Phishing Activity Trends Report

1st

Quarter

2022

APWG

Unifying the

Global Response

To Cybercrime

Activity January-March2022

Published 7 June 2022

Phishing Report Scope

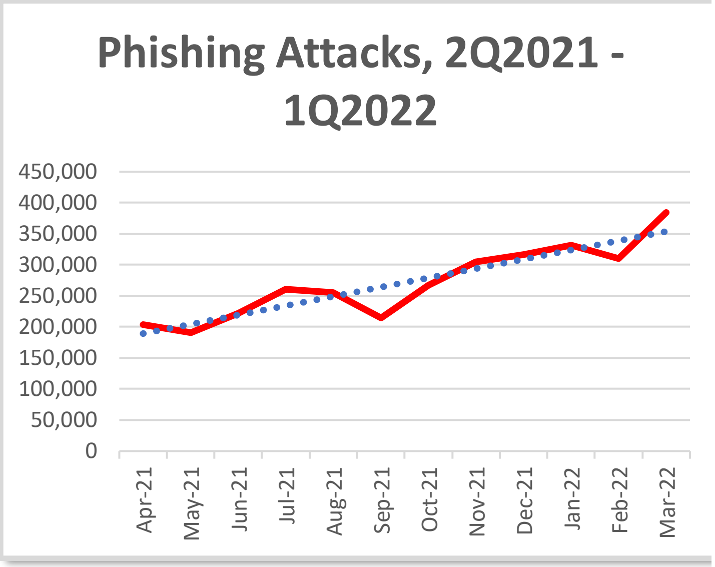
The *APWG Phishing Activity Trends Report* analyzes phishing attacks and other identity theft techniques, as reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org.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



Phishing Activity Trends Summary

- In the first quarter of 2022, APWG observed 1,025,968 total phishing attacks. This was the worst quarter for phishing that APWG has ever observed, and the first time that the quarterly total has exceeded one million. [pp. 3-4]
- Most sectors saw a decrease in the overall number of ransomware attacks against them, but the Financial Services industry saw an 35% increase in the number of attacks during 1Q2022. [pp. 6-7]
- There was a 7% increase in credential theft phishing against enterprise users. [p. 10]
- The impersonation of corporate executives on social media was an increasing observed business risk. [p. 11]
- The financial sector was the most frequently victimized by phishing in Q1, with 23.6% of all attacks. Attacks against SaaS and webmail providers continued to be numerous. Phishing against cryptocurrency targets inched up to 6.6% of attacks. [p. 5]

Statistical Highlights for the 1st Quarter 2022

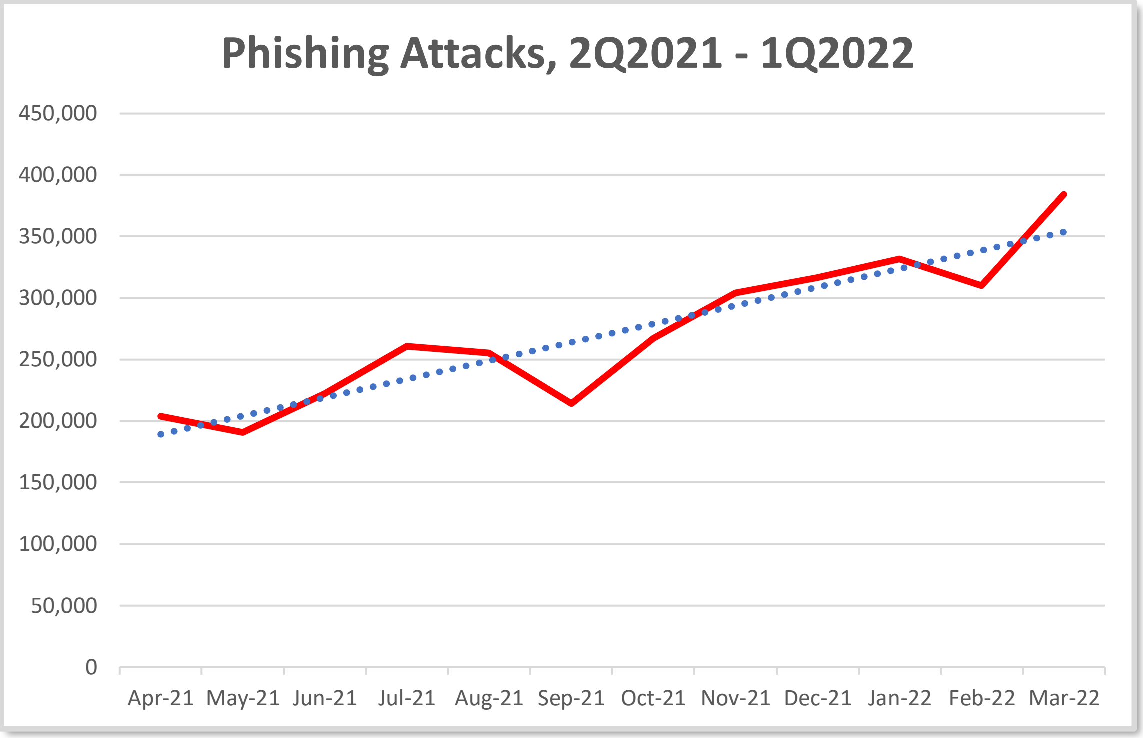
APWG's contributing members study the ever-evolving nature and techniques of cybercrime. With this report, the APWG has refined the methodologies it uses to report phishing. APWG has two sources of phishing data: phishing emails reported to it by APWG members and by members of the public, and phishing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

The APWG tracks:

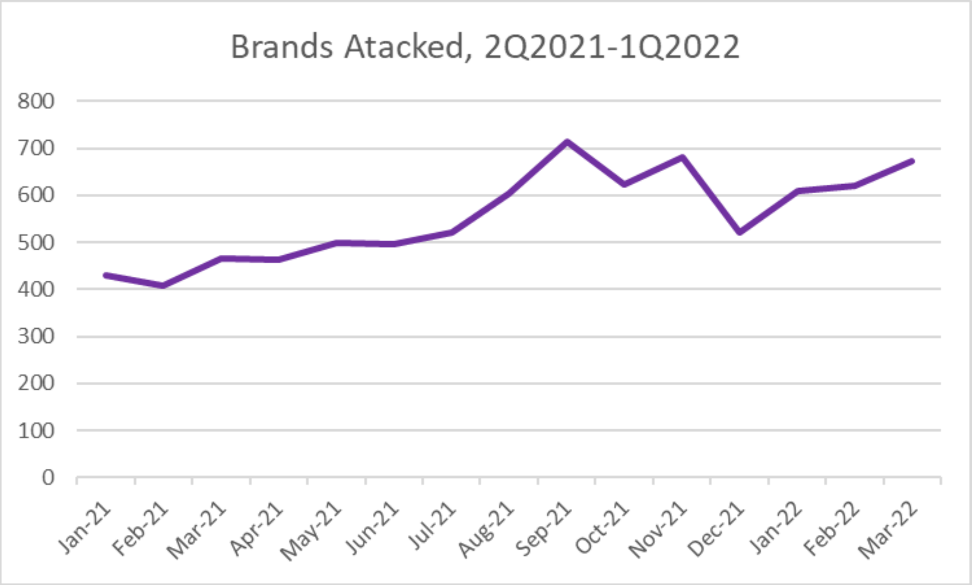
- **Unique phishing sites**. This is a primary measure of reported phishing across the globe. This is determined by the unique base URLs of phishing sites found in phishing emails reported to APWG's repository. (A single phishing site may be advertised as thousands of customized URLs, all leading to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

	January	February	March
Number of unique phishing Web sites (attacks) detected	331,698	309,979	384,291
Unique phishing email subjects	15,275	14,176	24,187
Number of brands targeted by phishing campaigns	608	621	673

APWG saw 384,291 attacks in March 2022, which was the highest monthly total in APWG's reporting history. In the first quarter of 2022, APWG observed 1,025,968 total phishing attacks. This was the worst quarter for phishing that APWG has ever observed, and the first time that the quarterly total has exceeded one million. The previous record was 888,585 attacks, observed in the fourth quarter of 2021. The number of phishing attacks has more than tripled since early 2020, when APWG was observing between 68,000 and 94,000 attacks per month.

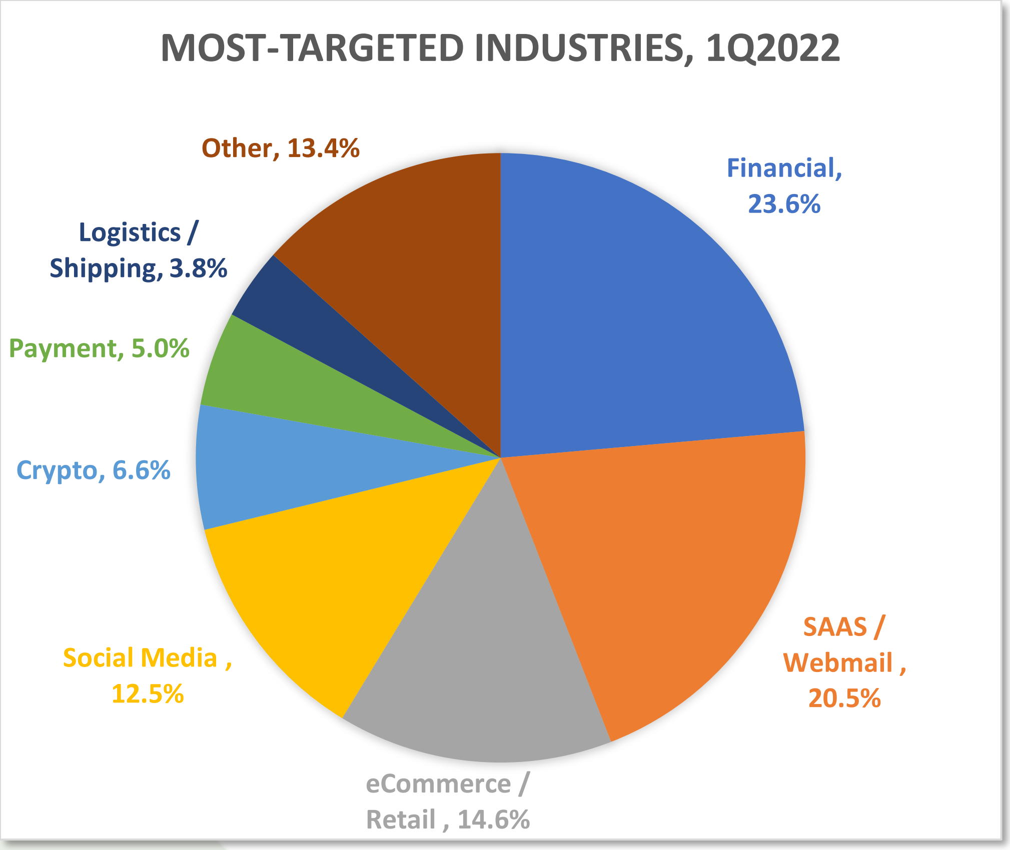


The number of Unique Subjects has dipped as more submitted emails have had duplicative subject lines. The number of brands attacked each month has remained below the high of 715 observed in September 2021, still reaching as high as 673 in March, 2022:



Most-Targeted Industry Sectors – 1st Quarter 2022

In the first 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 23.6 percent of all phishing. Attacks against webmail and software-as-a-service (SAAS) providers remained prevalent with attacks against retail/ecommerce sites falling from 17.3 to 14.6 percent after the holiday shopping season. Phishing against social media sets rose from 8.5 percent of all attacks in 4Q2021 to 12.5 percent in 1Q2022. Phishing against cryptocurrency targets—such as cryptocurrency exchanges and wallet providers—remained steady from late 2021, inching up from 6.5 to 6.6 percent in the latest quarter. OpSec Security offers world-class brand protection solutions.

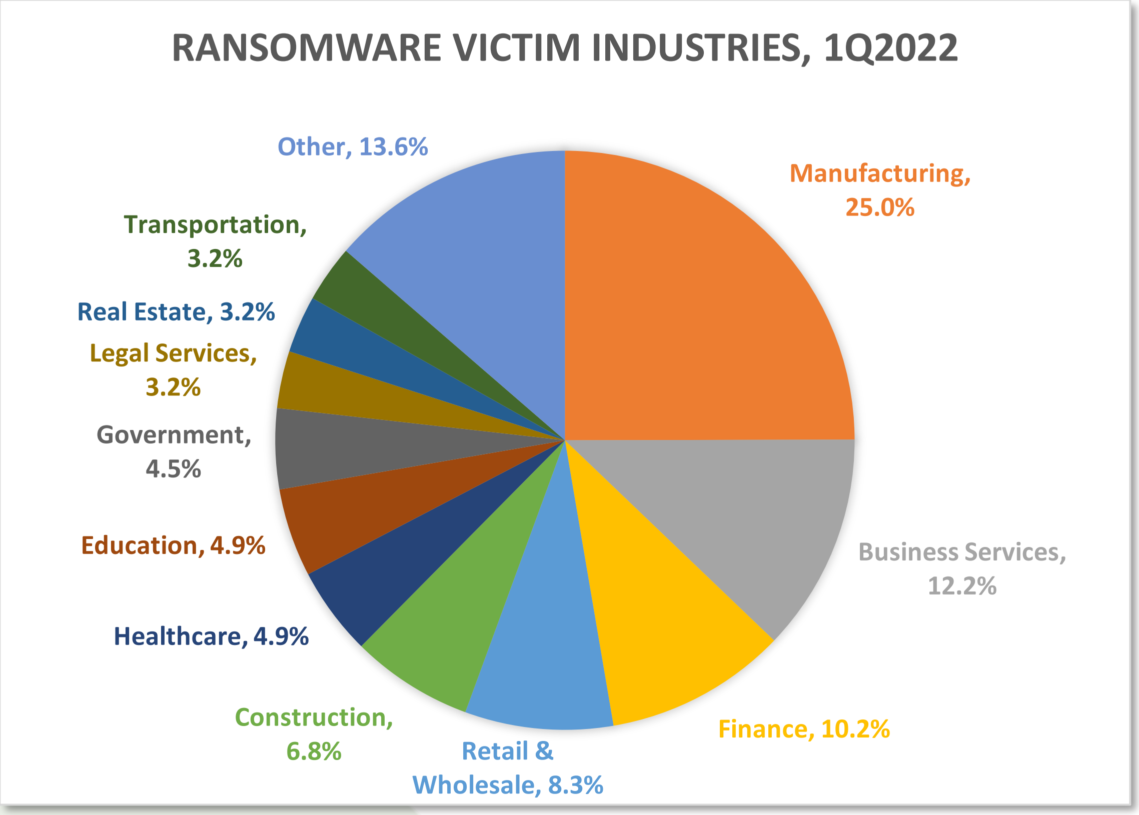


Ransomware - 1st Quarter 2022

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.

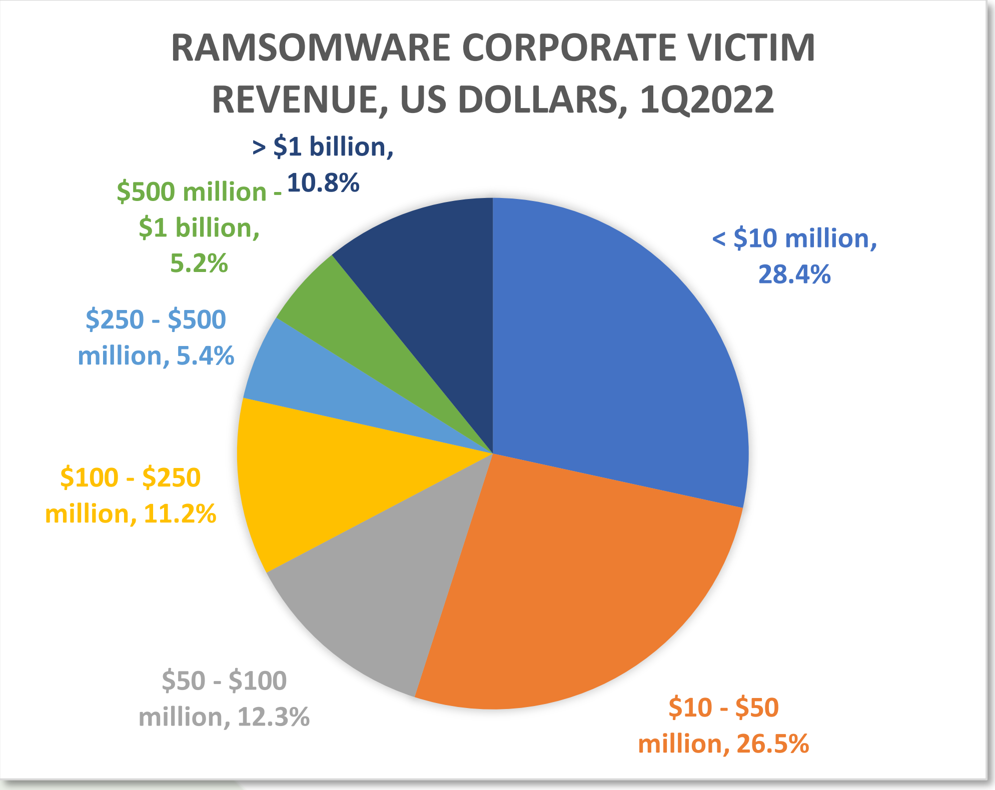
Abnormal Security found the total number of ransomware attacks decreased by 25 percent in the first three months of 2022, falling to a similar level that Abnormal observed in the third quarter of 2021. This decrease seems to be primarily caused by a big drop in attacks from two prolific ransomware groups.

The top industries impacted by ransomware in Q4 2021 were manufacturing, business services, finance, and retail and wholesale firms:



Nearly all industries saw a decrease in the overall number of ransomware attacks targeting companies in their sectors. The notable exception to this was the Financial Services industry, which saw a 35 percent increase in the number of attacks during 1Q2022. Attacks against financial institutions have been on an upward trend over the past year, with attacks 75 percent higher than Abnormal observed in the first quarter of 2021. The main driver behind this growth appears to be an increased focus on financial institutions by the LockBit crime group, primarily on smaller accounting and insurance firms.

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 the first quarter of 2022, the median annual revenue of companies victimized by malware was US$31 million. About 55 percent of victimized companies had less than US$50 million in revenue, down from about 66 percent in 2021. These smaller companies are generally unable to invest large amounts of money in cybersecurity, which makes them better opportunistic targets. But almost 11 percent of the victim corporations had revenues of more than US$1 billion:



Less than half of ransomware attacks victimized North American companies for the first time since at least the beginning of 2020. Attacks against European targets peaked in the first quarter of 2022. About a quarter of ransomware attacks in 2021 went after companies in Europe, but in 1Q2022, more than a third of all ransomware attacks victimized European institutions, primarily targets in Western Europe.

"The first quarter of 2022 saw the emergence of two new impactful groups to the ransomware scene: ALPHV and Stormous" said Crane Hassold, Director of Threat Intelligence at Abnormal Security. "ALPHV, which has also been known as BlackCat, initially appeared in December 2021, but really started ramping up their operations in the first part of 2022. ALPHV targets a representative range of industry types, but the median annual revenue of its victims was $57 million, compared to just $31 million for ransomware victims globally, indicating that ALPHV has a potential preference for larger enterprise targets."

Hassold also noted that Stormous emerged in January 2022 and quickly became the fourth-most active ransomware group. Stormous is different from most other ransomware groups in that it primarily announces its victims via a Telegram chat group rather than a blog on the dark web, although the group did stand up a dark web presence at the end of March.

Business e-Mail Compromise (BEC), 1st Quarter 2022

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 Q1 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 materials. Agari protects organizations against phishing, BEC scams, and other advanced email threats.

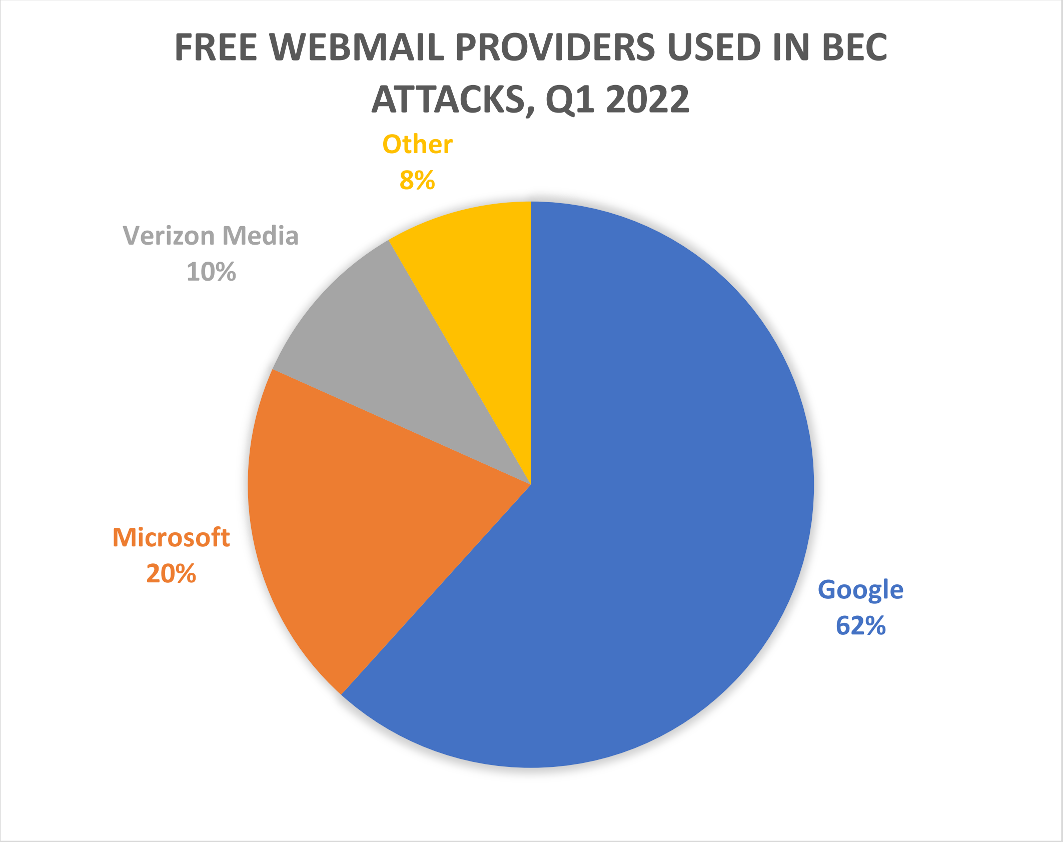
In Q1 2022, gift card requests remained the most popular cash-out method, involved in 63 percent of total attacks, followed by payroll diversion attempts (16%), and wire transfer schemes (9%). A variety of miscellaneous cash-out methods accounted for the remaining 12 percent. Q1 2022 saw an increase in advanced fee fraud and aging report scams. When Agari looked back a year, from Q1 2021 versus Q1 2022, Agari saw an increase in advanced fee fraud, cryptocurrency, and Zelle cash out attempts, with a corresponding decrease in wire transfer requests in 2022.

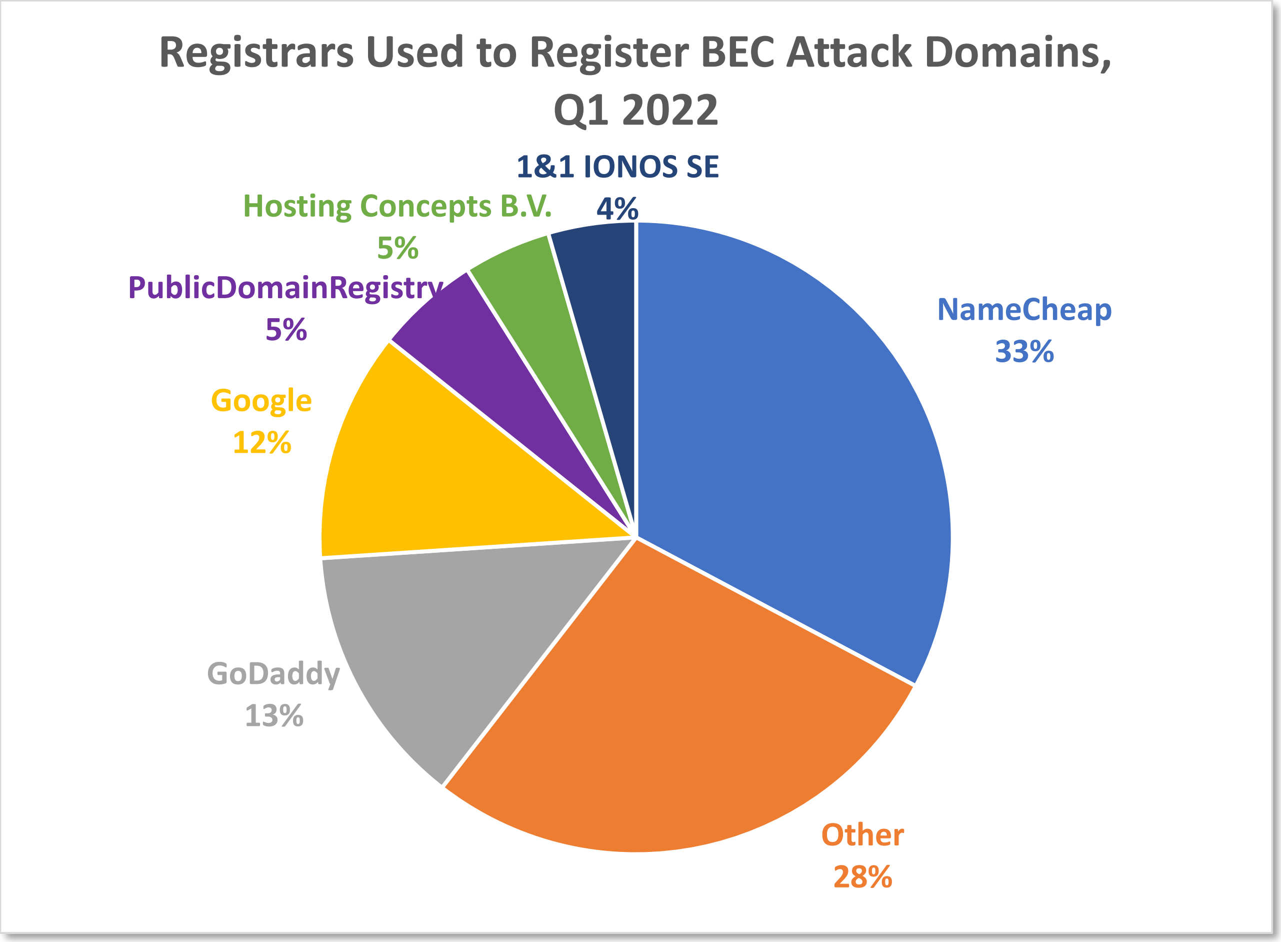
Google Play was the most requested gift card in Q1 2022, accounting for 47.4 percent of all gift card requests. This was followed by Amazon (19.6%) and Apple's offerings at 18 percent (Apple Store 13.4%

and iTunes 4.6%). Liquid cards not tied to a specific retailer, such as Mastercard, Visa, American Express, and One Vanilla, made up just 6 percent of gift card requests.

Agari found that the average amount requested in wire transfer BEC attacks in Q1 2022 was $84,512, an increase of 69 percent from Q4 2021's average of $50,027. The higher Q1 2022 average was due to a 280 percent increase in requests for amounts greater than $100,000. In Q1 2022, 21.6 percent of wire transfer requests sought more than $100,00, versus just 7.7 percent in Q4 2021.

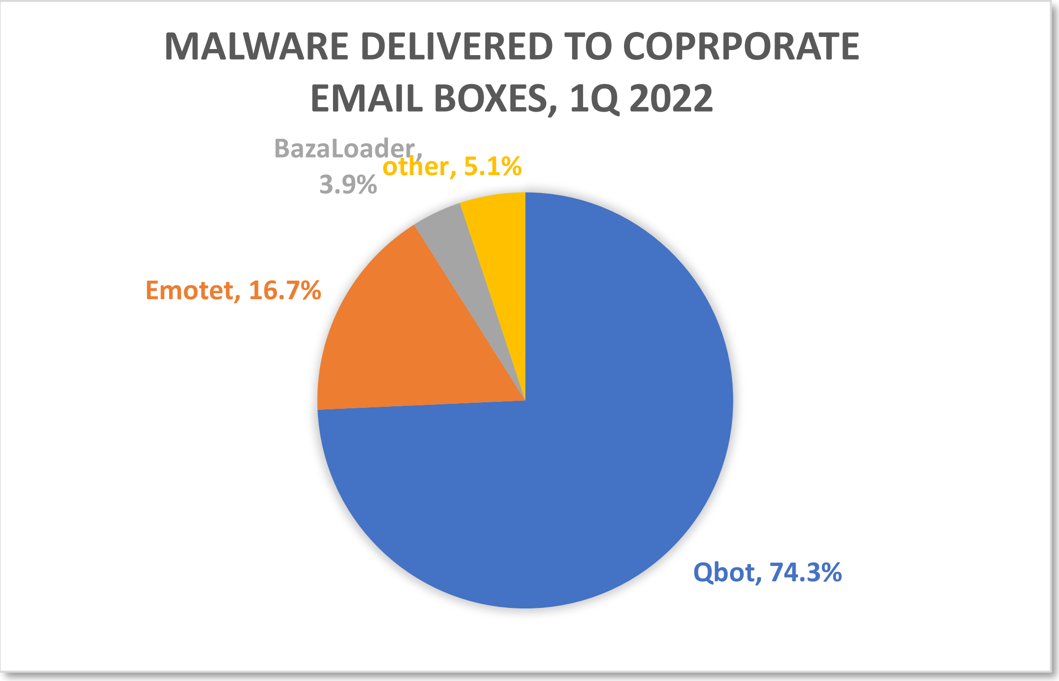
John Wilson, Senior Fellow, Threat Research at HelpSystems, notes that "In Q1 2022, 82 percent of Business Email Compromise messages were sent from free webmail accounts. Of those, 60 percent used Gmail.com. For the 18 percent of BEC messages sent from attacker-controlled domains, NameCheap was the most popular registrar. One third of all maliciously registered domains use for BEC attacks were registered via NameCheap."



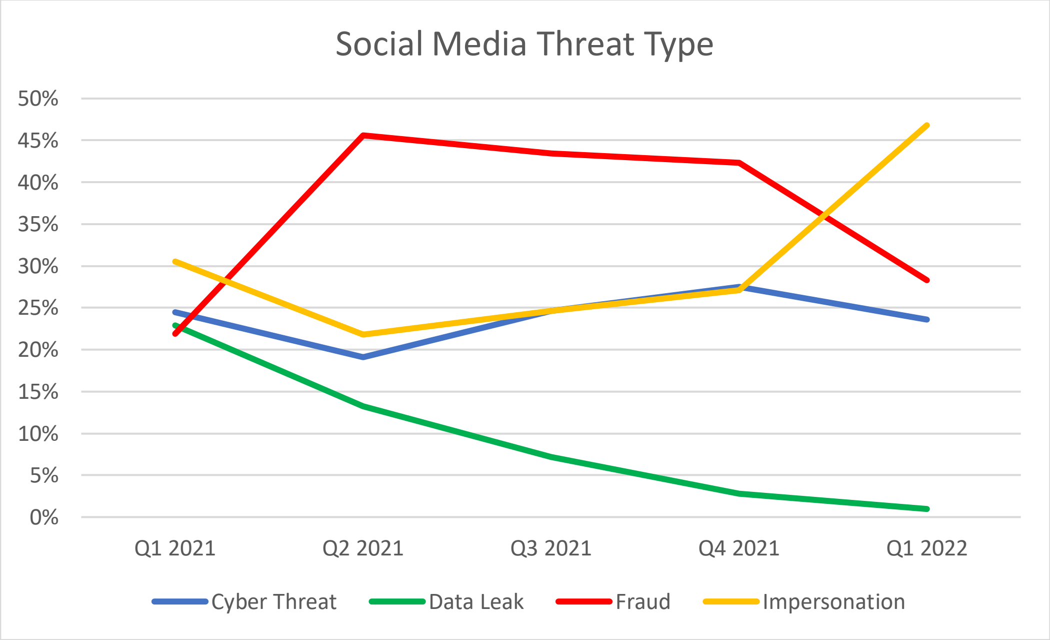


Email-based Threats, 1st Quarter 2022

APWG member PhishLabs by HelpSystems analyzes malicious emails reported by corporate users. John LaCour, Principal Product Strategist at PhishLabs by HelpSystems, said that "In Q1 2022, we observed a 7 percent increase in credential theft phishing against enterprise users, up to nearly 59 percent of all malicious emails." Though down slightly, malware attacks via email are still a concern. "The good news is that Zloader malware has tapered off to nearly zero after being 29 percent of malware in 4Q 2022. But the bad news is Emotet was back in early 2022, and Qakbot is still the number one malware threat via email," LaCour said.



“Social media attacks against business continue to grow quickly,” observed LaCour. “The average company is targeted nearly three times a day via social media.” In Q1 2022, impersonation attacks were 47 percent of social media threats, up from 27 percent the prior quarter. “A lot of companies don’t realize that their executives are being spoofed on social media. This is a huge business risk,” said LaCour.



APWG Phishing Activity Trends Report Contributors

Abnormal Abnormal Security provides a leading cloud email security platform to stop attacks that evade traditional Secure Email Gateways.	AGARI Agari by HelpSystems protects organizations against phishing, business email compromise (BEC) scams, and other advanced email threats.	///AXUR Axur works to identify and fight the threats in the cyberspace that interfere with the interests of companies, governments, and individuals.
ILLUMINTEL Illumintel provides intelligence, analysis, due diligence, and public policy advising in the areas of cybersecurity and Internet-based commerce.	OpSec SECURITY OpSec Security offers world-class brand protection solutions.	PHISHLABS PhishLabs by HelpSystems provides managed threat intelligence and mitigation services that protect brands, customers, and the enterprise from digital risks.
	RISKIQ 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. 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 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 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 currently deployed by 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.