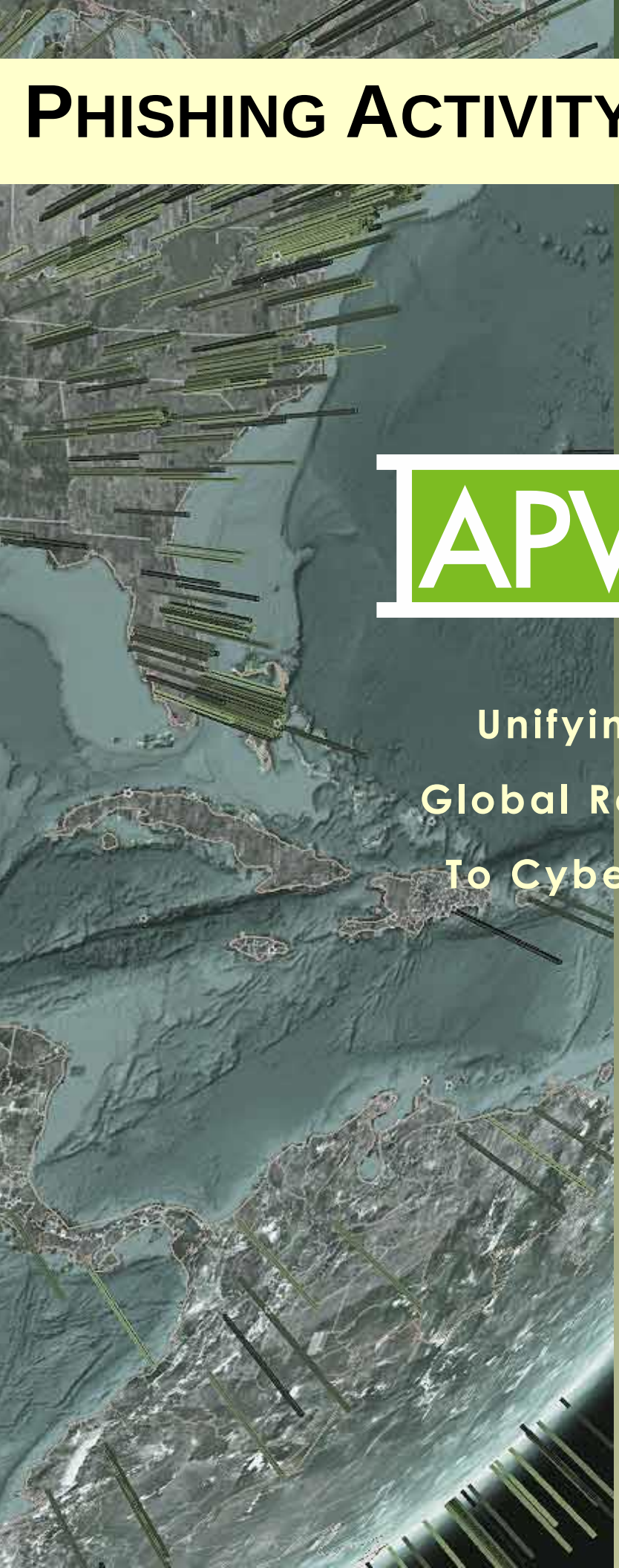
Phishing Activity Trends Report



3rd Quarter 2022

APWG

Unifying the
Global Response
To Cybercrime

Activity July-September 2022

Published 12, December 2022

Phishing Report Scope

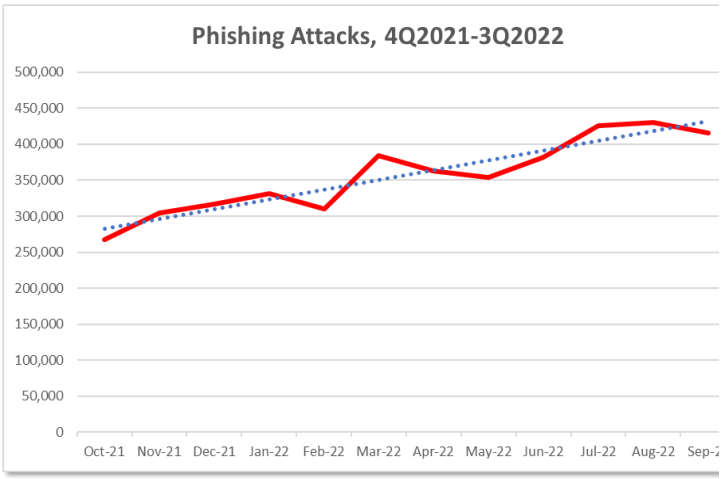
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. 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 New Quarterly High in Late 2022



Phishing Activity Trends Summary

- In the third quarter of 2022, APWG observed 1,270,883 total phishing attacks, a new record and the worst quarter for phishing that APWG has ever observed. [pp. 3-4]
- Fewer companies were victimized by ransomware than at any point since early 2021. [pp. 6-7]
- Attacks against the financial sector represented 23.2% of all phishing attacks. [p. 5]
- Business Email Compromise (BEC) attacks continued to be troublesome, and the number of wire transfer BEC attacks in Q3 increased by 59%. [p. 8]
- Advance fee fraud scams launched via email increased by 1,000% in Q3. [p. 9]

Statistical Highlights for the 3rd Quarter 2022

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.

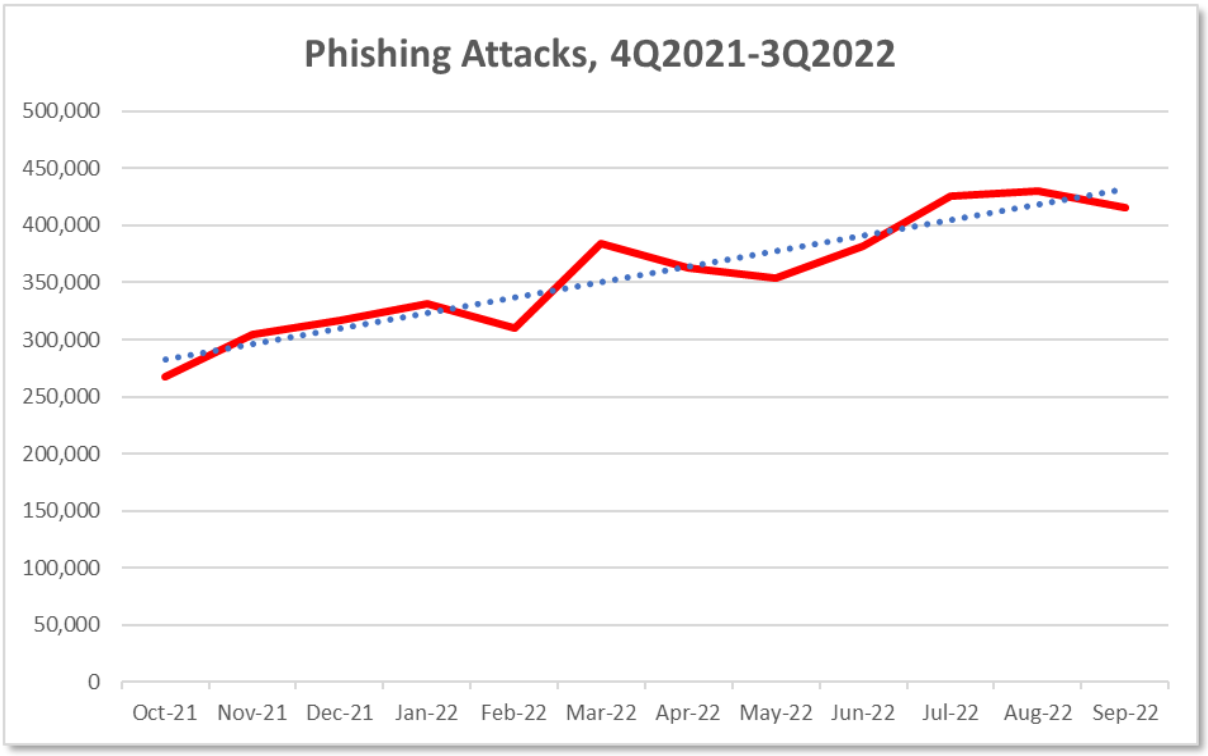
The APWG tracks:

- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique 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.

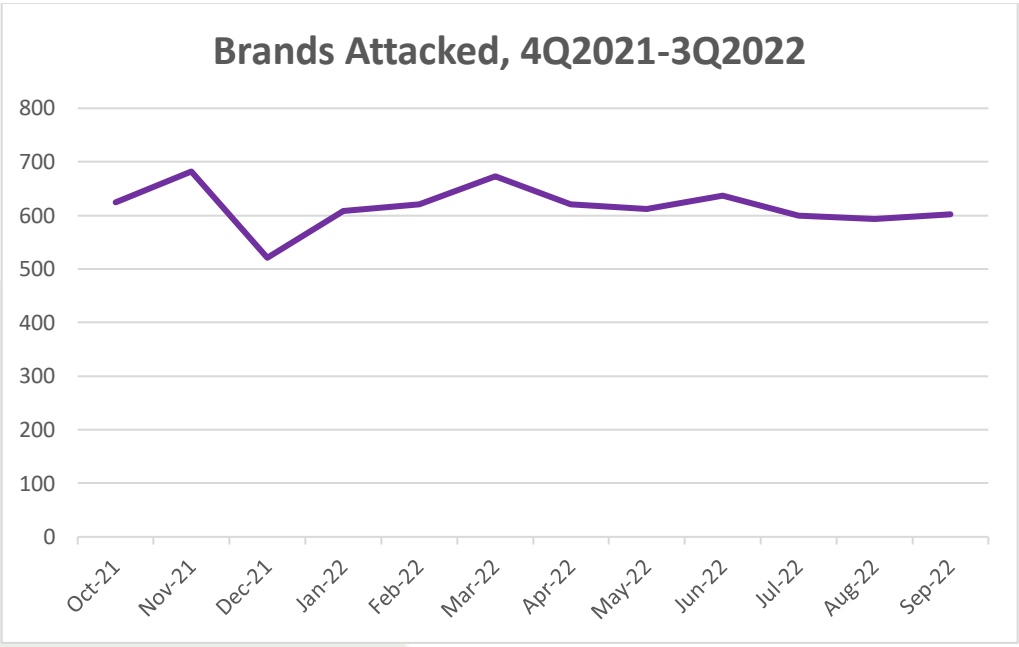
	July	August	Sept
Number of unique phishing Web sites (attacks) detected	425,112	430,141	415,630
Unique phishing email subjects	64,696	38,228	23,994
Number of brands targeted by phishing campaigns	621	612	637

In the second quarter of 2022, APWG observed 1,097,811 total phishing attacks, a record at the time. **In the third quarter of 2022, APWG observed 1,270,883 total phishing attacks, a new record and the worst quarter for phishing that APWG has ever observed.** The total for August 2022 was 430,141 attacks, which is the highest monthly total reported. The number of reported phishing attacks reported to APWG has more than quintupled since the first quarter of 2020, when APWG observed 230,554 attacks.

The rise in Q3 2022 is attributable in part to increasing numbers of attacks reported against several specific targets. These targets suffered from large numbers of attacks from persistent phishers.



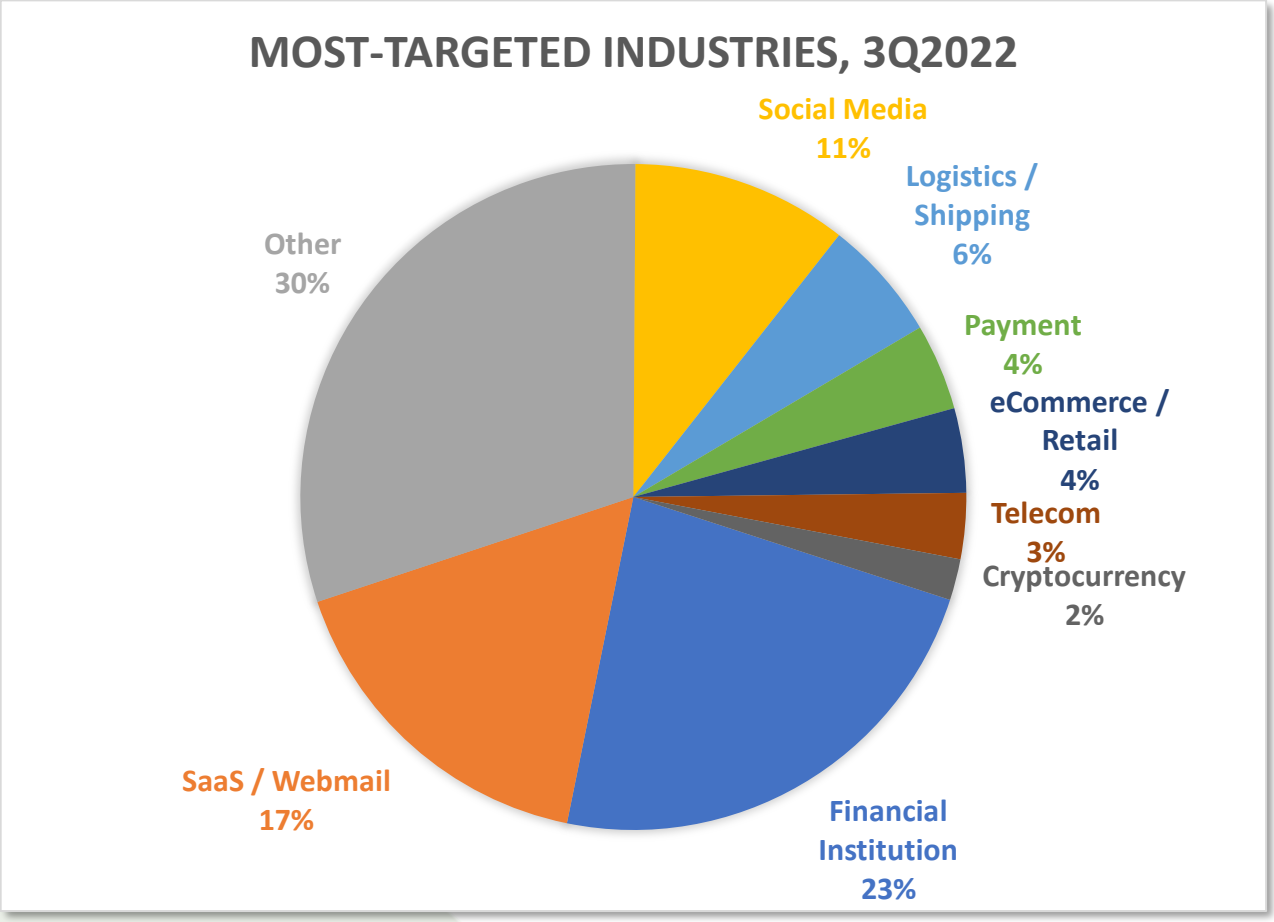
The number of Unique Subjects grew as more submitted emails had differing subject lines. The number of brands attacked each month has remained steady, and below the high of 715 observed in September 2021:



Most-Targeted Industry Sectors – 3rd Quarter 2022

In the third quarter of 2022, APWG founding member OpSec Security found that phishing attacks against the financial sector, which includes banks, remained the largest set of attacks, accounting for 23.2 percent of all phishing, down from 27.6 percent in Q2. Attacks against webmail and software-as-a-service (SAAS) providers remained steady, while attacks against retail/ecommerce sites fell to 4.1 percent, down from 14.6 percent in Q1. Phishing against social media companies trended downward, after fluctuating from 8.5 percent of all attacks in 4Q2021 to 15.5 percent in 2Q2022. Phishing against cryptocurrency targets – such as cryptocurrency exchanges and wallet providers—fell from 4.5 percent in Q2 to 2.0 percent in Q3 as the crypto market was roiled by falling values.

Matthew Harris, Senior Product Manager, Fraud at OpSec Security, noted: "The Logistics and Shipping sector saw a large fraud volume increase, led specifically by a large increase in phishing against the U.S. Postal Service. And continuing a trend we observed in Q2, we're tracking a huge increase in mobile phone-based fraud; vishing detection volumes are more than three times what we saw in Q2."

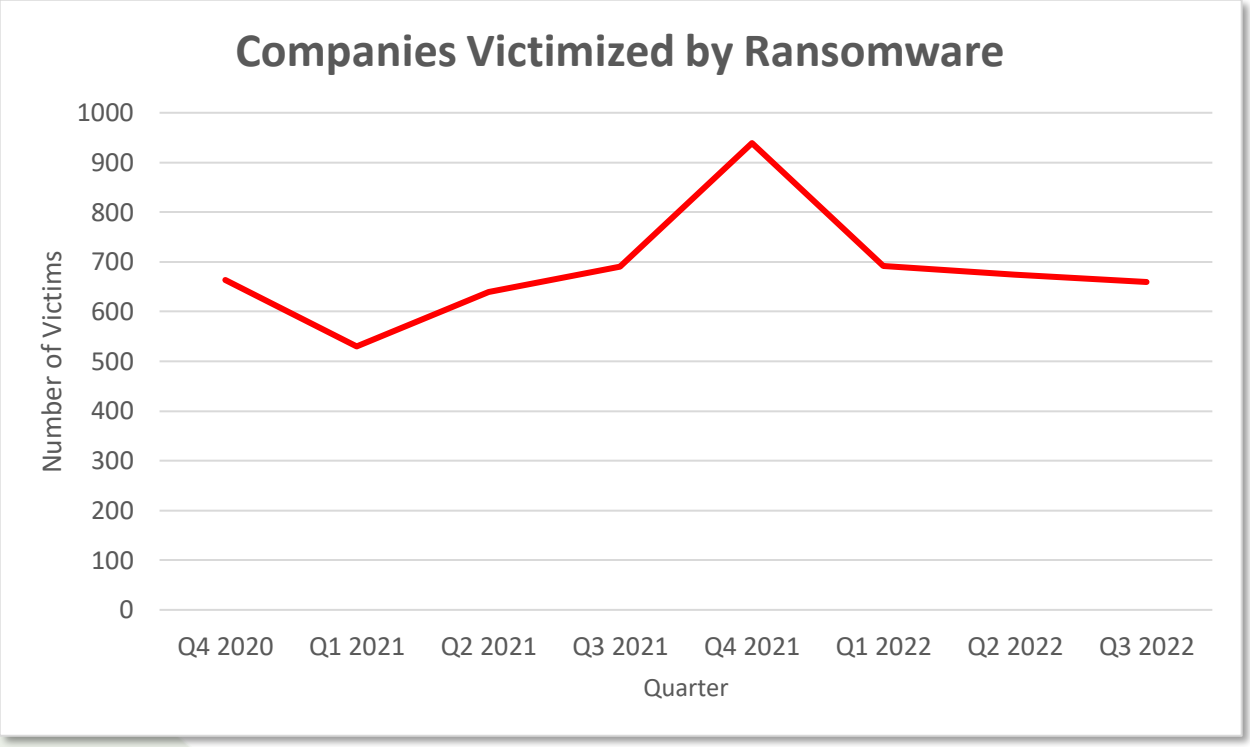


OpSec Security offers world-class brand protection solutions.

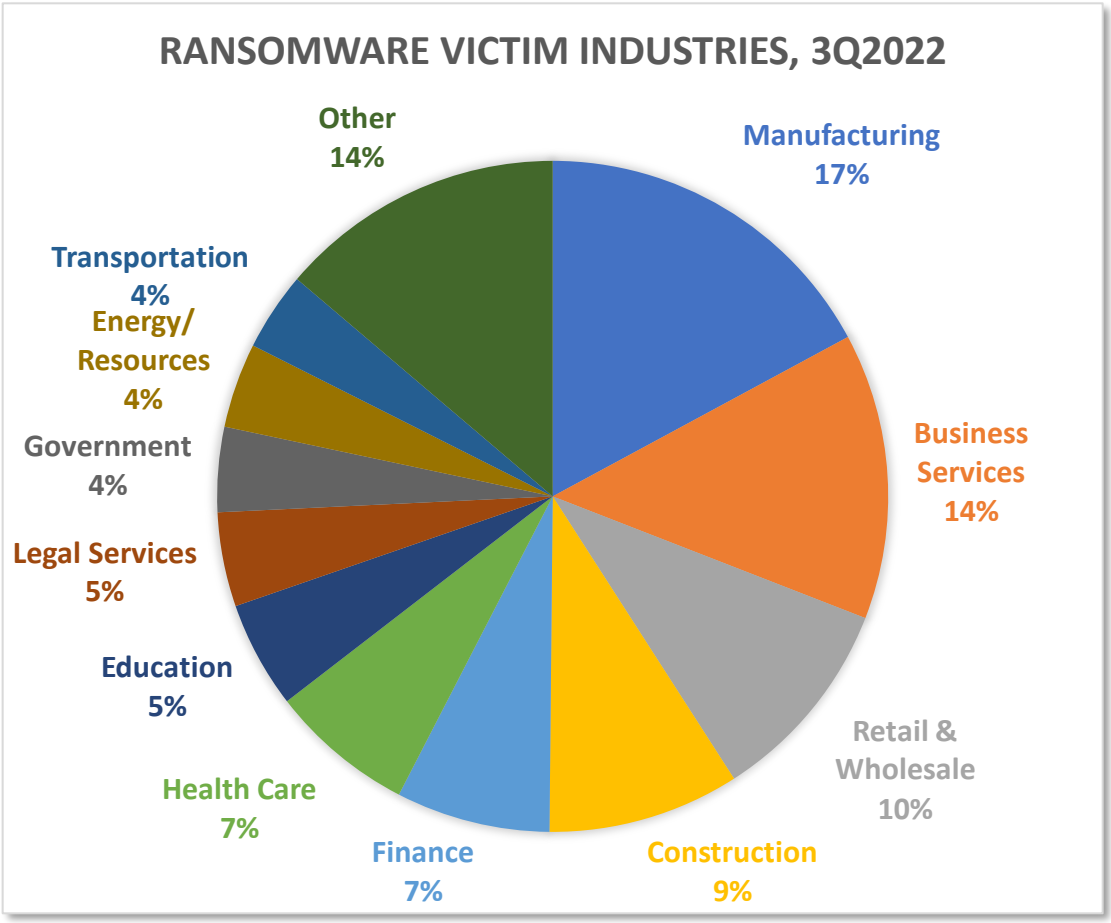
Ransomware – 3rd Quarter 2022

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.

After falling to an 18-month low at the end of Q2, ransomware activity leveled off in the third quarter, with the number of ransomware victims decreasing 2 percent compared to Q2. The volume observed in Q3 was 5 percent lower than what Abnormal saw in Q3 2021.



Crane Hassold, Director of Threat Intelligence at Abnormal Security, analyzed the ransomware activity over the quarter. "Historically, the top target of ransomware attacks has been the Manufacturing industry, peaking in Q1 of 2022 with a target share of 25 percent. While manufacturing organizations were still the number one victim of ransomware attacks in Q3, the overall number of manufacturing victims dropped substantially, falling 30 percent compared to the previous quarter." However, attacks against related sectors such as Construction and Transportation were also frequent:



Abnormal found that the LockBit cybercrime group is the primary player in the ransomware space, responsible for 35 percent of all ransomware attacks observed in Q3. "Filling the void left by other groups that have exited the ransomware space recently is a revolving door of smaller groups trying to establish a foothold of their own. Of the 33 groups we observed in Q3, ten of them were new groups that weren't active the previous quarter," said Hassold.

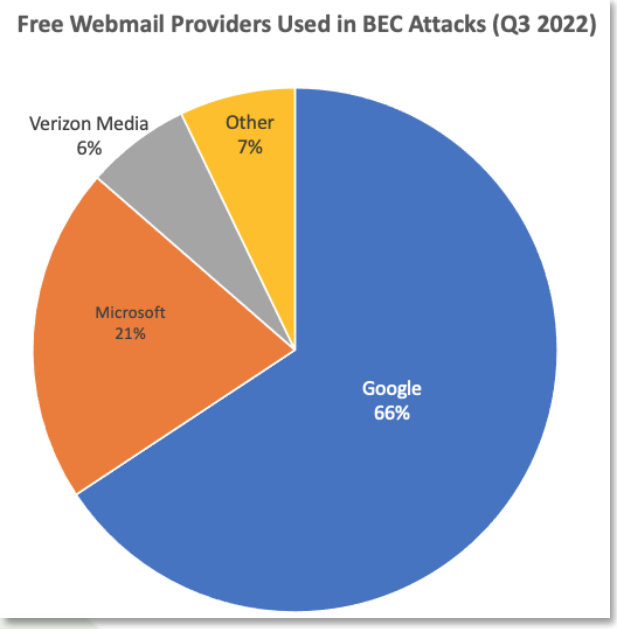
Abnormal found that 39 percent of ransomware attacks targeted American companies. France and the United Kingdom were second with 5 percent each. In Q3, attacks on Spanish companies increased to 4 percent of the world total, primarily driven by attacks from a new ransomware group, Sparta, which emerged in September 2022 and thus far only victimized organizations in Spain.

Business e-Mail Compromise (BEC), 3rd Quarter 2022

APWG member Agari by Fortra 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 during Q2 2022. 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 data. Agari protects organizations against phishing, BEC scams, and other advanced email threats.

Agari found that the number of wire transfer BEC attacks in Q3 increased by 59 percent compared to Q2 2022. The average amount requested in wire transfer BEC attacks in Q3 2022 declined 14 percent to $93,881, down from the Q2 average of $109,467.

During Q3 2022, gift card requests were the most popular cash-out method, making up 38.5 percent of the total. This was followed by advance fee fraud (30.9%), payroll diversion attempts (12.5%), and wire transfers (4.9%), with miscellaneous cash-out methods accounting for the balance. While the share of payroll diversion attempts fell to 12.5 percent versus 26 percent in the previous quarter, the number of attempted payroll diversions increased 182 percent in the same timeframe.



Amazon surpassed Google Play as the most requested gift card type in Q3, with 38 percent of fraud attempts requesting Amazon vs. just 22 percent asking for Google Play. Apple's offerings remained in third place (Apple Store 14.0% + iTunes 5%), followed by eBay (4%), Steam (4%), American Express (3%), and Visa (3%).

Agari found that 85 percent of BEC attacks in Q3 2022 were launched using a free webmail domain, up from 73 percent in Q2. The remaining 15 percent of BEC attacks in Q3 utilized maliciously registered domains and compromised email accounts. While still the favorite webmail provider of BEC scammers, Google's Gmail slipped from a 72 percent share in Q2 to 66 percent in Q3 2022. Microsoft's webmail properties powered 21 percent of webmail-based BEC attacks in Q3, versus just 8 percent in Q2. Verizon Media made up 6 percent of webmail-based BEC attacks in Q3, with a long tail of providers accounting for the remaining 7 percent.

Email-based Threats, 3rd Quarter 2022

APWG member PhishLabs by HelpSystems analyzes malicious emails reported by corporate users. John Wilson, Senior Fellow, Threat Research at Fortra, notes that "We saw a 488 percent increase in response-based email attacks in Q3 2022 compared to Q2. While every subtype of these attacks increased compared to Q2, the largest increase was in Advance Fee Fraud schemes, which rose by a staggering 1,074 percent."

Wilson also added: "Though down slightly in Q3 compared to the historic level seen in Q2, social media threats targeting the enterprise continued to represent a significant business risk. While impersonation remained the largest category of social media threats to the enterprise, physical threats surpassed fraud for the first time since Q1 of 2021."

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 Fortra 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 Fortra provides managed threat intelligence and mitigation services that protect brands, customers, and the enterprise from digital risks.

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); Anil Prasad at Abnormal Security (www.abnormalsecurity.com/contact), Stefanie Wood Ellis of OpSec Security (sellis@opsecsecurityonline.com); Rachel Woodford for Agari and PhihsLabs (Rachel.Woodford@helpsystems.com), Eduardo Schultze of Axur (eduardo.schultze@axur.com,+55 51 3012-2987). **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 eCrimeX

APWG's clearinghouses for cybercrime-related machine event data send more than two 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 data correspondents worldwide to develop new data resources.

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

STOP|THINK|CONNECT MESSAGING CONVENTION

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