COFENSE
EMAIL SECURITY

CATCH MORE PHISH

Q1 2024 | Phishing Intelligence Trends Review

COFENSE
EMAIL SECURITY

Contents

Executive Summary:

Q1 2024 saw a significant increase in emails delivering common malware that is easily accessible to threat actors and is typically cheap or free. Cofense Intelligence implemented several improvements to enhance our tools and detection capabilities this quarter, which also contributed to the increase in volume and quality of identified malicious events. Beyond the increase in email volume for common malware, Cofense Intelligence saw an increase in active threat reports (ATRs) covering small, time-bound, advanced campaigns delivering malware. This was reported on in our Strategic Analysis and Flash Alert during the quarter. Despite the continued absence of QakBot and Emotet, no single malware has taken up the gap left behind. Advanced malware such as DarkGate and PikaBot have done their best, but the gap left by Emotet and QakBot has not been filled and reporting levels reflect this. Q1 2024 also saw an overall slight decrease in credential phishing ATRs.

The Key Highlights for Q1 2024 Include:

- **ATRs related to taxes saw a 314% increase and benefits-themed ATRs saw a 644% increase.**
- Due to new tooling, common malware-related emails have increased by anywhere from 300% (FormBook) to **1318% (Agent Tesla Keylogger)**.
- Web3-related service cloudflare-ipfs[.]com saw a 423% increase in usage from Q4 2023 indicating that Web3 services being used for credential phishing may be making a comeback.
- The most popular RAT from Q4 2023, Remcos RAT, was replaced in Q1 2024 by STR RAT with almost 403% more emails.
- PDF files continue to make up approximately 60% of all file attachments in phishing emails successfully reaching enterprise users. PDFs are used in both credential phishing and moderate to advanced malware campaigns.
- The PikaBot loader saw a 40% decrease in volume, whereas DarkGate saw a 368% increase. This shows a favoritism between the two malware families that were believed to be incorporated by operators looking to find a replacement for the notorious QakBot.

Credential Phishing Activity

Credential phishing emails went down by around 13% from Q4 2023 to Q1 2024. However, Q1 2024 saw an overall 43% decrease in credential phishing emails when compared to Q1 2023. This indicates that while Q1 2024 was more or less in line with the prior quarter, it in fact saw a significant decrease compared to what would normally be expected for this time of year. This may be due to an increase in complex but low-volume credential phishing campaigns, much like the increase in complex but low-volume malware campaigns covered in this quarter's strategic analyses.

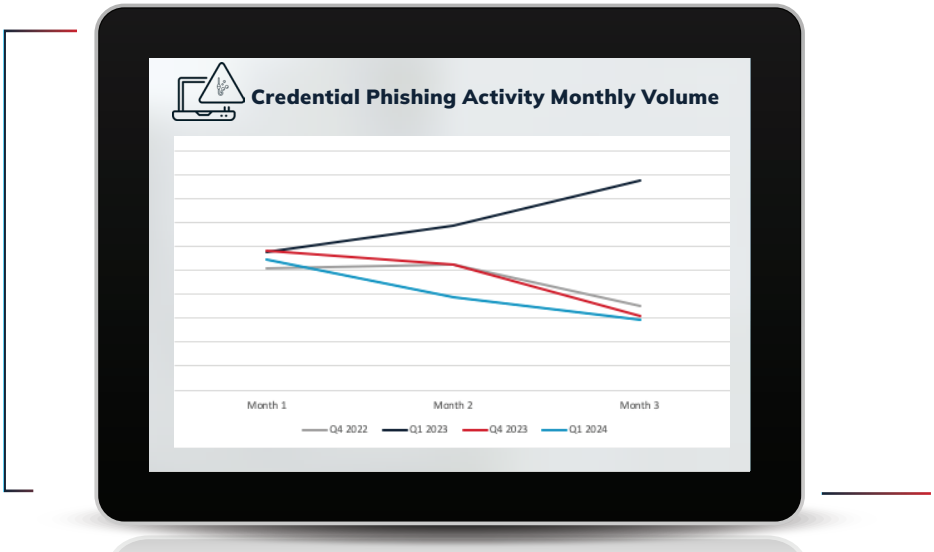


Figure 1: Comparison of monthly volume of credential phishing emails observed in Q4 and Q1 during 2022, 2023, and 2024.

Figure 2: Comparison of weekly volume of credential phishing emails observed in Q4 2023 and Q1 2024.

Prevalent Malware in Q1 2024

Improvements to our tooling in early February provided greater-than-ever volume of emails associated with reports, specifically of reports delivering common malware such as Agent Tesla Keylogger, STR RAT, Remcos RAT, Snake Keylogger, and FormBook.

These improvements led to an increase in common malware reports but, more notably, to better association of email volume with given reports.

Table 1: Top five malware types with the top family of each type in Q1 2024.

TOP 05 Malware Types	TOP FAMILY Family in Type
Keylogger	Agent Tesla Keylogger
RAT	STR RAT
Information Stealer	FormBook
Loader	PikaBot
Other	Reconnaissance Tool

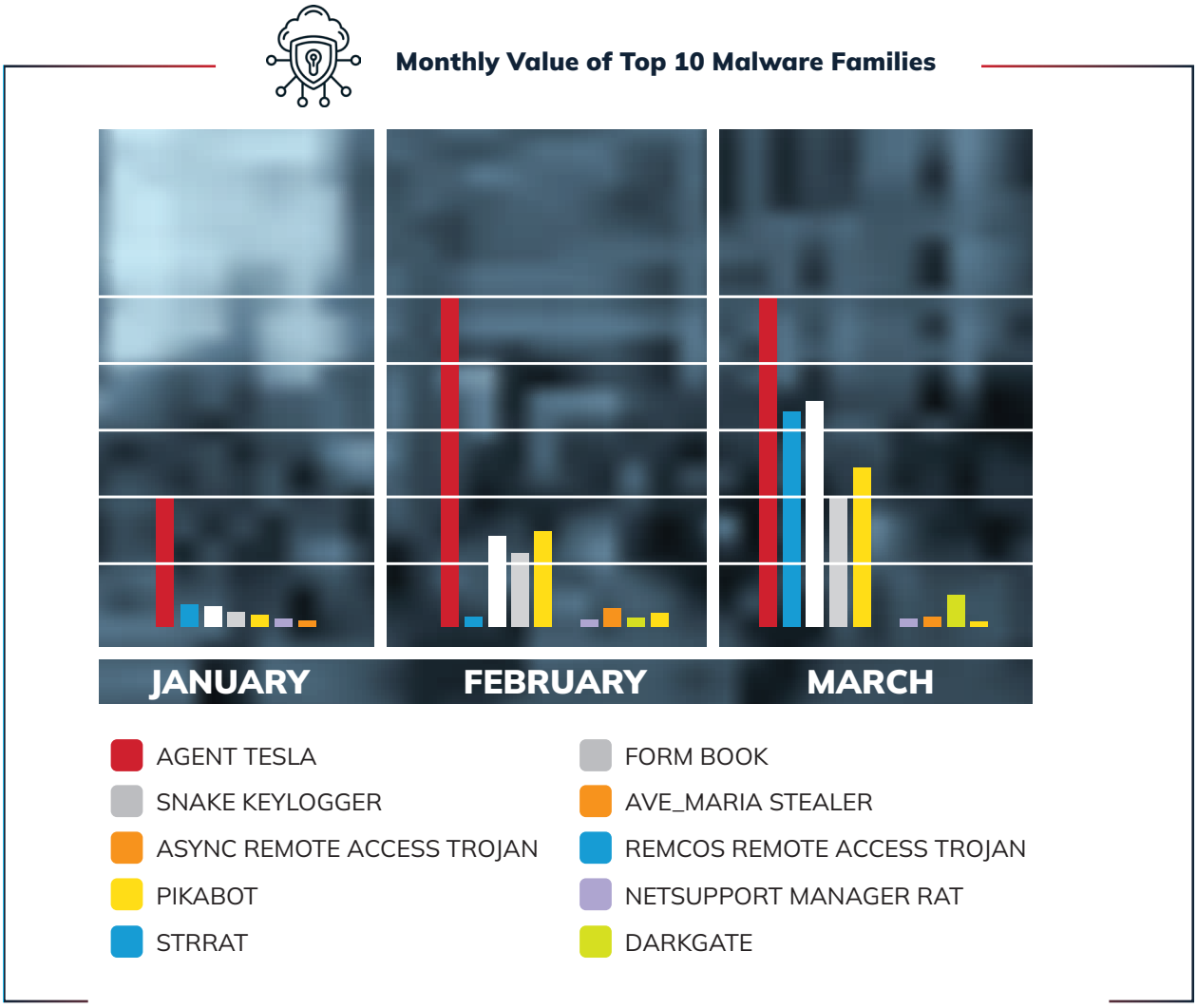


Figure 3: Monthly volume of top ten malware families of each type in Q1 2024. Agent Tesla Keylogger is truncated at 1/5th of total value for Feb and Mar so that differences in the other families can be seen.

Agent Tesla Keylogger continued to be the most popular malware family by far with email counts increasing by 1318%, leading to Keyloggers being the most popular malware type. Information Stealers have typically been in first or second place, however, this time RATs, led by STR RAT, took second place. This is a surprise since STR RAT volume is usually overshadowed by more popular RATs due to a successful STR RAT infection requiring Java to be installed on the target's machines. Information Stealers, led by FormBook, were the only malware type and family that saw about the same number of emails in Q1 2024 as compared to Q4 2023. The Loader malware type, which has been primarily made up of PikaBot in both Q4 2023 and Q1 2024, managed to take 4th place followed by the "Other Malware" type which was primarily composed of Reconnaissance Tools in Q1 2024. The Banker malware type, which has been on the decline for some time, did not even make the top 5.

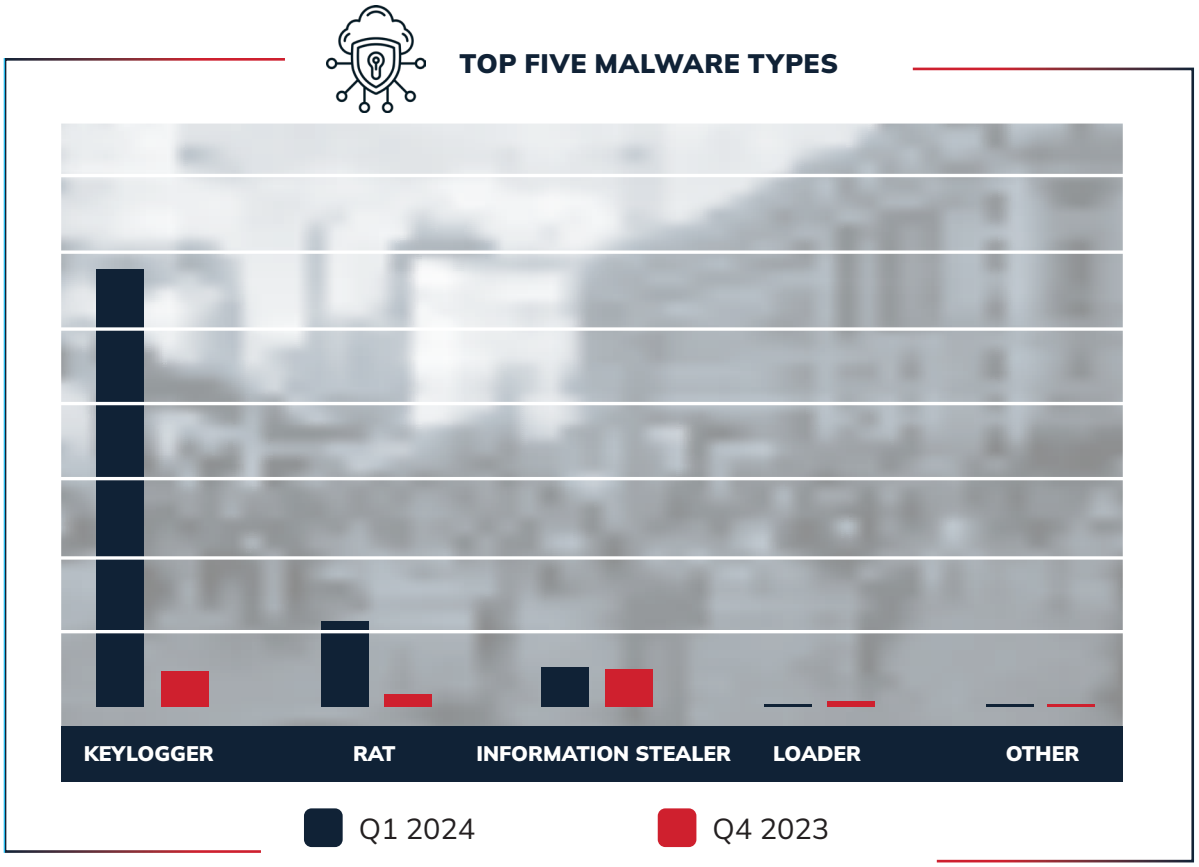


Figure 4: Top five malware types in Q4 2023 and Q1 2024 by volume of emails.

Delivery Mechanism Rundown

The well-known **CVE-2017-11882** which has been plaguing enterprises for years and has been the most popular delivery mechanism for some time, continued to be the most popular by a fair margin in Q1 2024. DotNETLoaders, which led the next closest ranking by another significant margin, actually went up in the rankings. In Q4 2023, they trailed 2nd place by only 6%, but in Q1 2024 they were in 2nd place and trailed 1st place by 16%. This significant increase is due to the fact that they were largely used to deliver Agent Tesla Keylogger and other common malware families that were impacted by improved Cofense Intelligence tooling. The 3rd and 5th place delivery mechanisms remained consistent with Q4 2023, but Office Documents replaced JSDroppers. This meteoric increase in Office Documents (657% from Q4 2023) is due to the usage of Office Documents to deliver the popular DarkGate RAT.

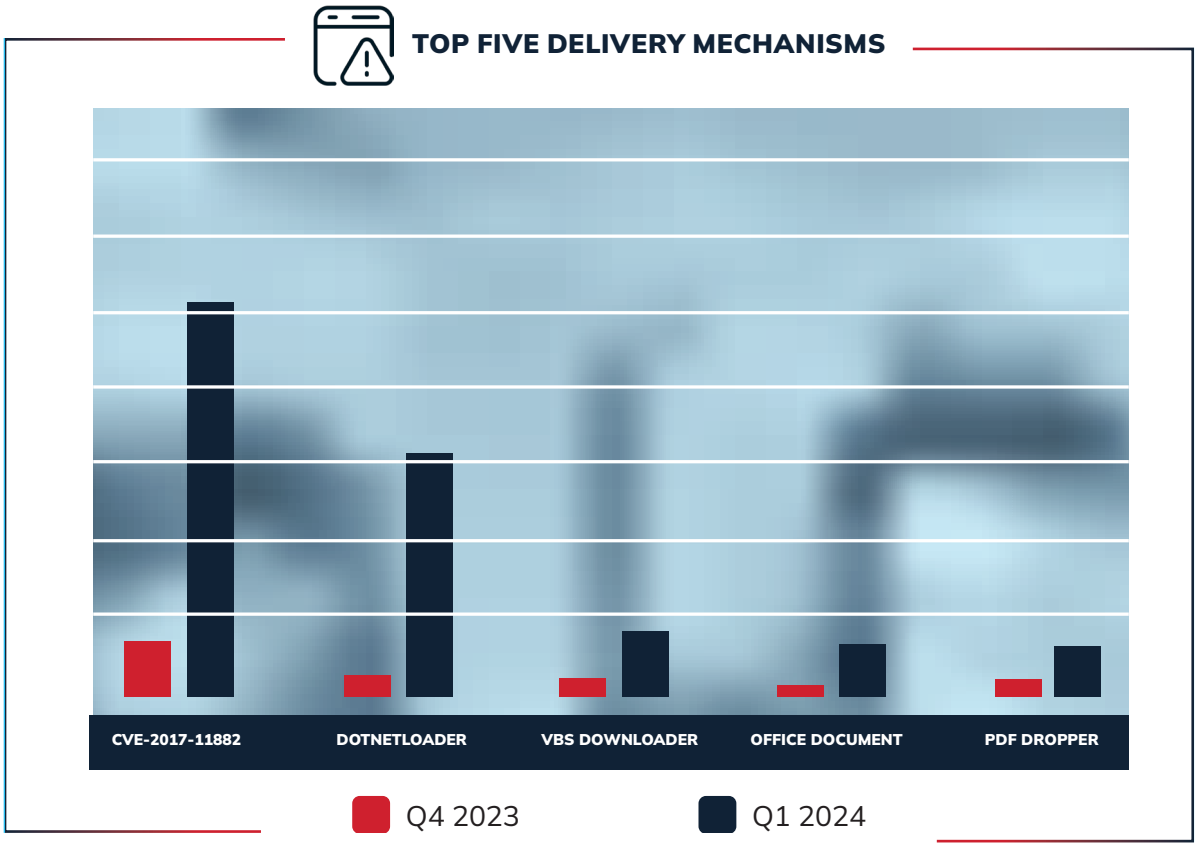


Figure 5: Top five malware delivery mechanisms by email volume in Q1 2024, with Q4 2023 totals for comparison.

The CVE-2017-11882 exploit has always been a popular delivery mechanism seen by Cofense. The pie chart in Figure 6 shows the top malware families delivered via CVE-2017-11882. Agent Tesla Keylogger continues to be the most common; however, Remcos RAT took the place of FormBook as the next most commonly delivered payload. The last place, currently belonging to NanoCore RAT, frequently changes and is indicative of the currently trending free RAT among threat actors.

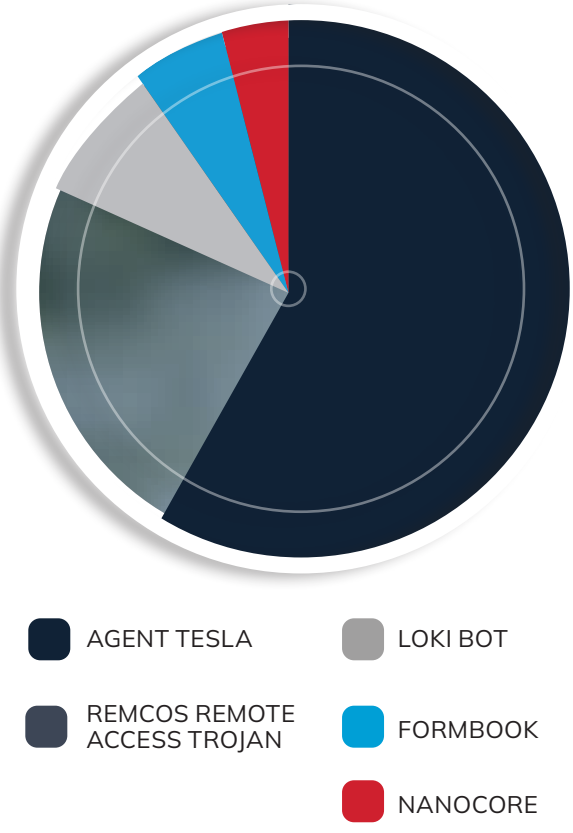


Figure 6: Top five malware families delivered by CVE-2017-11882 in Q1 2024

Domains and TLDs Used in Credential Phishing

Each quarter, Cofense Intelligence analyzes credential phishing emails that reached users in environments protected by secure email gateways (SEGs). We identify the individual domain names and top-level domains (TLDs) that were most prominent. Stage 1 URLs are embedded in the phishing email itself, while Stage 2 URLs are used as redirects or embedded in credential phishing websites. The ten most common .com domains used in both stages combined are represented in Table 2. Of the domains, several trusted cloud platforms can be identified, showing continued abuse by credential phishing threat actors.

RANK	Q4 2023	Q1 2024
1	Google	Cloudfare-ipfs
2	Bing	Adobe
3	Adobe	Google
4	DropBox	Linode Objects
5	Linode Objects	Sharepoint
6	Dynamics	Beehiiv
7	Microsoft	DropBox
8	Mycloud	Dynamics
9	Baidu	Microsoft
10	Box	Myqcloud

Table 2: Q1 2024 and Q4 2023 ten most common .com domains used in credential phishing campaigns.

The majority of credential phishing threat actors use .com domains in their campaigns. During Q1 2024, threat actors changed only a small portion of the most commonly abused .com domains. Several of the sites on the list during Q1 2024, including Google, Beehiiv, and Linodeobjects, contain an open redirect which has been heavily abused by threat actors during this quarter and previous quarters. **One surprising site on the Q1 2024 list is cloudflare-ipfs which typically uses a number of anti-analysis techniques and a specialized hosting system that makes takedowns difficult.**

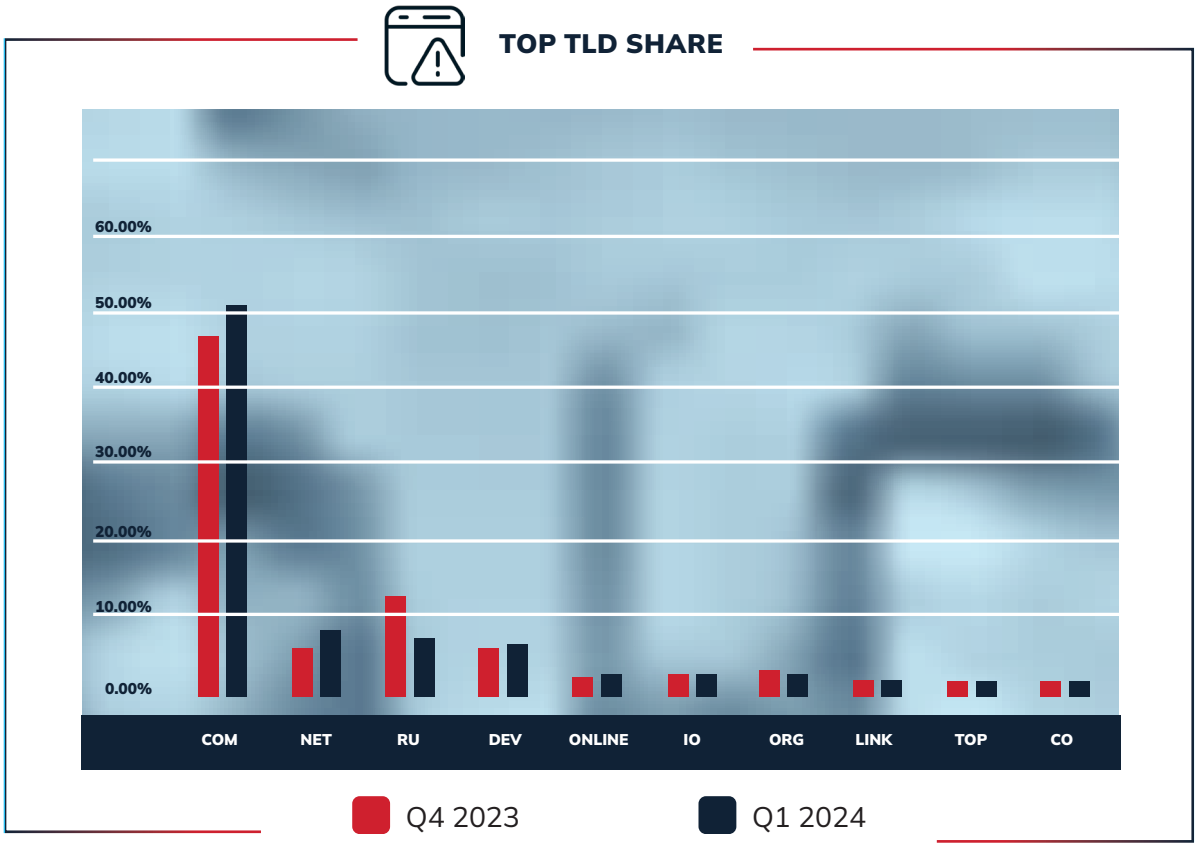


Figure 7: The top ten TLDs for both stages in Q1 2024, with Q4 2023 totals for comparison.

Between Q4 2023 and Q1 of 2024, all but one TLD remained primarily the same. The only noticeable differences between the quarters would be slight changes in the numbers of the top 5 TLDs and the replacement of the 9th place .com.br in Q4 2023 with .top in Q1 2024.

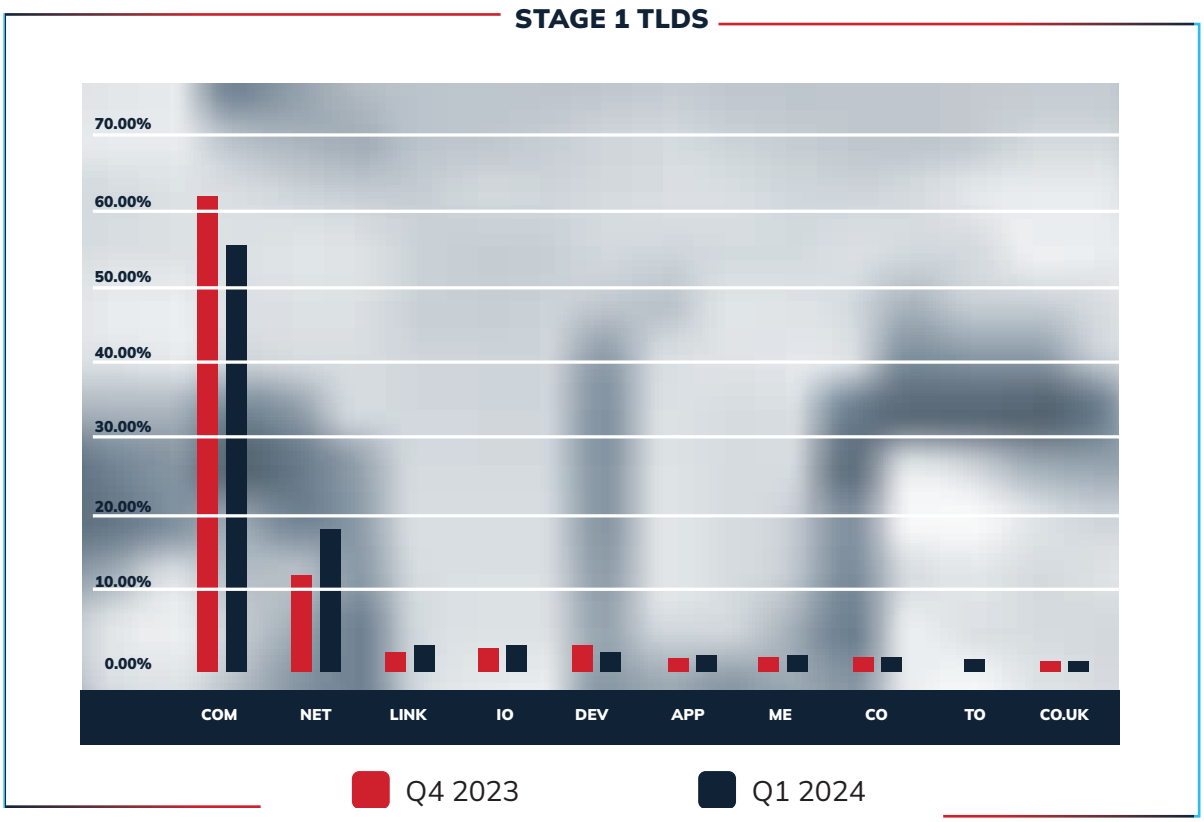
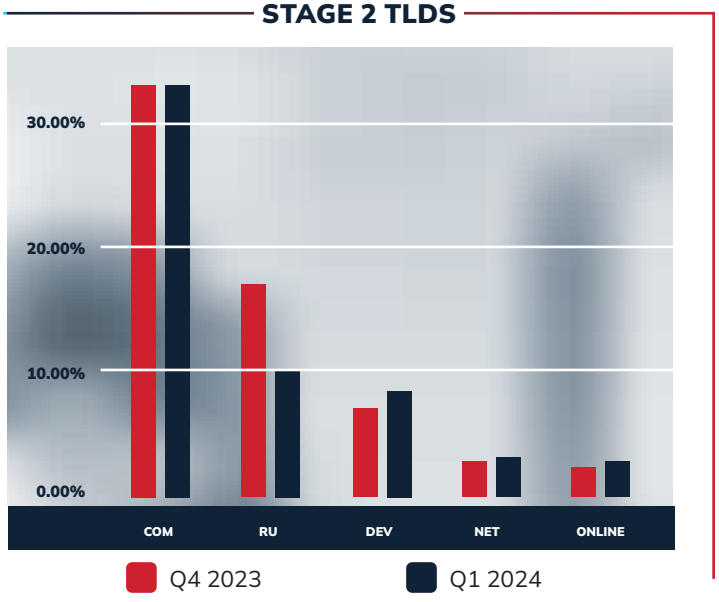


Figure 8: The top ten STAGE 1 TLDS in Q1 2024, with Q4 2023 totals for comparison.

Q1 2024 saw a slight decrease in the prevalence of the .com TLD amongst stage 1 TLDs. This was offset by an increase in the usage of the .net TLD. The .ru, .org, and .com.br TLDs from Q4 2023 were replaced by .app, .to, and .co.uk in Q1 2024. The .app TLD was heavily featured in campaigns spoofing Meta and the .co.uk TLD was often seen as part of google[.]co[.]uk embedded URLs that redirected to credential phishing pages.



TLDs used in Stage 2 were mostly consistent with the last quarter save for differences in volumes of the 1st and 2nd place. Although the .com TLD was used less in Stage 1, it was used more frequently enough in Stage 2 that it was still overall more common in both stages in Q1 2024 than in Q4 2023. The .io and .com.br TLDs from Q4 2023 were replaced by .site and .xyz in Q1 2024. Both the .site and .xyz TLD were used largely in campaigns spoofing Microsoft.

Figure 9: The top ten STAGE 2 TLDS in Q1 2024, with Q4 2023 totals for comparison.

File Extensions of Attachments

PDFs were once again the most commonly seen file extension on email attachments that bypassed SEGs. PDFs can be used in many different ways but are most often used to provide credential phishing via either embedded links or embedded QR codes, which are becoming more popular. The HTM(L) file extensions continued to maintain their 2nd and 3rd place positions. RTF files made a surprising comeback after not even being present for Q4 2023. RTF files are frequently used with CVE-2017-11882 but are also often used as fake "award notification" or "law enforcement warnings" to initiate scams. The .ics files are typically used to initiate fake meetings designed to scam the recipient and the other file extensions can be used for a multitude of purposes including delivering credential phishing or malware.

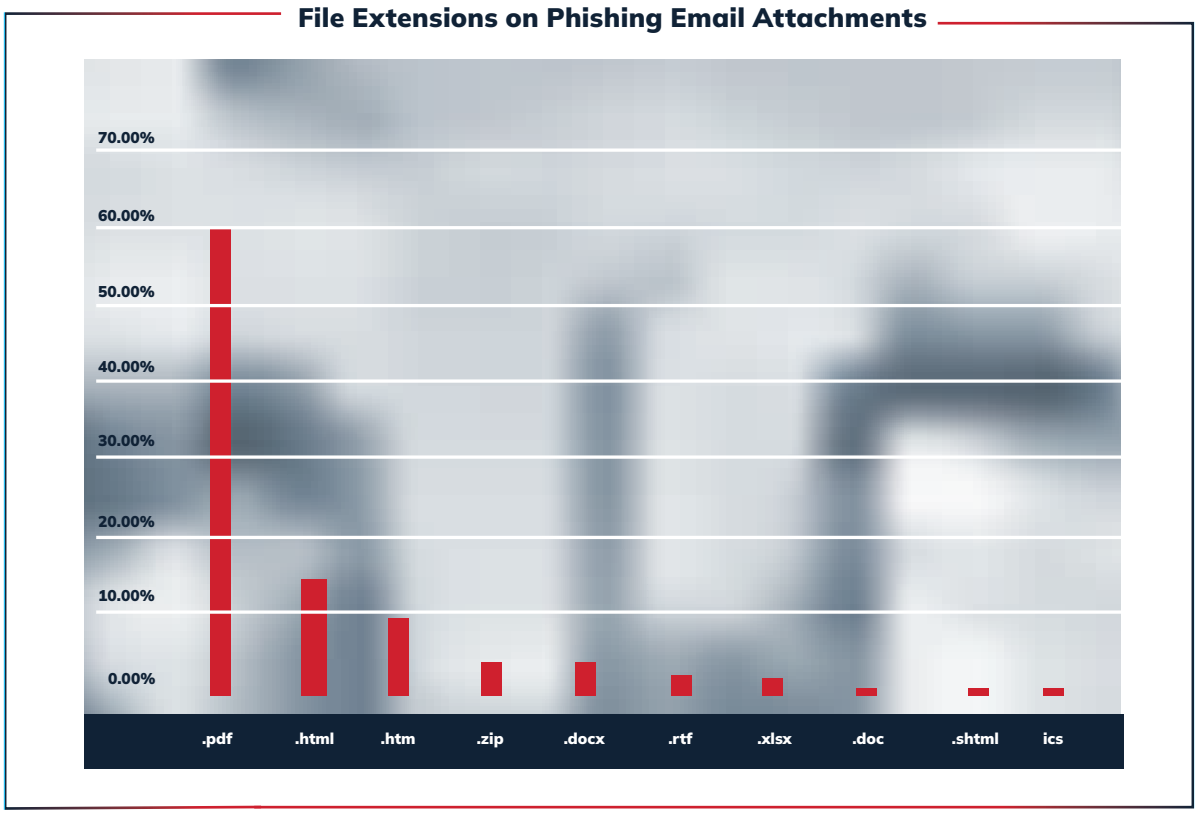


Figure 10: Top 10 most common attachment file extensions found in environments protected by SEGs in Q1 2024.

Command and Control Server Locations

Tracking Command and Control (C2) servers provides insight into a range of malicious cyber activities across the globe. These C2 nodes can deliver phishing campaigns or command malware, often receiving information and exfiltrated data from infected hosts. There were a few only minor differences between Q4 2023 and Q1 2024. Hong Kong was replaced by Bulgaria while the 2nd through 5th place countries all had lower percentages in Q1 2024 than in Q4 2023. To balance this out, the United States had a higher share of the C2 locations. Potentially due to the number of proxy services located in it, the United States continues to be the most popular C2 location.

Note: these statistics do not directly correlate with the full range of infrastructure threat actors use and they should only be interpreted as C2 locations, rather than where operations originate.

Q4 2023		Q1 2024	
COUNTRY	PERCENTAGE	COUNTRY	PERCENTAGE
UNITED STATES	71.63 %	UNITED STATES	75.27 %
GERMANY	5.76 %	GERMANY	4.59 %
RUSSIA	1.78%	RUSSIA	1.45 %
HONG KONG	1.69 %	CANADA	1.45 %
CANADA	1.56 %	BULGARIA	1.33 %

Figure 11: Q1 2024 and Q4 2023 percentages for C2 sources by IP address geolocation.

Projections for Q2 2024 and Beyond

SMALL TIME-BOUND ADVANCED CAMPAIGNS WILL BE MORE COMMON

Several important but small-scale and highly targeted campaigns were covered this quarter including Rhadamanthys Stealer, SVG files, and an advanced NetSupport RAT campaign. These campaigns are indicative of the fact that threat actors seem to be more frequently using small time-bound but advanced campaigns to deliver malware.

LAW ENFORCEMENT TAKEDOWNS MAY LEAD TO MORE DIVERSE RANSOMWARE DELIVERY

The increase in law enforcement takedowns of "large players" could lead to a more diverse threat landscape, specifically with ransomware delivery. The most recent takedown of the LockBit RaaS, in addition to last year's takedown of QakBot, is sure to have an impact on the threat landscape as we currently know it. As a result, threat actors will likely seek to employ new methods of ransomware delivery and new types of malware loaders in their campaigns.

DotNET Loader Payload Location
hxxps://heygirlisheeverythingyouwantedinanaman[.].com/get/65d35993z42e8c15ce8175af
DotNET Loader Payload Location
hxxps://artemis-rat[.]com/get/65eef7bdc904

Figure 12: Proxy services used by DotNET Loaders to disguise payload locations.

These services will be used as a proxy to download the actual malicious payload. Based on our analysis of delivery mechanisms, it may lead to less detections than directly downloading the payload. This trend has rapidly grown in Q1 2024 and is expected to continue growing in the future.

WEB3 CREDENTIAL PHISHING WILL MAKE A COMEBACK

Web3 services being used for credential phishing, led by cloudflare-ipfs[.]com, made a comeback (423% increase) this quarter. Other Web3 services like cf-ipfs[.]com and chainsafe[.]io also saw

FINISHED INTELLIGENCE: TOPICS AND TRENDS

Strategic Analysis - Shipping-Themed Emails Not Just for The Holidays

The importance of fast and efficient shipping solutions has increased for households and businesses. This is especially true during the holiday season when demand for shipping services is high. Cofense Intelligence asked whether malicious shipping-themed emails increased during the holiday season. This sparked a three-year trend analysis from 2021 to 2023 that targeted several industries. While it might seem logical that the number of malicious emails related to shipping would increase during this time, the trend analysis suggests that the increase in malicious email volume only increases slightly during the holiday season. It also indicates that malicious shipping-themed email volumes significantly threaten several industries all year round as volume trends tend to be consistent, with higher volumes in June, October, and November and the lowest in April.

Strategic Analysis - Most Common Phishing Email Themes of 2023

Each phishing campaign that Cofense Intelligence analyzes is given a title which includes a theme. This theme is important because it characterizes the campaign and provides insight into the threat actor's intentions. Knowing that a phishing email targeting the hospitality industry has a travel assistance theme, rather than a generic finance theme, is significant as it enables a more focused response. It also assists companies in better selecting relevant phishing simulations to use on their employees. This report covered some of the more common themes, what they are composed of, and what trends Cofense Intelligence was able to observe with them. The key points we found were that the highest variation of themes occurred in Q3 and Q4 of 2023. Benefits-themed emails were most common in Q1 and Q4 of 2023. Fax- and document-themed emails were most common in Q1 of 2023. Legal-themed emails were most common in Q3 and Q4 of 2023. Tax- and notification-themed emails were most common in Q3 of 2023. Closing (as in closing on a property)-themed emails were most common in Q1 and Q3 of 2023.

Strategic Analysis - ThreatHQ Cofense's Interactive Threat Hunting Platform

Cofense Intelligence provides a unique and interactive platform for users to search through threat reports and aid in their research known as ThreatHQ. In this report, we dove into a basic overview of what ThreatHQ is and the features it provides, while also taking a closer look at how Cofense analysts use the platform for research, as well as threat hunting. ThreatHQ is a hub for an endless amount of ATRs, which are Intelligence reports that contain actionable intelligence on the threats that matter, especially those that have proven to successfully bypass SEGs. It also holds access to Cofense Intelligence Finished Intelligence reports which are strategic and analytical looks into developing threats, malware changes, and new or evolving tactics, techniques, and procedures (TTPs).

Strategic Analysis - Car Insurance Emails Drives for NetSupport RAT Infection

A relatively small malicious car insurance/financial-themed email campaign landed in inboxes in late January 2024. These basic malicious emails promised the user a large financial sum via an invitation to click the embedded marketing or Google Ad link. This link led to what was likely a compromised website, where the victim could download instructions to claim their lump sum of money. The website delivered a JavaScript file that infected the victim's Windows machine with a modified version of the legitimate software known as NetSupport RAT to gain unauthorized remote access to the user's machine.

Flash Alert - New MaaS InfoStealer Malware Campaign Targeting Oil & Gas Sector

This Flash Alert covered an emerging advanced campaign that successfully reached intended targets in the oil and gas industry. The campaign delivered an uncommon, but advanced, Malware-as-a-Service (MaaS) information stealer, the Rhadamanthys Stealer. Based on a report by Cyberint published on January 22nd, the malware family recently received a major update on the black market which could be the reason we saw such an unfamiliar family appear in such an advanced campaign. When the report was released, there was a high volume of phishing emails that employed several TTPs known to assist in bypassing SEGs to deliver the malware.

Strategic Analysis - SVG Files Abused in Emerging Campaigns

Scalable Vector Graphic files, or SVG files, are image files that have become an advanced tactic for malware delivery that has greatly evolved over time. The use of SVG files to deliver malware was made even easier when the tool AutoSmuggle, a program used to deliver malicious files embedded in HTML or SVG content, was released in May 2022. Threat actors have recently started to extensively exploit AutoSmuggle in 2 unique campaigns starting in December 2023 and January 2024.

Strategic Analysis - Recently Updated Rhadamanthys Stealer Delivered in Federal Bureau of Transportation Campaign

On February 21, 2024, Cofense Intelligence identified an advanced phishing campaign that targeted the oil and gas sector to deliver Rhadamanthys Stealer, an advanced information stealer offered as MaaS. The campaign incorporated several complex TTPs along with a unique vehicle incident lure that spoofs the Federal Bureau of Transportation. This campaign followed closely behind several updates to the Rhadamanthys MaaS on the market, and law enforcement's takedown of the LockBit ransomware group, one of the most notorious Ransomware-as-a-Service on the market. Due to the uniqueness of the campaign and success rate at which emails were reaching targets, a Cofense Intelligence Flash Alert, "New MaaS InfoStealer Malware Campaign Targeting Oil & Gas Sector," was published.