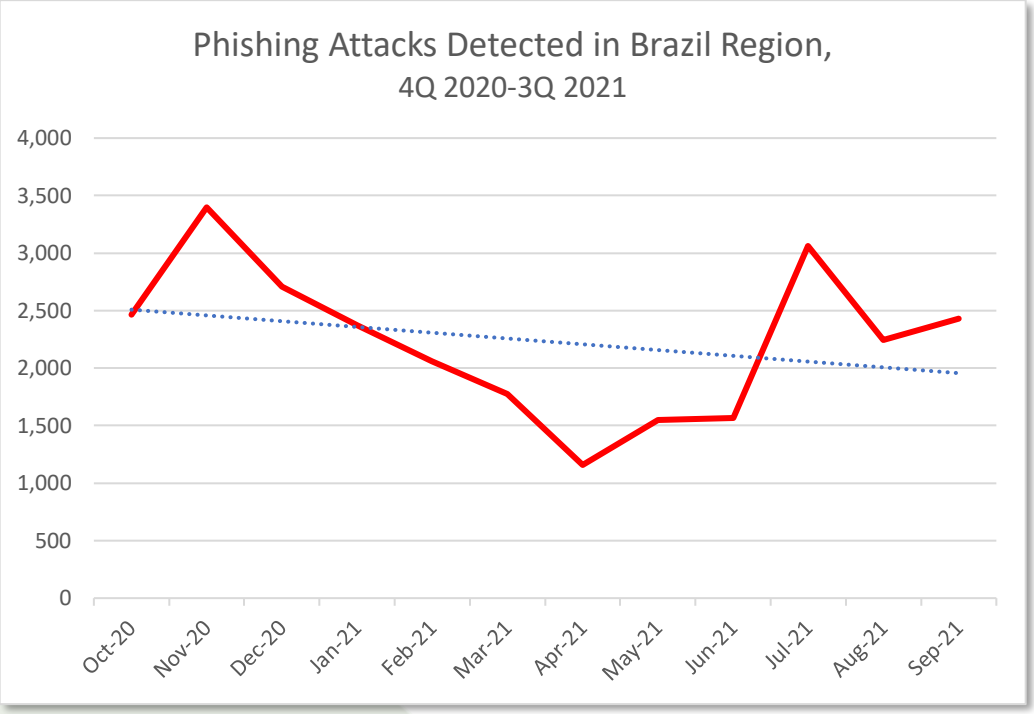
During the third quarter, RiskIQ also profiled the bulletproof hosting provider Flowspec, which was used by threat groups for phishing campaigns and malware delivery

"Besides making it harder to get in and limiting the scope of damage, we all need to do a better job of preventing ransomware from getting into networks in the first place, and of becoming more resilient. A way to strengthen cybersecurity protection is to mature the Zero Trust security posture of your organization," says Jonathan Matkowsky, a Principal Researcher at Microsoft.

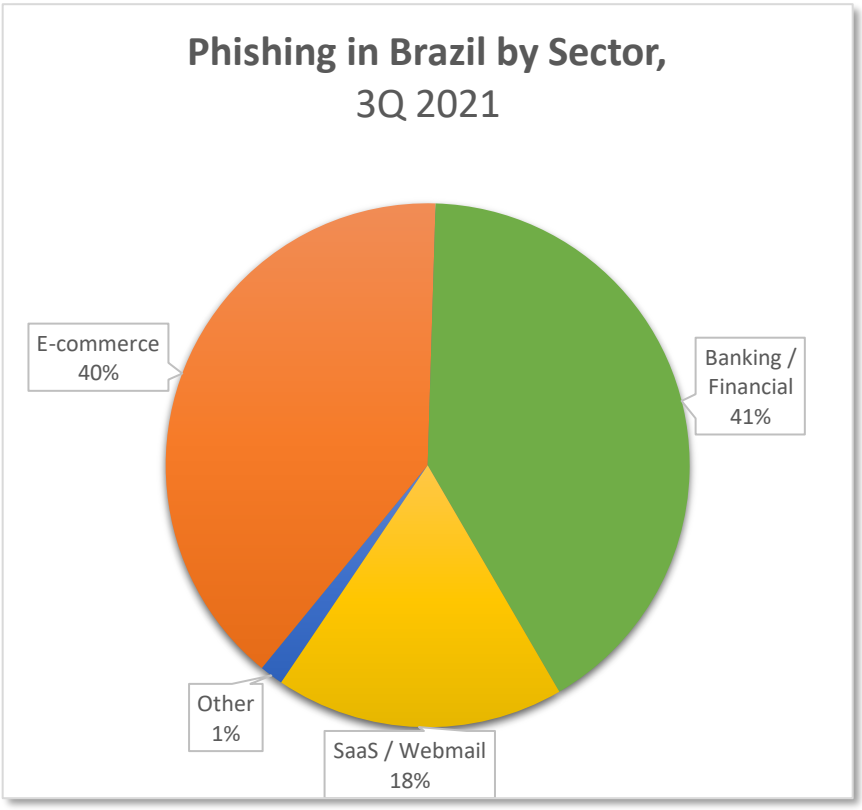
Online Criminal Activity in Brazil

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 local and international problems. Axur's observations also demonstrate how cybercrime's intensity and methods can vary from one locale to another.

In Q3 2021, Axur's systems identified 7,741 attacks, up from 4,275 in Q2, and 6,209 in Q1:



Phishing against SaaS and Webmail companies fell back from 40 percent of all attacks in Q2 to 18 percent of all attacks in Q3. Phishing against e-commerce companies increased from 27 percent to 40 percent of all attacks:



APWG Phishing Activity Trends Report Contributors

Agari by HelpSystems protects organizations against phishing, business email compromise (BEC) scams, and advanced email threats.

Axur works to identify and fight the threats in the cyberspace that interfere with the interests of companies, governments, and individuals.

Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.

OpSec Security offers world-class brand protection solutions.

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.apwg.org>; the website of the STOP. THINK. CONNECT. Messaging Convention <http://www.messagingconvention.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 Wood at OpSec Security (swood@opsecsecurityonline.com); Angela Tuzzo of Agari by HelpSystems (atuzzo@mrb-pr.com); Eduardo Schultze of Axur (eduardo.schultze@axur.com,+55 51 3012-2987); Stacy Shelley of PhishLabs (stacy@phishlabs.com, +1.843.329.7824); Holly Hitchcock of RiskIQ (holly@frontlines.io). **Analysis and editing by Greg Aaron, Illumintel Inc., www.illumintel.com**