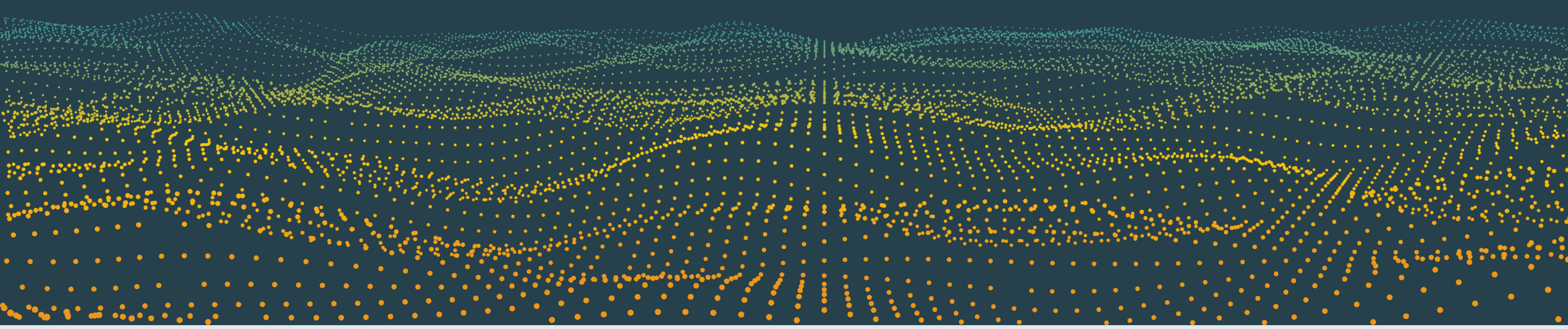
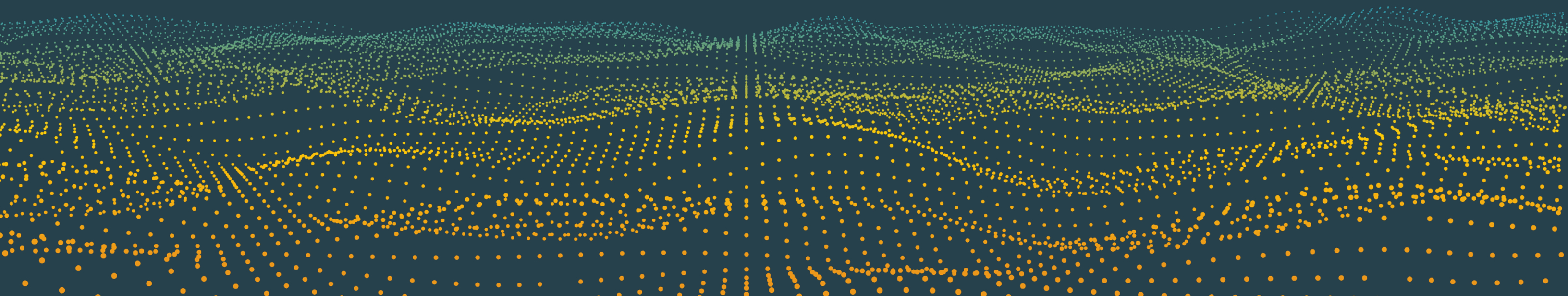
PHISHLABS
by HelpSystems

QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT

FEBRUARY 2022



CONTENTS



ABOUT THE REPORT

In Q4 and throughout 2021, 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 Increased in 2021

Phishing attack volume grew 28%.

Vishing Attacks are Skyrocketing

Vishing attacks initiated by email have increased 554%.

Social Media Threats Double

Threats increased 103% in volume from Q1 to Q4.

Ransomware Payloads are a Moving Target

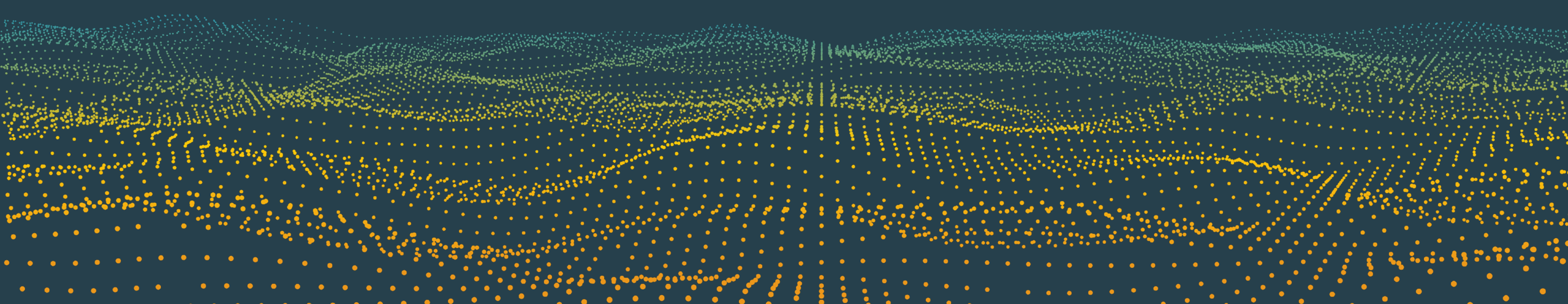
Malware reports nearly tripled, with Qbot and ZLoader leading attacks.

Free Tool Abuse Remains Popular with Threat Actors

Half of all phishing sites observed in Q4 were staged using a free tool or service.

Chat and Card Data Dominate The Dark Web

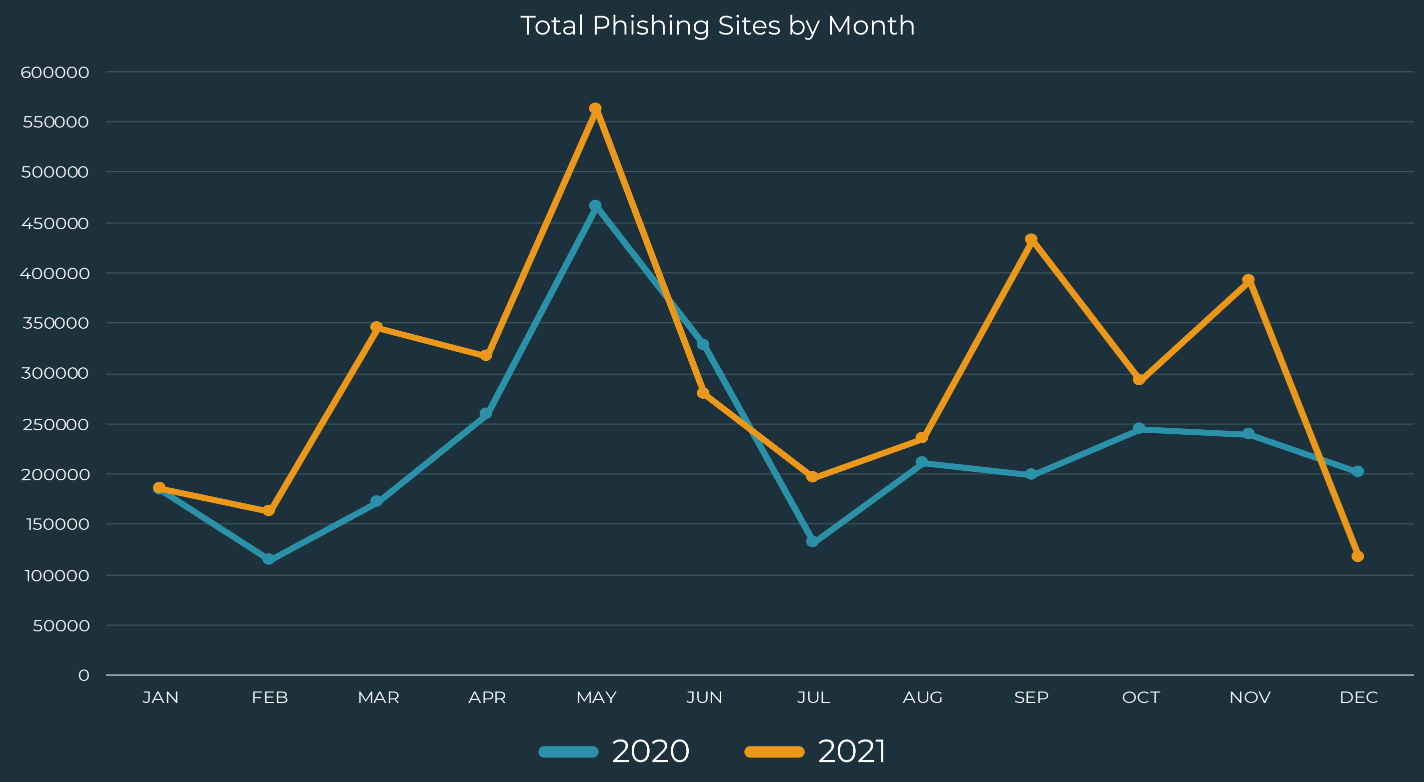
70% of ads for stolen data took place on Chat-based Services and Carding Marketplaces.



PHISHING THREAT TRENDS OVERVIEW

2021 PHISHING OUTPACES 2020

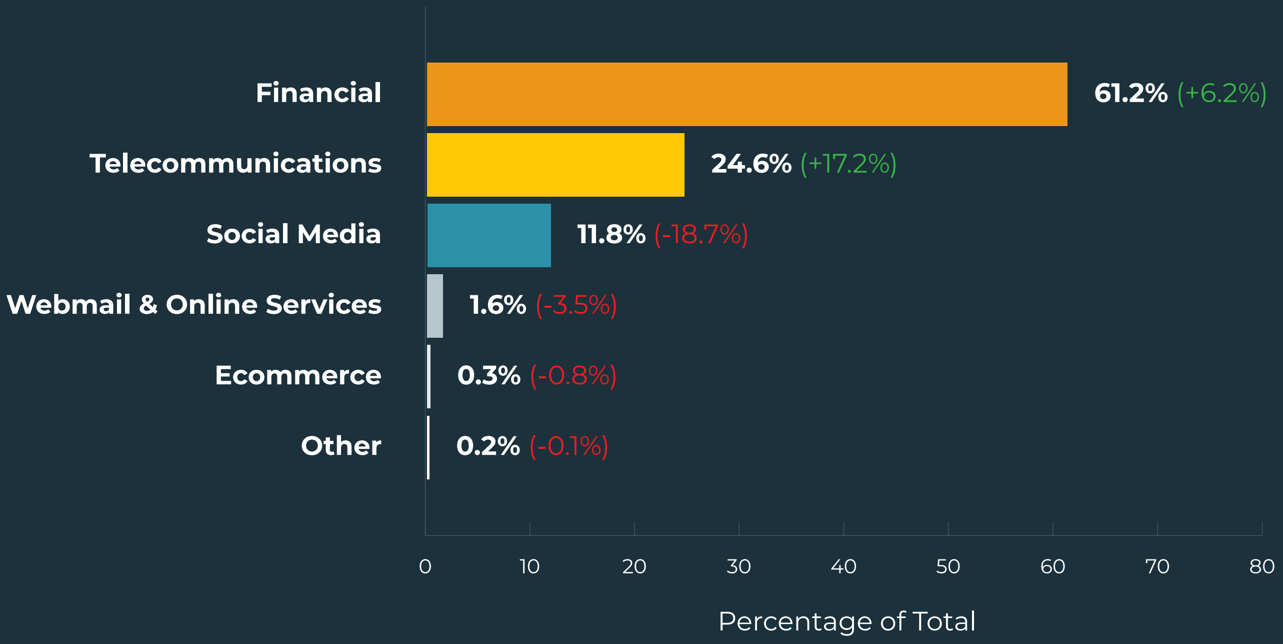
In 2021, the total number of phishing sites observed increased 28%. Despite outpacing last year's volume, month-to-month phishing activity in 2021 proved to be erratic. Phishing volume ranged from a two-year high in May to a nearly two-year low in December. October attack volume was similar year-over-year, while November attacks represented the third highest reported monthly volume in 2021.



TOP TARGETED INDUSTRIES

In Q4, the Financial, Telecommunications, and Social Media Industries were responsible for nearly 98% of all phishing sites. Phishing attacks targeting Financials climbed consistently in share throughout 2021, including a 6.25% increase in share in Q4. Telecommunications (24.6%) experienced the second highest percent of phishing sites, overtaking Social Media (11.8%). Other industries targeted by phishing sites in Q4 included Webmail and Online Services (1.6%), and Ecommerce businesses (0.3%), both dropping in share from Q3.

The percentage of phishing attacks targeting Financial Institutions increased 27.5% from Q1 to Q4 2021.

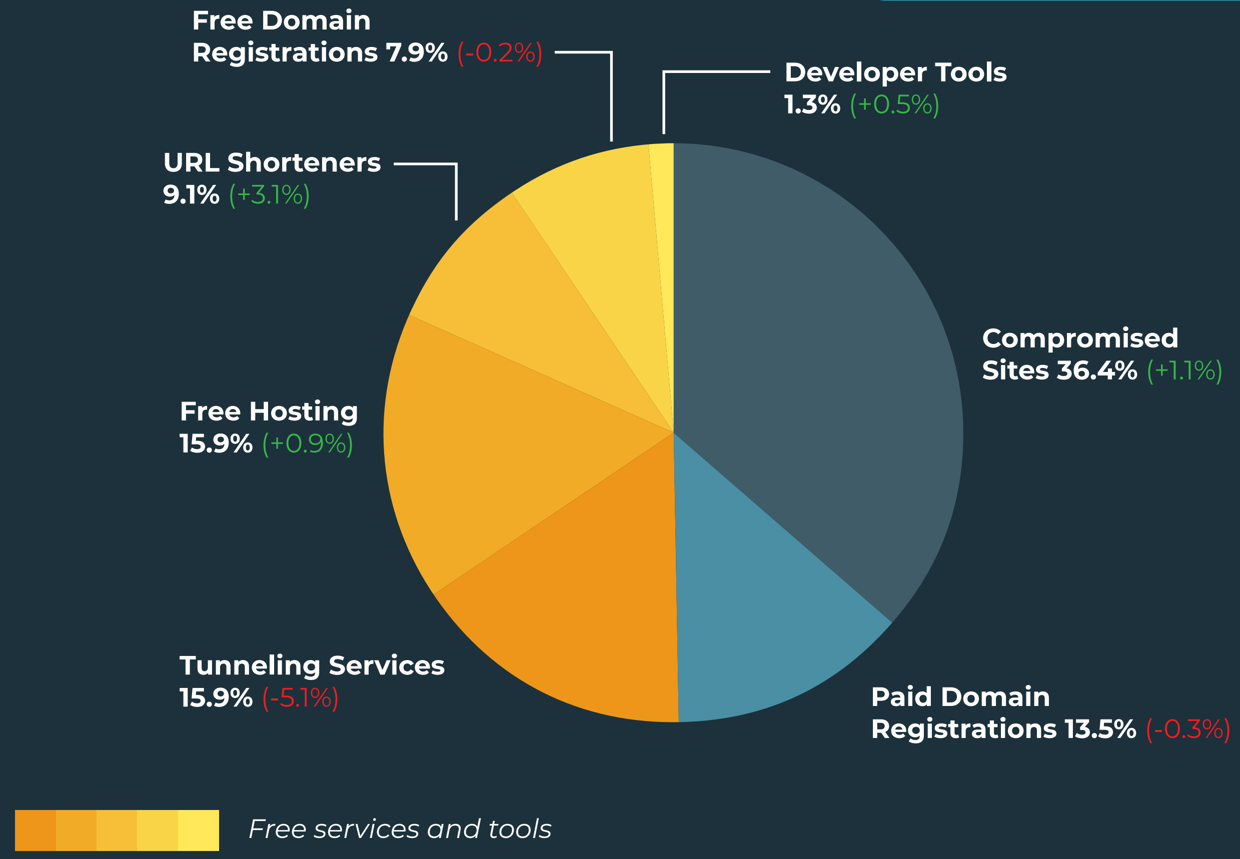


STAGING METHODS

In Q4, just over half of all phishing sites (50.1%) were staged by abusing free sites and resources, including Tunneling Services, Free Hosting, URL Shorteners, and Free Domain Registrations. Although nominal changes were seen across all staging methods, Tunneling Services had the most significant change in share, declining 5.1% from Q3.

In aggregate, while Free Sites and Resources were popular with threat actors, compromising existing websites remained the single most abused method for threat actors to stand up phishing sites in Q4, climbing in percentage of share to 36.4%.

In Q4, just over half (50.1%) of all phishing sites abused some form of free service or tool.



In Q4, while threat actors continued to rely heavily on .com to stage phishing sites, .ca and 6 other ccTLDs accounted for an additional one-third of all malicious activity.

DOMAIN ABUSE

Almost 57% of all phishing scams reported in Q4 used Legacy generic Top-Level Domains for staging phishing sites. While Legacy TLDs remained the domain of choice for threat actors in 2021, ccTLDs (Country Code) were also used widely in Q4, increasing 10% in share from Q3. Of the TLDs abused by threat actors, the Legacy Top-Level Domain .com accounted for half of all phishing activity, despite decreasing in share 4.9%.

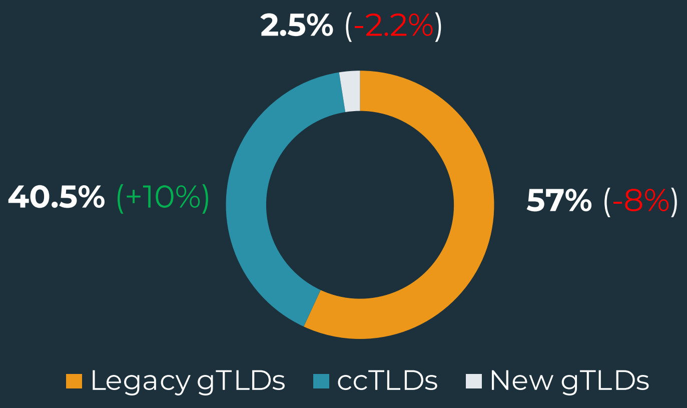
The domain experiencing the largest increase in abuse was .ca, contributing to nearly 20% of all phishing activity. Notably, seven ccTLDs made the top 10 list in Q4, accounting for one-third of all phishing sites staged.

Other changes in TLD abuse include the activity of ccTLD, .uk, which increased to the third most abused TLD, up from the 22nd position in Q3. Similarly, ccTLDs .hk and .ng made their debut on the top 10, rising to 7th from 137th and 9th from 81st, respectively.

Top 10 TLDs Abused

TLD	TYPE	% PHISH	+/-
.COM	Legacy gTLD	49.9%	-4.9%
.CA	ccTLD	19.6%	+9.3%
.UK	ccTLD	8.6%	+8.2%
.ORG	Legacy gTLD	4.3%	-1.3%
.KE	ccTLD	1.8%	-0.8%
.HK	ccTLD	1.7%	+1.7%
.NET	Legacy gTLD	1.5%	-1.7%
.BR	ccTLD	0.8%	-
.NG	ccTLD	0.7%	+0.7%
.PH	ccTLD	0.5%	+0.3%

Percent of Phish per TLD



PHISHING REPORTED BY CORPORATE USERS

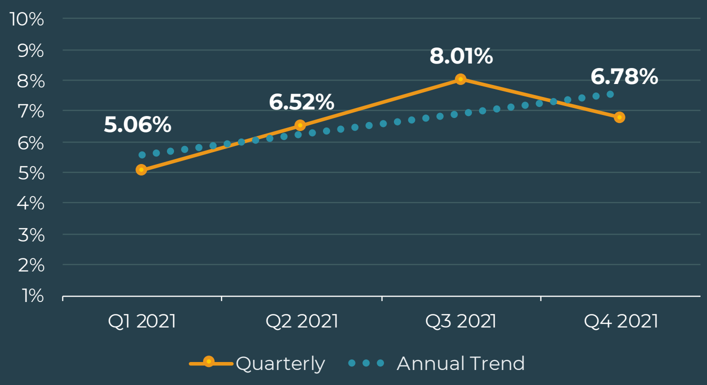
In 2021, the share of employee-reported emails classified as Malicious increased nearly 34%, peaking in Q3.

MALICIOUS EMAILS ON THE RISE IN 2021

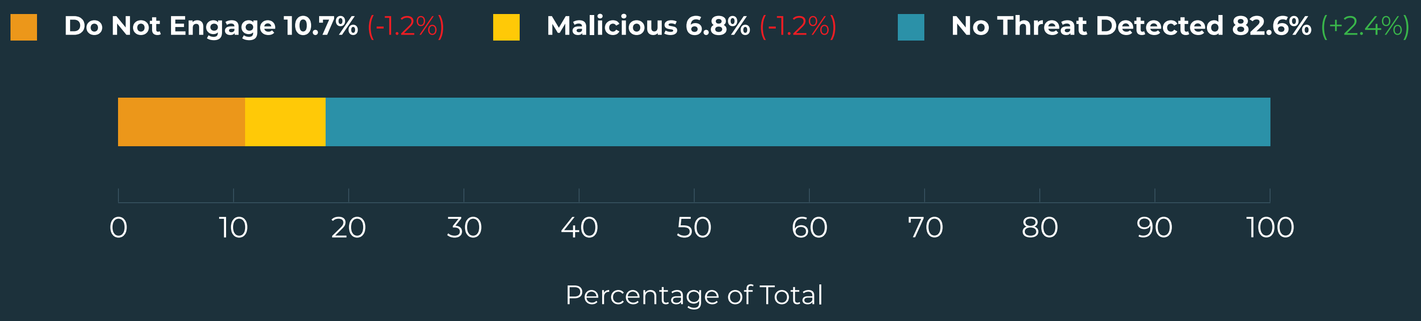
Employee-reported emails are a critical part of any organization's Digital Risk Protection strategy. On average, the majority of suspicious emails reported by employees are not malicious, however a large percentage are legitimate threats. This places significant value on a trained and highly alert workforce to help identify emails that make it past automated security stacks.

In Q4, approximately 18% of reported emails were confirmed Malicious or classified as Do Not Engage by security teams. While the total percentage (6.78%) of Malicious Emails reported was down slightly from Q3, the second half of 2021 experienced a nearly 30% increase over H1 2021.

Percent of Reported Emails Identified as Malicious in 2021



Q4 2021 Employee-reported Emails

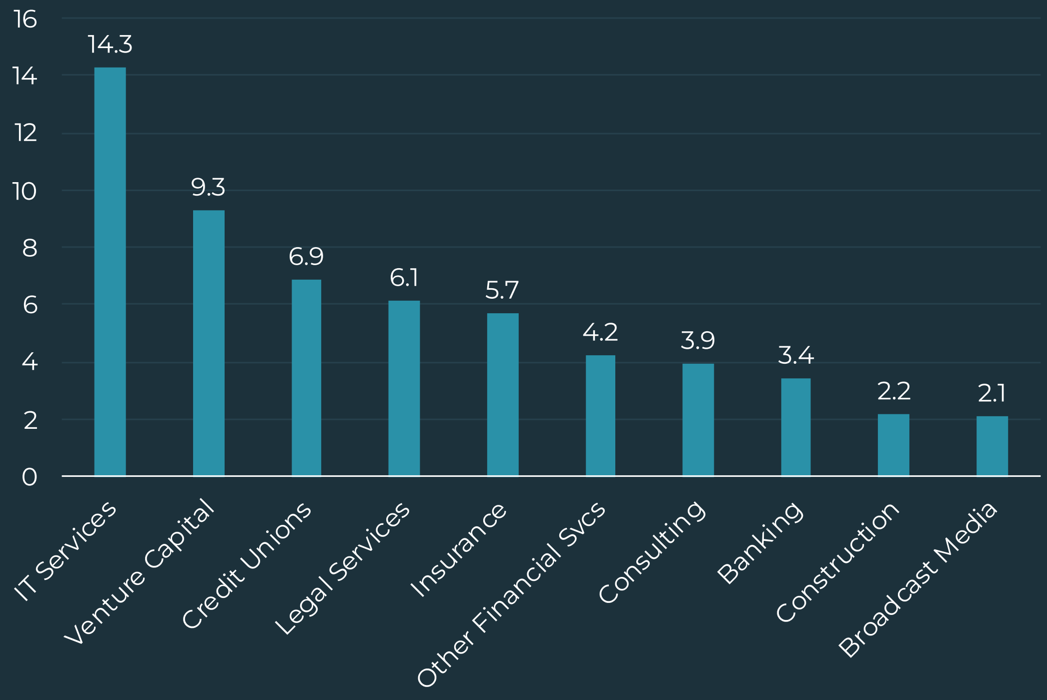


On average, individual employees reported 3.3 suspicious emails in 2021.

EMPLOYEE-REPORTED EMAILS BY INDUSTRY

In 2021, PhishLabs found that on average, across all industries, each employee within an organization was responsible for reporting 3.3 suspicious emails per year. Employees within IT Services reported with the highest frequency (14.3), followed by Venture Capital (9.3), employees of Credit Unions (6.9), Legal Services (6.1), and Insurance (5.7). Employees in these industries and others were responsible for collectively identifying and stopping hundreds of thousands of malicious and highly suspicious emails that could have resulted in substantial financial damage.

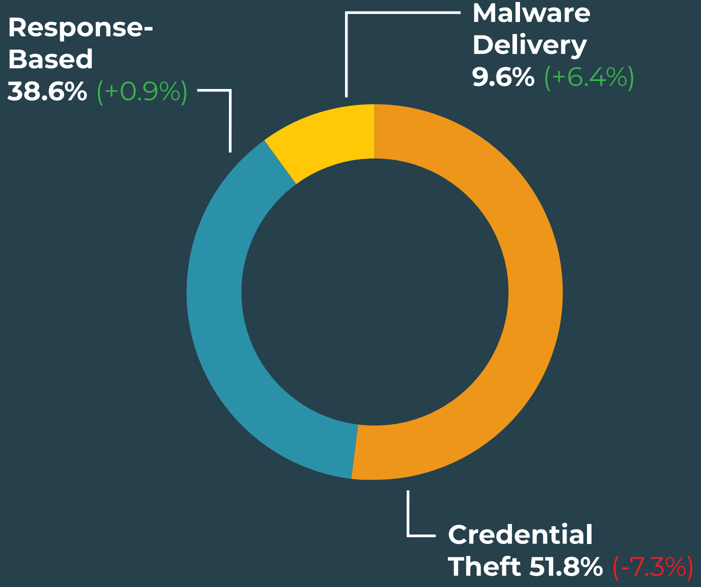
Average Annual Employee-Reported Emails By Industry



THREATS FOUND IN CORPORATE INBOXES

In Q4 and throughout 2021, Credential Theft incidents and Response-Based social engineering attacks accounted for just over 90% of all reported email threats reaching corporate user inboxes. While Credential Theft cases continued to be the most predominant email threat facing employees, their share declined through the second half of 2021. Response-Based threats slowly increased in share consistently each quarter in 2021, demonstrating the continued effectiveness socially engineered attacks have on unsuspecting users.

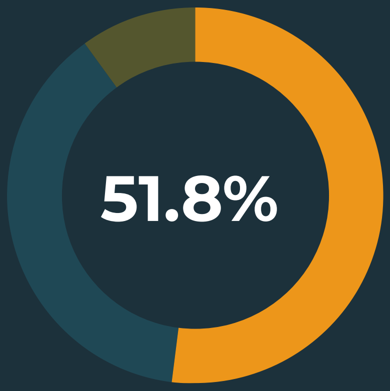
While the percentage of its share is smaller, Malware Delivery cases tripled from Q3 to Q4, increasing from 3.2% to 9.6%. The increase in reported activity during Q4 is the highest percentage in share and volume of reported malware incidents for 2021.



CREDENTIAL THEFT

In Q4, over half (51.8%) of all reported emails reaching corporate user inboxes were Credential Theft attempts. While the total share of Credential Theft cases has declined for two consecutive quarters, it remains the dominant email threat employees face.

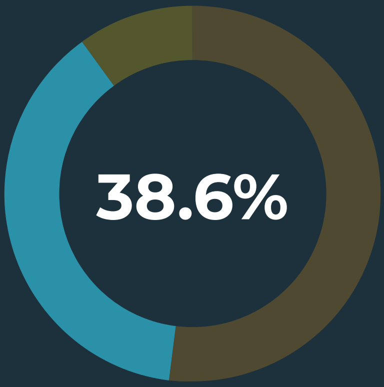
Within the group, 82% of Credential Theft attacks included phishing links. More than 40% of these links targeted Office 365 accounts, which if compromised, would give threat actors access to a broad range of enterprise data and applications. An additional 18% of Credential Theft attacks were classified as Docuphish, including malicious attachments. The percentage in share of Docuphish observed in relation to all Credential Theft incidents remained relatively flat throughout 2021.



Phishing Link	82%
Attachment	18%

RESPONSE-BASED SCAMS

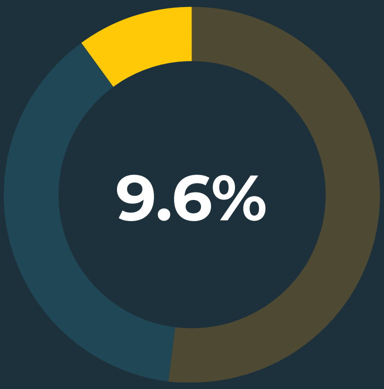
While 419 “Nigerian Prince” scams continued to account for over half of all Response-Based email threats in 2021, Vishing threats have skyrocketed in volume and share. From Q1 to Q4, Vishing threats grew 554%, accounting for over 27% of all Response-Based email threats reported in Q4. The majority of this growth can be attributed to multi-stage Vishing attacks initiated via email. These attacks rely heavily on social engineering to convince victims to call the mobile number provided, and disclose sensitive information to a fake representative. BEC scams (11.3%) were the third most reported Response-Based email threat, followed by Job Scams (9.4%), and Tech Support scams (1.4%).



419	50.8%	-1.5%
Vishing	27.1%	+6.0%
BEC	11.3%	-4.2%
Job Scams	9.4%	-0.7%
Tech Support	1.4%	+0.4%

MALWARE PAYLOAD FAMILIES

Malware threats in user inboxes nearly tripled in Q4. This increase was led by a strong resurgence from Qbot and ZLoader, which collectively accounted for almost 89% of observed payload families. Individually, the Qbot banking trojan was the top payload family, contributing to 59.3% of reports. Qbot led all other payloads in the first half of 2021, before experiencing a dip in volume in Q3. ZLoader had the second highest payload volume among known families in Q4, contributing to almost 30% of reports. A variant of the Zeus banking trojan, ZLoader is a popular MaaS that has maintained a dominant presence throughout 2021.



Payload Family	Q4	Q3	+/-
Qbot	59.3%	7.8%	+51.5%
ZLoader	29.4%	5.2%	+24.1%
Trickbot	3.9%	2.6%	+1.3%
Emotet	2.1%	0.0%	+2.1%
Dridex	1.7%	10.4%	-8.7%
IcedID	1.1%	0.0%	+1.1%
VBS Downloader	0.9%	10.4%	-9.5%
FormBook	0.6%	3.9%	-3.3%

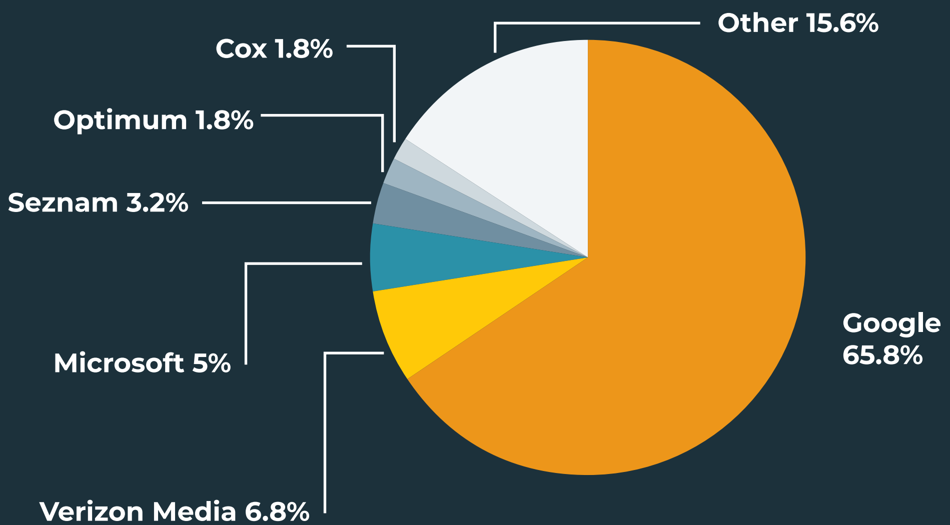
INFRASTRUCTURE USED FOR BEC ATTACKS

In Q4, Agari by HelpSystems examined thousands of BEC attacks that were attempted during Q4 2021. Agari classifies 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. In Q4 nearly three-quarters (74.6%) of all BEC attacks observed were administered through Free Webmail accounts, while maliciously registered and compromised accounts accounted for 25.4%. Of the Free Webmail providers used in BEC Attacks, Google led the way, making up 65.8% of incidents. Other free solutions that were widely abused by threat actors included Verizon Media (6.8%), Microsoft (5.0%), and Seznam (3.2%).

Infrastructure Used to Send BEC Attacks

Free Webmail	74.6%
Maliciously Registered / Compromised	25.4%

Free Webmail Providers Used in BEC Attacks



BEC data courtesy of: agari by HelpSystems

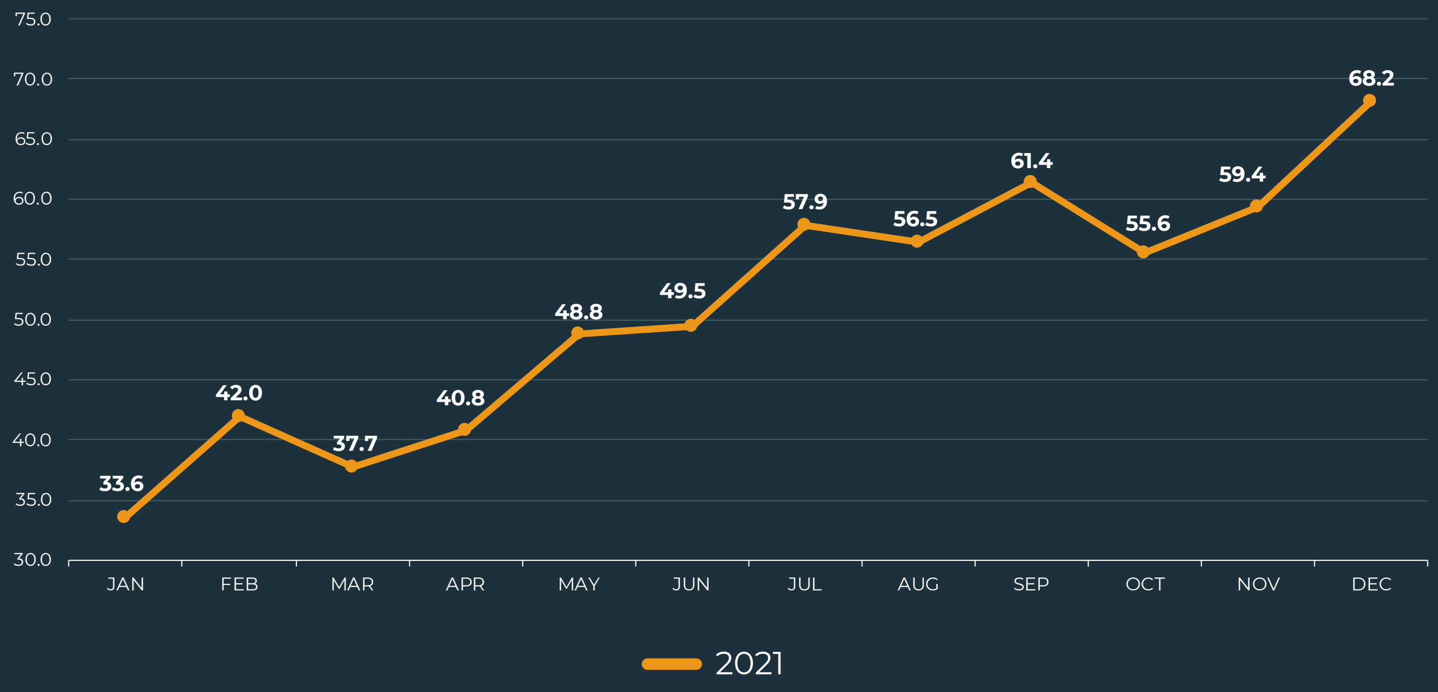
SOCIAL MEDIA THREAT TRENDS

SOCIAL MEDIA THREATS DOUBLE IN 2021

2021 was another record-setting year for Social Media as a threat channel. On average, PhishLabs' clients experienced more than a two-fold increase in Social Media attacks as the year progressed. The number of Social Media attacks per target increased 103% from January, when on average, enterprises were experiencing just over one threat per day. In December, enterprises averaged over 68 attacks per month, or more than two per day.

103% Increase in attacks JAN to DEC 2021.

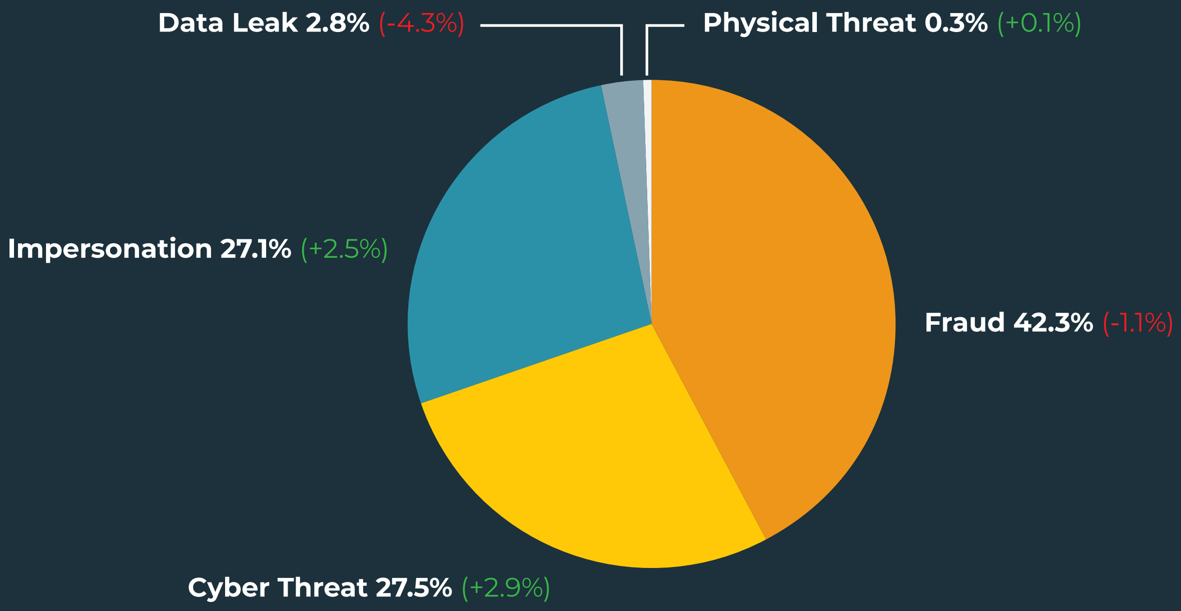
Monthly Social Media Attacks Per Target



TOP SOCIAL MEDIA THREATS

Fraud-related Social Media attacks were the leading threat type encountered by enterprises, despite a slight decrease in Q4. Cyber Threats (such as hacking attempts) and Impersonations increased in share throughout the second half of 2021. Most notably, while Data Leaks continue to pose a significant threat for businesses of all sizes, the volume and percentage in share of attacks have consistently declined from Q1 (23%) to Q4 (2.8%), possibly suggesting a shift in strategy by threat actors.

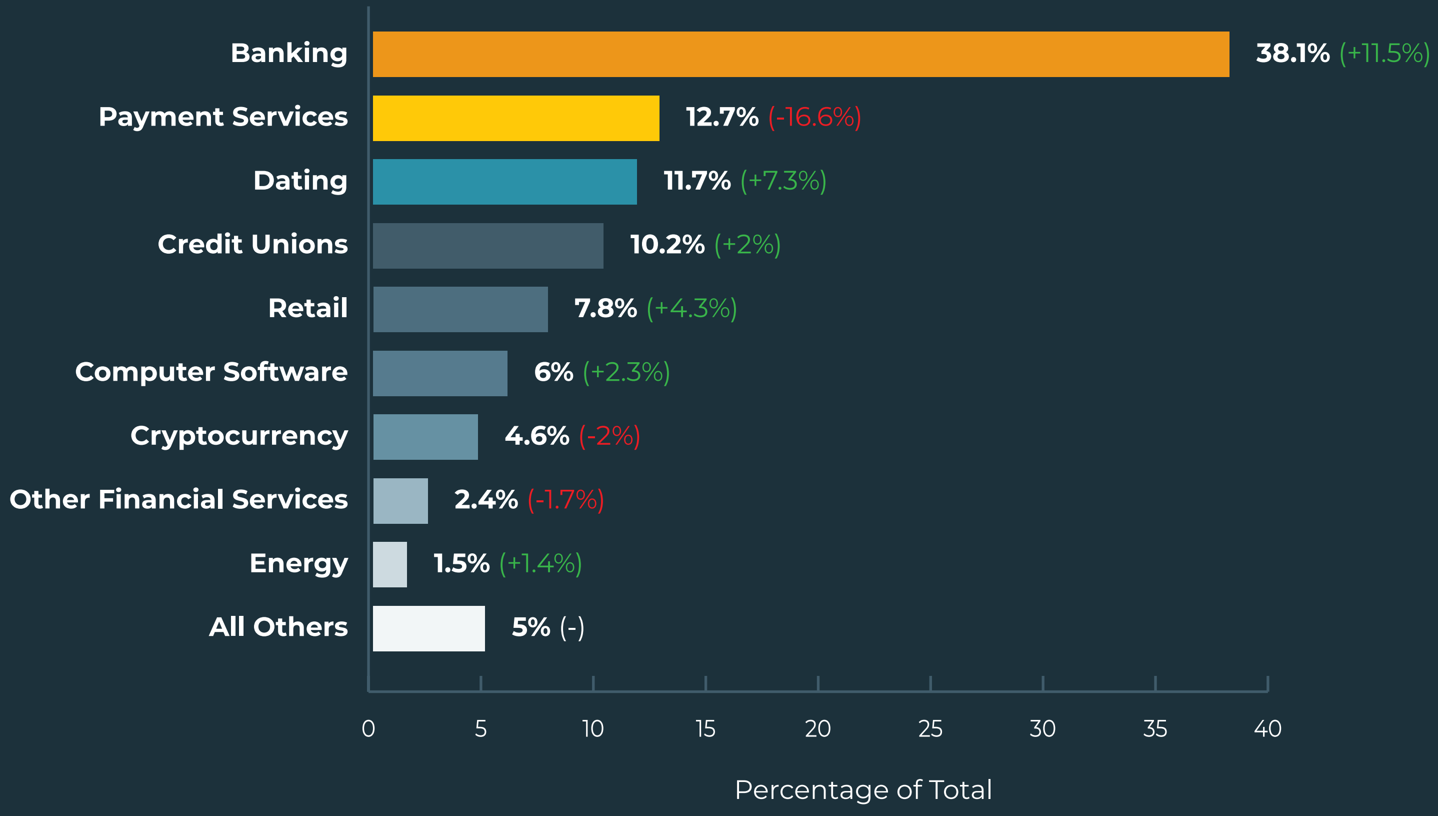
Fraud-related Social Media attacks decreased slightly from previous quarters but continued to account for the largest share of attacks in Q4.



ATTACKS BY INDUSTRY

Banking, Payment Services, Credit Unions, and Other Financial-related businesses represented the industries most impacted by Social Media attacks. Banking was the top targeted industry, experiencing 38.1% of all attacks observed in Q4. Payment Services represented the second most targeted sector, despite experiencing a decline in share of 16.6% from Q3. Threat actors actively target Financials because their services are often used broadly across several business sectors.

Outside of Financials, Dating Services experienced a 7.3% increase in attacks in Q4, contributing to 11.7% of total Social Media attacks. Dating has consistently remained among the top five industries targeted through Social Media during each quarter of 2021. Retail businesses experienced a 4.3% increase in attacks, moving from the tenth most targeted industry in Q3 to the fifth in Q4. This increase could be related to seasonal activity due to the holidays.



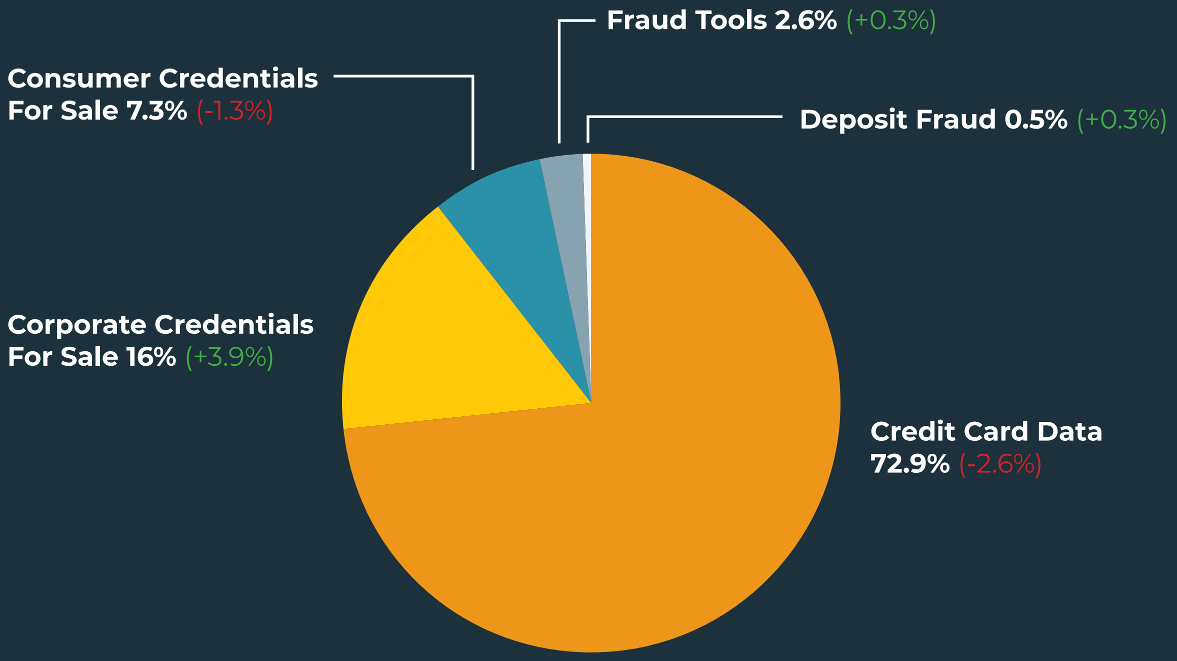
DARK WEB THREAT TRENDS

TOP DARK WEB THREATS

Threat actors advertising stolen credit and debit card data on the Dark Web accounted for almost 73% of all Dark Web threats experienced by PhishLabs clients in Q4. The sale of Corporate Credentials (aka Personally Identifiable Information) retained the second position, contributing to 16% of Dark Web threats encountered, and representing the largest quarter-over-quarter increase in share among all threats.

Consumer Account Credentials for Sale (7.3%), Fraud Tools (2.6%), and Deposit Fraud (0.5%) rounded out the five most common threats advertised to black market buyers in Q4.

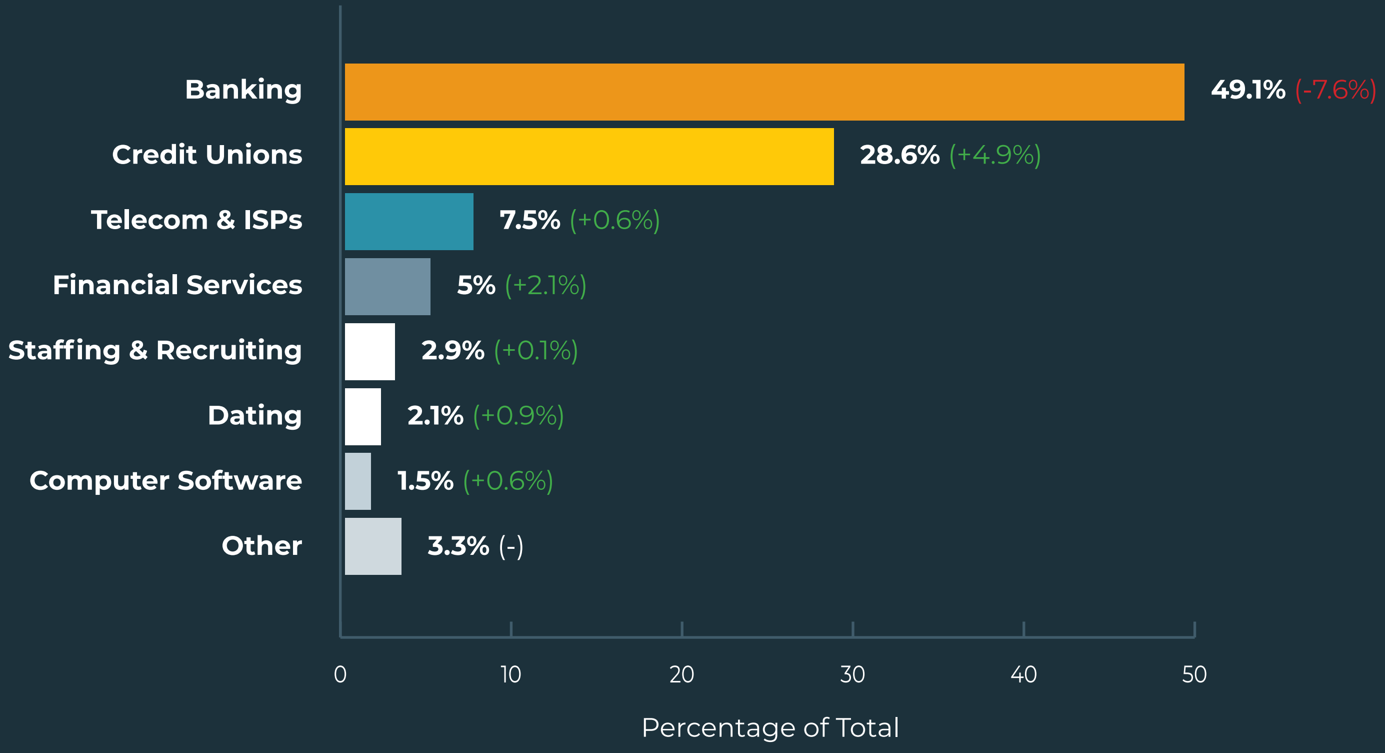
73% of threats encountered on the Dark Web involved stolen credit and debit card data.



TOP TARGETED INDUSTRIES

In Q4, Banking Services were targeted most on the Dark Web by threat actors, accounting for nearly half of all Dark Web attacks, despite a 7.6% decrease in activity. Financial Institutions as a whole, including Banking (49.1%), Credit Unions (28.6%), and Other Financial Services (5.0%), combined to represent 82.7% of all Dark Web activity. Data associated with the Financial Industry is high-value to Black Market customers because it can mean access to PII, login credentials, card data, and other sensitive information critical to launching attacks.

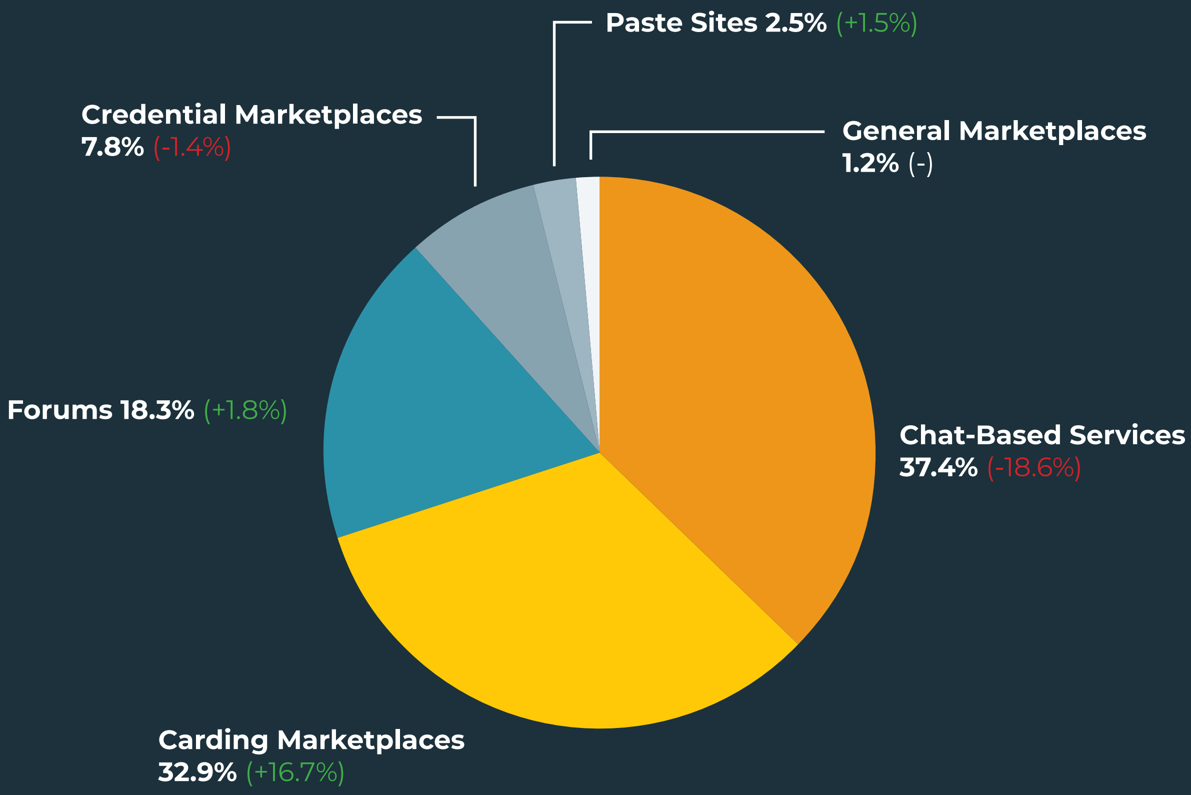
Other Industries targeted in Q4 include Telecommunications & ISPs (7.5%), Staffing & Recruiting (2.9%), and Dating (2.1%), all which experienced an increase in share from Q3.



In Q4, 70% of advertisements for stolen data were placed on Chat-Based Services and Carding Marketplaces.

WHERE STOLEN DATA IS MARKETED

While stolen data continues to be advertised through a wide variety of Dark Web sites, just over 70% of ads for stolen data were placed on either Chat-Based Services or Carding Marketplaces. Chat-Based Services made up 37.4% of all activity in Q4, retaining the top slot but declining in share from Q3 by 18.6%. These sites are most often used to transfer leaked credit card data quickly and anonymously from advertiser to buyer. Carding Marketplaces accounted for 32.9% of the activity, gaining 16.7% in share activity. Rounding out the top five, Dark Web Forums accounted for 18.3% of the share, while Credential Marketplaces and Paste Sites made up 7.8% and 2.5% of the volume, respectively.



SUMMARY & CONCLUSION

Throughout 2021, threat actors relied on a variety of attack vectors to carry out their campaigns. While the year was witness to an increased presence of emerging threats, traditional phishing methods still commanded a majority of threats facing enterprises.

Phishing remained the most dominant attack method across all online threats. From Q1 to Q4, phishing increased 28%. Attack volume this year was also more unpredictable than it was in 2020, with a significant spike in May and two-year low in December.

A notable trend in Response-Based email scams is the significant increase in Vishing attacks. While 419 scams continued to be reported the most by employees in 2021, Vishing scams initiated by email lures increased 554%. These hybrid attacks demonstrate how threat actors are evolving their tactics to enhance the success of malicious campaigns.

The volume of malware threats delivered via email nearly tripled from Q3 to Q4, primarily due to a strong resurgence in Qbot and ZLoader attacks. Reports of these payload families and others have been volatile throughout 2021, signaling that no single payload family stands out as a preferred choice for attackers but rather, criminals choose to use a variety of malware to target victims.

All eyes remain on Social Media threats as the average number of attacks per business continue to rise, doubling in 2021. Threat actors are using Social Media to commit fraud, impersonate brands and executives, and launch a variety of cyber threats, forcing security teams to monitor a variety of platforms for activity targeting their enterprise.

The increased volume in non-traditional attack methods and channels in 2021 reinforce how threat actors are quick to take advantage of new vectors when it enhances their odds of success. While actors continue to target high-value industries, they are also investing resources into exploiting ill-prepared organizations through platforms like social media. In 2022, enterprises must broaden their line of defense starting with strong, cross-channel monitoring, and building relationships with technology providers in new areas to minimize the scope of threats targeting their organization.

PHISHLABS
by HelpSystems

PhishLabs 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.

www.phishlabs.com
info@phishlabs.com
+1.877.227.0790