# Phishing Activity Trends Report

4th Quarter 2021

APWG

Unifying the Global Response To Cybercrime

Activity October-December 2021

*Published 23 February 2022*

### 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.

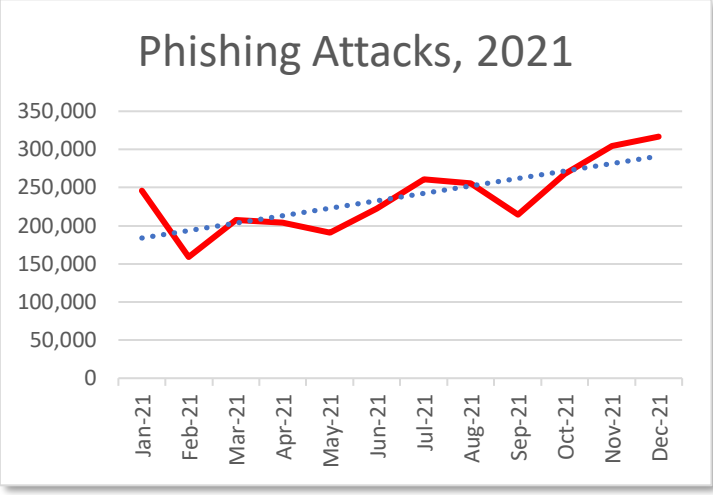
### Phishing Defined

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 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 Hits All-Time High in December 2021; Attacks Triple Since Early 2020




### Phishing Activity Trends Summary

- APWG saw 316,747 attacks in December 2021, which was the highest monthly total in APWG's reporting history. [pp. 3-4]
- The number of phishing attacks has tripled from early 2020. [pp. 3-4]
- The financial sector was the most frequently victimized by phishing in Q4, with 23.2% of all attacks. Attacks against SaaS and webmail providers continued to be numerous. Phishing against cryptocurrency targets — such as cryptocurrency exchanges and wallet providers — inched up to 6.5% of attacks. [p. 5]
- The number of companies observed being victimized by ransomware grew 36% from Q3 to Q4. [p. 6]
- Of emails reported by corporate users, 51.8% were credential theft phishing attacks, 38.6% were response-based attacks (such as BEC, 419, and gift card scams), and 9.6% involved malware delivery. [p. 10]
- Phishing attacks in Brazil declined. [p. 11]

## Statistical Highlights for the 4th Quarter 2021

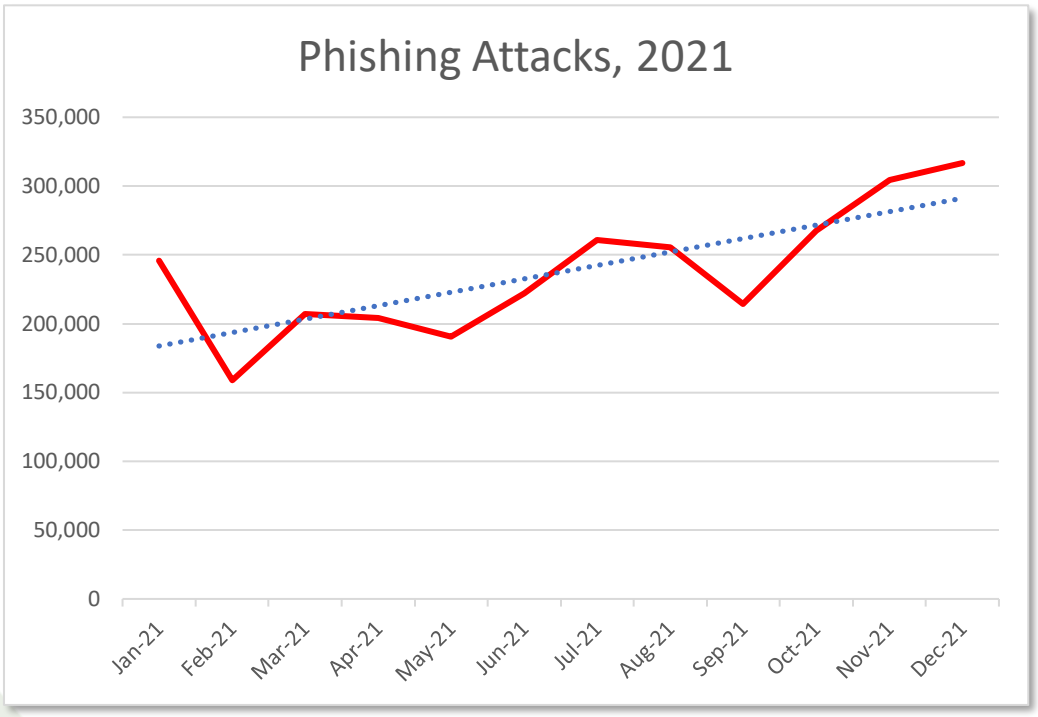
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. With this report, the APWG has refined the methodologies it uses to report phishing. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing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

The APWG tracks:

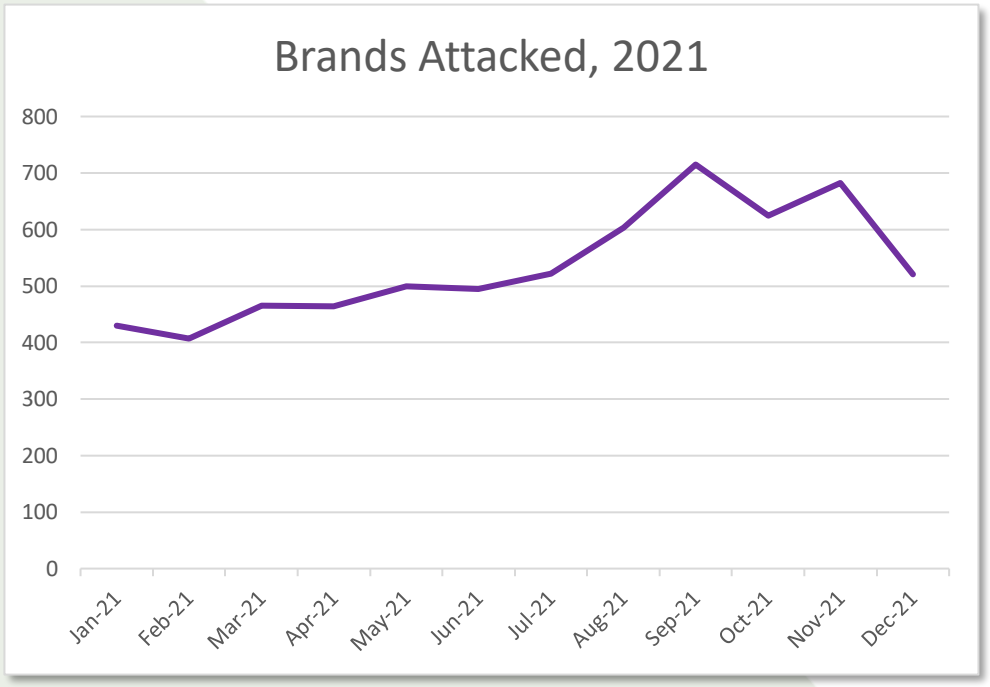
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique base URLs of phishing sites found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to 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.

| | October | November | December |
|---|---|---|---|
| Number of unique phishing Web sites (attacks) detected | 267,530 | 304,308 | 316,747 |
| Unique phishing email subjects | 12,350 | 13,937 | 16,461 |
| Number of brands targeted by phishing campaigns | 624 | 682 | 521 |

**APWG saw 316,747 attacks in December 2021, which was the highest monthly total in APWG's reporting history.** The number of recent phishing attacks has more than tripled since early 2020, when APWG was observing between 68,000 and 94,000 attacks per month.

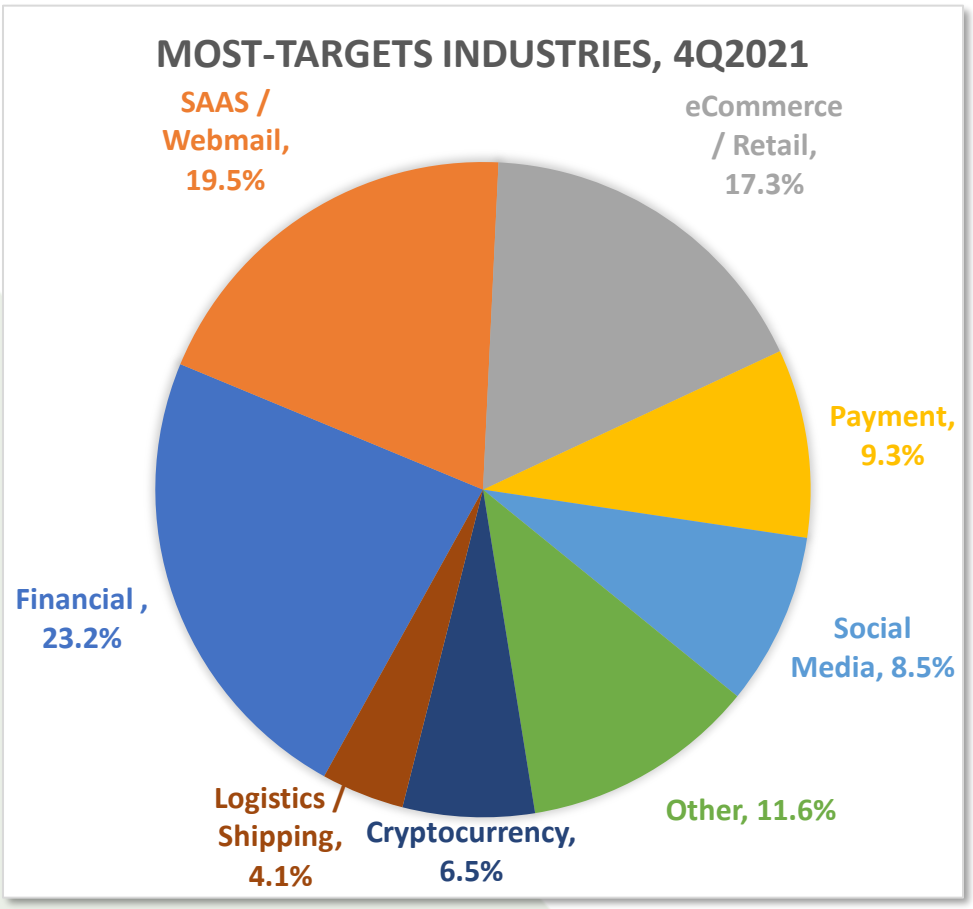



The number of Unique Subjects has dipped as more submitted emails have had duplicative subject lines. The number of brands attacked each month has trended downwards from the high of 715 in September 2021, cresting at 682 for the Q4 period in November.:



## Most-Targeted Industry Sectors – 4th Quarter 2021

In the fourth quarter of 2021, APWG founding member OpSec Security found that phishing attacks against the financial sector, which includes banks, became the largest set of attacks, accounting for 23.2 percent of all phishing. Attacks against webmail and software-as-a-service (SaaS) providers remained prevalent as well, but fell from 29.1 percent of all attacks in Q3 to 19.5 percent in Q4. Phishing against cryptocurrency targets — such as cryptocurrency exchanges and wallet providers — inched up to 6.5 percent of attacks. Attacks against the eCommerce/Retail and Payment sectors ticked upward, perhaps due to the holiday shopping season.




OpSesc observed increasing phishing volume during Q4, up 20 percent of Q3. OpSec also reported increased activity with smishing and vishing campaigns, typically utilizing fake customer support numbers or offering cheap/free products, targeting email and finance organizations.

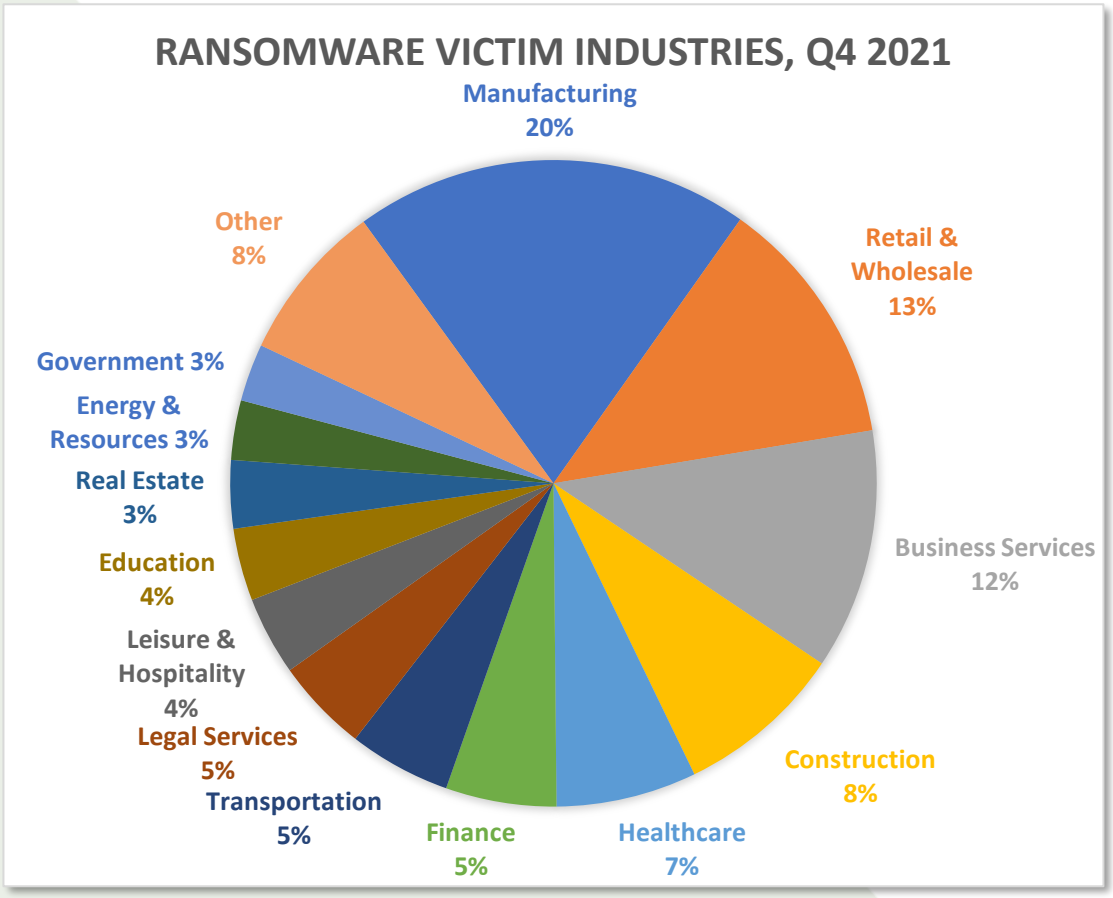
OpSec Security offers world-class brand protection solutions.

## Ransomware - 4th Quarter 2021

APWG member Abnormal Security tracks ransomware: malware that forces a company to pay a ransom to the perpetrator. The malware may encrypt the victim's data so that it cannot be used until the criminal unlocks it, or it makes the data or system otherwise inaccessible. Abnormal Security tracks and stops ransomware delivered via email to its customers, and tracks victims through a combination of ransomware extortion blog monitoring on the dark web and open-source intelligence collection. These methods provide a representative look at the overall ransomware threat landscape and lets the company make inferences about global ransomware trends.

Abnormal Security found that the number of companies it observed falling victim to ransomware in Q4 was 36 percent higher than in Q3, and the highest number the company has seen over the past two years. From the start of 2020 to the end of 2021, the Abnormal team identified 4,200 companies, organizations, and government institutions that fell victim to a ransomware attack.

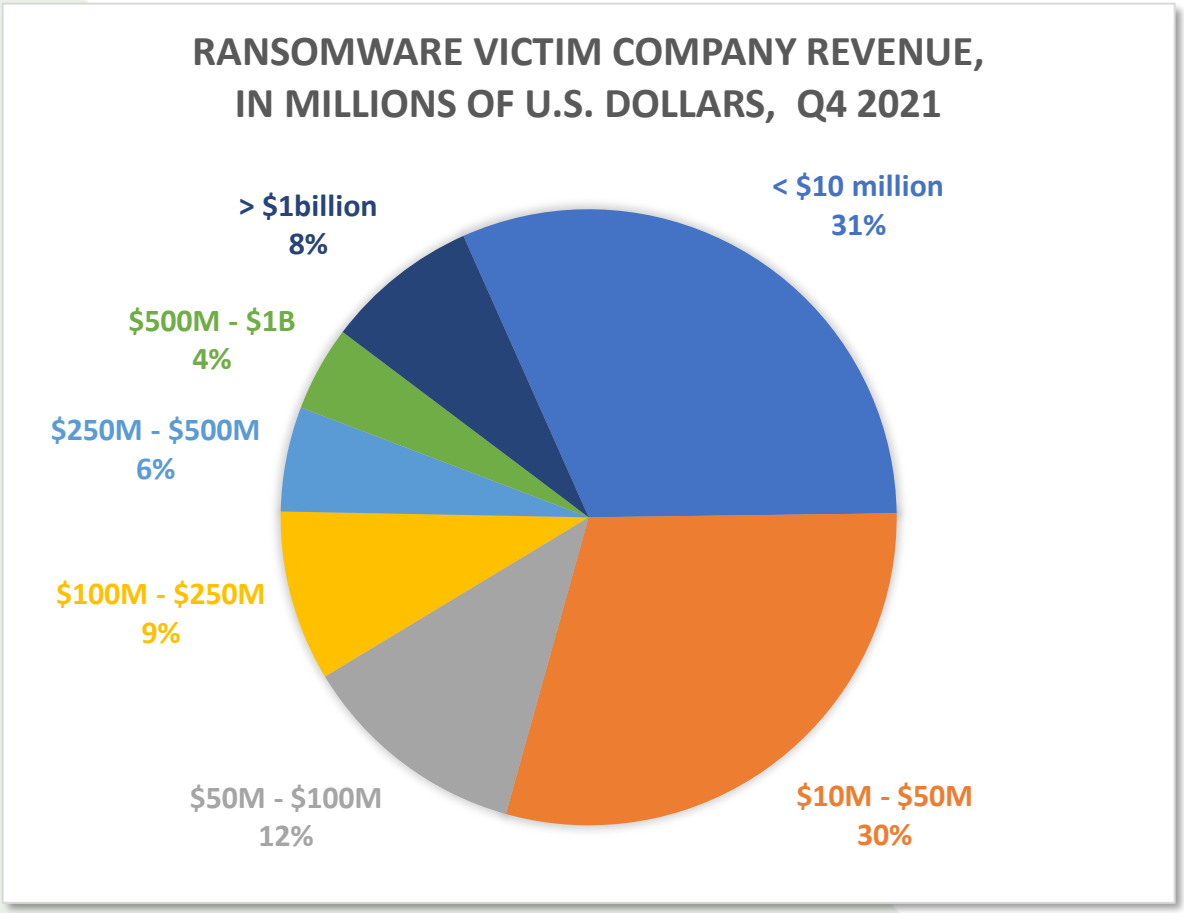
The top industries impacted by ransomware in Q4 2021 were manufacturing, retail & wholesale, business services, construction, and healthcare:



"But the overall distribution of ransomware victims indicates that ransomware attacks are industry-agnostic," said Crane Hassold, Director of Threat Intelligence at Abnormal Security. "Like with other financially-motivated cyber-attacks, the focus of most ransomware attacks is more about the ability to quickly profit from the exploitation of a corporate network and less about the characteristics of the victim company itself."

Most ransomware victims in Q4 were located in North America and Western Europe, which is consistent with historical trends. Nearly half of all ransomware victims were located in the United States, followed by the United Kingdom, France, Canada, and Germany.

Criminals spreading ransomware tend to target companies that are in a sweet spot: large enough to pay a ransom that makes the effort worthwhile for the criminal, but not so large that the company is well-defended. In Q4, nearly two-thirds of ransomware victim companies made less than $50 million in revenue a year, and a third made less than $10 million. These smaller companies are generally unable to invest large amounts of money in cybersecurity, which makes them better opportunistic targets.



More than half of all ransomware attacks in Q4 were linked to just three cybercrime groups: LockBit, Conti, and Pysa. These threat groups often provide "ransomware as a service," supplying tools to individual affiliated actors. Sometimes the members or affiliates of a group divide up the work involved in attacks, and the leadership of a group may approve the selection of targets. Abnormal Security has seen that whenever an important group has exited the scene, one or more new groups enters. "The silver lining to this top-heavy ecosystem is that disruptive actions against one of these primary groups, such as law enforcement takedowns, can have a significant impact on the overall landscape. This is different from a threat like business email compromise (BEC), where targeted disruptive actions are generally less impactful to overall attack volume due to the decentralized structure of the threat landscape," said Hassold.

## Business e-Mail Compromise (BEC), 4th Quarter 2021

APWG member Agari by HelpSystems tracks the identity theft technique known as "business e-mail compromise" or BEC, which has caused aggregate losses in the billions of dollars, at large and small companies. In a BEC attack, a scammer impersonates a company employee or other trusted party, and tries to trick an employee into sending money, usually by sending the victim email from fake or compromised email accounts (a "spear phishing" attack). Agari examined thousands of BEC attacks attempted during Q2. Agari counts BEC as any response-based spear phishing attack that involves the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive materials. Agari protects organizations against phishing, BEC scams, and other advanced email threats.

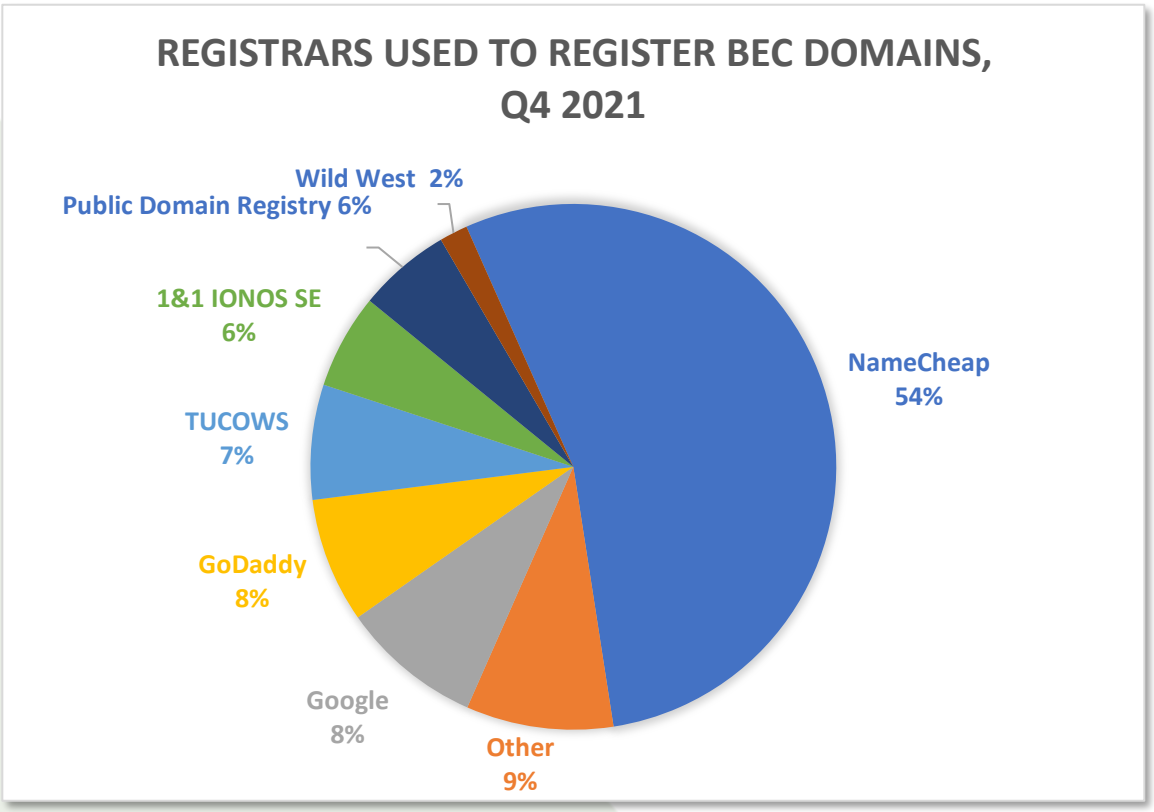
Agari found that the average amount requested in wire transfer BEC attacks in Q4 2021 was $50,027, down from $64,353 in Q3 2021. This decrease occurred as scammers requested fewer large transfers over $100,000. In Q4, only 8 percent of wire transfer requests sought more than $100,000 vs. 16 percent in Q3.

In Q4 2021, gift card requests were the most popular cash-out method, making up 68 percent of the total, followed by payroll diversion attempts (21%) and wire transfer schemes (9%). A variety of miscellaneous cash-out methods accounted for the remaining 2 percent. There was no significant shift in BEC cash-out methods between Q3 and Q4 2021. Looking back at Q4 2020 versus Q4 2021 however, there was a dramatic shift in cash-out methods. In Q4 2020, wire transfer schemes comprised 27 percent of the attacks, while gift card requests and payroll diversion attempts were at 56 percent and 14 percent respectively.

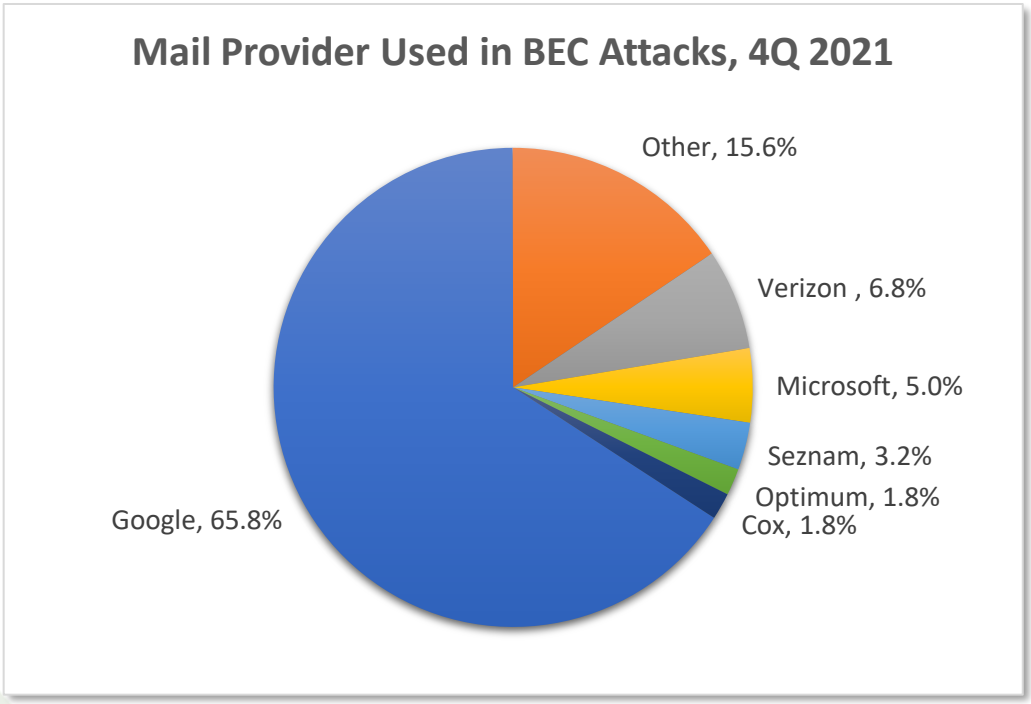
Google Play was the most requested gift card in Q4 2020, accounting for 41.5% of all gift card requests. This was followed by Apple's offerings (Apple Store 10.8% + iTunes 8.9%) and Amazon (13.9%). Liquid

cards not tied to a specific retailer, such as Mastercard, Visa, American Express, and One Vanilla, made up just 9.4 percent of gift card requests. To understand why Google Play is so popular, we need look no further than Paxful, a marketplace where people trade gift cards, bitcoin, and currency. eBay gift cards, which were the 2nd most popular card in Q4 2020, are only getting 59 to 63 cents on the dollar on Paxful today, while Google Play cards are fetching as much as 77 cents on the dollar.

Agari found that domain name registrar Namecheap was the primary registrar used by cybercriminals to register the domain names for BEC attacks in 4Q 2021. NameCheap accounted for more than half of all BEC domain registrations, with Google and GoDaddy each making up 8 percent. As the name implies, NameCheap is one of the least expensive places to register a domain. This is likely a factor in its popularity with scammers.

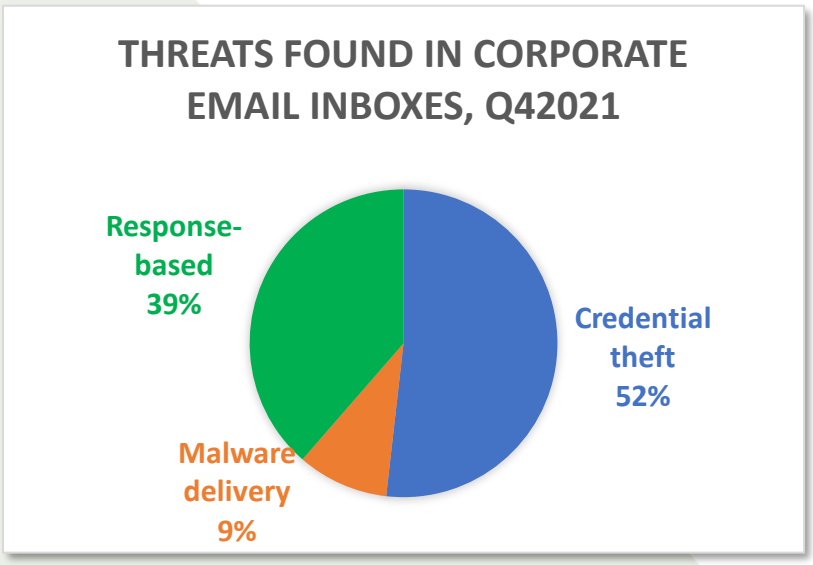



Agari found that Google's GMail was the primary e-mail service used by cybercriminals to create email addresses they used for BEC attacks in 4Q 2021:




## Email-based Threats, 4th Quarter 2021

APWG member PhishLabs, by HelpSystems, analyzes malicious emails reported by corporate users. PhishLabs found that 51.8 percent of them were credential theft phishing attacks, 38.6 percent were response-based attacks (such as BEC, 419, and gift card scams), and 9.6 percent were malware delivery.



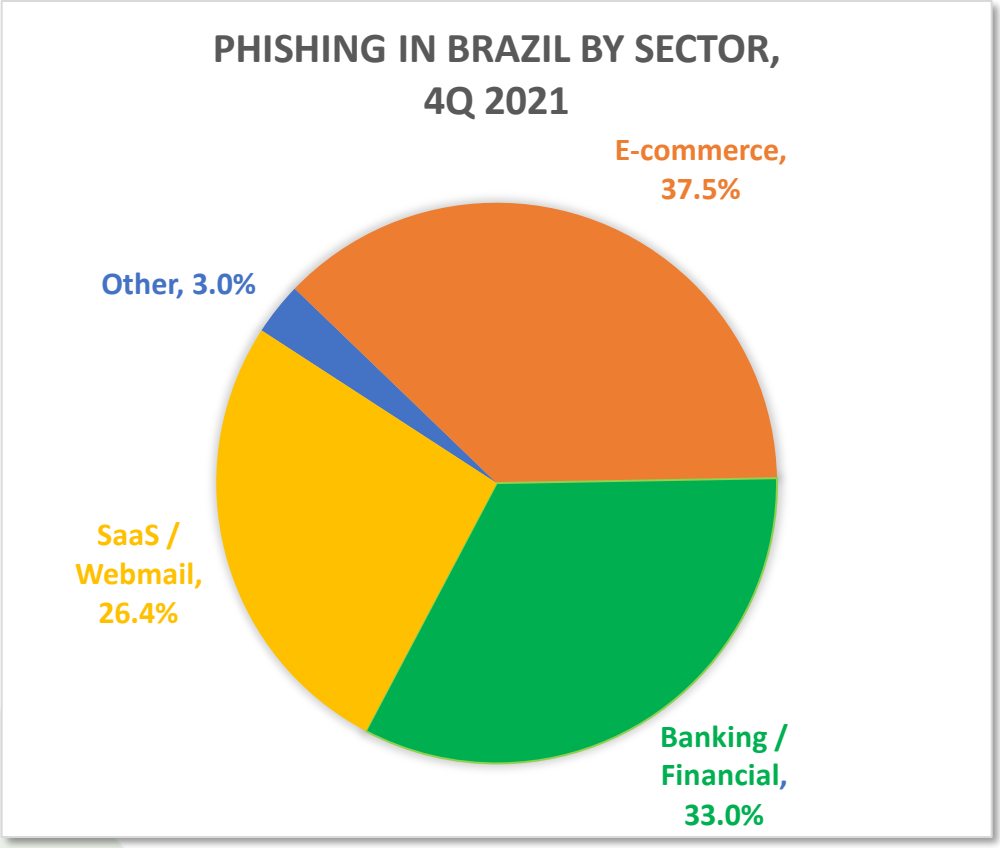
Also noted in the quarter was the return of Emotet, a malware attack usually delivered via email. "The big trend in malicious emails targeting corporate users was the dramatic increase in Qbot (a.k.a. Qakbot) emails. Fifty-nine percent of malware delivered via email in the quarter was attributed to Qbot," noted John LaCour, Founder and CTO of PhishLabs, by HelpSystems.

## 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 Q4 2021, Axur's systems identified 7,101 phishing attacks, down from 7,741 in Q3:


Phishing against SaaS and Webmail companies corrected, totaling 26.4 percent of all attacks after falling to 18 percent in Q3. Phishing against e-commerce companies were 37.5 percent of all attacks.




## Use of Domain Names for Phishing

APWG member RiskIQ (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 13,947 confirmed phishing URLs reported to APWG in Q4 2021. RiskIQ found that they were hosted on just 1,444 unique second-level domains. In comparison, in Q3 RiskIQ analyzed 4,340 confirmed phishing URLs and found that they were hosted on 2,649 unique second-level domains—almost twice as many domains. In 4Q, many phishing URLs in the study set were hosted on a few domains operated by service providers that offer subdomains, such as DuckDNS.ORG, NGROK.IO, and BIT.LY.

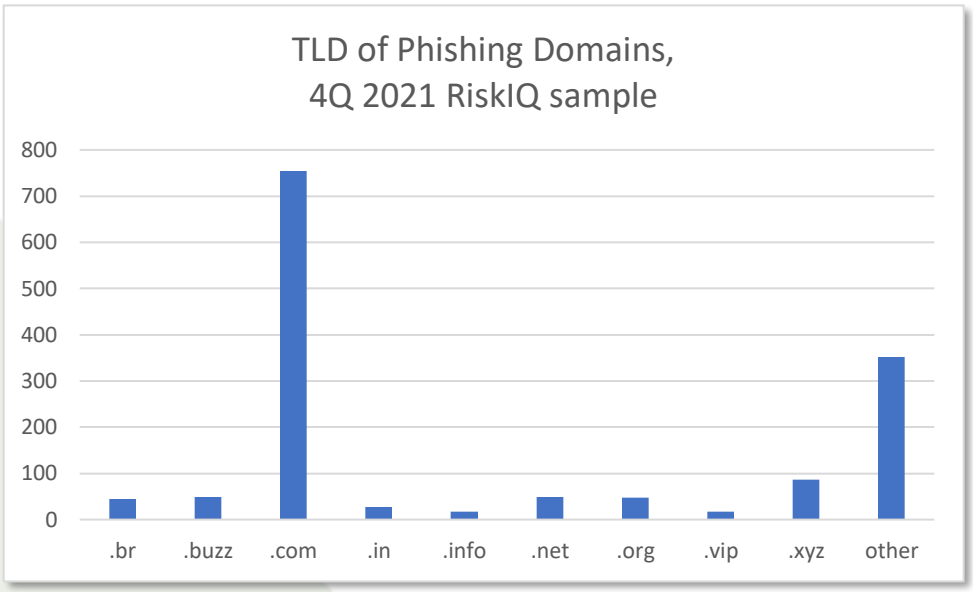
There are three types of top-level domains (TLDs) for purposes of this report:

- "Legacy" generic TLDs, which existed before 2011. These include .COM, .ORG, and TLDs such as .ASIA and .BIZ. They represented about 52 percent of the domain names in the world as of the

beginning of Q4 2021, and represented 60 percent of the phishing domains in the sample set. There were 875 legacy gTLD domains in the sample set. Most of those were in .COM, which had 754 domains in the set.

- The new generic top-level domains (nTLDs), such as .XYZ and .BUZZ, were released after 2011. The nTLDs represented about 6 percent of the domains in the world, but about 14 percent of the domains in the sample set (207 domains).
- The country code domains (ccTLDs), such as .UK for the United Kingdom and .BR for Brazil. ccTLDs were about 42 percent of the domains in the world, but were just 25 percent of the domains in the Q3 sample set (362 domains).

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




During this quarter, RiskIQ observed that hybrid phish kits pieced together from free or readily available kits and services have become increasingly popular.

"The quarterly trends observed by APWG this year are consistent with the 2021 Microsoft Digital Defense Report, insofar as the surge in phishing continued steadily with an increase in the overall number of phishing emails," says Jonathan Matkowsky, a Principal Researcher at Microsoft.

## APWG Phishing Activity Trends Report Contributors

Abnormal Security provides a leading cloud email security platform to stop attacks that evade traditional Secure Email Gateways.

Agari by HelpSystems protects organizations against phishing, business email compromise (BEC) scams, and other 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, by HelpSystems, provides managed threat intelligence and mitigation services that protect brands, customers, and the enterprise from digital risks.

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

The *APWG Phishing Activity Trends Report* is published by the APWG on a quarterly basis as a service to the public and for the industries effected by cybercrime of all types. For further information about the APWG and this publication, please contact APWG Deputy Secretary General Foy Shiver (foy@apwg.org, +1.404.434.728). For media inquiries related to the content of this report, please contact APWG Secretary General Peter Cassidy (pcassidy@apwg.org, +1.617.669.1123); Anil Prasad at Abnormal Security (www.abnormalsecurity.com/contact), Stefanie Wood Ellis of OpSec Security (sellis@opsecsecurityonline.com); Rachel Woodford of Agari (Rachel.Woodford@helpsystems.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**

## 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 multilateral 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 machine event data send more than a billion data elements per month outbound to APWG's members to inform security applications, forensic routines and research programs, helping to protection millions of software clients and devices worldwide. APWG Engineering continues to work with APWG member data correspondents worldwide to develop new data resources.

APWG eCrimeX

STOP | THINK | CONNECT MESSAGING CONVENTION

APWG's STOP. THINK. CONNECT. cybersecurity awareness campaign has officially engaged campaign curators from 26 nations, deploying STOP. THINK. CONNECT. through cabinet-level government ministries 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.

eCrime2022
Symposium on Electronic Crime Research

**Contact**: PR@apwg.org