agari by HelpSystems

PHISHLABS by HelpSystems

QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT

AUGUST 2022

CONTENTS

ABOUT THE REPORT

In Q2, 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

Phishing is Steadily on the Rise
Phishing attacks are up nearly 6% in Q2 from Q1 2022

Social Media is an Accessible and Preferred Threat Channel
Social media attacks have increased more than 100% in a year

Response-Based Phishing Continues to Climb
Response-Based threats targeting corporate inboxes reached the highest volume since 2020

Emotet Leads Ransomware Payloads
Emotet has fully recovered, representing nearly 50% of all malware payload attacks in Q2

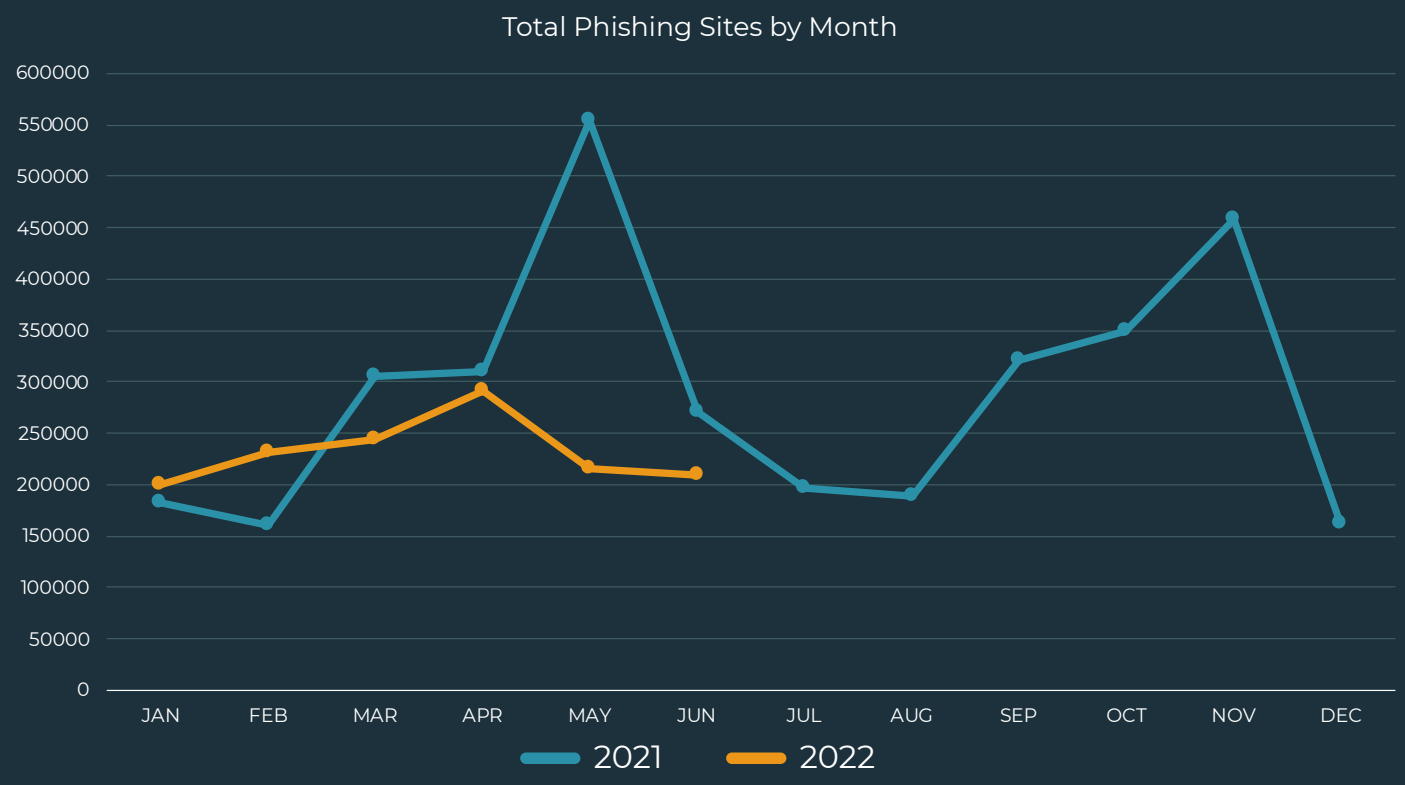
Hybrid Vishing Attack Volume Trending Up
Hybrid Vishing attacks have increased 625% in volume since Q1 2021

O365 Credentials Coveted by Criminals
Nearly 60% of credential theft phishing attacks targeted O365 credentials in Q2

PHISHING THREAT TRENDS OVERVIEW

Q2 PHISHING UP, DISPLAYS CONSISTENT ACTIVITY

In Q2 2022, phishing volume increased 5.95% from Q1. The total phishing sites observed displayed consistent activity, with month-to-month volume trending downward from April to June. Phishing activity in 2022 has remained steady, lacking the erratic activity and high-volume campaigns that characterized much of 2021. During the second half of 2022, we anticipate phishing volume will steadily climb as bad actors identify vulnerable businesses lacking the security controls needed to address attacks targeting their brand.



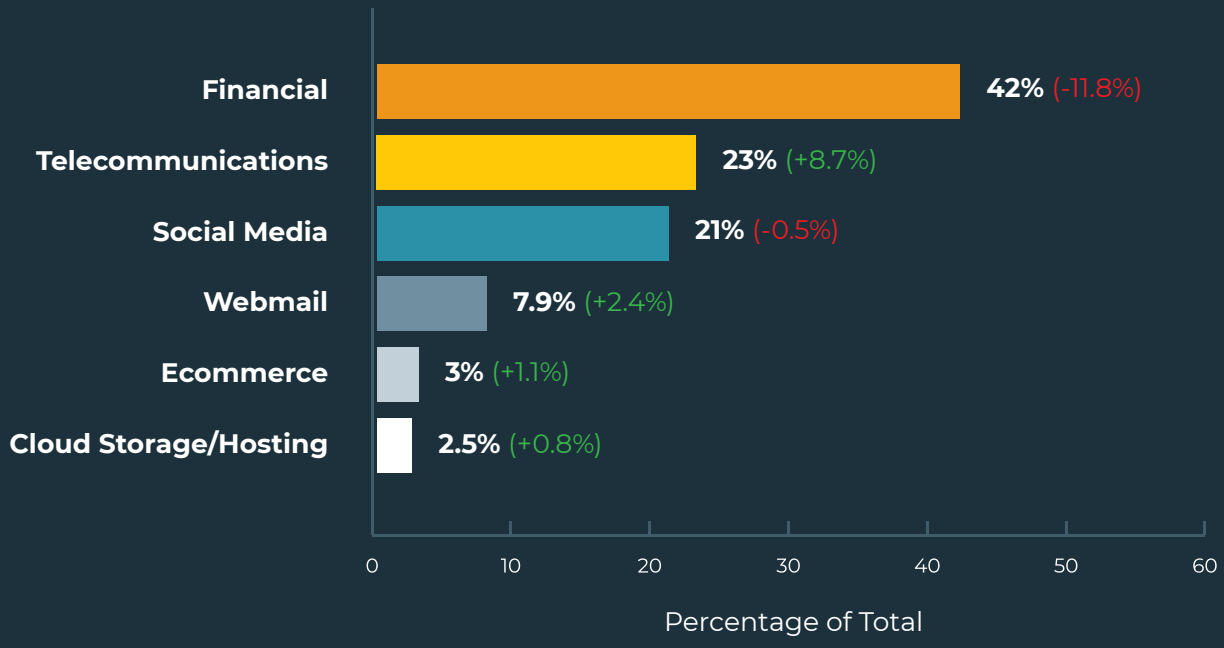
TOP TARGETED INDUSTRIES

Financial Institutions were targeted most by phishing sites in Q2, experiencing 42% of all attacks. While it is historically the top targeted industry, this is the second consecutive quarter incidents have declined. Year to date, attacks targeting the financial industry are down more than 19%.

Telecommunications was the second most targeted industry after experiencing a nearly 9% increase in share during Q2. This was the largest increase among top targeted industries. Telecom incidents contributed to 23% of observed phishing attacks.

Other prominent technology sectors combined to make up 34.4% of credential theft phishing incidents in Q2. Social Media was 21% of overall industry volume despite a slight decrease in attacks. Webmail (7.9%), Ecommerce (3%), and Cloud Storage/Hosting (2.5%) all experienced increases in Q2.

Financials continued to experience a majority of phishing attacks, accounting for 42% of all incidents.



In Q2, only 17% of phishing sites were staged using Paid Domain Registrations.

STAGING METHODS

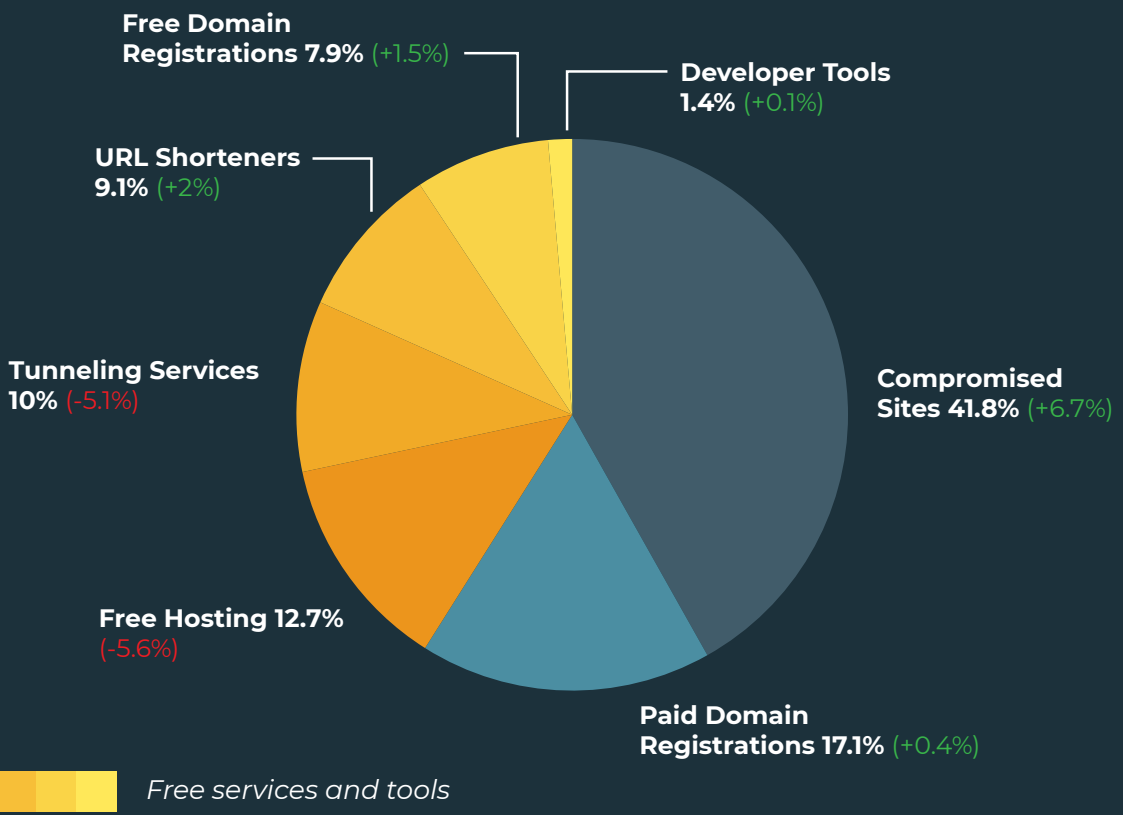
In Q2, 4 out of every 5 phishing sites were staged on infrastructure that required no investment by threat actors, including Free Services and Tools or Compromised Sites. However, abuse of Free Hosting and Tunneling Services fell during the quarter, suggesting those providers have taken measures that have made them less attractive to cybercriminals.

Compromising existing websites was the preferred method to stage phishing campaigns, contributing to 41.8% of the overall share. Compromised Sites also experienced the greatest growth in activity, increasing 6.7% over Q1.

The use of Free Services and Tools has declined steadily since the onset of 2022. In Q2, Free Services dropped nearly 7% in share from Q1, accounting for only 41% of all incidents.

Free Hosting represented most of the activity within the group, accounting for 12.7% of abuse. Free Hosting also experienced the largest decrease, declining 5.6%. Tunneling Services were the second most abused free service, representing 10% of all activity.

URL Shorteners (9.1%), Free Domain Registrations (7.9%), and Developer Tools (1.4%) all experienced nominal increases.



Nearly 60% of all phishing sites observed in Q2 were staged using Legacy gTLDs, but the use of ccTLDs substantially increased.

DOMAIN ABUSE

Nearly 60% of all phishing sites were staged using three Legacy Generic Top-Level Domains (gTLDs): .com, .org, and .net. This is despite a combined 6.4% decline in share of abuse. Legacy gTLD .com activity decreased for the second consecutive quarter, declining 2.4% from Q1. Despite this, .com continued to represent the majority of Top-Level Domain abuse, contributing to 46.9% of overall volume.

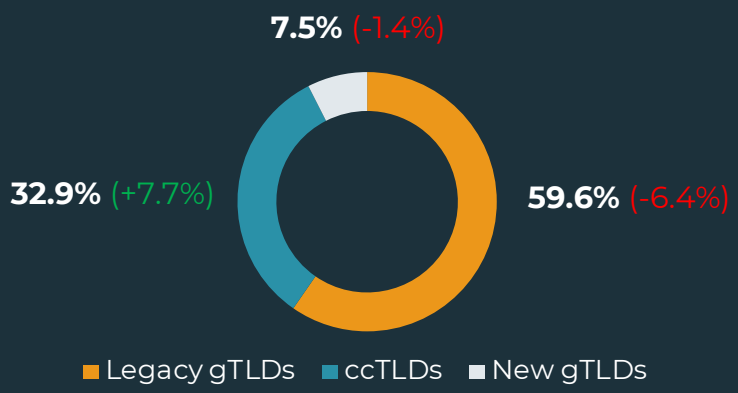
The number of Country-Code Top-Level Domains (ccTLDs) present within the top 10 doubled in Q2, representing 32.9% of the entire share of abuse. This is a 7.7% increase over Q1. The majority of ccTLD volume was driven by .CV, contributing to 8.8% of total share. It was also the second most abused TLD in the quarter.

Abuse of New Generic Top-Level Domains (New gTLDs) declined in Q2, accounting for 7.5% of abused domains. New gTLD .XYZ was the only representative within the top ten.

Top 10 TLDs Abused

TLD	TYPE	% PHISH	+/-
.COM	Legacy gTLD	46.9%	-2.4%
.CV	ccTLD	8.8%	+8.8%
.ORG	Legacy gTLD	8.5%	-3.0%
.CA	ccTLD	4.2%	+3.9%
.NET	Legacy gTLD	3.1%	-0.3%
.XYZ	New gTLD	2.0%	+1.0%
.ML	ccTLD	1.6%	+0.6%
.TK	ccTLD	1.3%	+0.3%
.ID	ccTLD	1.3%	+0.7%
.CN	ccTLD	1.3%	+0.5%

Percent of Phish per TLD



PHISHING TARGETING CORPORATE USERS

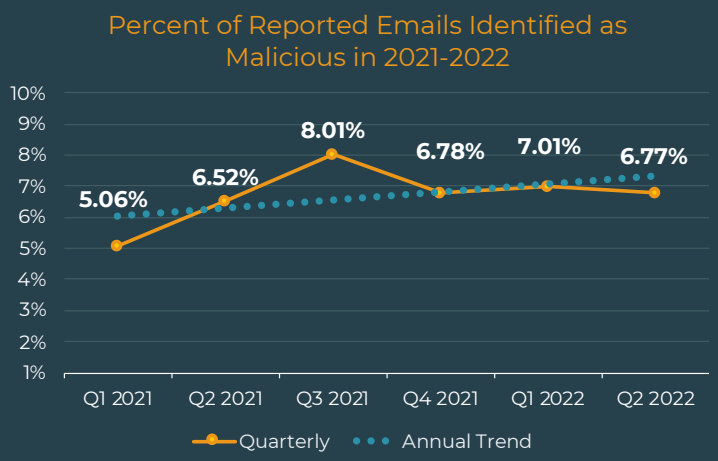
The combined percentage of threats classified as Malicious and Do Not Engage reached a three-quarter high in Q2.

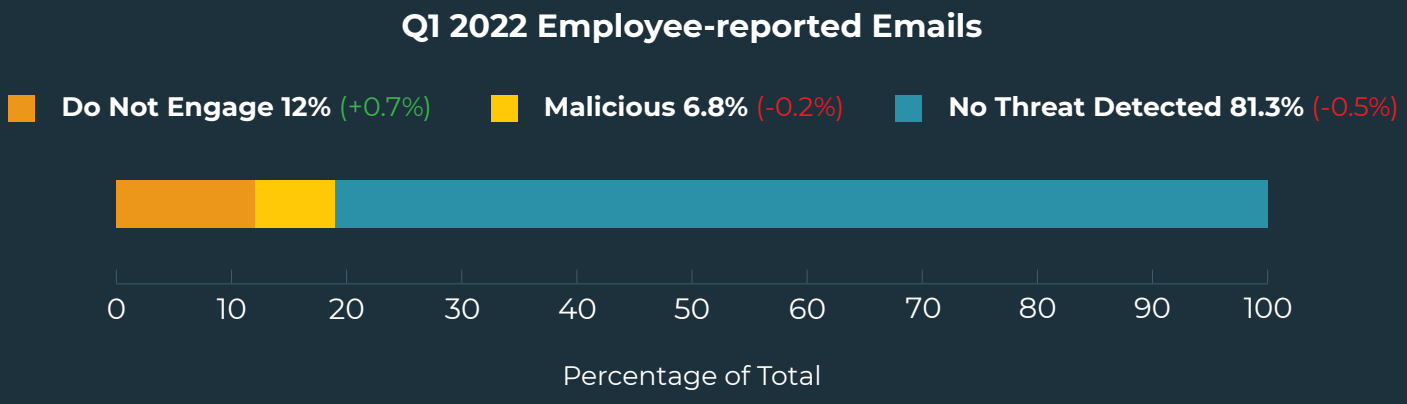
SLIGHT INCREASE IN MALICIOUS EMAIL VOLUME

In Q2, malicious emails found in employee inboxes continued to increase in volume, despite having a slight decrease in share of emails reported by users. Emails classified as malicious have steadily grown since Q1 2021. In Q2, 6.8% of all emails reported by users were malicious.

Suspicious emails classified as Do Not Engage increased in both volume and share, contributing to 12% of employee-reported emails. Emails considered Do Not Engage lack clear malicious indicators yet may still pose a danger to employees. The percentage of Do Not Engage and Malicious emails reached a combined three-quarter high of 18.8% in Q2.

Employee-reported emails classified as No Threat Detected experienced a slight decline in Q2. While most reported emails are typically not malicious, the proactive identification and reporting of suspicious emails is critical to keeping enterprises secure from credential theft, response-based, and malware attacks.



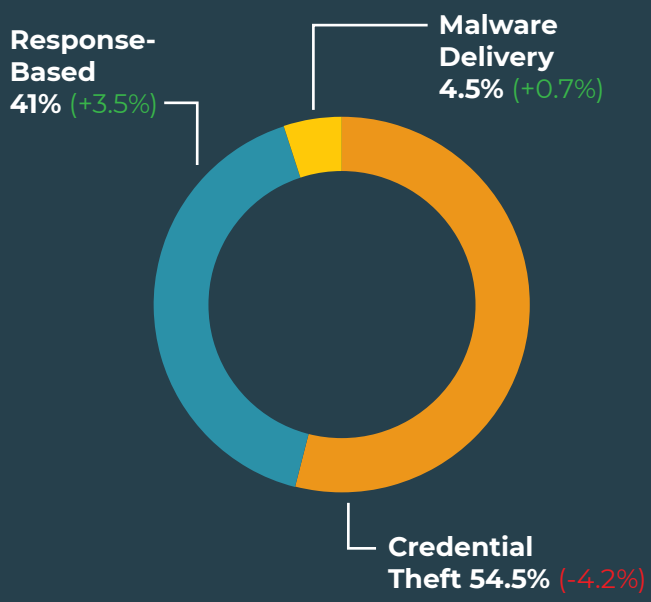


THREATS FOUND IN CORPORATE INBOXES

Credential Theft attacks reported in corporate inboxes represented nearly 55% of all email-based threats in Q2, despite experiencing a 4.2% decline in activity. Credential Theft incidents are repeatedly the top threat-type targeting organizations.

Response-Based attacks reported in corporate inboxes have climbed to the highest count and share in volume since 2020, representing 41% of email-based scams in Q2. Response-Based volume has increased steadily every quarter since Q1 2021, apart from a negligible decline in Q1 2022. Response-Based attacks consistently represent a significant portion of phishing volume, evidence that social engineering tactics continue to prove effective for criminals.

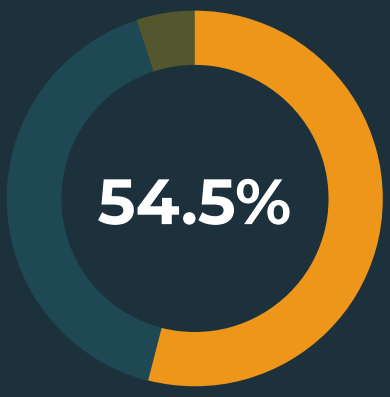
Malware Delivery increased 0.7% in Q2, contributing to 4.5% of share of attack volume.



CREDENTIAL THEFT

Credential Theft attacks targeting Office 365 accounts reached a six-quarter high in share and volume during Q2. More than 58% of all Credential Theft phishing links were delivered with the intent to steal O365 login credentials, up 17.7% compared to Q4 2021.

The increased focus on O365 account information is one example of the value bad actors place on credentials associated with network-wide collaboration and productivity applications. Malicious attachments such as Docuphish declined in Q2, representing 15% of Credential Theft attacks.

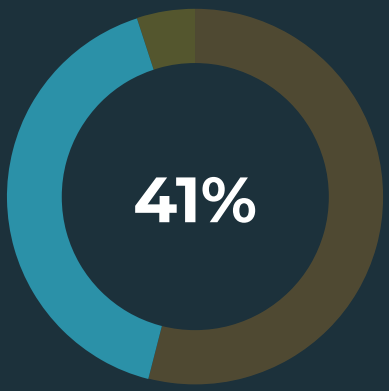


Phishing Link	85%	+5.2%
Attachment	15%	-5.2%

RESPONSE-BASED SCAMS

In Q2, Advanced-Fee Scams (419) were 54.2% of Response-Based email threats. This threat-type has increased 3.4% in share of reports in 2022 and routinely makes up a majority of Response-Based attacks. Business Email Compromise (BEC) also increased in Q2, contributing to 16.3% of attack volume.

Despite a slight decline in share, hybrid Vishing cases continue to climb by count. In Q2, reports of Vishing were the highest in six quarters. The total share of Vishing attacks remained relatively consistent over Q1, totaling 24.6%. Job Scams declined in share during Q2, contributing to 4.8% of attacks. We anticipate this category will grow in Q3 and Q4 due to seasonal hiring.

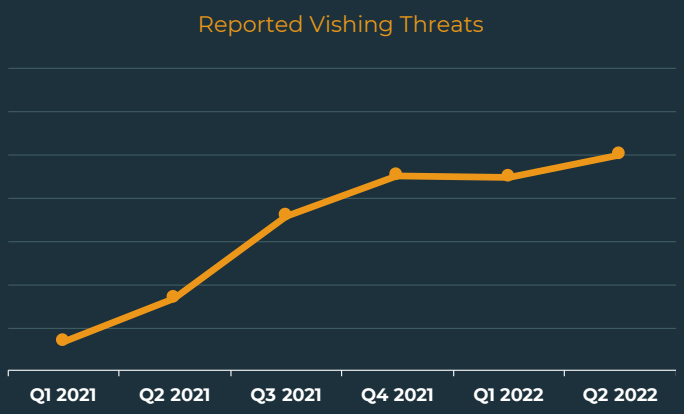


419	54.2%	+0.1%
Vishing	24.6%	-1.6%
BEC	16.3%	+3.4%
Job Scams	4.8%	-1.9%
Tech Support	0.2%	0.0%

VISHING VOLUME CONTINUES AN UPWARD TREND

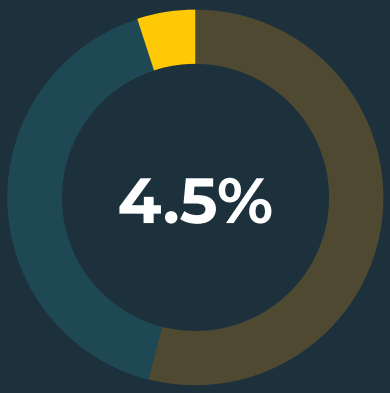
Hybrid Vishing attacks reached a six-quarter high in Q2, increasing 625% from Q1 2021. This threat-type also contributed to 24.6% of overall share of Response-Based threats. While this is the second quarter hybrid Vishing attacks have declined in share due to the overall increase of Response-Based threats, Vishing volume has steadily increased in count over the course of the year.

Hybrid Vishing threats are multi-stage attacks that differ from traditional Vishing by first interacting with the victim via email. The actor includes a mobile number within the body of the email as a lure, which is designed to trick the victim into calling and submitting sensitive information to a fake representative.



MALWARE PAYLOAD FAMILIES

In Q2, Emotet reports increased more than 30% in share, surpassing all other payload volume since being taken down in January 2021. Emotet contributed to nearly 50% of attacks, narrowly overtaking QBot. Together, Emotet and QBot payload volume exceeded 90% of all malware reported in user inboxes. Newcomer Bumblebee was the third most reported payload, contributing to 2.9% of attacks. Bumblebee was first detected in March 2022 and has code similar to the Trickbot botnet. Trickbot was absent in Q2.

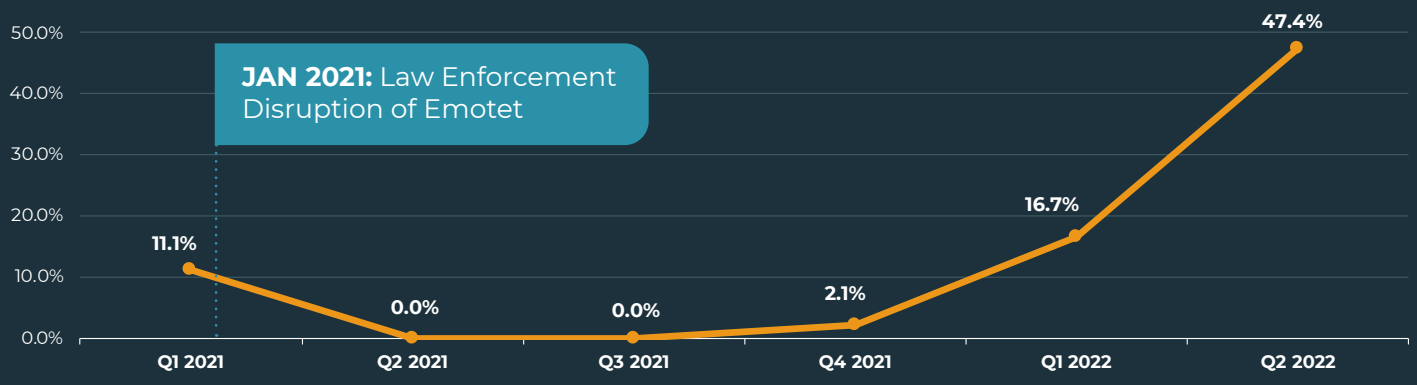


Payload Family	Q2	Q1	+/-
Emotet	47.4%	16.7%	+30.7%
QBot	42.8%	74.3%	-31.5%
Bumblebee	2.9%	0.0%	+2.9%
SnakeKeyLogger	1.4%	0.0%	+1.4%
Agent Tesla	1.2%	0.0%	+1.2%
Remcos RAT	1.2%	0.0%	+1.2%
AsyncRAT	0.7%	0.8%	+0.1%
VBS Downloader	0.7%	1.2%	-0.5%
BazaLoader	0.0%	3.9%	-3.9%

EMOTET STAGES A COMEBACK

Emotet has regained its status as a preferred payload among criminals. It's disruption by authorities in January 2021 resulted in increased attack volume by QBot, Trickbot, and other smaller malware families. Since Emotet's reemergence last November, campaigns have been documented performing actions not previously associated with the malware, as operators are believed to be testing new tactics in smaller cyberattacks to gauge their effectiveness.

Emotet Percentage of Share Among Common Payload Families



INFRASTRUCTURE USED FOR BEC ATTACKS

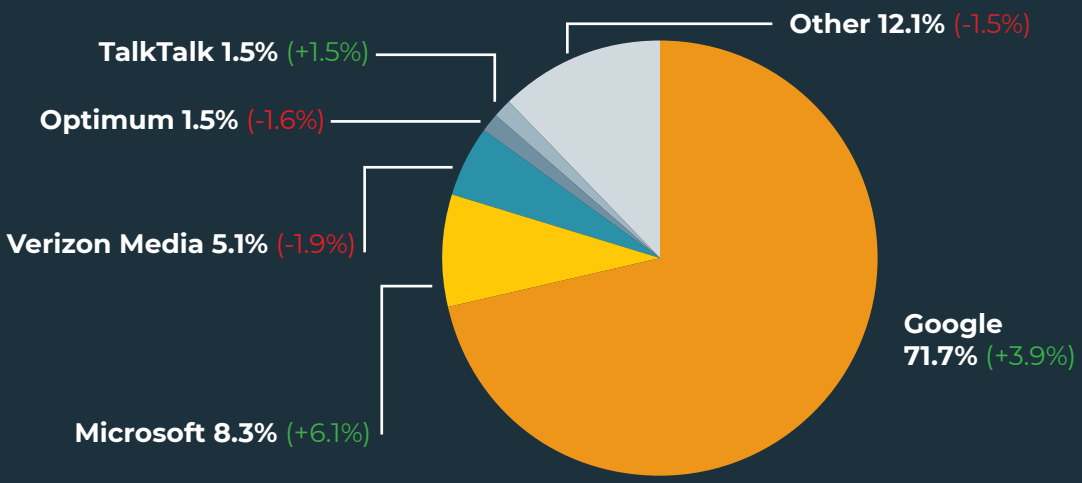
In Q2, nearly three-quarters of BEC attacks were launched using Free Webmail services. Free Webmail abuse was up 3.2% this quarter compared to Q1. In contrast, Maliciously Registered or Compromised Accounts declined 3.2%, representing 27% of attack volume. Agari and PhishLabs define BEC as any response-based spear phishing attack involving the impersonation of a trusted party to trick victims into making an unauthorized financial transaction or send sensitive materials.

In Q2, Google/GMAIL was the top webmail provider abused by criminals for BEC attacks, contributing to 71.7% of total volume. Google experienced a 3.9% increase in abuse from Q1. A grouping of "Other" solutions claimed the second spot, aiding in BEC attacks 12.1% of the time. Microsoft experienced the largest increase in share of abuse, growing more than 6% in Q2, and contributing to 8.3% of all incidents. Verizon Media and Optimum both declined in usage in Q2, representing 5.1% and 1.5%, respectively.

Infrastructure Used to Send BEC Attacks

Free Webmail	73%	+3.2%
Maliciously Registered / Compromised	27%	-3.2%

Free Webmail Providers Used in BEC Attacks

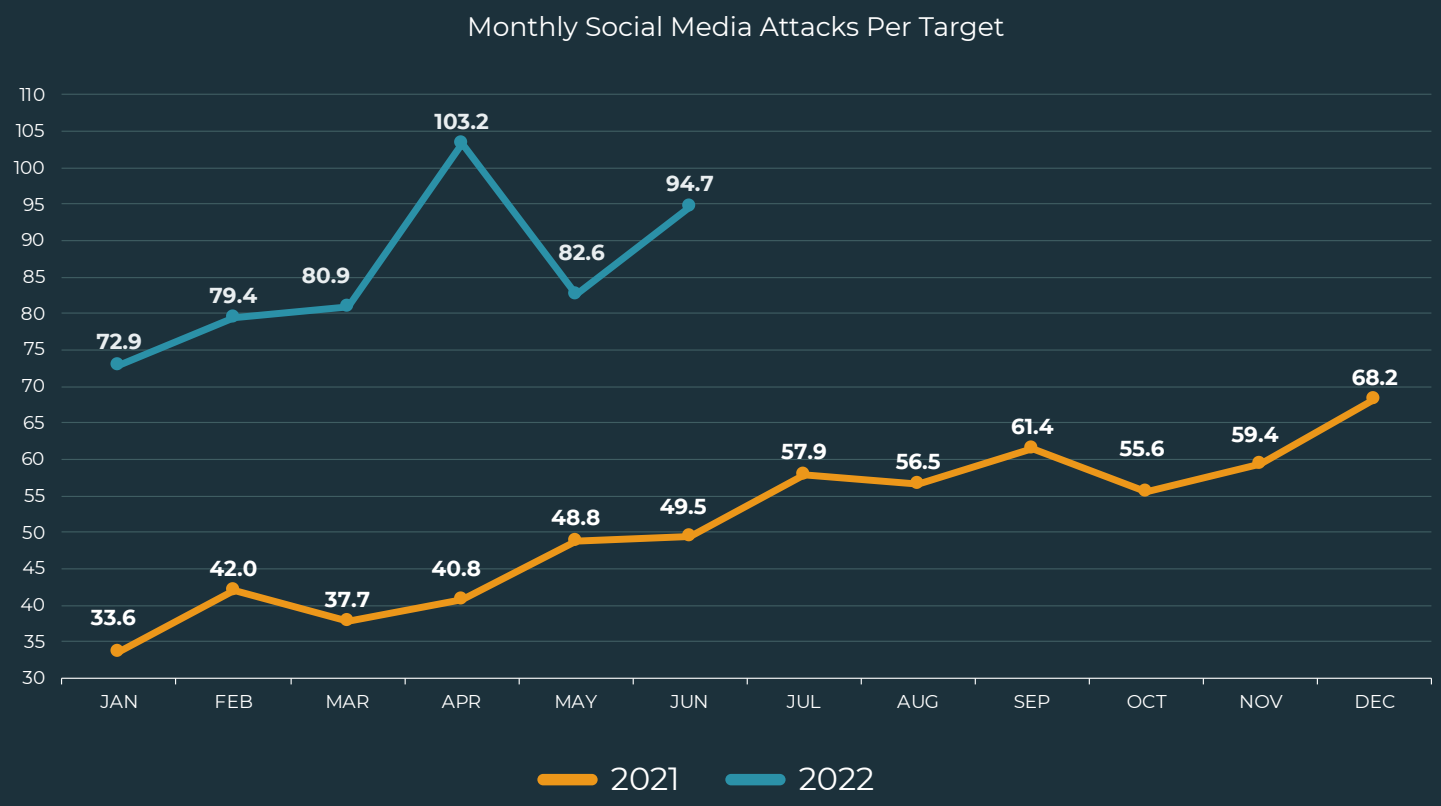


SOCIAL MEDIA THREAT TRENDS

SOCIAL MEDIA ATTACKS CONTINUE TO CLIMB

Threatening behavior targeting organizations on Social Media continues to increase, as social platforms make it possible to reach massive populations of potential victims. In Q2, Social Media attacks increased 20.3% from Q1, averaging nearly 95 attacks per enterprise, per month. This represents a more than 100% increase in attacks in the last 12 months.

Attacks per target increased 102% from Q2 2021 to Q2 2022.

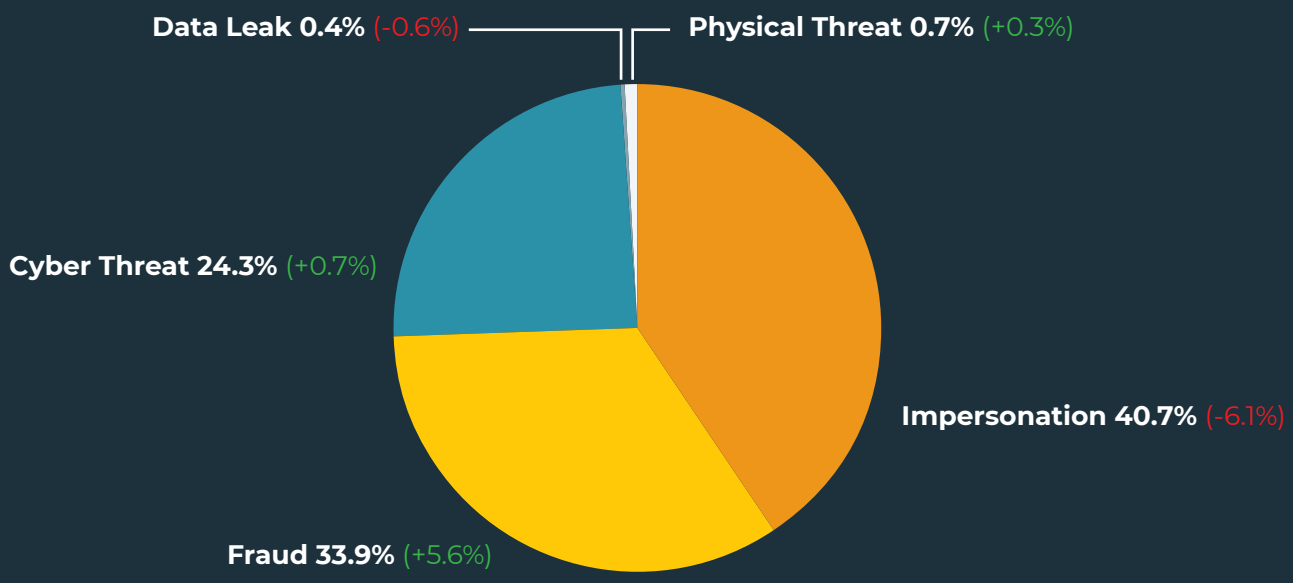


TOP SOCIAL MEDIA THREATS

Impersonation scams on social media were the top threat type in Q2, despite declining in share more than 6%. This is the second consecutive quarter Impersonation has claimed the top spot among social media threats, contributing to 40.7% of all incidents. Impersonation includes the purposeful spoofing of a corporate brand, executive, or employee.

Fraud grew the most among threat types, increasing 5.6% from Q1 to Q2. Nearly 34% of all social media attacks were incidents of Fraud, as the accessible nature of social platforms create an ideal environment for banking and deposit fraud scams. Cyber Threats, such as hacking, increased slightly during Q2, contributing to 24.3% of share of incidents. Notably, while Data Leaks on social media accounted for nearly a quarter of all threat-types in Q1 2021, they have since declined for six quarters in a row. In Q2 2022, Data Leaks represented only 0.4% of social media threat-types.

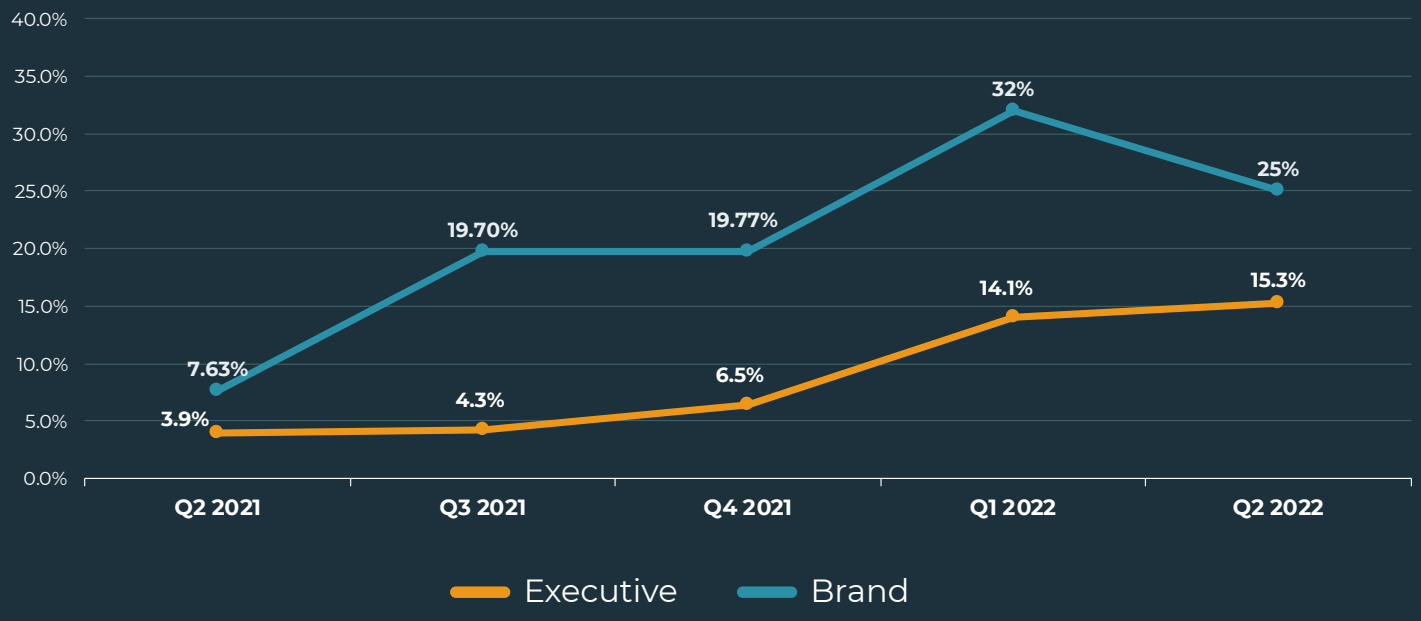
In Q2, Social Media Impersonations continue to plague enterprises.



BRAND AND EXECUTIVE IMPERSONATION

Brand and Executive Impersonation represented more than 40% of share of attacks on Social Media in Q2. Impersonation of a Brand declined 7% from Q1, contributing to 25% of share. Executive Impersonation increased for the fourth straight quarter, accounting for 15.3% of Social Media attack volume. Investment in brand-building and a healthy executive presence on Social Media is increasingly essential to the success of an organization. However, threat actors also see the value and are actively abusing the names, trademarks, and IP of businesses on Social Media to engage with current and would be customers for malicious purposes.

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

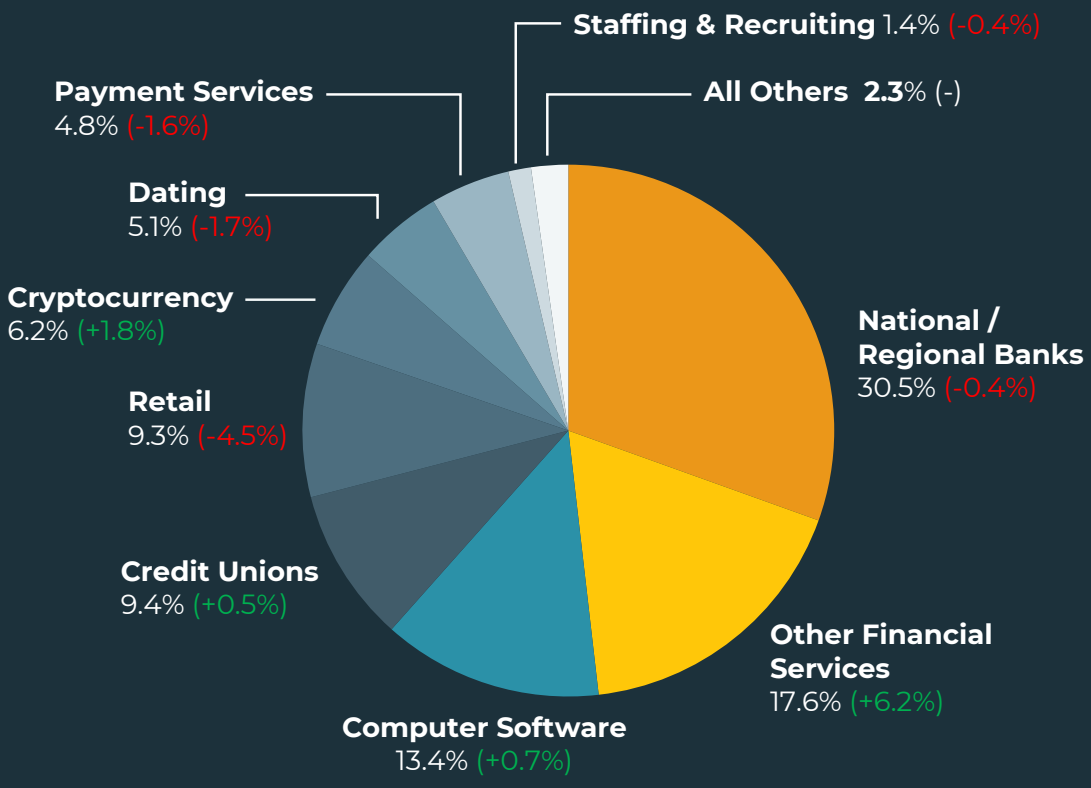


ATTACKS BY INDUSTRY

The Financial Industry as a whole continues to experience extensive abuse on Social Media. Banks, Other Financial Services (i.e. asset management and financial advisory firms), Credit Unions, Cryptocurrency, and Payment Services experienced more than 68% of share of attacks in Q2, fueled primarily by increased fraud and impersonation of a brand or executive.

While National/Regional Banks (30.5%) claimed most of the abuse in Q2, Other Financial Services (17.6%) experienced the most significant increase in attack volume, moving up multiple positions to represent the second most targeted industry. Computer Software (13.4%) and Credit Unions (9.4%) claimed the third and fourth spots, after experiencing increased attacks in Q2. Despite a slight decline in share, Retailers continued to be heavily targeted by impersonation attacks. In Q2, Retail experienced 9.3% of overall abuse.

Attacks targeting Cryptocurrency continue to grow as social platforms prove the ideal environment for cyber threats and impersonation scams. In Q2, attacks on Cryptocurrency increased 1.8% of share to represent 6.2% of attack volume.



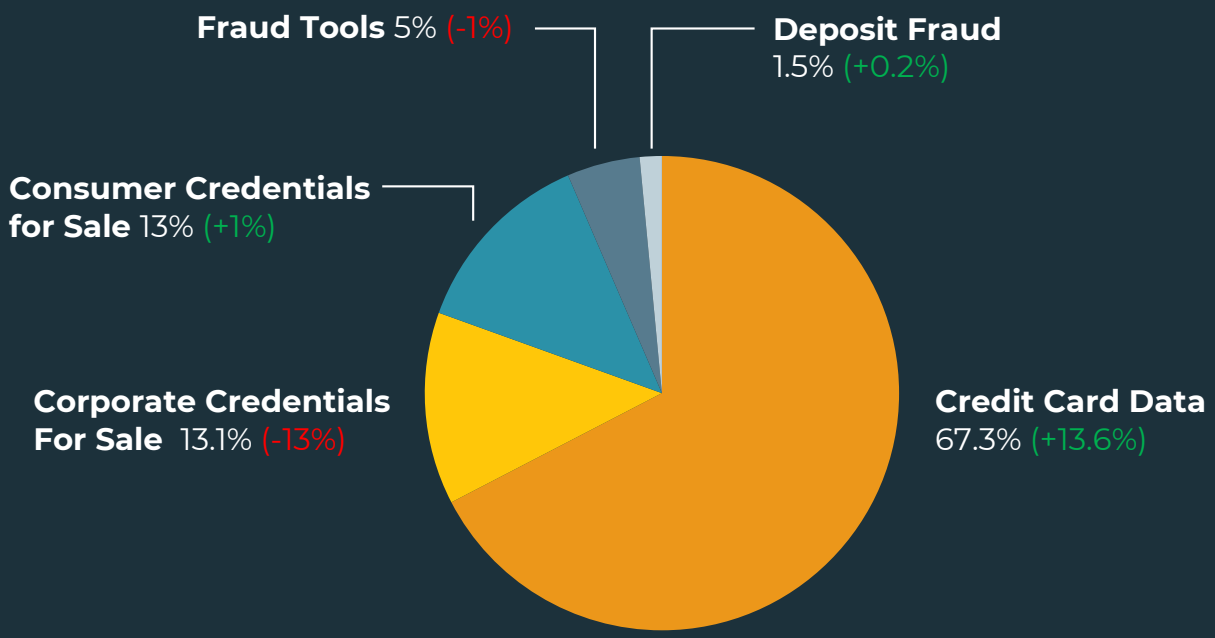
DARK WEB THREAT TRENDS

TOP DARK WEB THREATS

In Q2, Credit and Debit Card Fraud contributed to 67.3% of all incidents on the Dark Web after experiencing an increase of nearly 14% over last quarter. Despite the volatile nature of illegal activity on the Dark Web, stolen card data consistently represents the most common threat advertised by criminals. The percentage of Corporate Credentials (Personally Identifiable Information) for sale declined by nearly half its share in Q2 yet represented the second most common Dark Web threat.

Corporate Credentials contributed to 13.1% of share of Dark Web threats advertised in Q2. Consumer Credentials for Sale displayed nearly identical volume, making up 13% of share of all Dark Web threats. The share of Consumer Credentials advertised on the Dark Web increased 1.0% in Q2. Fraud Tools designed to compromise corporate networks also decreased 1.0%, contributing to 5% of overall Dark Web volume.

Credit and Debit Card Data for Sale experienced the largest increase in Q2, remaining the top Dark Web threat.

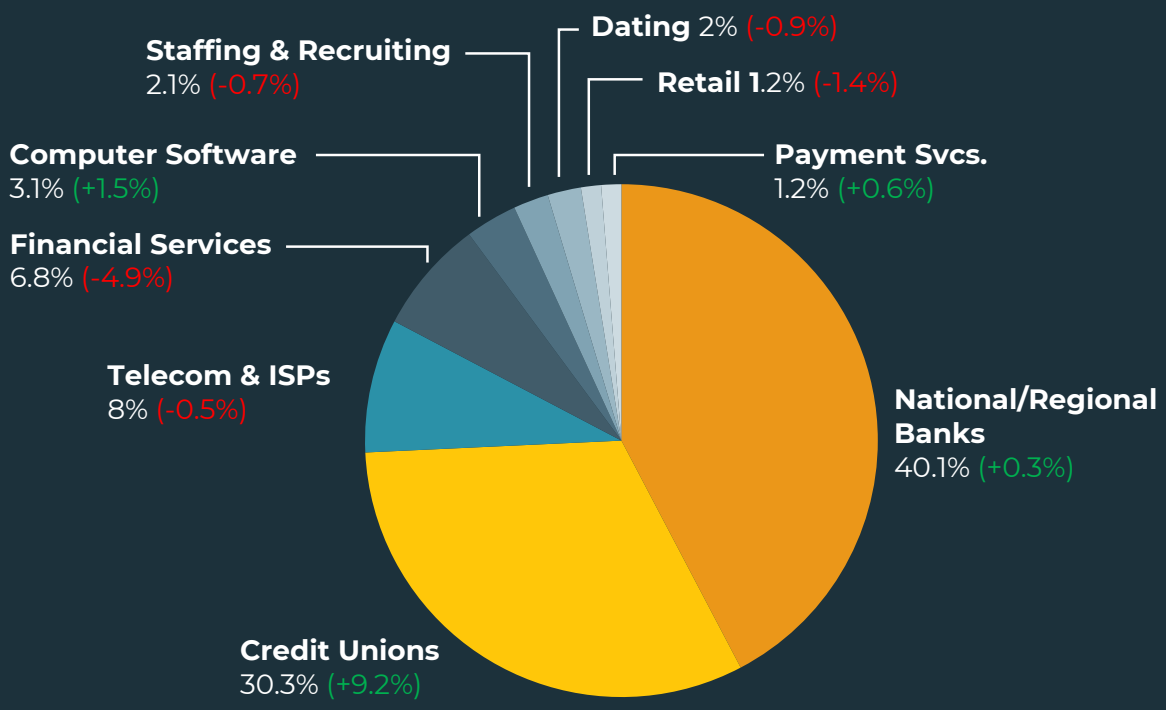


TOP TARGETED INDUSTRIES

In Q2, more than three quarters of all Dark Web threats specifically targeted compromised data associated with Financial Institutions. Banks, Credit Unions, Other Financial Services, and Payment Services contributed to nearly 79% of Dark Web attacks, up from 73% in Q1 2022. National and Regional Banks were abused most, experiencing 40.1% of Dark Web attacks and surpassing second most abused Credit Unions by nearly a ten-point margin.

Credit Unions experienced the greatest volume of attacks within their industry in four quarters, after a 9.2% jump in abuse. Credit Unions represented 30.3% of share of attacks on the Dark Web. Financial Services were the only industry within the group to experience a decline in abuse in Q2, experiencing 6.8% of attacks.

Telecom & ISPs were the third most targeted industry on the Dark Web, contributing to 8.0% of share of abuse. Other non-financials such as Computer Software (3.1%) jumped to the fifth most targeted industry in Q2 after a 1.5% increase in attacks. Staffing & Recruiting (2.1%), Dating (2.0%), and Retail (1.2%) all experienced a decline in activity.

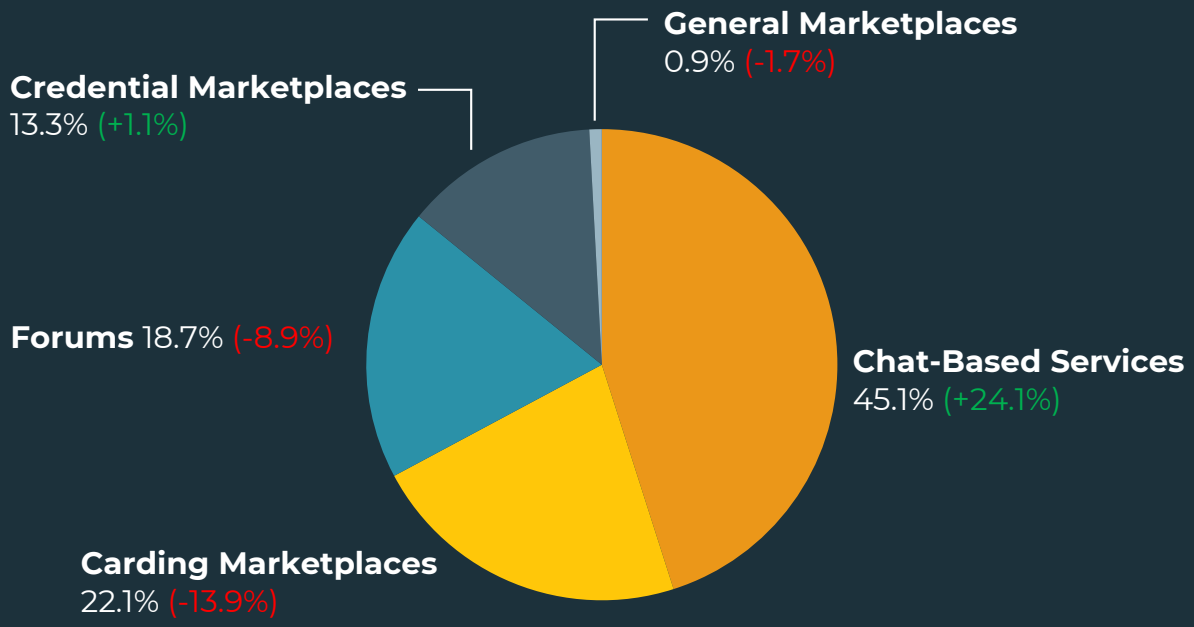


WHERE STOLEN DATA IS MARKETED

In Q2, Stolen data on the Dark Web was most frequently marketed through Chat-Based Services. More than 45% of stolen data listings were observed on these services. Activity on Chat-Based Services increased 24.1% in share this quarter, the first since Q3 2021. Carding Marketplaces specializing in the sale of account and card data dropped to the second spot after a 13.9% decrease from Q1. Carding Marketplaces represented 22.1% of share of all Dark Web activity.

Forums used to engage in unethical activity such as the exchange of hacking information, fraud tactics, and more, contributed to 18.7% of activity on the Dark Web. This represents a nearly 9% decrease over Q1. Stolen account-based data marketed on Credential Marketplaces increased slightly in Q2, contributing to 13.3% of share of Dark Web activity.

In Q2, threat actors relied on Chat-Based Services 45% of the time to market and share stolen data.



SUMMARY & CONCLUSION

Threat actors are actively abusing unconventional attack methods and online channels to maximize the effectiveness of campaigns. While email phishing remains the most dominant threat type, these modified tactics and external environments supplement traditional means of deception.

Phishing continues to be the top online threat to organizations. In 2022, phishing volume has remained steady, increasing nearly 6% from Q1 to Q2. Month-to-month volume has trended slightly down. This is in contrast to 2021, when high-volume campaigns caused several spikes in attack volume.

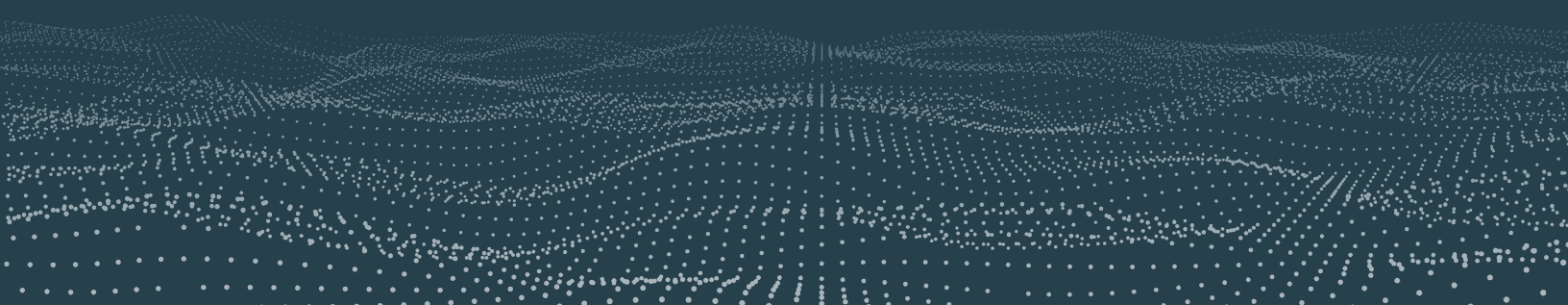
Response-Based email scams such as 419, BEC, and Vishing continue to climb, with the threat group reaching its highest recorded volume since 2020. While all three threat types grew in incident count, hybrid Vishing attacks initiated via email reached a six-quarter high, increasing 625% from Q1 2021. Hybrid Vishing attacks are one example where bad actors have modified traditional tactics to evade security controls and fool victims.

Since November 2021, Emotet attacks have steadily increased as threat actors rebuilt thought to be defunct operations. In Q2, Emotet officially regained its status as the top payload after increasing 30.7% to represent nearly half of all malware attacks. Notably, newcomer Bumblebee jumped from unknown to the third spot, and may be linked to former preferred payload Trickbot.

Social Media attacks have grown more than 100% over the course of a year as social platforms become a hotspot for impersonation attacks and counterfeit activity. Increased brand presence and business-to-consumer interaction makes Social Media an ideal environment for the unauthorized use of trademarked materials as well as misleading messages. The average business can now anticipate experiencing nearly 95 attacks per month on social channels.

During the first half of 2022 threat actors targeted organizations more, with increased investment in diverse, non-traditional tactics. While tried and true attacks such as Response-Based email scams reached all-time highs, threat actors also embraced and exploited changes in technology and communications to grow their odds of turning a profit. Going forward, security teams should counteract the attack footprint by investing in cross-channel monitoring and partnerships with technology providers where abuse may occur.

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 delivers Digital Risk Protection through curated threat intelligence and complete mitigation. PhishLabs provides brand impersonation, account takeover, data leakage and social media threat protection in one complete solution for the world's leading brands and companies. 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.