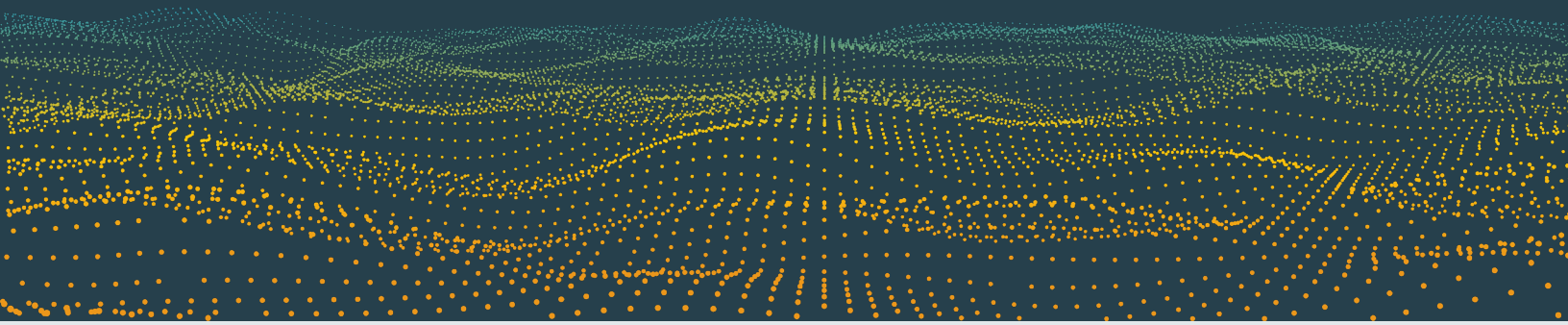
PHISHLABS
by HelpSystems

QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT

NOVEMBER 2021



CONTENTS

ABOUT THE REPORT

In Q3, PhishLabs analyzed hundreds of thousands of phishing and social media attacks targeting enterprises, their employees, and their 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 Threat Continues to Grow

Phishing volume is up nearly 32% year-over-year.

Vishing Attacks are Skyrocketing

Vishing incidents have more than doubled for the second consecutive quarter.

Social Media Threats On The Rise

Social Media threats are up 82% from January and remain a leading threat.

O365 Credentials Valued by Threat Actors

Office 365 phish have increased for 4 consecutive quarters.

Ransomware is Driving Shifts in Payload Usage

BazaLoader was the tool of choice, but new variants appeared in Q3.

Threats Span Across Digital Channels

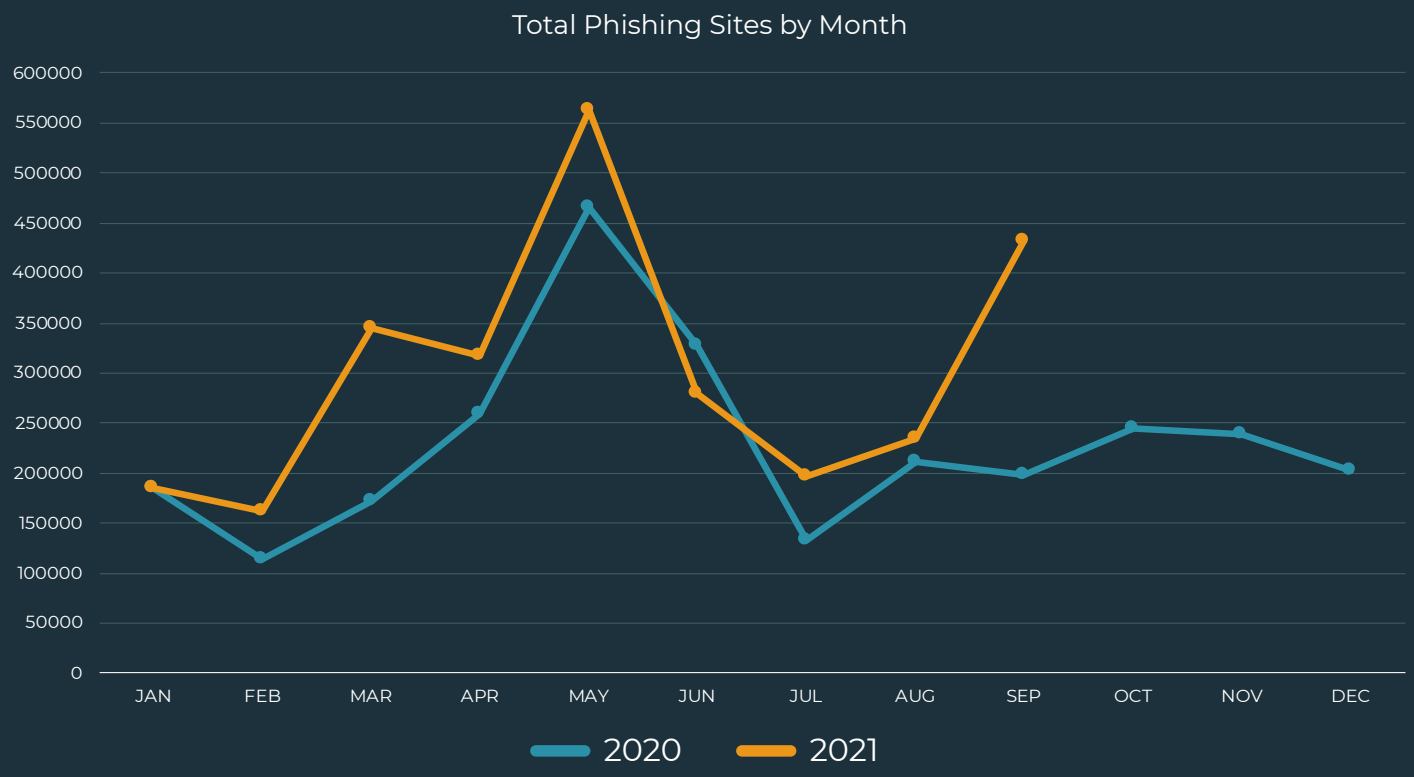
Threat actors are relying on a variety of attack vectors: Email, Social Media, Mobile, and others.

PHISHING THREAT TRENDS OVERVIEW

2021 PHISHING OUTPACES 2020

To date, the total number of phishing sites identified in 2021 has outpaced 2020 by nearly 32%. Similar to the unpredictable nature of phishing activity in Q2, Q3 appeared stable in July and August, before experiencing a significant spike in September.

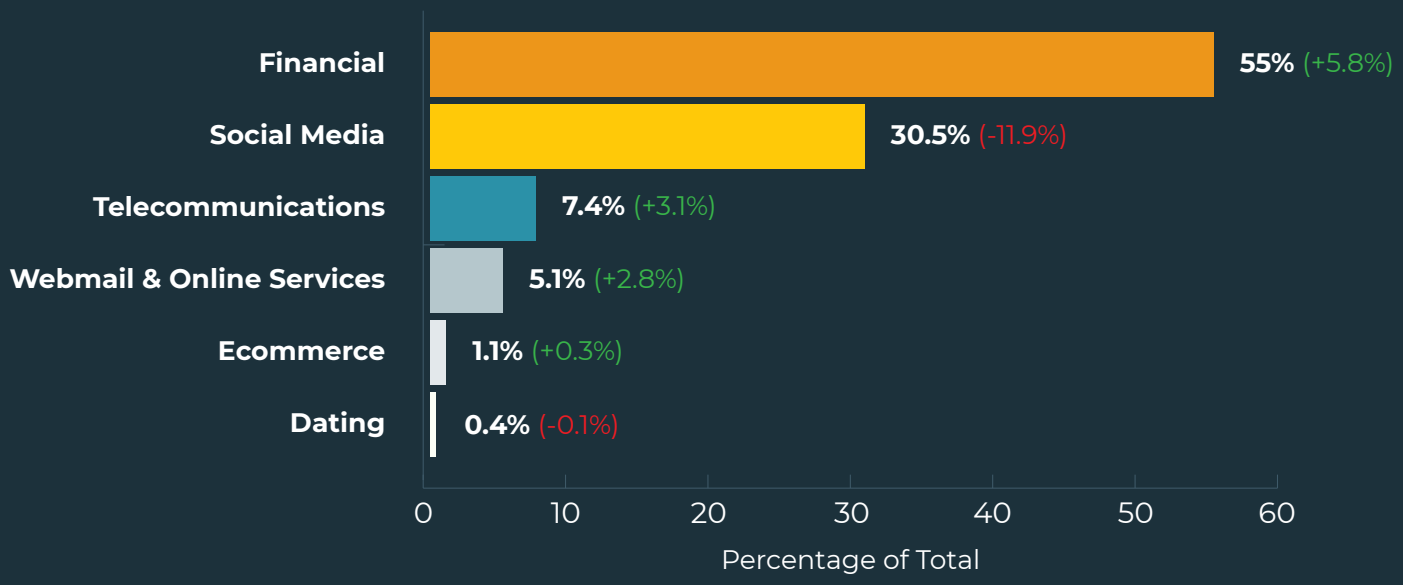
Phishing volume in Q3 2021 exceeded Q3 2020 by nearly 60%, and September's volume more than doubled from the previous year. We anticipate volume will continue trending up throughout Q4.



TOP TARGETED INDUSTRIES

There were noticeable fluctuations in the top six industries targeted by phishing attacks in Q3. Financials continued to be the top targeted industry in Q3 and experienced a 5.8% increase in phishing attacks. While Social Media businesses retained the second slot, the industry continued its slide from the most targeted in Q1, with an 11.9% reduction in attacks in Q3.

Even though Social Media experienced fewer phish, accounts associated with Single Sign-On (SSO) for secondary accounts, including Social Media, Webmail & Online Services, and Ecommerce industries, still experienced a combined 37% of phishing attacks.

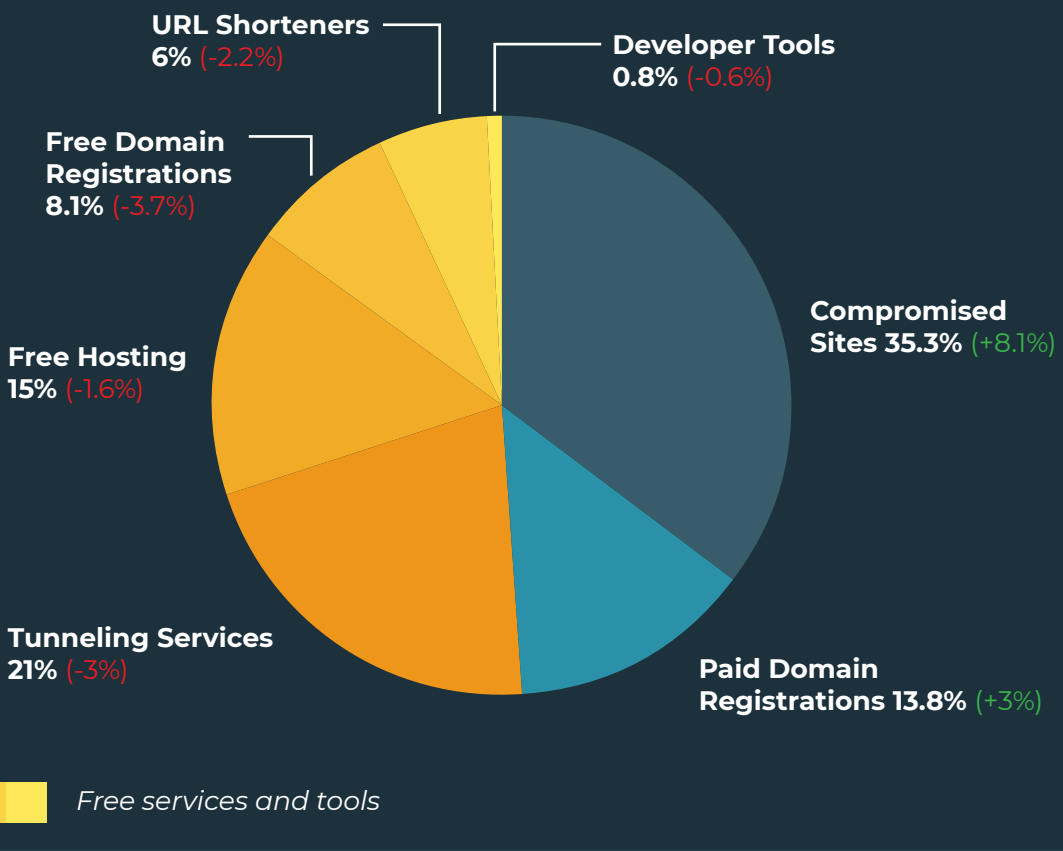


STAGING METHODS

In Q3, threat actors continued to rely on a variety of methods to stage phishing sites. While a slim majority (51%) of phishing sites continued to be staged by abusing free services and tools, Q3 saw a shift away from this activity as actors increasingly used Compromised Sites for phishing site staging. Abuse of Paid Domain Registration services also grew.

While abuse of free services to stage phishing sites continued to be strong, all five categories of free services experienced a downturn in activity compared to Q2.

In Q3, more than half (51%) of all phishing sites abused some form of free service or tool.



In Q3, threat actors relied heavily on .com to stage phishing sites, while abuse of .ca experienced consecutive quarterly increases.

DOMAIN ABUSE

Over 65% of all phishing scams reported in Q3 used Legacy generic Top-level domains. This was led by .com, which was up 15.2% from Q2 and contributed to nearly 55% of all TLDs abused. The ccTLD (Country Code) .ca also experienced a significant surge in Q3, making up 10.3% of the total TLDs abused.

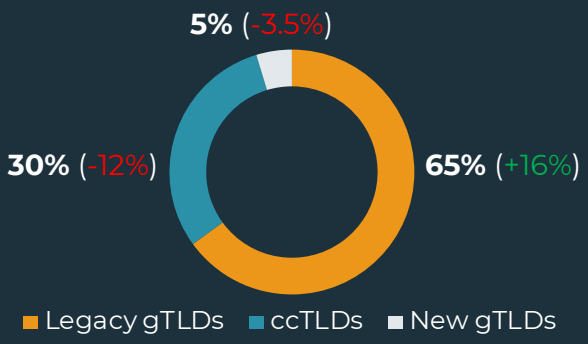
Most notably, ccTLDs .mx, .uz, .monster, and .ae dropped from the Top 10. Additionally, popular ccTLDs that offer free domain registrations (.ml, .tk, .cf, .ga, and .gq) were once again absent.

While none of these cracked the Top 10, they still remained within the top 10% of TLDs abused in phishing attacks. Combined, these free domains made up 2.3% of all phishing in Q3.

Top 10 TLDs Abused

TLD	TYPE	% PHISH	+/-
.COM	Legacy gTLD	54.9%	+15.2%
.CA	ccTLD	10.3%	+6.2%
.ORG	Legacy gTLD	5.7%	-0.2%
.NET	Legacy gTLD	3.2%	-
.KE	ccTLD	2.6%	+1.6%
.IO	ccTLD	1.7%	-2.0%
.XYZ	New gTLD	1.2%	-0.2%
.LY	ccTLD	1.2%	+1.1%
.CO	ccTLD	1.1%	-1.3%
.US	ccTLD	1.0%	+0.7%

Percent of Phish per TLD



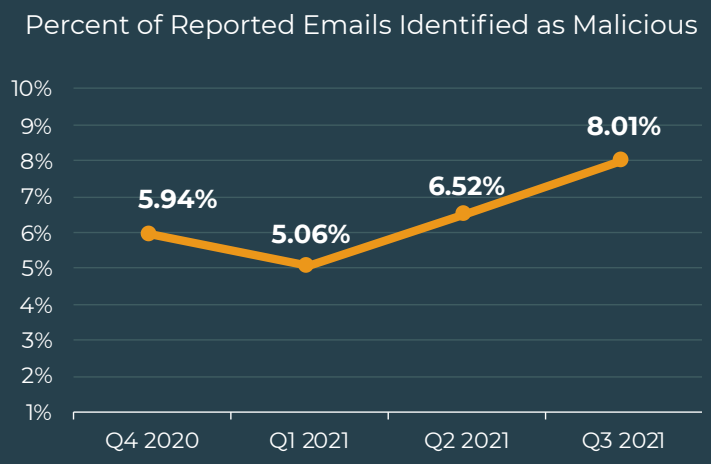
PHISHING REPORTED BY CORPORATE USERS

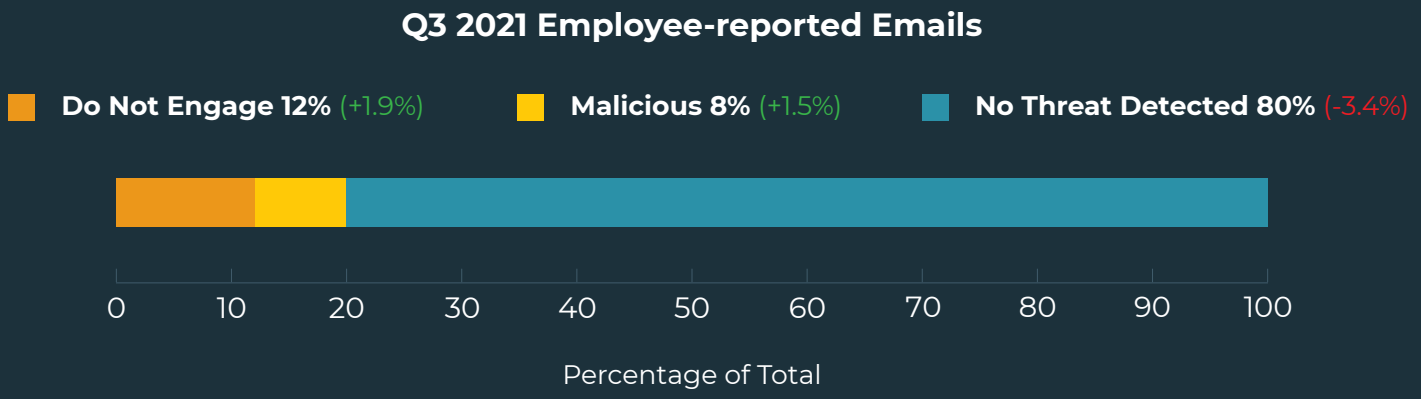
In the past 12 months, the share of employee-reported emails classified as Malicious increased 35%.

MALICIOUS EMAILS ON THE RISE

Employee-reported emails play a critical role in an organization's Digital Risk Protection strategy. While a large majority of reported emails are benign, the share of employee-reported emails classified as risks remains significant. Emails classified as Malicious have increased in both count and share for the last two quarters, making up 8% of the volume in Q3. This is a 35% increase in share from Q4 2020.

While not specifically identified as Malicious, an additional 12% of employee-reported emails were classified as Do Not Engage, suggesting that while the email didn't include specific threatening characteristics, correspondence with the sender could be hazardous.



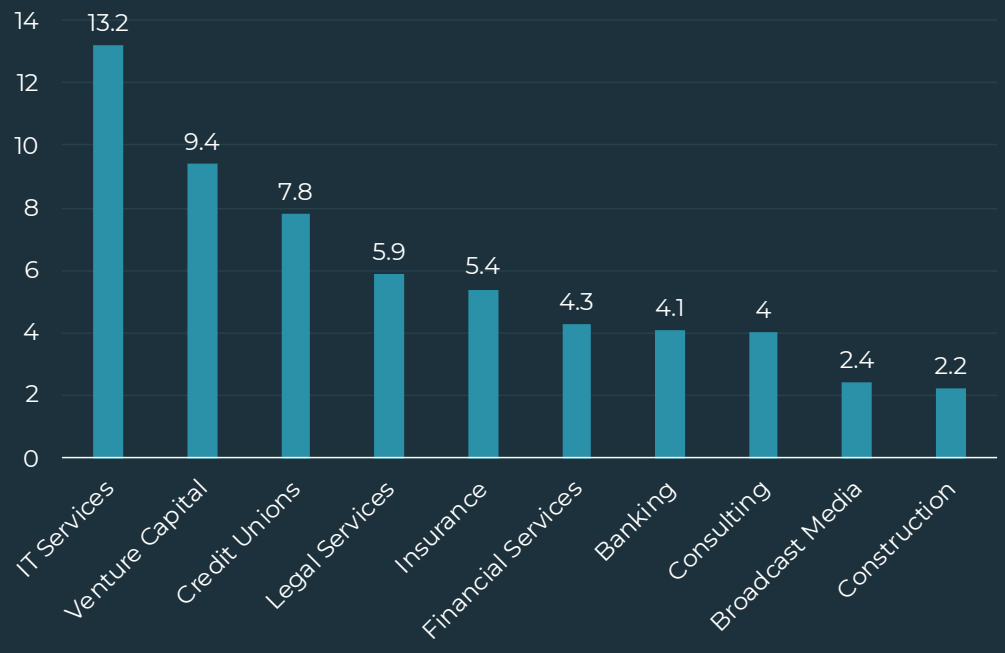


EMPLOYEE-REPORTED EMAILS BY INDUSTRY

From Q4 2020 to Q3 2021, PhishLabs found that on average and across all industries, each employee within an organization reported 3.3 suspicious emails per year. IT Services' employees led the way, reporting an average of 13.2 emails per year, followed by employees of Venture Capital & Private Equity firms (9.4) and Credit Union employees (7.8).

On average, each employee reports 3.3 suspicious emails per year.

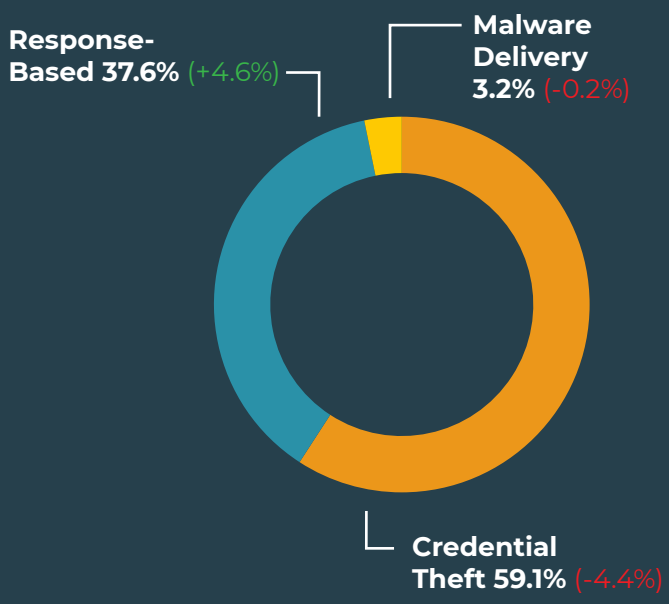
Average Annual Employee-Reported Emails By Industry



THREATS FOUND IN CORPORATE INBOXES

Credential Theft and Response-Based social engineering attacks continue to make up a significant majority, contributing to nearly 97% of the email threats reaching corporate user inboxes. While Credential Theft remained the most commonly reported email threat, Response-Based threats have steadily increased the past two quarters, showing the continued effectiveness socially engineered attacks have on unsuspecting users.

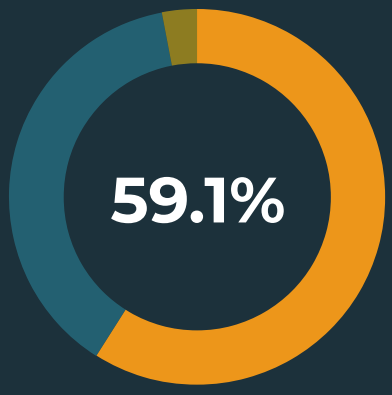
Although ransomware continues to have damaging effects on enterprises, reported emails containing malware steadily declined in share for the fourth consecutive quarter. This may be attributed to the dismantling of key payload families earlier in the year, as well as highly-tuned security controls becoming more adept at stopping malware.



CREDENTIAL THEFT

Although down slightly from Q2, Credential Theft attacks continue to lead the way among the various threats reaching corporate inboxes. In Q3, 59% of reported corporate emails were Credential Theft attempts. Of that percentage over half (51.6%) of the attacks reported targeted Office 365 accounts. Since Q4 2020, Office 365 Credential Theft incidents have increased both in count and percentage of share for four consecutive quarters.

This consistent growth signifies the high value threat actors place on Office 365 credentials for access to a broad range of enterprise data and applications.

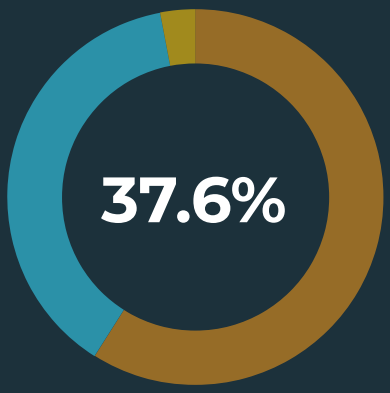


Phishing Link	81%
Attachment	19%

RESPONSE-BASED SCAMS

419 scams continue to make up more than half of all Response-Based scams. However, Vishing incidents overtook BEC scams as the second most reported threat type in Q3, more than doubling in number for the second consecutive quarter. Additionally, we are seeing an increased shift away from traditional Vishing tactics to multi-stage attacks led by malicious emails.

In this type of campaign, actors use a mobile number in the email as a lure, then rely on social engineering and impersonation to trick victims into calling a fake representative. In addition to 419 and Vishing increases, Job Scam incidents were on the rise in Q3, most likely attributed to seasonal recruiting.

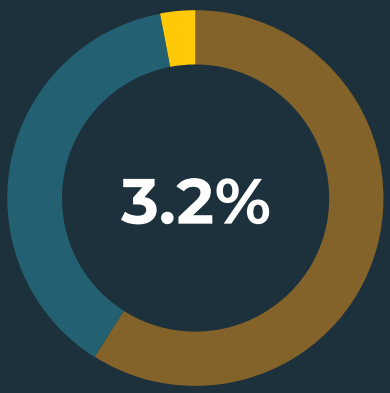


419	52.3%	+1.9%
Vishing	21.2%	+5.2%
BEC	15.4%	-9.9%
Job Scams	10.1%	+4.9%
Tech Support	1.0%	-2.1%

MALWARE PAYLOAD FAMILIES

In Q3, the number of lesser known, one-off payload attacks increased significantly. This may be attributed to unskilled actors taking advantage of a lower barrier to entry with "as-a-service" models that enable easy access to sophisticated, malicious software.

Activity among commonly tracked Payload families continued as well. BazaLoader led the way in Q3, accounting for 24.7% of attacks, followed by Agent Tesla, Dridex, VBS Downloader, and Qbot.



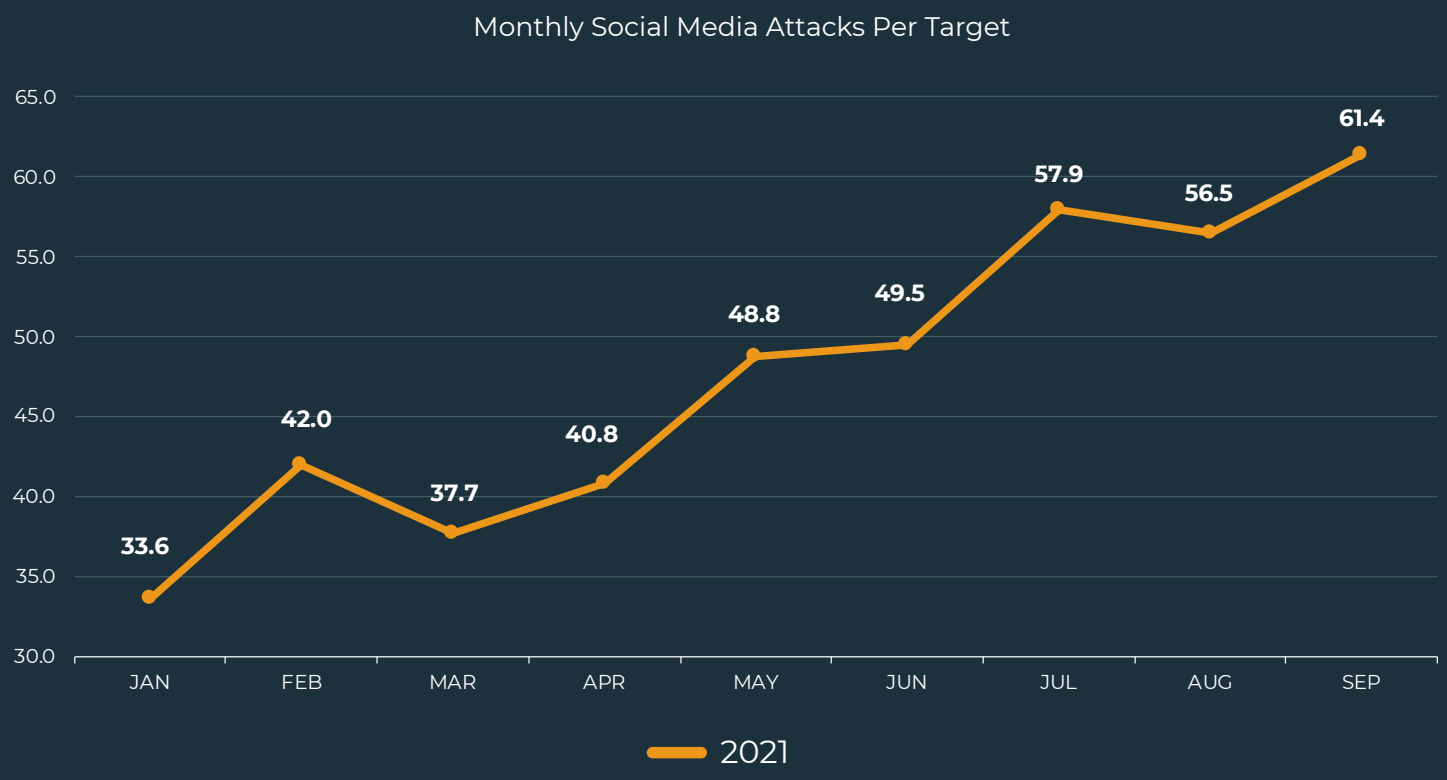
Payload Family	Q3	Q2	+/-
BazaLoader	24.7%	0.0%	-
Agent Tesla	14.3%	1.7%	+12.6%
Dridex	10.4%	1.3%	+9.1%
VBS Downloader	10.4%	0.0%	+10.4%
Qbot	7.8%	54.1%	-46.3%
Ursnif/Gozi	6.5%	3.5%	+3.0%
ZLoader	5.2%	9.5%	-4.3%
AsyncRAT	5.2%	5.2%	0.0%

SOCIAL MEDIA THREAT TRENDS

SOCIAL MEDIA THREATS ON THE RISE

In January, the average target organization experienced nearly 34 attacks through Social Media. As the year has progressed, this number has significantly increased. By September, the average target organization encountered 61 attacks per month, which is an 82% increase in three quarters. While the average represents a variety of enterprises and fluctuates higher or lower based on industry, it signifies an urgent need for security teams to more closely monitor and manage Social Media activity.

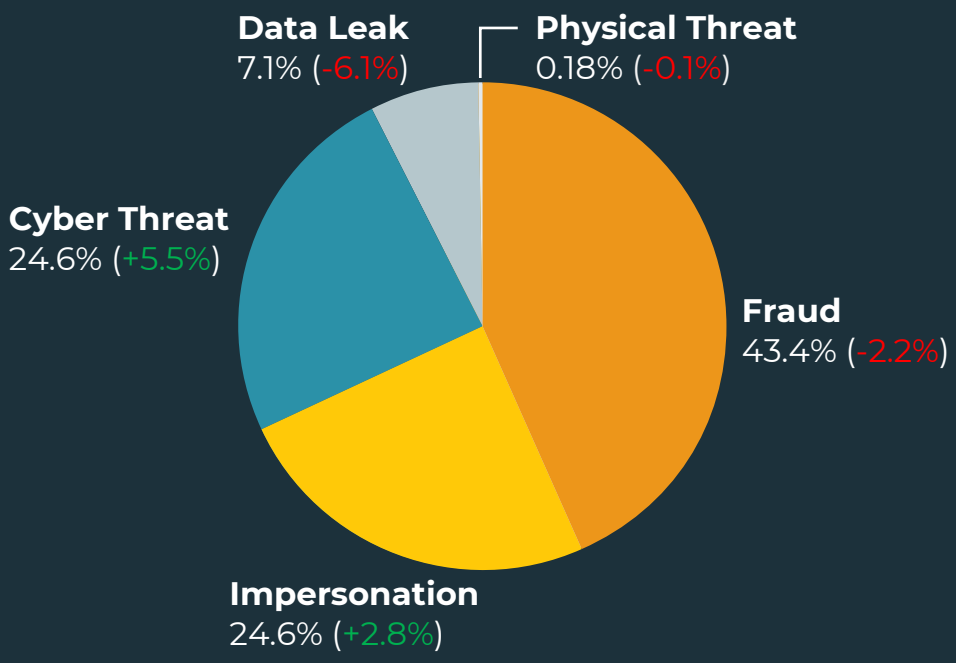
82% Increase in attacks JAN to SEP 2021.



TOP SOCIAL MEDIA THREATS

While the percentage of Fraud-related Social Media attacks leveled off in Q3 after a significant increase in Q2, the threat type continued to make up the lion's share of attacks. Cyber Threats experienced the largest increase among all threat types in Q3, growing 5.5% from Q2 and accounting for approximately one quarter of the threats encountered. Employee, Brand, and Executive Impersonations increased slightly as well, making up an additional quarter of the Social Media threats encountered.

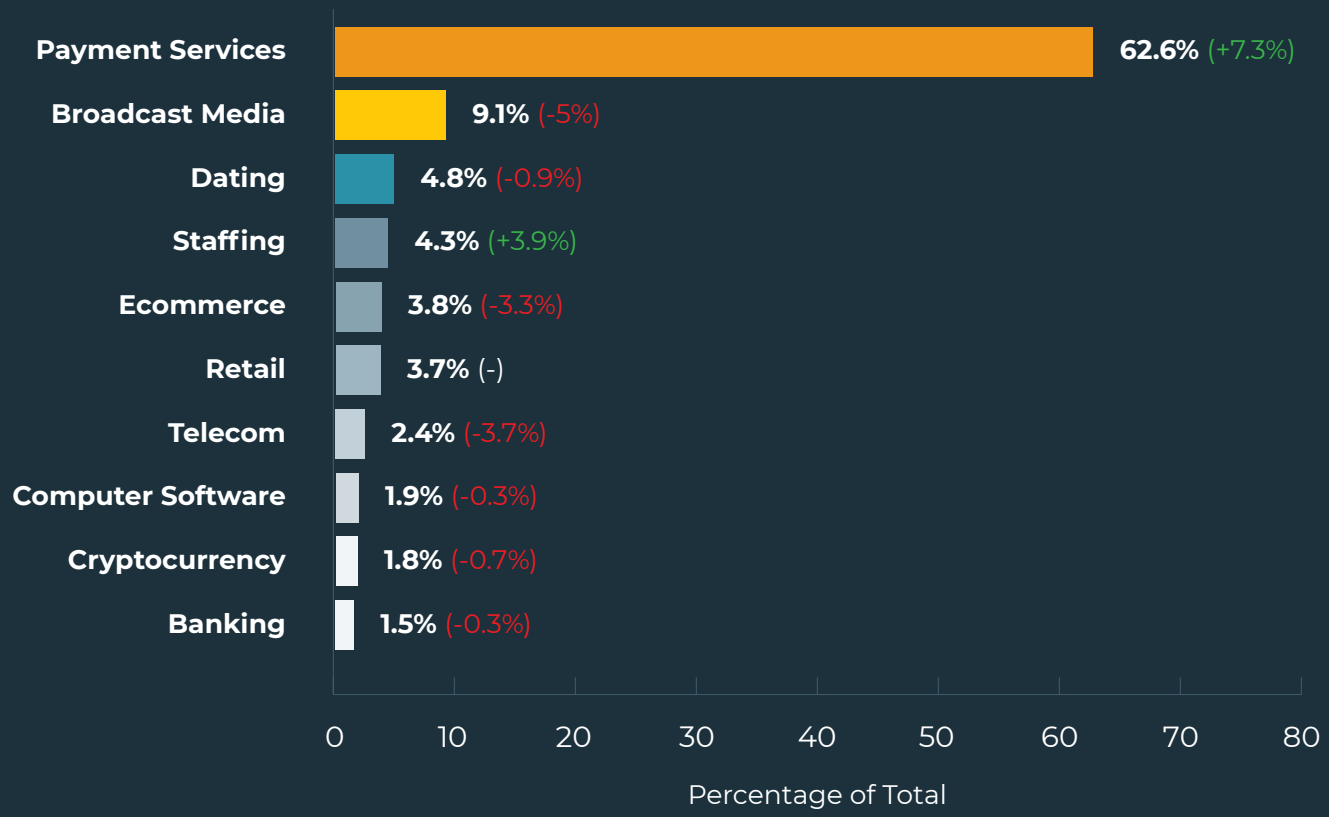
Fraud-related Social Media attacks were down slightly from Q2 but still accounted for most of the attacks encountered in Q3.



ATTACKS BY INDUSTRY

Payment Services was among the business sectors targeted most by Social Media attacks. This industry is a natural target for threat actors because their services are used broadly across several business sectors. Increasing 7.3% in share during Q3, it retained the top slot in Social Media attacks among all industries.

The Staffing and Recruiting sector experienced the steepest increase in attacks compared to Q2, moving from outside the Top 10 to the fourth most targeted. A portion of this increase is possibly due to seasonality and threat actors preying on job seekers during end-of-year recruiting.

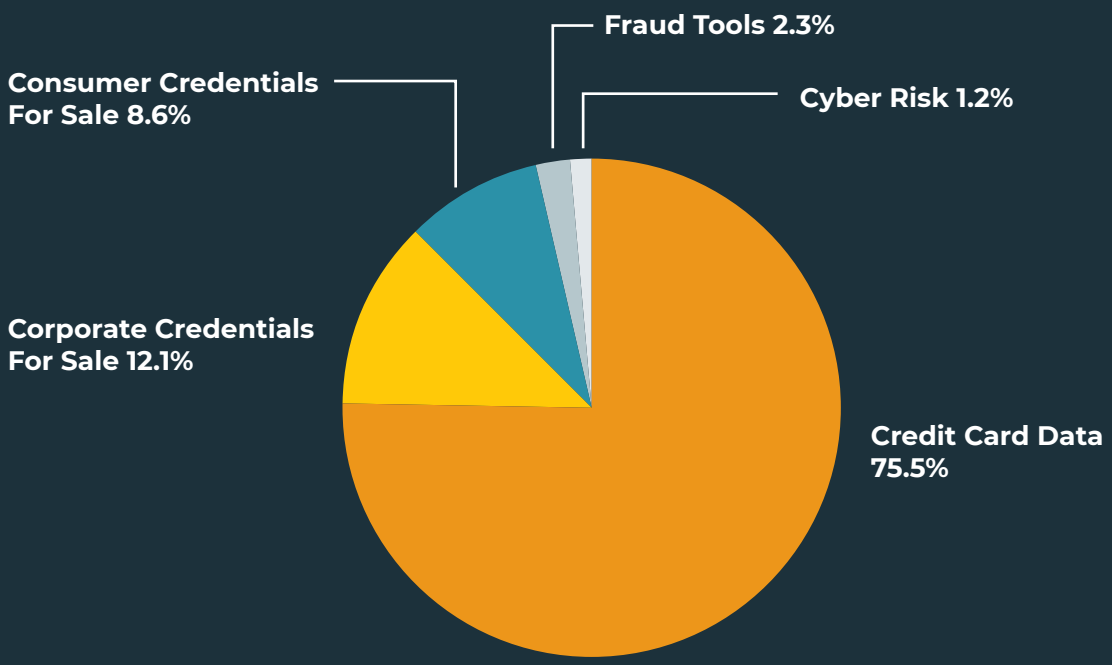


DARK WEB THREAT TRENDS

TOP DARK WEB THREATS

Threat actors marketing stolen credit and debit card data was the most common Dark Web threat observed in Q3, accounting for over 75% of Dark Web threats observed. The sale of Personally Identifiable Information (PII) accounted for 12% of Q3 threats and was primarily made up of threat actors marketing employee email addresses to black market buyers.

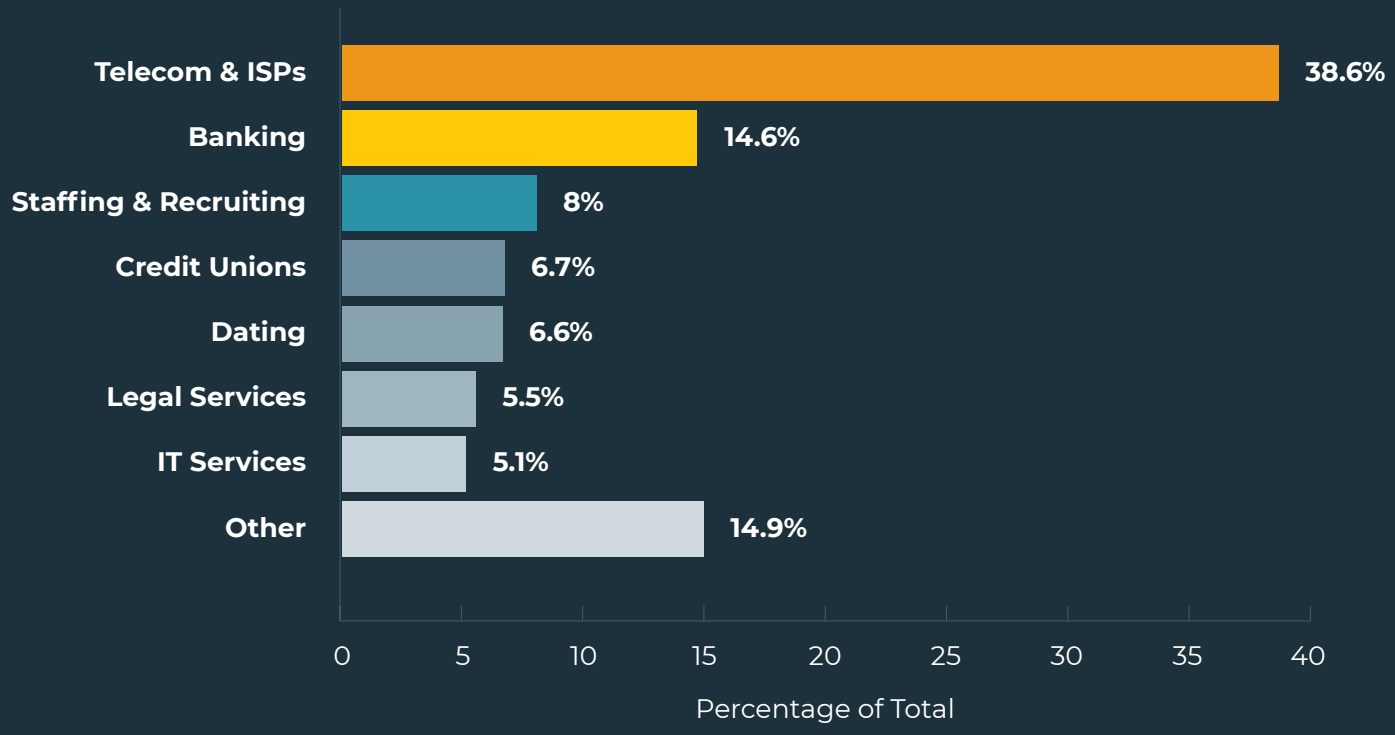
More than 75% of threats observed on the Dark Web are related to stolen credit and debit card data.



TOP TARGETED INDUSTRIES

Telecommunications & ISP data continued to be highly marketed on Dark Web sites. Threat actors who gain access to account data often have access not only to payment method data, but also login credentials and highly sensitive PII.

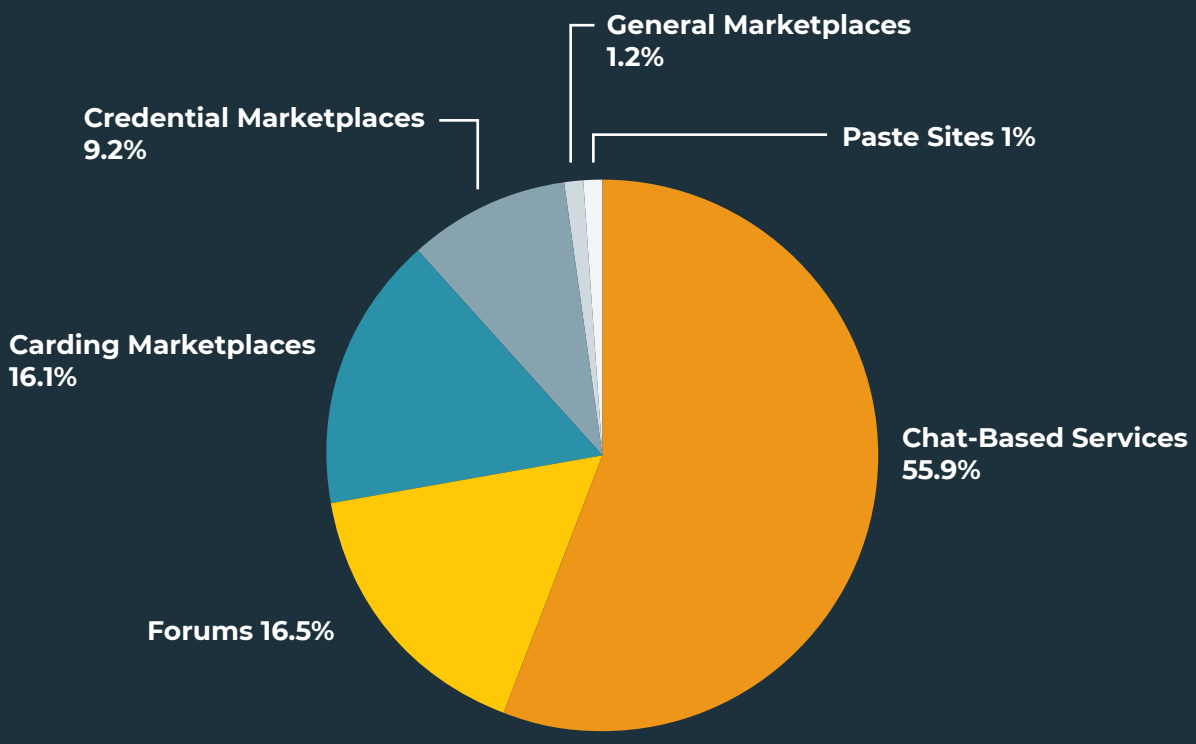
Other industries of note in Q3 include Staffing & Recruiting, which experienced the third highest average number of Dark Web threats during the quarter. This elevated ranking could be attributed to common increases in hiring activity during Q3 in preparation for the new year. Finally, Dark Web cases associated with Dating Services ranked fifth among all Dark Web threats observed in Q3. Dating Services have recently been targeted by threat actors trying to gain access to PII tied to online dating apps. These apps have experienced a surge in account activity due to the pandemic.



SITES WHERE DATA IS MARKETED

Stolen data is marketed through a broad spectrum of Dark Web sites, however, in Q3 nearly 56% of threats observed were marketed using Chat-Based Services. Most of this activity was the marketing and exchange of leaked credit and debit card information, as it is easy for this kind of data to be quickly and anonymously shared via chat. Forums experienced the second highest level of activity, accounting for 16.5% of threats. Carding Marketplaces came in third, contributing 16.1% of activity.

Chat-Based Services prove their popularity with threat actors, making up nearly 56% of Q3 Dark Web threat volume.



SUMMARY & CONCLUSION

More than ever, it is evident that threat actors are relying on a variety of attack vectors to steal from consumers and disrupt enterprises.

Phishing remains a dominant attack method. Attacks are up nearly 32% from last year, with a significant spike in September more than doubling the same month in 2020. Threat actors are experimenting with new methods of phishing, but email remains the most widely used vector for distributing lures.

The average number of Social Media attacks per target has also climbed steadily throughout 2021, increasing 82% since January. Threat actors target enterprises on Social Media through Impersonation, Fraud, sharing Data Leaks, and other Cyber Threats.

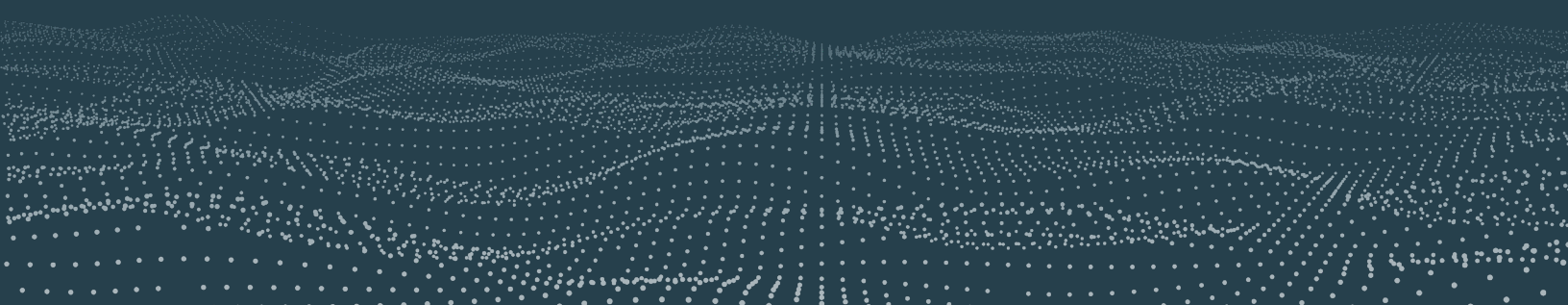
Office 365 credentials continue to remain highly valued by threat actors in Q3 due to the extensive access they provide to enterprise infrastructures. The count and percentage of O365 phish increased for the fourth consecutive quarter, making up 51.6% of Credential Theft phishing attacks reported by corporate users.

The ransomware ecosystem remained volatile in Q3, as shifts in the usage of malware payloads providing access to end users fluctuated. BazaLoader was the tool of choice in Q3, however the emergence of new variants raises doubts on which payload will be utilized most in Q4.

Once again, Credential Theft phishing and Response-Based attacks posed the greatest risk for corporate email users. Combined, the two accounted for over 96% of the email threats reaching user inboxes. Most notably, Vishing threats continued to evolve in complexity and more than doubled in number for the second consecutive quarter, suggesting a shift in Response-Based threat strategies.

Strategically, it is clear that digital transformation continues to create opportunities for threat actors to exploit. While new technologies and communication channels move us all forward, they are also abused to carry out attacks and commit fraud. With proactive intelligence across digital channels and robust mitigation capabilities, enterprises can minimize the financial and reputation impact of these threats.

This page intentionally left blank.



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