Phishing Activity Trends Report

3rd Quarter 2024

APWG

Unifying the Global Response To Cybercrime

Activity July-September 2024

Published 4 December 2024

Scammers Add Personalized Menace to Phishing Attacks

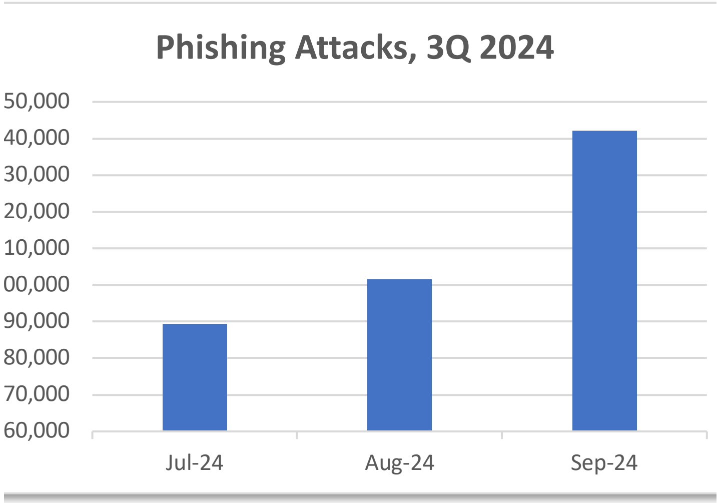
Phishing Report Scope

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@apwg.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 messages, bogus web sites, and deceptive domain names. 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 Activity Trends Summary

- In Q3 of 2024, APWG observed 932,923 phishing attacks, up from 877,536 in the second quarter. [pp. 3-4]
- Scammers are now sending personalized emails that include Google Street View images of targeted marks' homes. [p. 7]
- Social media platforms were once again the most frequently attacked sector, representing 30.5 percent all phishing attacks. [p. 4]
- Smishing—phishing advertised via SMS and text messages—increased more than 22 percent in the third quarter. [p. 5]
- Gmail accounts were used to perpetrate 83.1 percent of all Business Email Compromise (BEC) scams. [pp. 7-8]

Statistical Highlights for the 3rd Quarter 2024

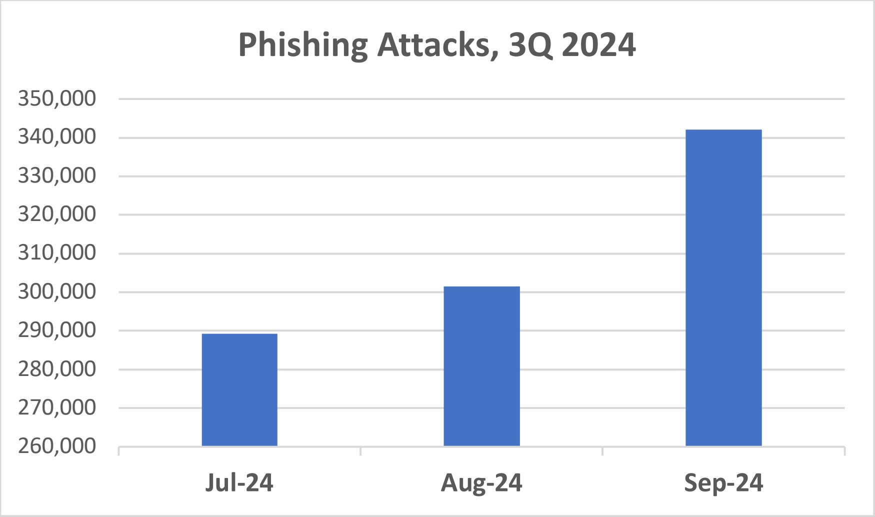
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing URLs reported by APWG members into the APWG eCrime eXchange.

The APWG tracks:

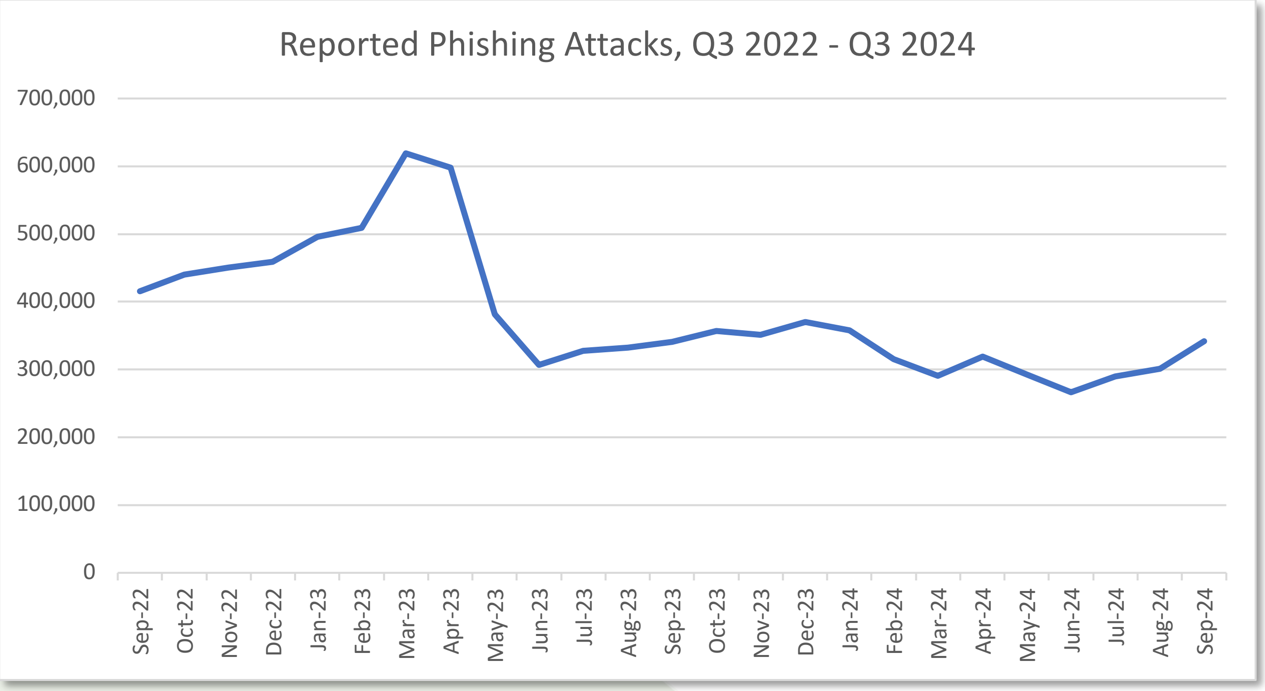
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique bases of phishing URLs found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same destination.) Thus APWG measures reported phishing *sites*, which is a more relevant metric than URLs. A synonym for sites is *attacks*.
- **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	September
Number of unique phishing Web sites (attacks) detected	289,324	301,507	342,092
Unique phishing email campaigns	33,424	27,643	25,358
Number of brands targeted by phishing campaigns	299	315	322

In the third quarter of 2024, APWG observed 932,923 phishing attacks, up from 877,536 in the second quarter:



The number of reported phish has been in a zone since June 2023, varying between 290,000 and 370,000 attacks per month:

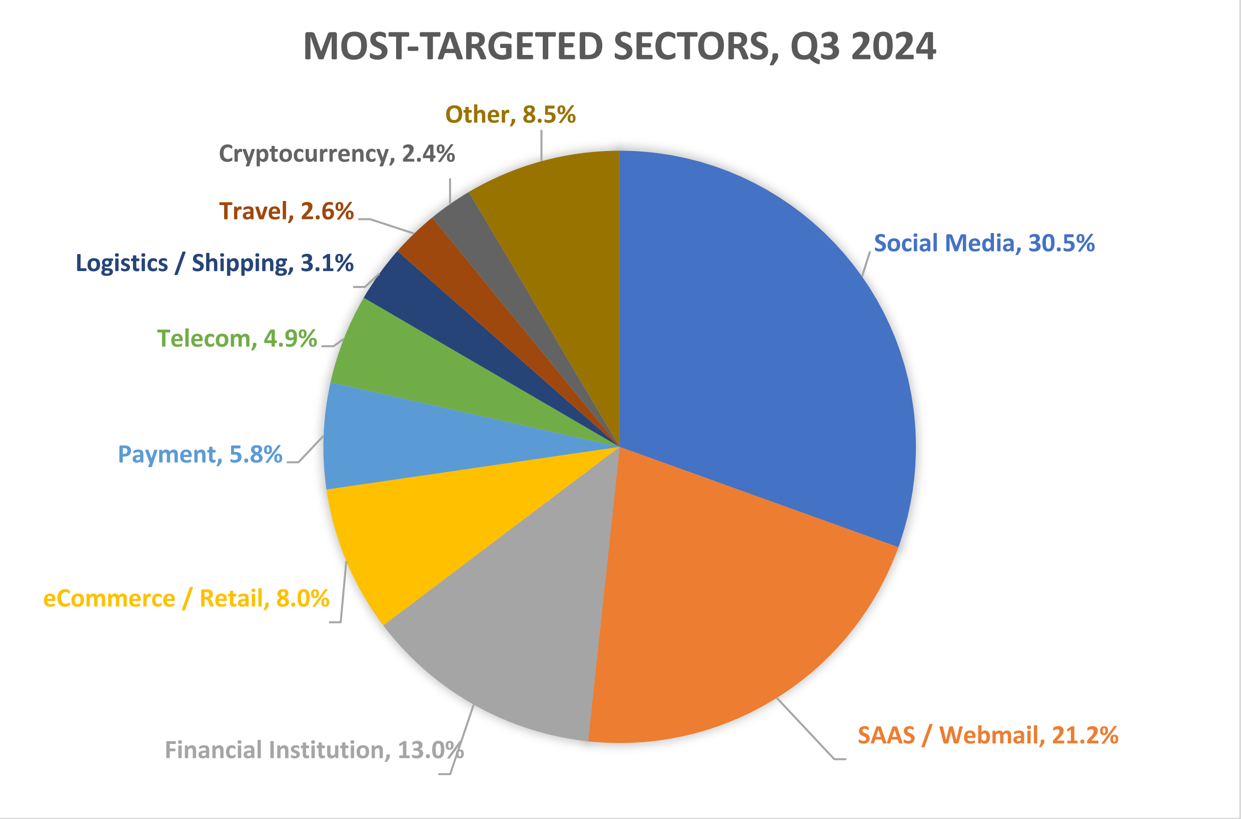


Interisle Consulting recently published a global study of phishing that took place from May 2023 to April 2024. Interisle used phishing reports made to APWG's eCrime Exchange, plus reports from OpenPhish, Spamhaus, and PhishTank. Interisle found that year-over-year, the number of phishing attacks grew by 50,000, to just under 1.9 million attacks – a slight rise, and also confirming the stable trend.

Email providers have been making it more difficult for users to report phishing to APWG and to other anti-abuse actors and law enforcement authorities. For years, APWG has asked users to forward suspected phishing emails to *reportphishing@apwg.org* for analysis. It has become apparent from complaints and testing that some major email providers are now blocking these outbound messages forwarded by the original recipients. (Ironically, these providers deliver the phishing emails to their users, but then prevent their users from reporting out the phishing.) The situation suggests the providers are not finding the phishing URLs in the emails they are delivering to their users, but are later finding the phishing URLs when the user tried to forward a message. To help get around this issue, APWG is setting up new web forms for users.

Most-Targeted Industry Sectors – 3rd Quarter 2024

In the second quarter of 2024, APWG founding member OpSec Security found that social media platforms were once again the most frequently attacked sector, representing 30.5 percent all phishing attacks. Phishing against the brands of the Financial Institution (banking) represented 13 percent of all recorded attacks, down from 24.9 percent in Q3 2023.



Attacks against online payment services (such as PayPal, Venmo, Stripe, and similar companies) were down, with another 5.8 percent of all attacks. Attacks against cryptocurrency exchanges and platforms accounted for 2.4 percent of all attacks in the third quarter.

Matthew Harris, Senior Product Manager, Fraud at OpSec said that in Q3 the company detected a strong volume increase in vishing: voice phishing, a type of cybercrime where criminals use phone calls to steal personal information from victims. "Vishing incidents in Q3 increased more than 28 percent over Q2 volumes. And smishing incidents – phishing advertised via SMS and text messages—increased more than 22 percent," Harris said.

Harris added: "We have recently observed vishing and smishing campaigns that impersonate organizations that are targeted less often, such as local gas and electric companies, and city services such as parking ticket payment systems."

OpSec saw traditional URL phishing volume go down. "We believe this is not a sign of an overall industry change, and we expect the trend for traditional email-based phishing to go back up for Q4," Harris said.

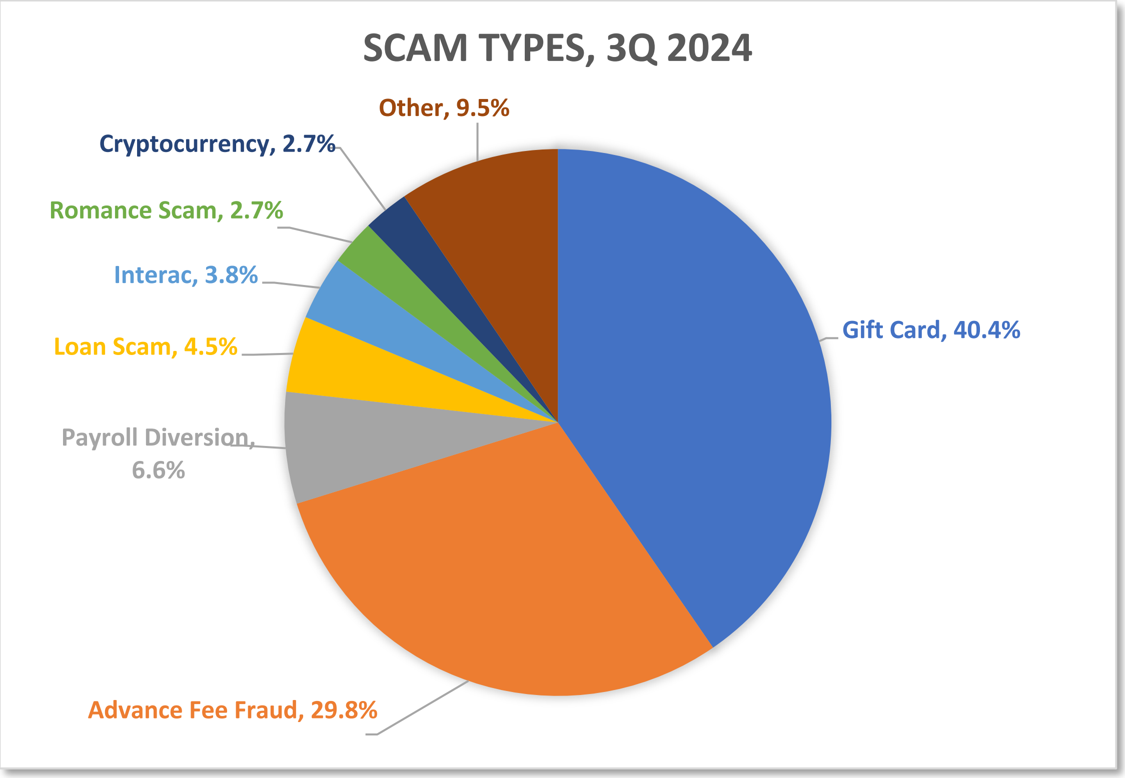
OpSec also saw that the number of unique brands targeted has largely remained steady in 2024.

OpSec Security offers world-class brand protection solutions.

Business e-Mail Compromise (BEC), 3rd Quarter 2024

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.9 billion dollars in losses in the U.S. in 2023 according to the FBI's Internet Crime Complaint Center (IC3). In a BEC attack, a threat actor impersonates an employee, vendor or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q3 2024. Fortra protects organizations against phishing, BEC scams, and other advanced email threats.

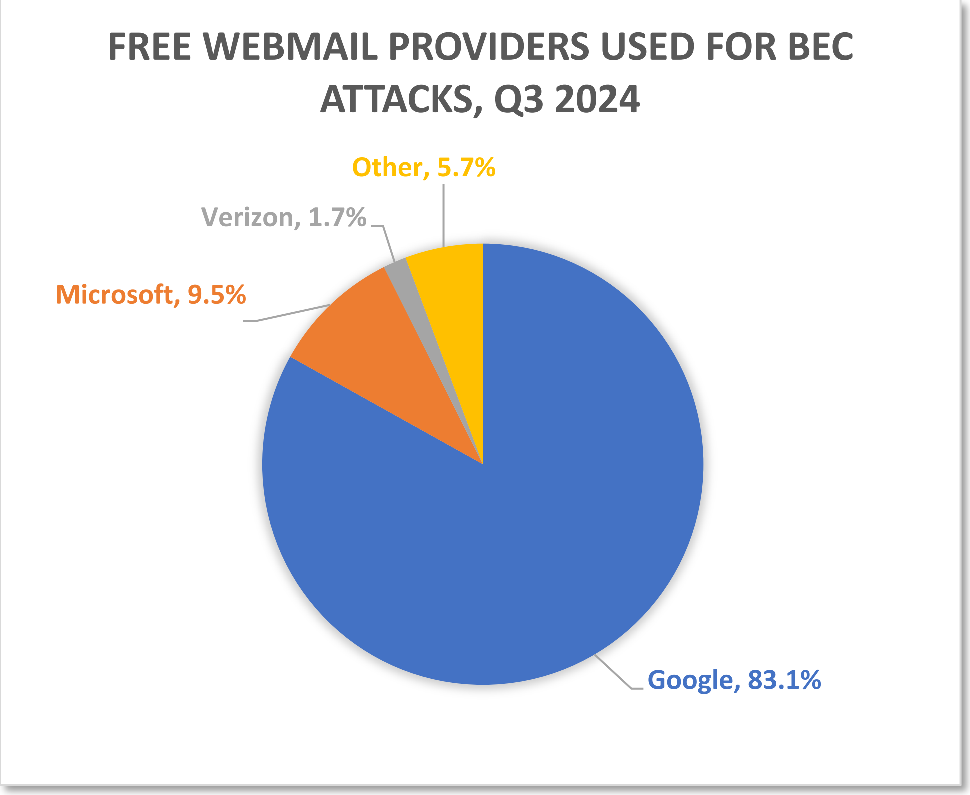
Fortra found that the average amount requested in wire transfer BEC attacks in Q3 2024 was $67,145, down 25 percent from Q2's average of $89,520. The volume of wire transfer BEC attacks in Q3 2024 decreased by 25.5 percent compared to Q2.



During the third quarter of 2024, gift card scams were once again the most popular scam type, comprising 40.4 percent of the total. 29.8 percent of attacks were advance fee fraud scams. Payroll diversion remained a popular attack type, making up 6.6 percent of attacks. Extortion scams demanding cryptocurrency as payment made up 2.7 percent of the attacks — a significant uptick from the previous quarter, when just 0.6 percent of attacks involved cryptocurrency.

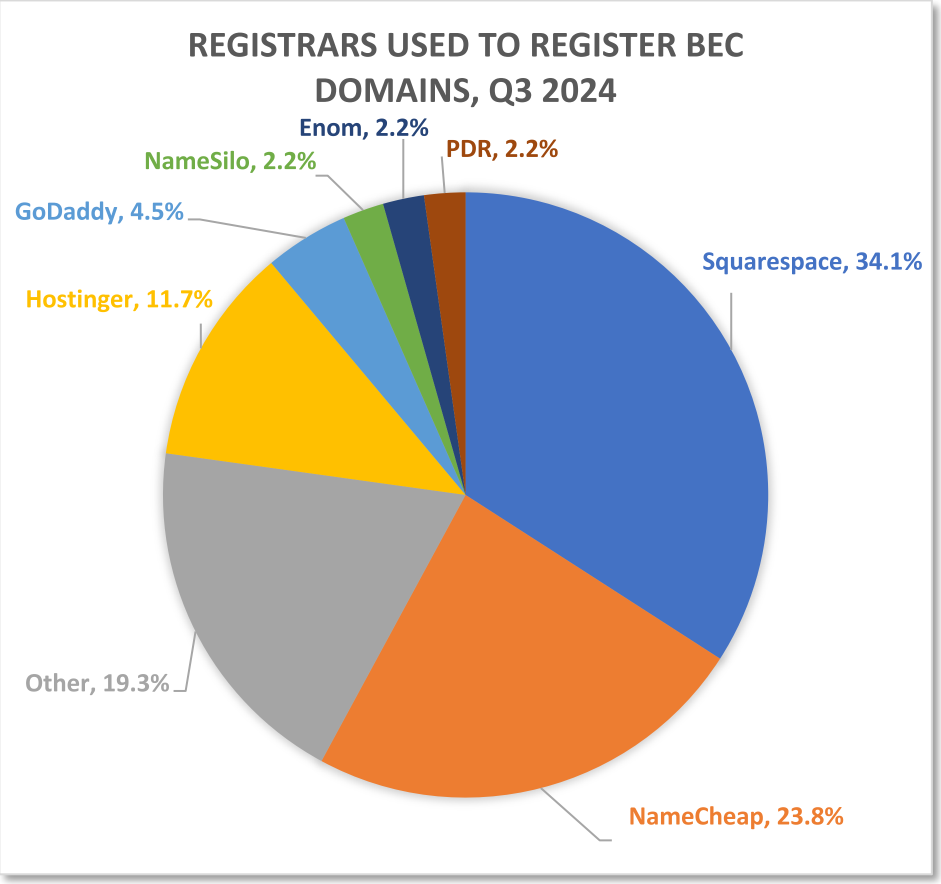
John Wilson, Senior Fellow, Threat Research at Fortra, described a devious new scam technique that started in Q3 2024. Extortion scams have been around for years; in them the scammer claims that he has access to embarrassing information about the victim and demands money from them.

Wilson said: "In the third quarter of 2024, we saw an alarming new trend in extortion emails. Previous extortion messages tended to be generic. We now see bad actors customizing their threats. Attack emails we began to see late in Q3 included the recipient's phone number and home address as part of the lure. Many of these messages even contained a Google Street View image of the intended victim's home. The use of personal data in the extortion message is clearly meant to scare the victim into compliance with the attacker's demands."



Fortra found that 70 percent of BEC attacks in Q3 2024 were launched using a free webmail domain. The remaining 30 percent of BEC attacks utilized a combination of maliciously registered domains and compromised email accounts. Google's Gmail was by far the most popular free webmail provider used by BEC scammers — Gmail was used for 83.1 percent free webmail accounts that scammers set up for BEC scams. This was up from 72.4 percent in Q2 2024. Microsoft's webmail properties powered 9.5 percent 16.3 percent of webmail-based BEC attacks in Q3, down from 16.3 percent in Q2 2024.

Fraudsters acquired the domain names that they used to run their BEC attacks at the following domain name registrars:



Wilson also noted: “Fortra observed a significant increase in the percentage of malware-laden messages reaching end-user inboxes in Q3 2024, with 12.3 percent of threat messages directing the recipient to a malicious payload. The most common malware family observed by Fortra was the Remcos RAT.”

APWG Phishing Activity Trends Report Contributors

Forta's mission is to help organizations increase security maturity while decreasing operational burden. Forta's brands include PhishLabs and Agari. www.fortra.com	Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce. www.illumintel.com	OpSec Security is the leading provider of integrated online protection and on-product authentication solutions for brands and governments. www.opsecsecurity.com

The *APWG Phishing Activity Trends Report* is published by and is © the APWG. For info about the APWG, please contact APWG Deputy Secretary General Foy Shiver (foy@apwg.org, +1.404.434.728). For media inquiries related to company-provided content in this report, please contact: APWG Secretary General Peter Cassidy (pcassidy@apwg.org, +1.617.669.1123); Stefanie Wood Ellis of OpSec Security (sellis@opsecsecurityonline.com); Rachel Woodford of Fortra (Agari and PhishLabs) (Rachel.Woodford@fortra.com). **Analysis and editing by Greg Aaron, Illumintel Inc., illumintel.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 financial institutions, online retailers, ISPs, solutions providers, the law enforcement community, government agencies, multilateral treaty organizations, and NGOs. There are more than 2,200 enterprises worldwide participating in the APWG.

Operationally, the APWG conducts its core missions through: APWG, a US-based 501(c)6 organization; the APWG.EU, the institution's European chapter established in Barcelona in 2013 as a non-profit research foundation incorporated in Spain and managed by an independent board; the STOP. THINK. CONNECT. Messaging Convention, Inc., a US-based non-profit 501(c)3 corporation; and the APWG's applied research secretariat <http://www.ecrimeresearch.org>.

APWG's directors, managers and research fellows advise: national governments; global governance bodies such as the Commonwealth Parliamentary Association, Organisation for Economic Co-operation and Development, International Telecommunications Union and ICANN; hemispheric and global trade groups; and treaty organizations such as the European Commission, the G8 High Technology Crime Subgroup, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe, Europol EC3 and the Organization of American States. APWG is a founding member of the steering group of the Commonwealth Cybercrime Initiative at the Commonwealth of Nations.

APWG's clearinghouses for cybercrime-related data send more than two billion data elements per month to APWG's members to inform security applications, forensic routines and research programs, helping to protection millions of users, software clients, and devices worldwide.

APWG's STOP. THINK. CONNECT. cybersecurity awareness campaign has officially engaged campaign curators from 26 nations, 13 of which are curated by cabinet-level ministries, government CERTs and national-scope NGOs.

The annual APWG Symposium on Electronic Crime Research, proceedings of which are published by the IEEE, attracts scores of papers from leading scientific investigators worldwide. The conference, founded in 2006 by APWG, is the only peer-reviewed conference dedicated exclusively to cybercrime studies.