agari by HelpSystems

PHISHLABS by HelpSystems

QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT

MAY 2022

CONTENTS

ABOUT THE REPORT

In Q1, Agari and PhishLabs analyzed hundreds of thousands of phishing and social media attacks targeting enterprises, their employees, and brands. This report uses the data from those attacks to present key trends shaping the threat landscape.

Security leaders and practitioners can use this information to better understand these threats and to take proactive measures to reduce risk.

KEY TAKEAWAYS

Social Media Impersonations on the Rise

Brand Impersonations are a convenient target for threat actors up 339% in one year.

Social Media a Leading Threat Channel

Average number of attacks per target up 105% from Q1 2021 to Q2 2022.

Ransomware Payload Landscape is Ever-Changing

Qbot led the way for second consecutive quarter with a reemergence of Emotet.

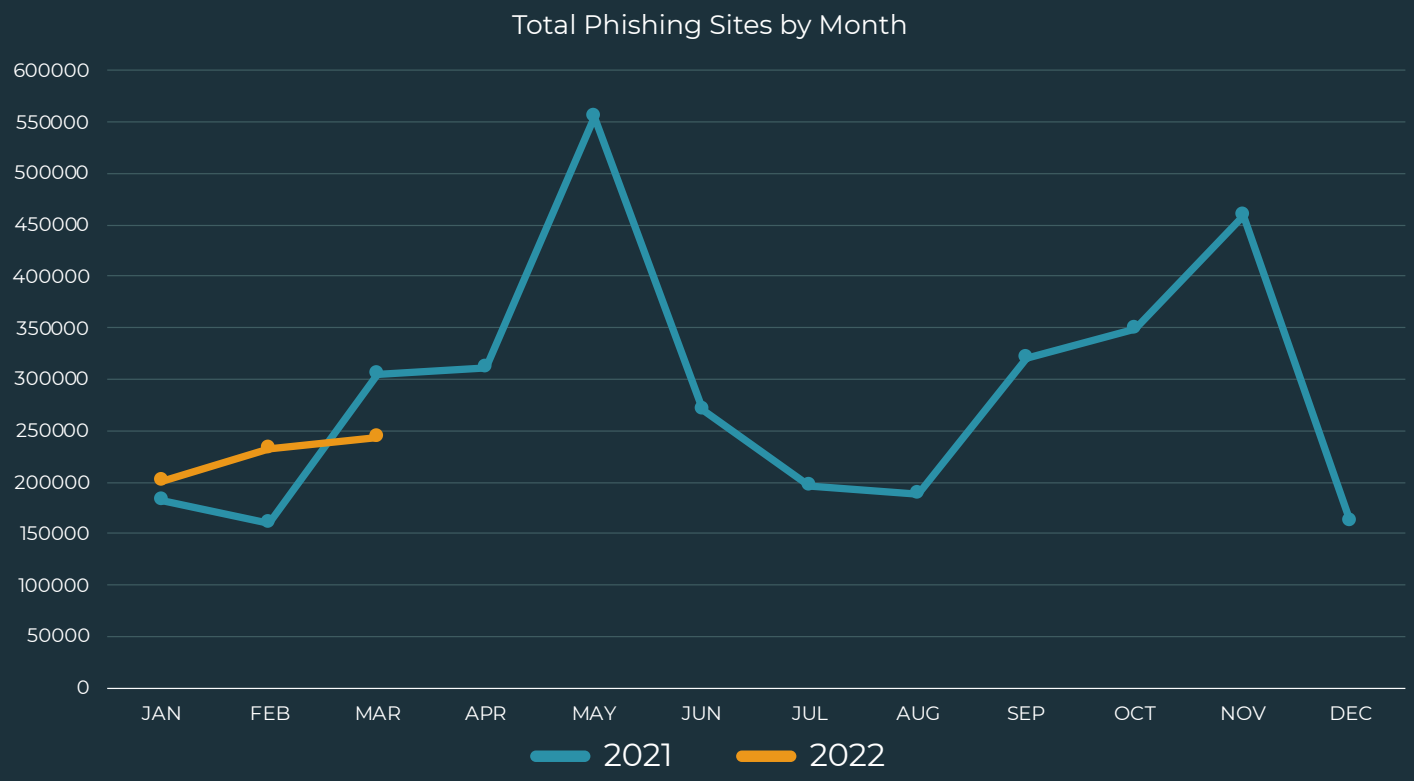
Vishing Maintains a Menacing Presence

Attacks are up almost 550% in volume from Q1 2021.

PHISHING THREAT TRENDS OVERVIEW

Q1 2022 PHISHING UP AND LESS VOLATILE THAN 2021

In Q1 2022, phishing volume increased 4.4% from Q1 2021. The total phishing sites observed in Q1 2022 grew steadily from January to March, displaying significantly less volatility than in 2021. Overall, Q1 2022 phishing volume was on par with Q1 2021, however month-to-month volume was predictable and lacking the erratic activity we witnessed last year. Looking ahead, we anticipate high-volume attack campaigns will generate spikes in activity throughout 2022 as opportunistic actors target vulnerable brands and businesses.



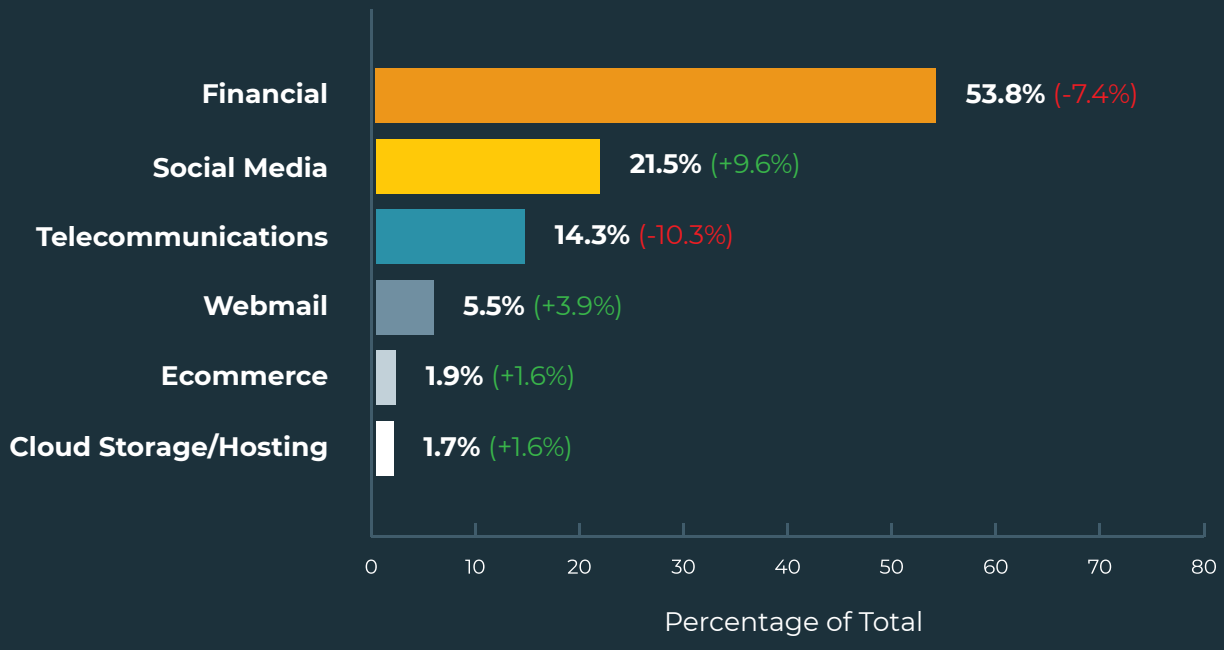
TOP TARGETED INDUSTRIES

In Q1, Financial businesses were targeted most by credential theft phish, representing 53.8% of all attacks. Financials have been heavily targeted for four consecutive quarters and continue to represent the majority of attacks in Q1, despite experiencing a decline of 7.4% from Q4.

The technology sector as a whole was targeted more in Q1. Social Media led the group, representing 21.5% of credential theft phish and experiencing the largest increase in attack volume (+9.6%). Webmail/Online Services (5.5%), Ecommerce (1.9%), and Cloud Storage/Hosting (1.7%) also experienced increases in attack volume.

Telecoms were the only industry to experience a decline in Q1, dropping 10.3% in share from Q4 to represent 14.3% of observed phishing attacks.

Financials continued to experience a majority of phishing attacks, accounting for 53.8% of all incidents.

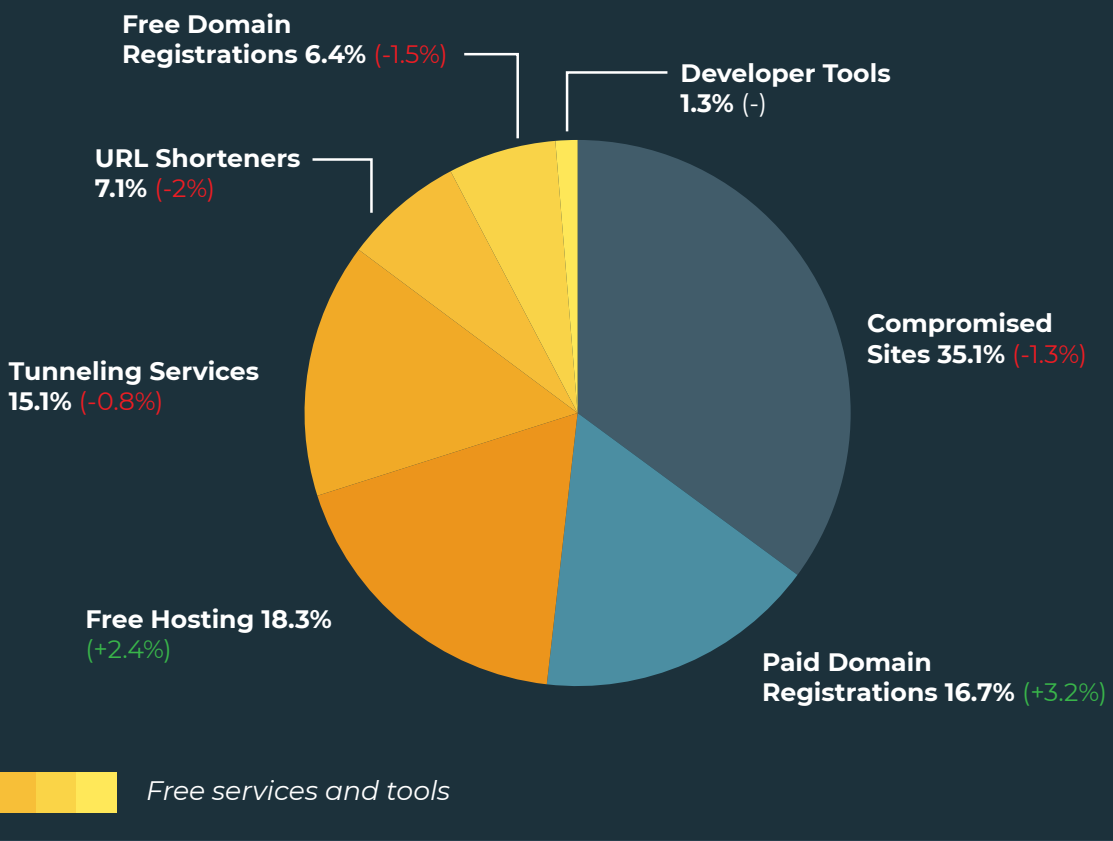


In Q1, nearly 52% of phishing sites were staged through compromised sites or by a threat actor registering a paid domain.

STAGING METHODS

Q1 2022 was the first in five consecutive quarters where the majority of phishing sites were staged using Paid Domain Registrations or Compromised Sites. Nearly 52% of phishing sites abused paid services, the milestone fueled in part by a steady increase in abuse every quarter throughout 2021 and finally a 3.2% increase of Paid Domain Registrations from Q4. Compromising existing websites remained the most common staging method in Q1, representing 35.1% of all incidents.

Free Services and Tools were used to stage phishing sites 48% of the time, with Free Hosting experiencing the only increase in share within the group. Tunneling Services experienced 15.1% of overall abuse, declining slightly from Q4. URL Shorteners and Free Domain Registrations also experienced a decrease in volume, representing 7.1% and 6.4% of staging abuse volume, respectively.



Nearly 66% of all phishing sites observed in Q1 were staged using Legacy gTLDs.

DOMAIN ABUSE

In Q1, nearly 66% of all phishing sites observed were staged on four Legacy Generic Top-Level Domains (gTLDs). This represents a 9.1% increase in abuse from Q4. Legacy gTLD .com once again contributed to almost half of all phishing activity, despite decreasing in share. Legacy gTLD .org experienced the greatest increase in share of abuse within the group, and accounted for 11.5% of all phishing sites staged.

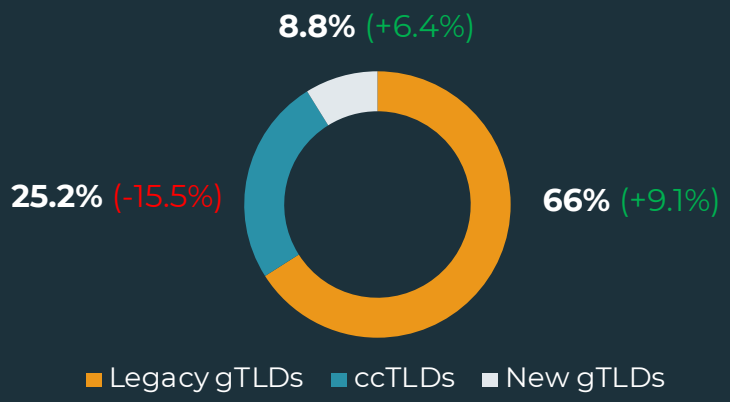
Threat actor abuse of Country-Code Top-Level Domains (ccTLDs) declined 15.5% in share in Q1, with only three ccTLDs making the top ten list. Notably, ccTLD .ca, formerly representing the second most abused domain in Q4, dropped completely from the top ten in Q1.

New Generic Top-Level Domains were abused 6.4% more in Q1, accounting for nearly 9% of phishing activity.

Top 10 TLDs Abused

TLD	TYPE	% PHISH	+/-
.COM	Legacy gTLD	49.3%	-0.6%
.ORG	Legacy gTLD	11.5%	+7.2%
.BR	ccTLD	3.6%	+2.8%
.NET	Legacy gTLD	3.3%	+1.8%
.LY	ccTLD	1.6%	+0.4%
.VIP	New gTLD	1.5%	+1.2%
.INFO	Legacy gTLD	1.5%	+0.9%
.XYZ	New gTLD	1.1%	+0.6%
.MONSTER	New gTLD	1.0%	+1.7%
.TK	ccTLD	1.0%	+0.7%

Percent of Phish per TLD



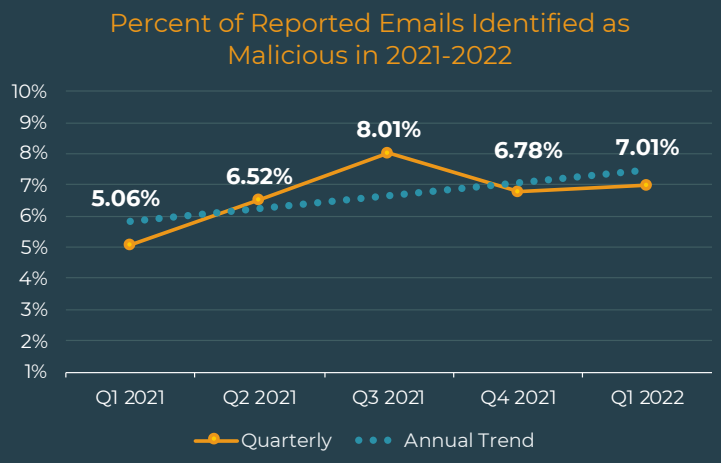
PHISHING TARGETING CORPORATE USERS

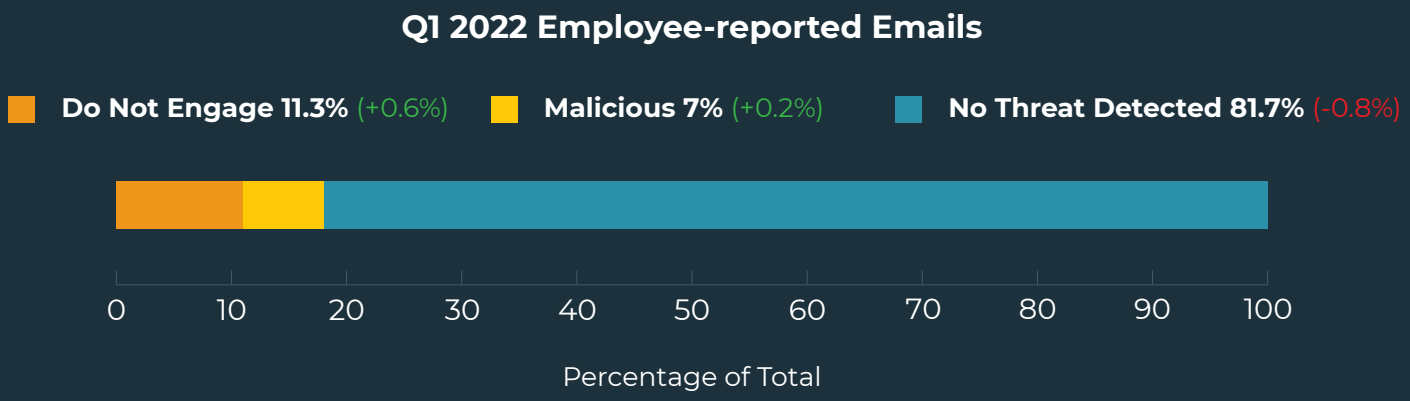
In Q1, the share of employee-reported emails classified as Malicious increased, supporting a continued upward trend in cases.

SLIGHT INCREASE IN MALICIOUS EMAILS REPORTED

In Q1, malicious emails targeting user inboxes increased, after a minor dip in reports during Q4. Employee-reported emails classified as malicious have steadily grown since Q1 2021 and pose a significant threat to organizations. While the majority of employee-reported emails are not classified as malicious, the identification and reporting of suspicious activity by a trained workforce is needed to prevent attacks that increasingly make it past email filters.

While nearly 82% of reported emails were classified as No Threat Detected, messages that were considered Malicious or suspicious enough that interaction could be considered hazardous increased in share to represent 18.3% of reports.

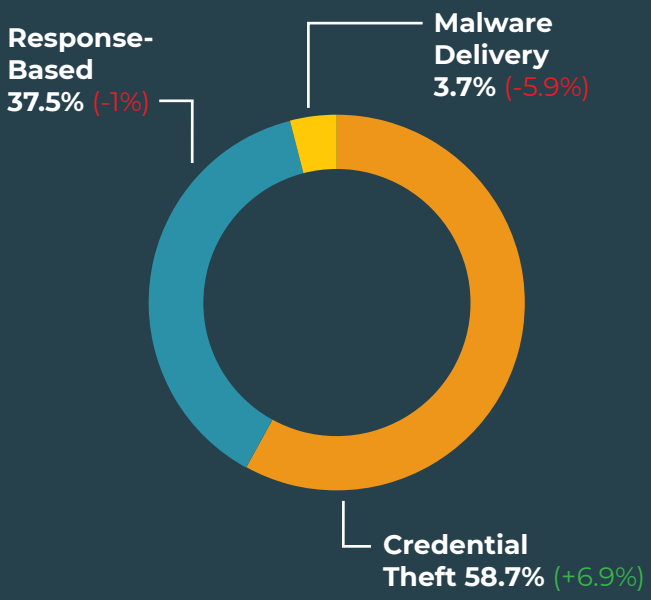




THREATS FOUND IN CORPORATE INBOXES

Credential Theft incidents and Response-Based social engineering attacks represented 96.2% of share of all email threats found in corporate inboxes in Q1. Credential Theft attacks were the most dominant threat-type, contributing to nearly 60% of attacks. This represents a 6.9% increase in share from Q4, and widens the gap between Credential Theft and other reported email threats.

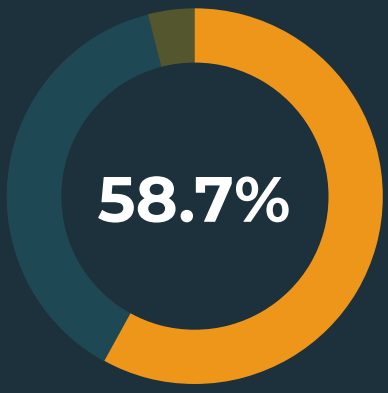
Although successful Ransomware attacks targeting businesses continue to climb, Malware Delivery experienced a 5.9% decline in share, representing just under 4% of threats found in corporate inboxes. Response-Based Threats remained somewhat steady, contributing to 37.5% of all email threats. This is a one percent decrease in share from Q4.



CREDENTIAL THEFT

In Q1, 58.7% of all reported emails targeting corporate inboxes were Credential Theft attacks. Credential Theft is consistently the top threat to employees quarter-over-quarter. Detection of this threat-type should be prioritized by security teams and employees should take part in consistent training that will aid in the identification of suspicious emails.

Within the category, 80% of all Credential Theft attacks contained a phishing link in the email body. This is a 2.2% decrease in share from Q4. Of those phishing links, half targeted Microsoft O365 accounts. This is a 9.2% increase in share from Q4, and a clear reminder that corporate credentials associated with O365 are highly sought-after by bad actors. Docuphish reports - any document that contains links to or redirects to an online phish - contributed to 20% of all Credential Theft attacks in Q1.

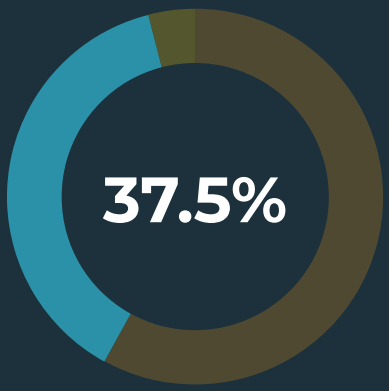


Phishing Link	80%	-2.2%
Attachment	20%	+2.2%

RESPONSE-BASED SCAMS

In Q1, 419 “Nigerian Prince” attacks contributed to 54.1% of Response-Based volume, maintaining its position as the top threat-type. Hybrid vishing campaigns continue to generate stunning numbers, representing 26.1% of total share in volume, despite a slight dip from Q4. Vishing attacks have overtaken BEC as the second most reported Response-Based threat since Q3.

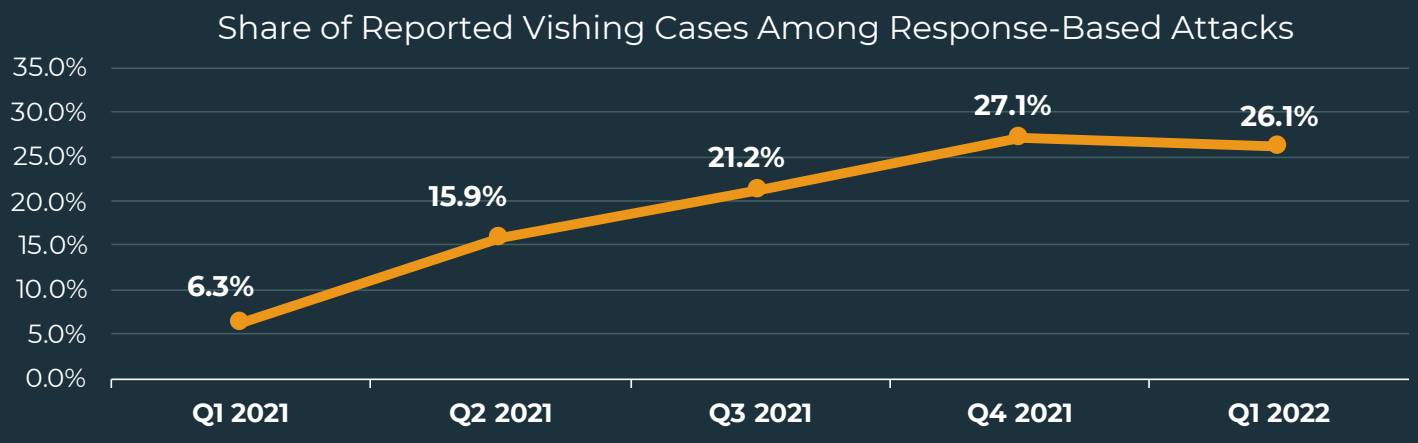
BEC scams represented the third highest reported threat, contributing to 12.8% of attacks after experiencing a 1.6% increase from Q4. Job and Tech Support Scams both declined in share, representing 6.7% and 0.2%, respectively.



419	54.1%	+3.3%
Vishing	26.1%	-1.0%
BEC	12.8%	+1.6%
Job Scams	6.7%	-2.7%
Tech Support	0.2%	-1.2%

VISHING CONTINUES TO THREATEN CORPORATE USERS

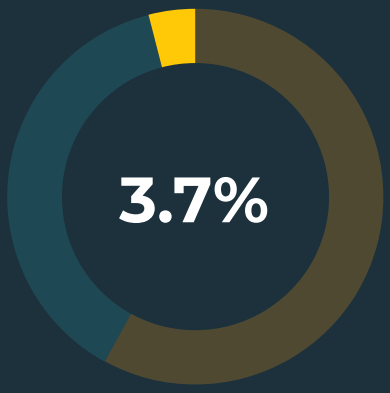
Notably, although Vishing cases are slightly down from Q4 2021, Q1 2022 experienced a nearly 550% increase in reported cases over Q1 of the previous year. In March, reports reached an all-time high, surpassing previous record numbers from September 2021.



MALWARE PAYLOAD FAMILIES

Qbot represented nearly 75% of all reported payload activity in Q1. This is the second consecutive quarter Qbot has led payload attacks, after experiencing a 15.1% increase in share from Q4 to Q1. Emotet experienced a similar surge in activity, contributing to 16.7% of reported payload volume. This makes Emotet the second most payload variety responsible for attacks to corporate users. Emotet was reportedly dismantled in January 2021, reemerged in November, and has steadily increased in attack volume.

BazaLoader contributed to 3.9% of reported payload activity, after experiencing a 3.5% increase. Notably, Trickbot experienced an identical decline in share of activity. BazaLoader and Trickbot operators have been linked to one another, and fluctuating attacks between varieties may be tied to the same criminal activity. ZLoader, formerly one of the most active payload varieties, was unreported in Q1, dropping nearly 30% in share from Q4.



Payload Family	Q1	Q4	+/-
Qbot	74.3%	59.3%	+15.1%
Emotet	16.7%	2.1%	+14.6%
BazaLoader	3.9%	0.4%	+3.5%
LokiBot	2.3%	0.0%	+2.3%
VBS Downloader	1.2%	0.9%	+0.2%
AsyncRAT	0.8%	0.4%	+0.4%
Trickbot	0.4%	3.9%	-3.5%
ZLoader	0.0%	29.4%	-29.4%

INFRASTRUCTURE USED FOR BEC ATTACKS

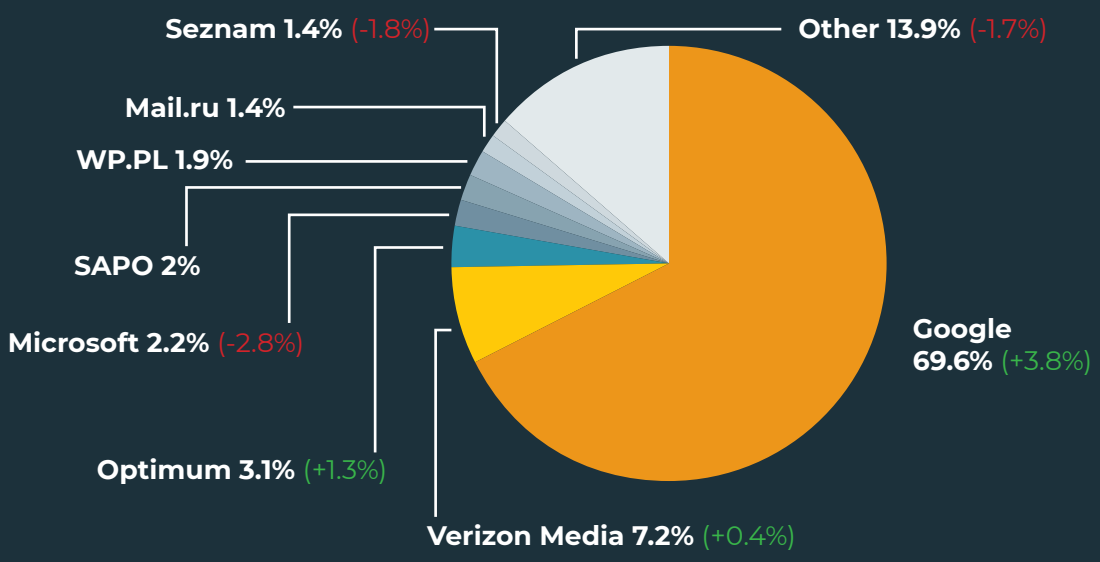
In Q1, we examined thousands of attempted BEC attacks used to launch advanced email attacks. A BEC attack is defined as any response-based spear phishing attack that involves the impersonation of a trusted party to trick victims into making a financial transaction or sending sensitive materials. While down nearly 5% from Q4, threat actors continue to rely on Free Webmail services (69.8%) to administer BEC Attacks. Maliciously Registered or Compromised Accounts increased 4.8%, accounting for 30.2% of overall volume.

In Q1, Google/GMAIL was the top Free Webmail provider abused to administer BEC attacks, representing nearly 70% of all incidents. Google/GMAIL also experienced the greatest growth in overall share of attacks, increasing 3.8% from Q4. Verizon Media was the second most abused, representing 7.2% of all incidents in Q1. Optimum came in third, contributing to over 3% of volume. Free Microsoft accounts declined in usage in Q1, dropping 2.8% from Q4.

Infrastructure Used to Send BEC Attacks

Free Webmail	69.8%	-4.8%
Maliciously Registered / Compromised	30.2%	+4.8%

Free Webmail Providers Used in BEC Attacks

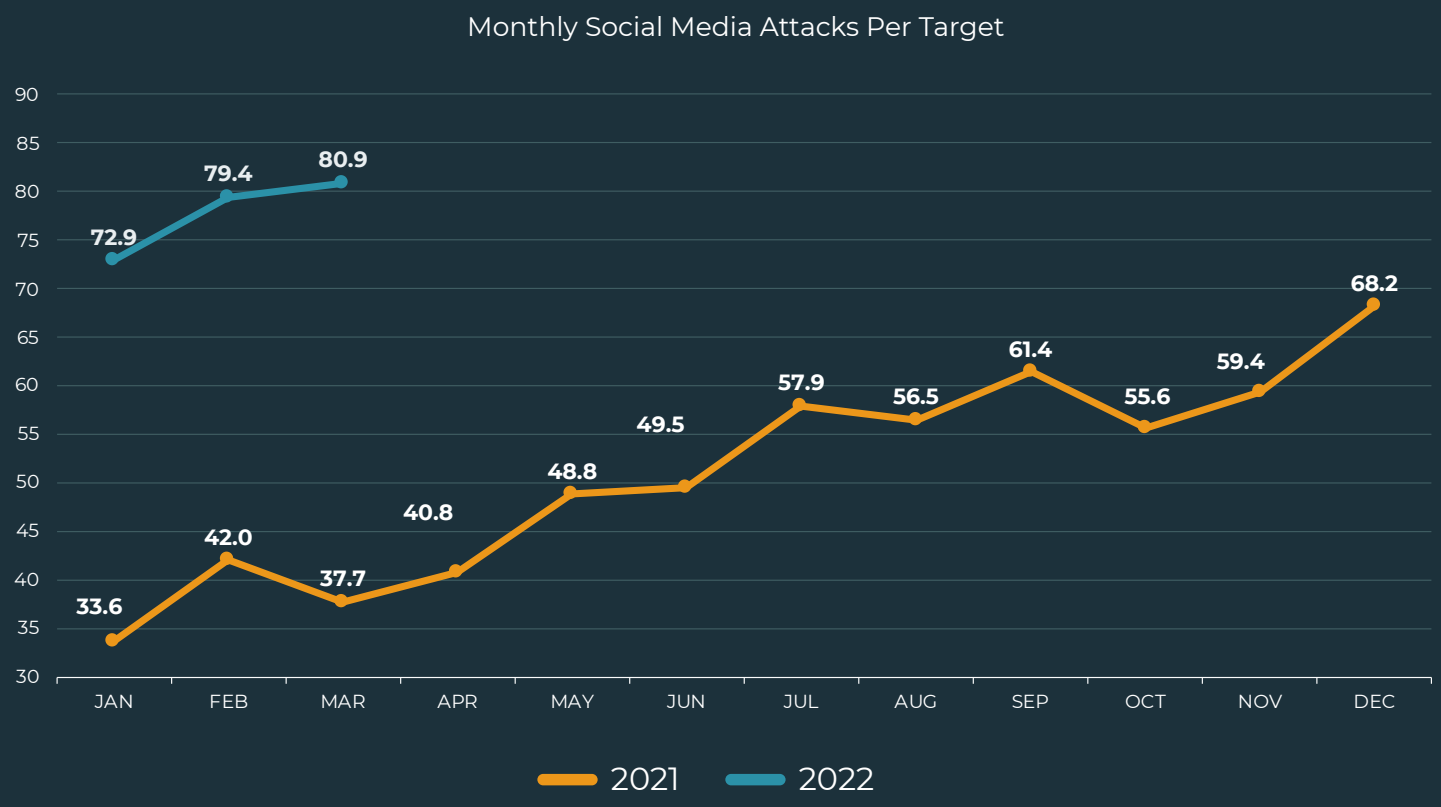


SOCIAL MEDIA THREAT TRENDS

SOCIAL MEDIA ATTACKS CONTINUE TO CLIMB

Social media has secured its status as a dominant and rapidly growing threat channel. In Q1, Social media attacks targeting enterprises have increased a dramatic 105% from the same time last year. Attack volume surged more than 27% from Q4 to Q1 alone, topping out in March with the average organization experiencing nearly 81 attacks.

Attacks per target increased 105% from Q1 2021 to Q1 2022.

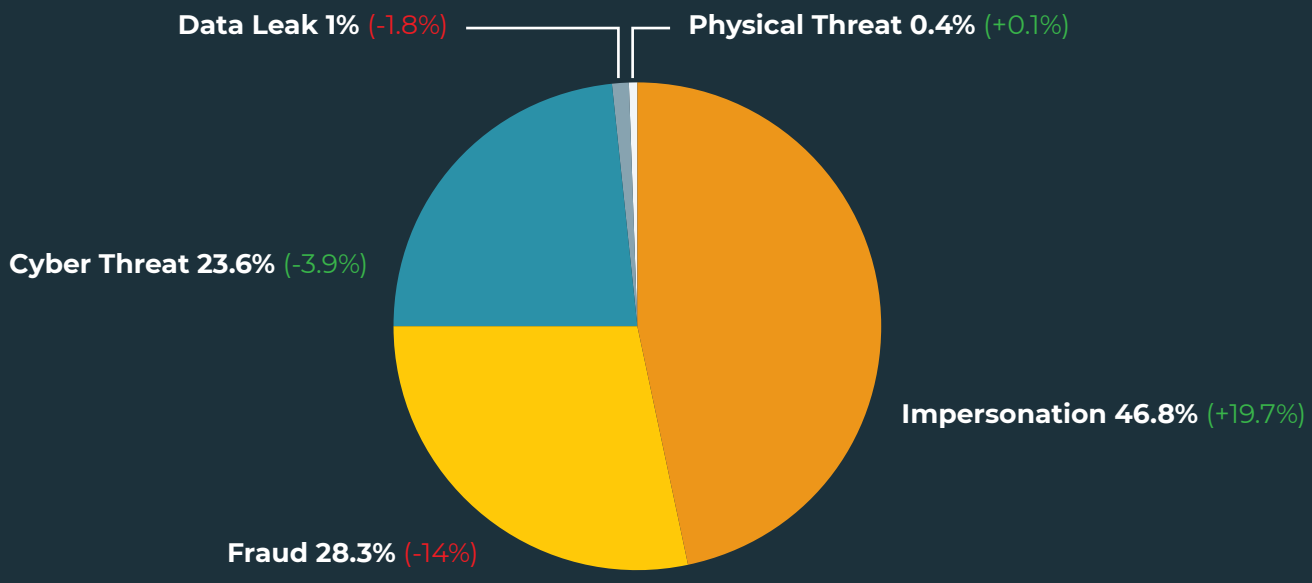


TOP SOCIAL MEDIA THREATS

In Q1, Impersonation scams surged to represent almost half of all attacks on social media after a 19.7% increase in share from Q4 to Q1. Impersonation attacks have now seen increases for three consecutive quarters. Historically, the top threat-type on social media, Fraud experienced a 14% decline in Q1, moving it to the second spot. Fraud represented 28.3% of all social media attacks.

Cyber threats such as hacking experienced a slight decrease in share in Q1, contributing to 23.6% of overall volume. Data Leaks and Physical Threats were present but minimal, representing 1.0% and 0.4%, respectively.

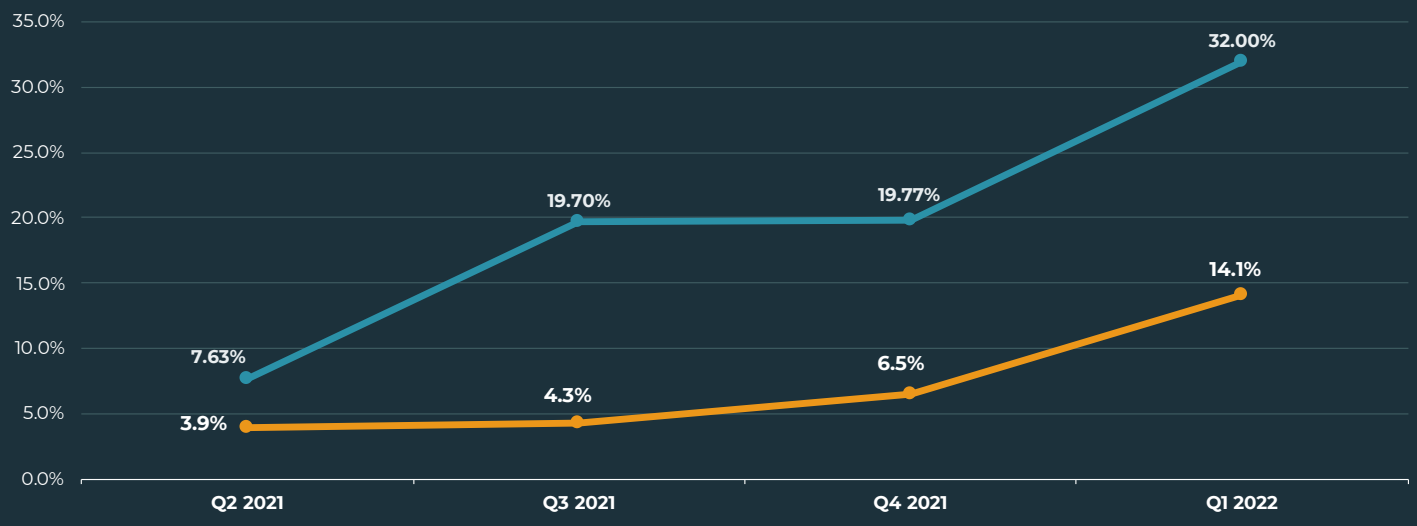
Brand and Executive Impersonations increased significantly in Q1, rising in count and share for 3 consecutive quarters.



IMPERSONATION ATTACKS ON THE RISE

The majority of Impersonations on Social Media are either Brand Impersonations or Executive Impersonations. Generally speaking, brands are more convenient targets for threat actors, but with some unique attacks, threat actors will also target executives. Both Brand and Executive Impersonations on social media have increased significantly the past 12-months. From Q4 to Q1, Brand Impersonation jumped to represent 32% of share of all social media attacks. The growth of brand abuse on social channels can be attributed to the increased presence of organizations on these platforms as advertising and customer communications become critical for a brand to remain relevant. Stolen trademarks and intellectual property can easily be repurposed for malicious use, and often go undetected due to lower security vigilance by users.

Share of Executive and Brand Impersonation Cases Among all Social Media Attacks



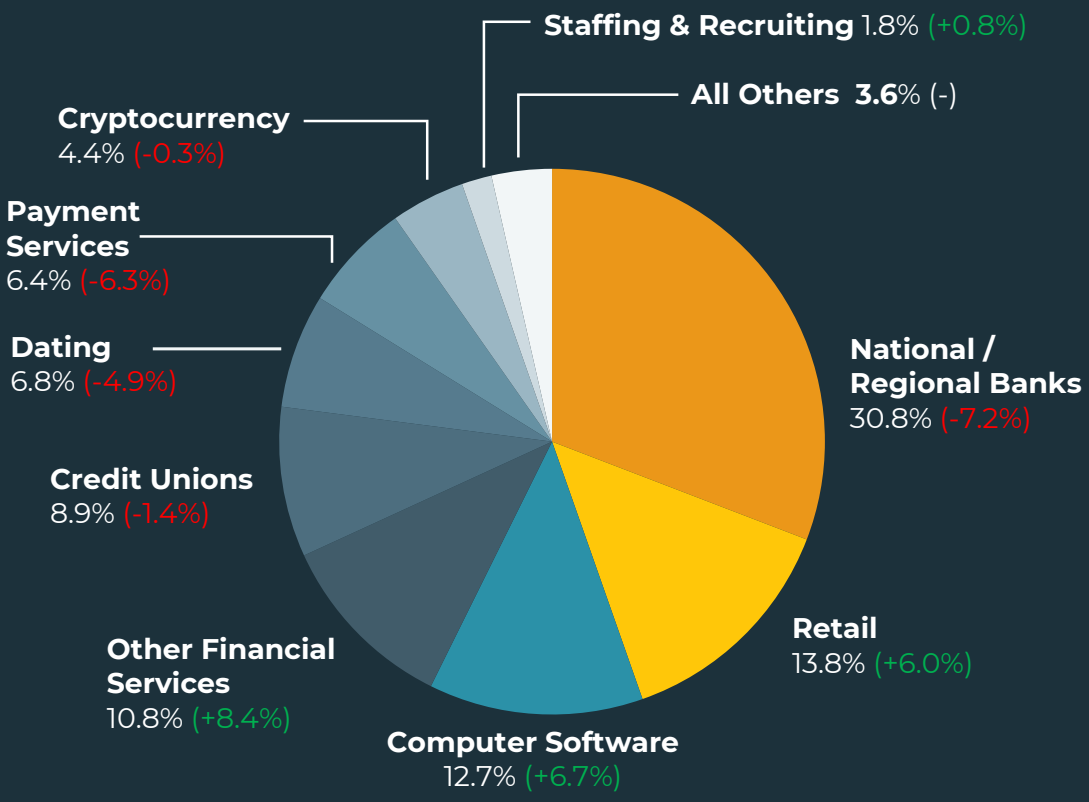
ATTACKS BY INDUSTRY

National and Regional Banks experienced the lion's share of social media attacks in Q1, representing more than 30% of total attack volume despite a decrease of 7.2% from Q4.

Retail continues to grow as a desirable target, becoming the second most abused industry after a 6% increase in share over the previous quarter. Threat actors have increasingly turned their focus to Retail as more businesses adopt an ecommerce-heavy business model relying on social media channels to drive consumer engagement.

Computer Software and Other Financials also experienced an increase in share in Q1, representing 12.7% and 10.8% of total volume, respectively. Attacks on Credit Unions declined slightly, representing just under 9% of share of attack volume.

Dating, consistently among the top five targeted industries throughout 2021, experienced a nearly 5% decrease in share, moving it to the sixth spot. Payment Services and Cryptocurrency also declined in share, representing 6.4% and 4.4% of attack volume, respectively.



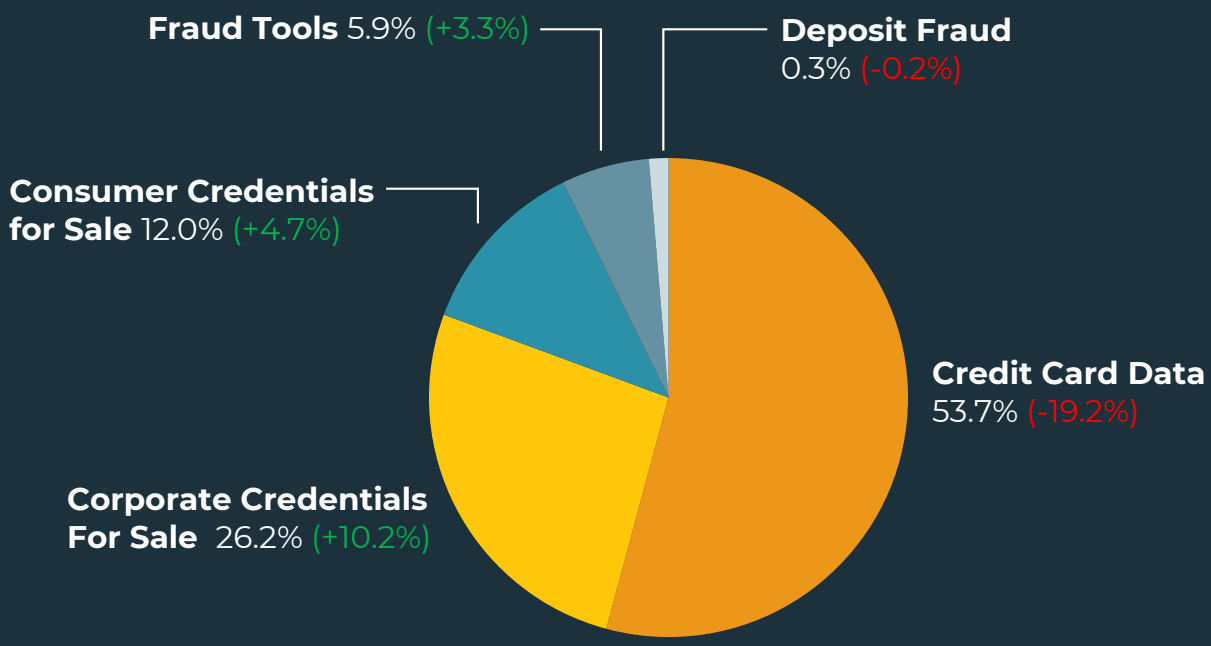
DARK WEB THREAT TRENDS

TOP DARK WEB THREATS

Credit Card Fraud was the most common dark web threat experienced by PhishLabs' clients in Q1, despite experiencing a nearly 20% decline in share. Stolen credit and debit card data is consistently the threat advertised most by bad actors on the dark web. In Q1, card data retained the top spot, accounting for more than half of all dark web incidents.

The sale of Corporate Credentials experienced the largest percentage gain among dark web incidents, jumping 10.2%. This is the second consecutive quarter Corporate Credentials have experienced the largest gain in share, once again securing its spot as the second most common dark web threat. Consumer Credentials for Sale represented 12% of all dark web threats, after a 4.7% increase in share from Q4 to Q1.

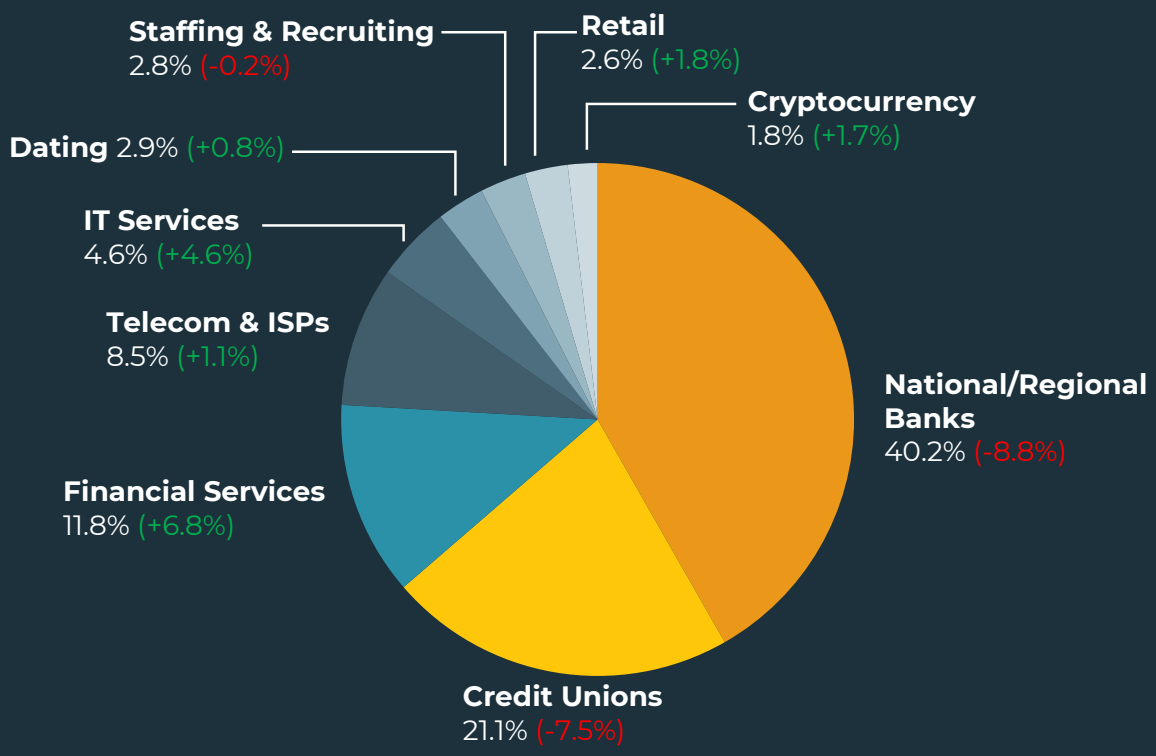
Corporate Credentials for Sale experienced the largest increase for 2 consecutive quarters.



TOP TARGETED INDUSTRIES

In Q1, Financial Institutions as a whole were targeted most by threat actors, contributing to 73.1% of all dark web attacks. This is despite a more than 16% combined decrease in share between National and Regional Banks, and Credit Unions. Other Financial Services contributed to 11.8% of attacks within the industry, and experienced the only increase in share of the group. Financial Institutions are historically targeted on the dark web because compromised data can mean access to card information, PII, and login credentials.

Telecom & ISPs (8.5%), IT Services (4.6%), and Dating (2.9%) all experienced an increase in share in Q1. Staffing & Recruiting declined in share, moving from the 5th most targeted industry in Q4 to the 7th in Q1. This may be attributed to the evening out of attacks after an uptick in abuse by bad actors targeting job seekers in preparation for the New Year.

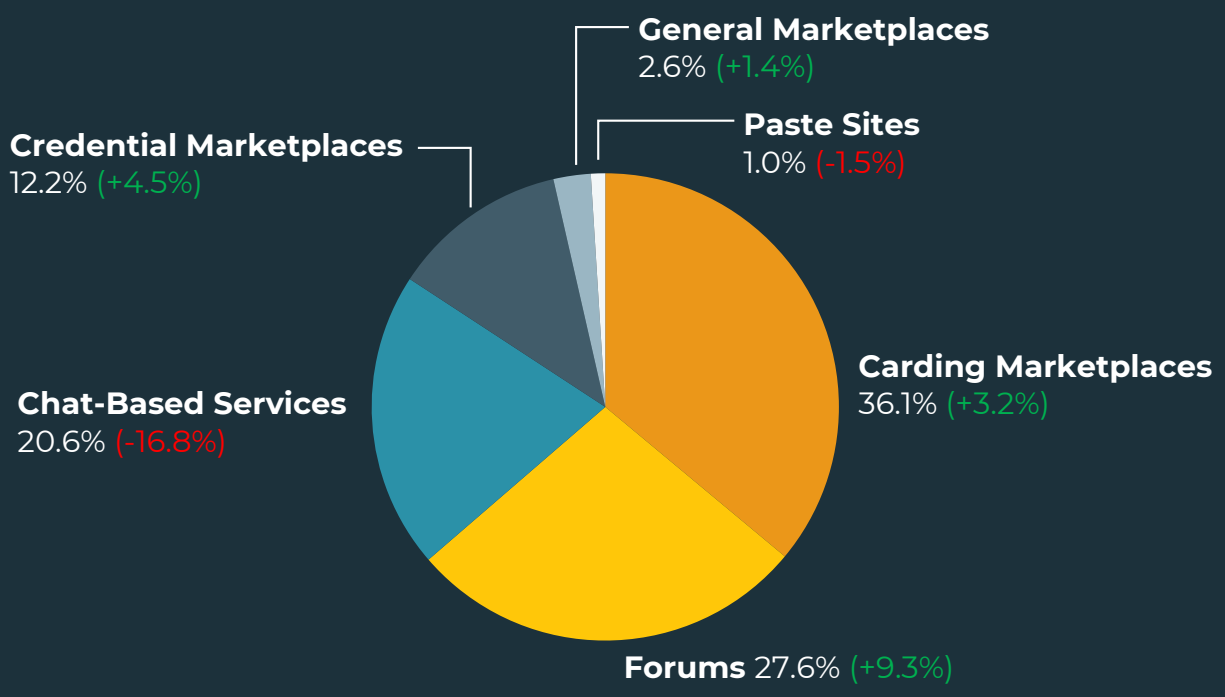


In Q1, nearly 64% of advertisements for stolen data were placed on Carding Marketplaces and Forums.

WHERE STOLEN DATA IS MARKETED

In Q1, nearly 64% of stolen data on the dark web was marketed on Carding Marketplaces and Forums after both experienced increased activity. Forums experienced the largest increase in share of activity of all dark web marketplaces, growing 9.3% from Q4 and moving it to the second spot behind Carding Marketplaces. Notably, the use of Chat-Based Services as an advertising platform declined for the second consecutive quarter, contributing to 20.6% of all incidents in Q1 2022, versus more than half (55.96%) of observed dark web cases in Q3. The decline in activity on Chat-Based Services may be attributed to a decrease in carding data being communicated through those services.

Credential Marketplaces that specialize in the selling of account-based data increased 4.5% in share during Q1, representing just over 12% of all incidents. General Marketplaces and Paste Sites rounded out the top five, contributing to 2.6% and 1% of activity, respectively.



SUMMARY & CONCLUSION

Attacks targeting enterprises and consumers are being delivered more than ever via a wide expanse of channels. The increase in activity through these unconventional platforms and mechanisms is an unmistakable mark of the opportunistic and expedient nature of today's threats, as well as the need for complete visibility across all online environments by security teams.

Phishing continues to be the most significant threat to enterprises, employees, and their customers. While reports of traditional email phishing grew slightly and remained balanced throughout the quarter, other methods of phishing grew in popularity.

Social Media has cemented its status as a preferred channel for threat actors, with attacks increasing 105% since this time last year. Attacks are delivered via fake pages, posts, and advertisements, easily set up by bad actors using stolen trademarks, intellectual property, and more. Consequently, this has resulted in a significant increase in impersonation attacks.

Credential Theft and Response-Based attacks remain the top threats encountered in corporate inboxes, contributing to more than 96% of reports. Hybrid Vishing attacks have overtaken BEC attacks becoming the second most common Response-Based email threat, increasing almost 550% in volume in one year. The growing number of two-pronged Vishing reports demonstrates how bad actors are increasingly relying on a combination of threat vectors in their attack campaigns.

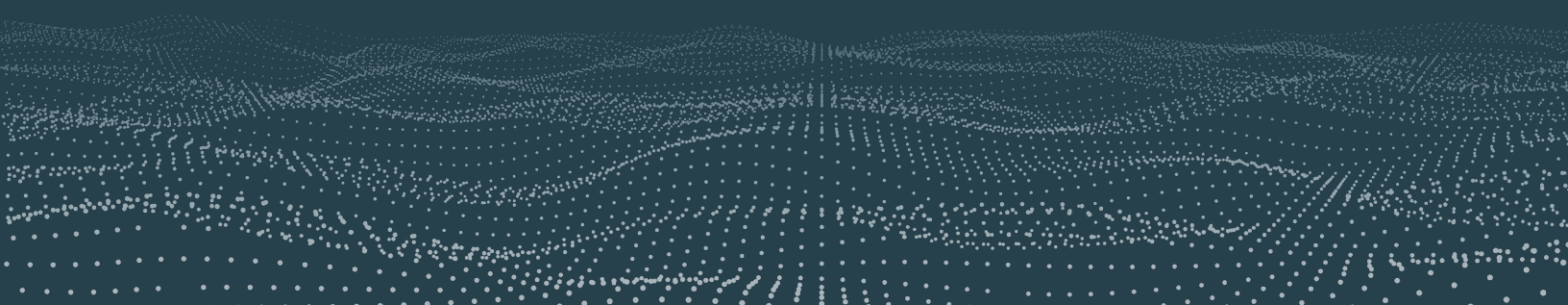
The primary delivery method of ransomware continues to be email payloads, with reports of malware varieties remaining largely inconsistent. Qbot was the exception in Q1, increasing in share and leading reports for back-to-back quarters. Emotet attacks are steadily increasing after operations resumed in November, accounting for 16.7% of all volume in Q1. Notably, Trickbot and ZLoader numbers were paltry, possibly an indication of actors shifting tactics.

Reports of emails classified as Malicious have increased steadily from Q1 2021, contributing to 7% of share of all employee-reported emails in Q1. Emails determined Malicious, coupled with others considered hazardous (Do Not Engage) grew to contribute to more than 18% of share of employee-reported emails in Q1, evidence that damaging messages continue to bypass network security and leave resulting actions to employees.

The variety of channels enterprises and their employees use to conduct operations and communicate with consumers has expanded, providing bad actors multiple vectors to exploit their victims. Most campaigns aren't built from scratch, but rather the result of the reshaping of traditional tactics and incorporation of multiple platforms.

It is no longer effective to only secure the network perimeter but rather, organizations must have visibility into a variety of external channels to proactively gather intelligence and monitor for threats. Additionally, security teams should invest in partnerships that will ensure the swift and complete mitigation of attacks before they result in reputational and financial damage.

This page intentionally left blank.



About Agari
Agari by HelpSystems restores trust to your inbox by increasing overall email deliverability and preserving brand integrity. It does this through an identity-centric approach that uniquely learns sender-receiver behavior. This model protects customers, partners, and employees from devastating phishing and socially engineered attacks, such as inbound business email compromise, supply chain fraud and account takeover-based attacks, as well as from outbound email spoofing. Learn more at www.agari.com.

About PhishLabs
PhishLabs by HelpSystems is a cyber threat intelligence company that protects against brand, account takeover, and data leakage threats. Founded in 2008, we deliver curated threat intelligence and complete mitigation across the digital risk landscape. The world's leading brands rely on PhishLabs to find and remediate external threats wherever they live. Learn more at www.phishlabs.com.

About HelpSystems
HelpSystems is a software company focused on helping exceptional organizations secure and automate their operations. Our cybersecurity and automation software protects information and simplifies IT processes to give our customers peace of mind. We know security and IT transformation is a journey, not a destination. Let's move forward. Learn more at www.helpsystems.com.