PHISHME
COFENSE
EMAIL SECURITY

# CATCH MORE PHISH

## Q3 2024 | Phishing Intelligence Trends Review

PHISHME
COFENSE
EMAIL SECURITY

# Contents

# Executive Summary:

In Q3 2024, Cofense Intelligence continued to focus on threats that made it to inboxes bypassing secure email gateways (SEGs) and saw the continued decline of keyloggers in favor of remote access trojans (RATs) that excelled at bypassing SEGs. RATs have been a popular choice for some time due to their widespread availability and generally low bar to entry for most threat actors, compounded by their largely low cost to operate. RATs also typically have most of the functions of the other malware families such as keylogging and credential theft either built in or available via a plugin, making them more of a toolkit rather than a stand-alone tool.

Following the RAT malware type's volume increase of 68% in Q2, RATs saw another 7-fold increase in comparative share of emails in Q3 2024. While RATs saw a significant increase, overall volumes of malware decreased from Q2. This is likely a continuation of the effect of multiple international law enforcement takedowns that removed large amounts of command-and-control infrastructure. Threat actors tend to become more wary and try to fly under-the-radar when takedowns are performed and the operations carried out in Q2 were particularly effective.

Analysis of exploitative files showed that Office documents, especially .docx attachments, increased dramatically in Q3 as threat actors increased their usage of QR codes embedded in attached documents. The credential phishing resulting from the QR codes and indeed the credential phishing threat landscape as a whole saw some changes as threat actors focused on exploiting effective methods of bypassing SEGs. The biggest notable change was that threat actors began using TikTok as an open redirect to credential phishing pages. Combined with open redirects using Google AMP, there was a significant increase in credential phishing using open redirects. There were also changes to the TLDs used for data exfiltration in credential phishing campaigns.

## The key trends for Q3 2024 include:

- TikTok became a major .com TLD used in credential phishing.
- Open redirect usage (such as TikTok and Google AMP) increased by 627%.
- Office documents became almost 600% more common.
    - These typically deliver credential phishing by either embedded links or QR codes (which increased by 67%).
- RATs increased their share of emails by 59%.
- Shipping themes decreased by 96%.
- Benefits-, legal-, and voicemail-themed campaigns increased slightly, while all others saw significant decreases.
- Campaigns using steganography decreased by 75%.
- Usage of the .ru and .su TLDs for data exfiltration on credential phishing pages increased significantly.

## Credential Phishing Activity

As seen in Figures 1 and 2, credential phishing activity in Q3 2024 decreased significantly from Q2 2024. This is in direct opposition to previous trends that saw credential phishing volume increase from Q2 to Q3. Although overall volumes were lower, it is likely that smaller-scale, more-advanced campaigns, such as the ones using SEG-encoded URLs to bypass SEGs, replaced the high-volume but typically less effective at SEG-bypass campaigns seen previously. In Figure 2, the final weeks of Q3 2024 can be seen almost doubling in volume. This is a common trend as threat actor activity typically increases going into the Q4 holidays but decreases during the holidays themselves.

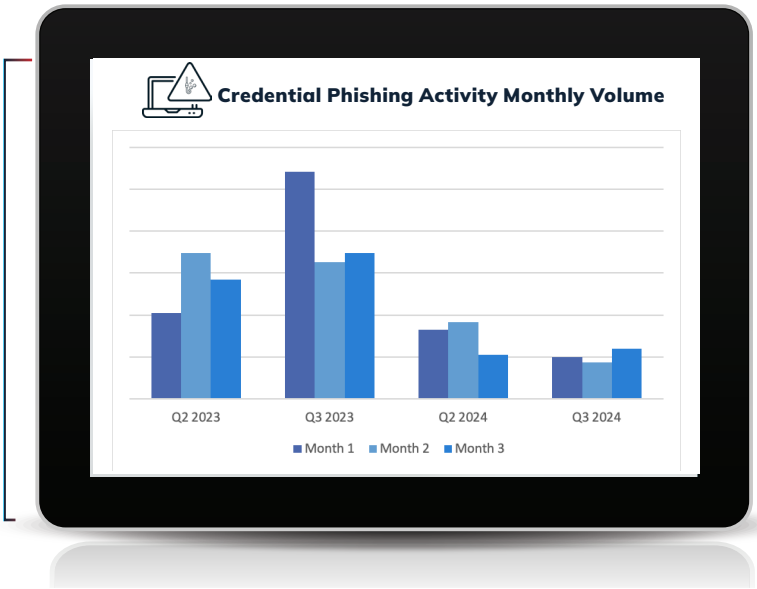


*Figure 1: Comparison of monthly volume of credential phishing emails observed in Q2 and Q3 during 2023 and 2024.*


*Figure 2: Comparison of weekly volume of credential phishing emails observed in Q2 2024 and Q3 2024.*

## Prevalent Malware in Q2 2024

Q3 saw the same lack of large-scale advanced botnets that Q2 did. Even DarkGate, which attempted to fill the void left by Emotet, Qakbot, and PikaBot in Q2, was absent. Instead, Q3 saw a high number of campaigns delivering Remcos RAT. Cryptocurrency miners returned from an extended hiatus caused by the fact that many malware families, such as NanoCore RAT and DcRAT, have built in cryptocurrency mining software or plug-ins making the utilization of stand-alone miners effectively obsolete. In Q3, threat actors used small, relatively simple, miners and cryptocurrency stealers to augment other infections. The regrouping and returning of more sophisticated families predicted after the law enforcement operations of Q2 have yet to occur, leaving the top malware families populated by comparatively simple, popular, and relatively cheap malware.

| TOP 05 Malware Types | TOP FAMILY Family in Type |
|---|---|
| RAT | Remcos RAT |
| Banker | Mispadu |
| Information Stealer | Waltuhium Grabber |
| Keylogger | Agent Tesla Keylogger |
| Cryptocurrency Miner | Phoenix Clipper |

*Table 1: Top malware types with the top family of each type in Q3 2024.*

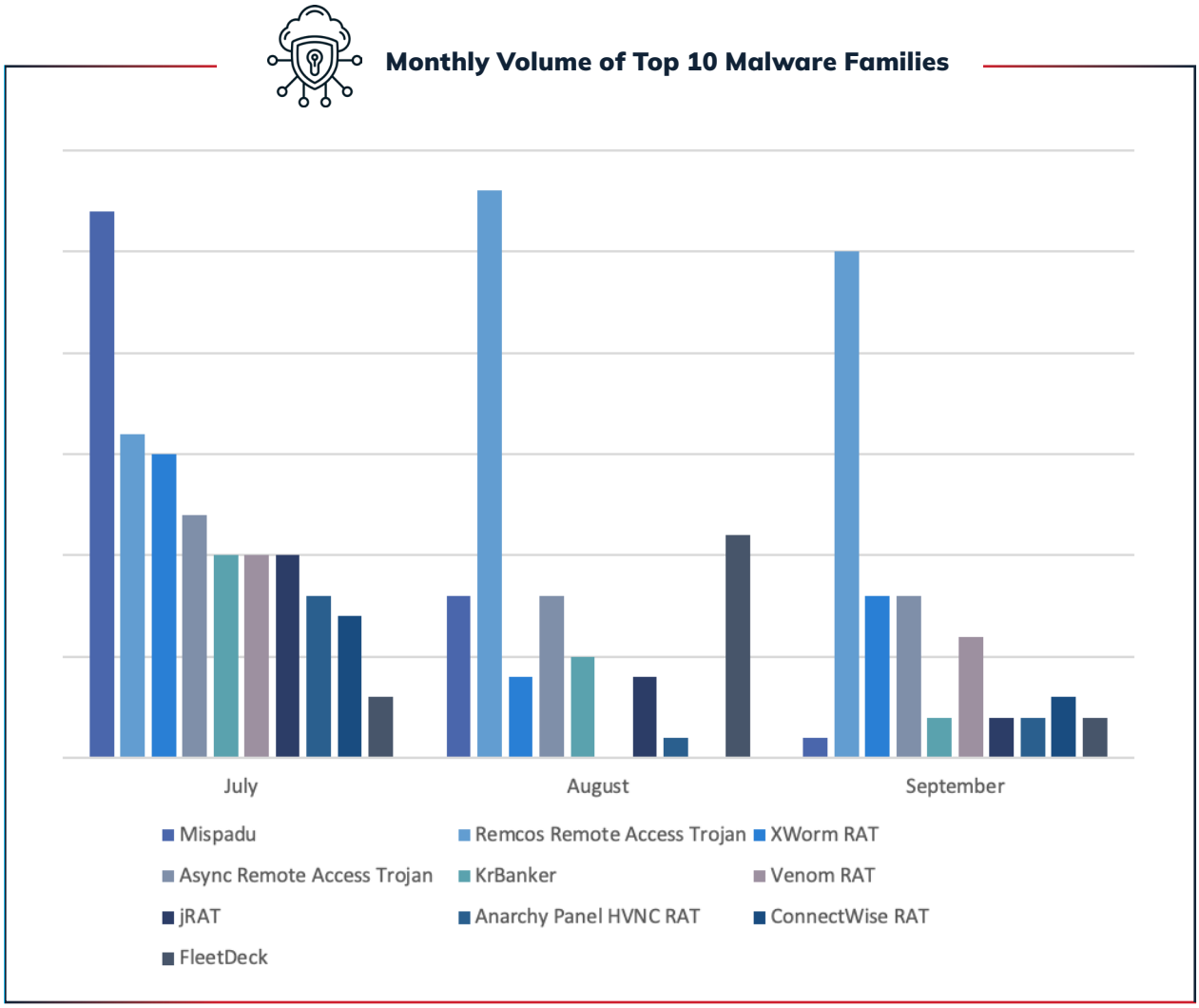


*Figure 3: Monthly volume of top ten malware families in each type in Q3 2024.*

Looking at Figures 3 and 4, it is clear that in Q3 2024 Remcos RAT and Mispadu have dominated the charts. Remcos RAT is typically delivered via a Google Drive link embedded in the email that, when clicked, downloads a password-protected archive containing the Remcos RAT executable. The use of a Google Drive link and password protection on the archive file allow these emails to bypass a large range of SEGs, while also avoiding Google's scanning of hosted files. Mispadu is typically delivered via links embedded in attached PDF documents. PDF documents are often allowed through by SEGs because of their frequent use in legitimate communications, which allows these Mispadu campaigns to also bypass a large number of SEGs. The next most frequently seen malware families were Async RAT and XWorm RAT. These RATs were often seen delivered in a group along with Anarchy Panel HVNC RAT and Venom RAT. Campaigns delivering these RATs in bulk spiked in July and September but declined considerably in August. These campaigns made use of more exotic delivery mechanisms such as LNK and URL files which allowed them to bypass some SEGs. The fifth most common malware family, KrBanker, was more regionally implemented than the others, specifically targeting Chinese language customers and frequently spoofing the State Taxation Administration of China.

These campaigns used yet another technique to bypass SEGs, having the malicious download URLs in an image and requiring the victim to type the URL out. This avoided SEGs scanning a URL embedded in the email text. It is clear that each of the most commonly seen malware families is recently so prevalent specifically because the threat actors behind the campaigns tailored them to bypass SEGs and confuse victims.

As seen in Figure 4, RATs led by Remcos RAT have taken the lead by a significant margin. What is unusual is that bankers have made a comeback from their near obscurity in Q2 2024. Bankers, in particular, were led by Mispadu which was the second most commonly seen malware family in Q3 2024. Information stealers, primarily in the form of Waltuhium Grabber, also increased from Q2 2024. Much like Venom RAT, XWorm RAT, and Anarchy RAT, Waltuhium Grabber was typically delivered in groups.

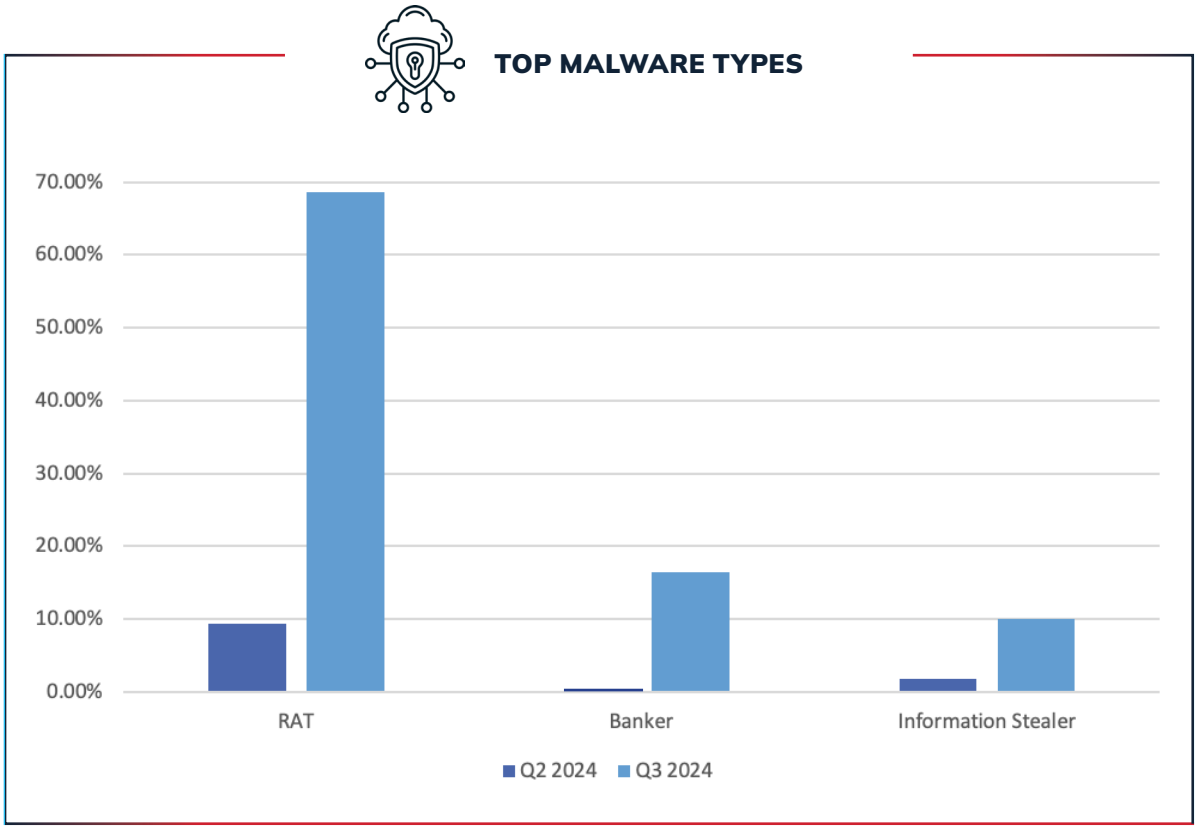


*Figure 4: Top malware types in Q2 2024 and Q3 2024 by volume of emails.*

# Delivery Mechanism Rundown

Q3 2024 saw a number of changes to the top delivery mechanisms seen in SEG-protected environments. CVE-2017-11882 has declined so far in popularity it is no longer even in the top 10. Instead, Office documents have skyrocketed 54% in popularity. These documents are very versatile, containing everything from clickable links to QR codes that deliver credential phishing. Some of them even contain links that download malware using special methods. JSDroppers and HTA files have risen from 10th and 15th place to 3rd and 5th place respectively. This is due to their widespread usage in campaigns delivering bundles of RATs and information stealers. The campaigns using JSDroppers, VBS downloaders, and HTA files typically are initiated by HTML, LNK, or PDF files, or the delivery mechanisms themselves. These campaigns typically consist of at least 3 steps.

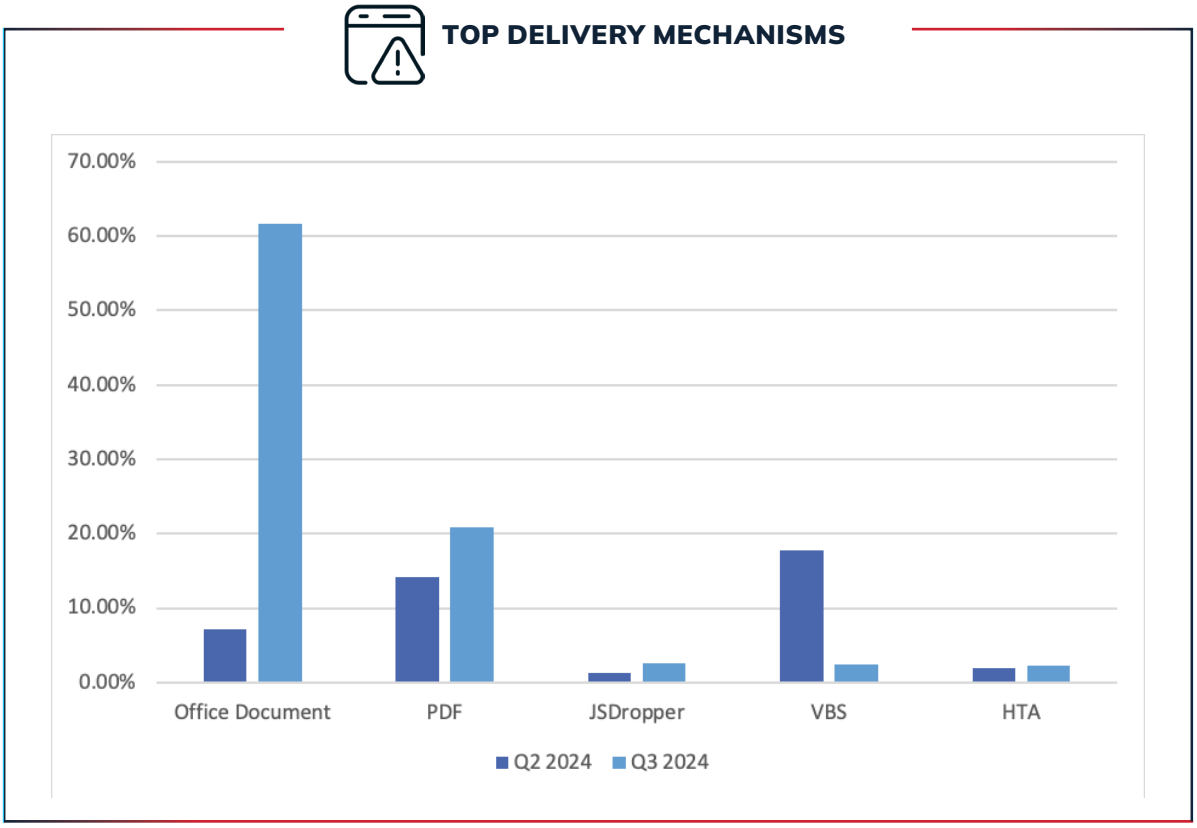


*Figure 5: Top malware delivery mechanisms by email volume in Q3 2024, with Q2 2024 totals for comparison.*

## 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 | Q2 2024 | Q3 2024 |
|---|---|---|
| 1 | dropbox | google |
| 2 | sharepoint | sharepoint |
| 3 | cloudflare-ipfs | amazonaws |
| 4 | google | office |
| 5 | dynamics | tiktok |
| 6 | adobe | beehiiv |
| 7 | linodeobjects | exactag |
| 8 | beehiiv | linodeobjects |
| 9 | amazonaws | dynamics |
| 10 | exactag | vk |

*Table 2: Q2 2024 and Q3 2024 ten most-common .com domains used in credential phishing campaigns.*

Most threat actors use .com domains for their credential phishing campaigns. During previous quarters, they regularly abused hosting services with open redirects to nest malicious URLs behind and within legitimate domains. In Q1 2024, cloudflare-ipfs saw a massive amount of activity, in Q2 it declined slightly into 3rd place, and in Q3 it completely dropped out of the top 10. It was instead replaced by the increasingly popular tiktok[.]com and office[.]com domains. TikTok[.]com was used from open redirects while Office[.]com was used with Office forms to steal credentials using a legitimate domain. This quarter saw .com domains being used equally for redirection and credential phishing hosting.

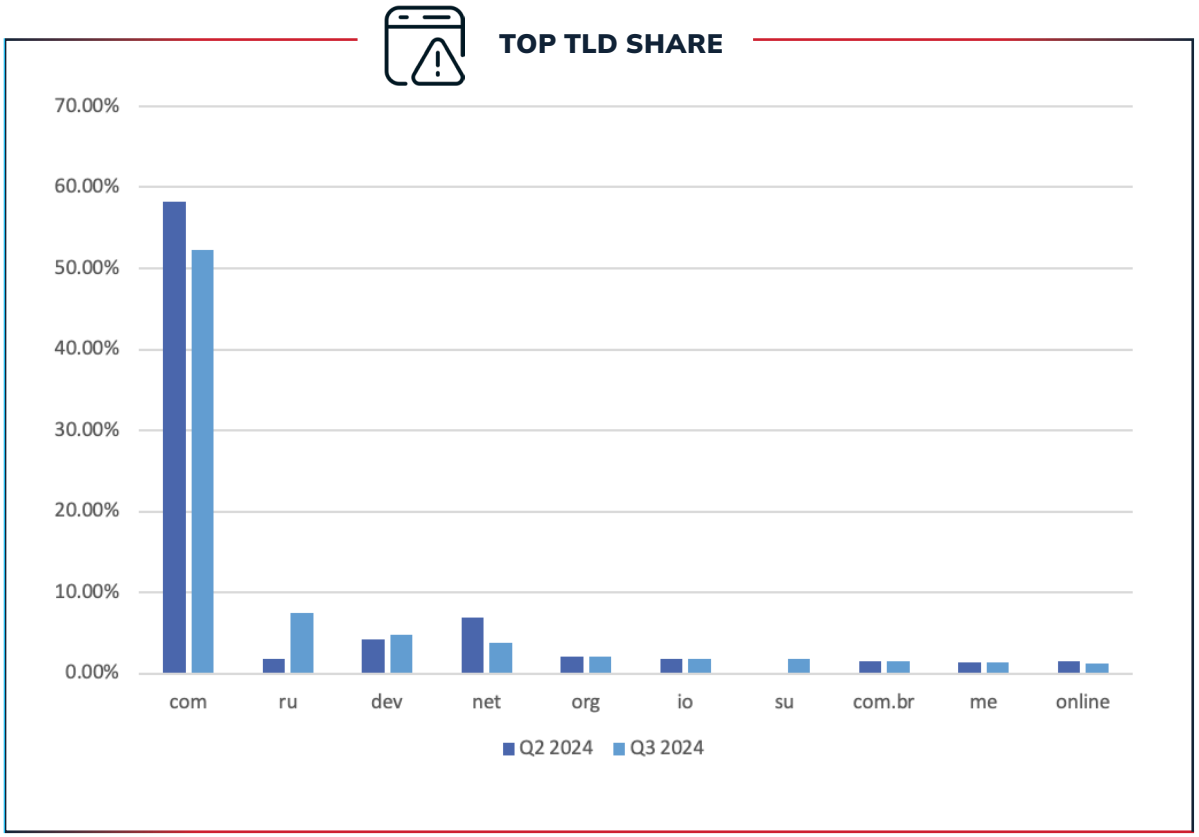


*Figure 6: The top ten TLDs for both stages in Q3 2024, with Q2 2024 totals for comparison.*

Across Q2 2024 and Q3 2024, most TLDs remained at similar levels. The .com TLD continues to be the most heavily used, while .su and .ru saw a substantial increase. This is a reversal from the last 2 quarters where the .ru TLD continued a downward trend. The .su TLD made a comeback and was seen primarily being used for data exfiltration.

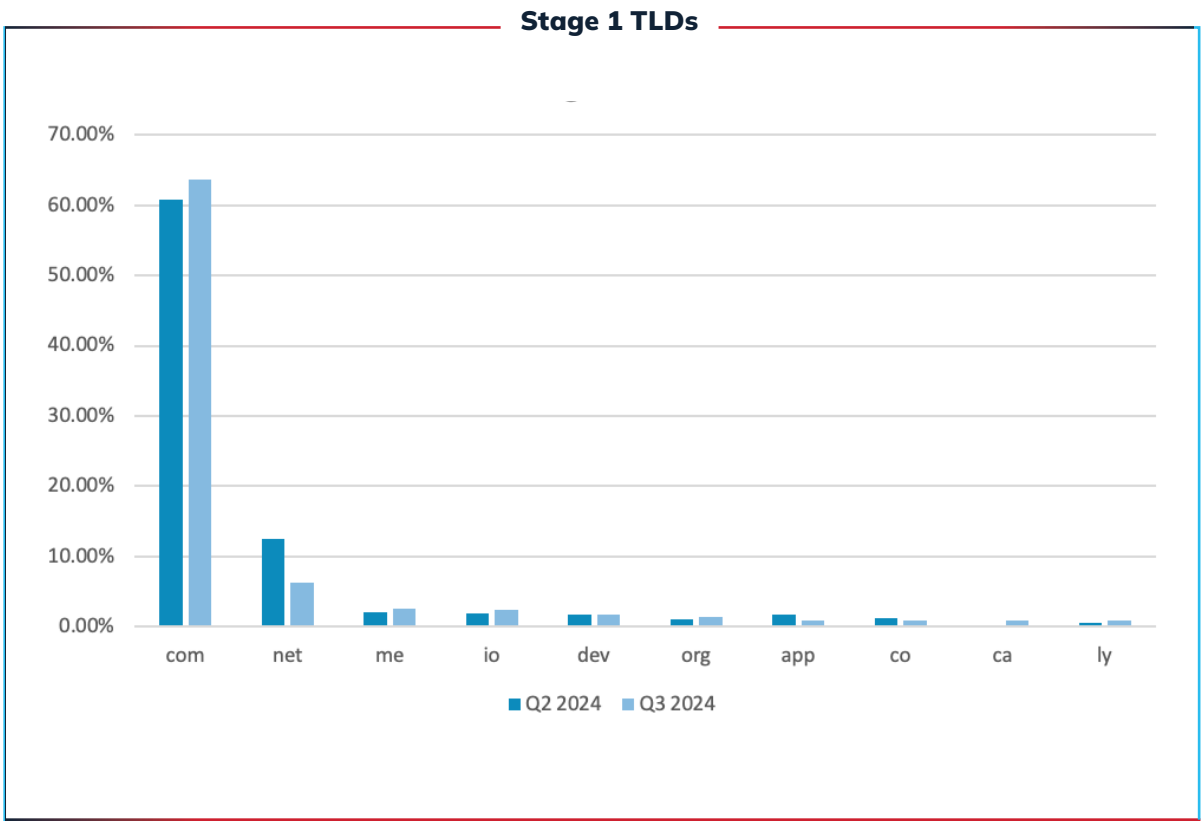


*Figure 7: The top ten Stage 1 TLDs in Q3 2024, with Q2 2024 totals for comparison.*

Q3 2024 saw relatively steady usage of Stage 1 TLDs with only .net showing a significant decline in volume. The .ca and .ly TLDs made a comeback into the top 10 but only by a slim margin.

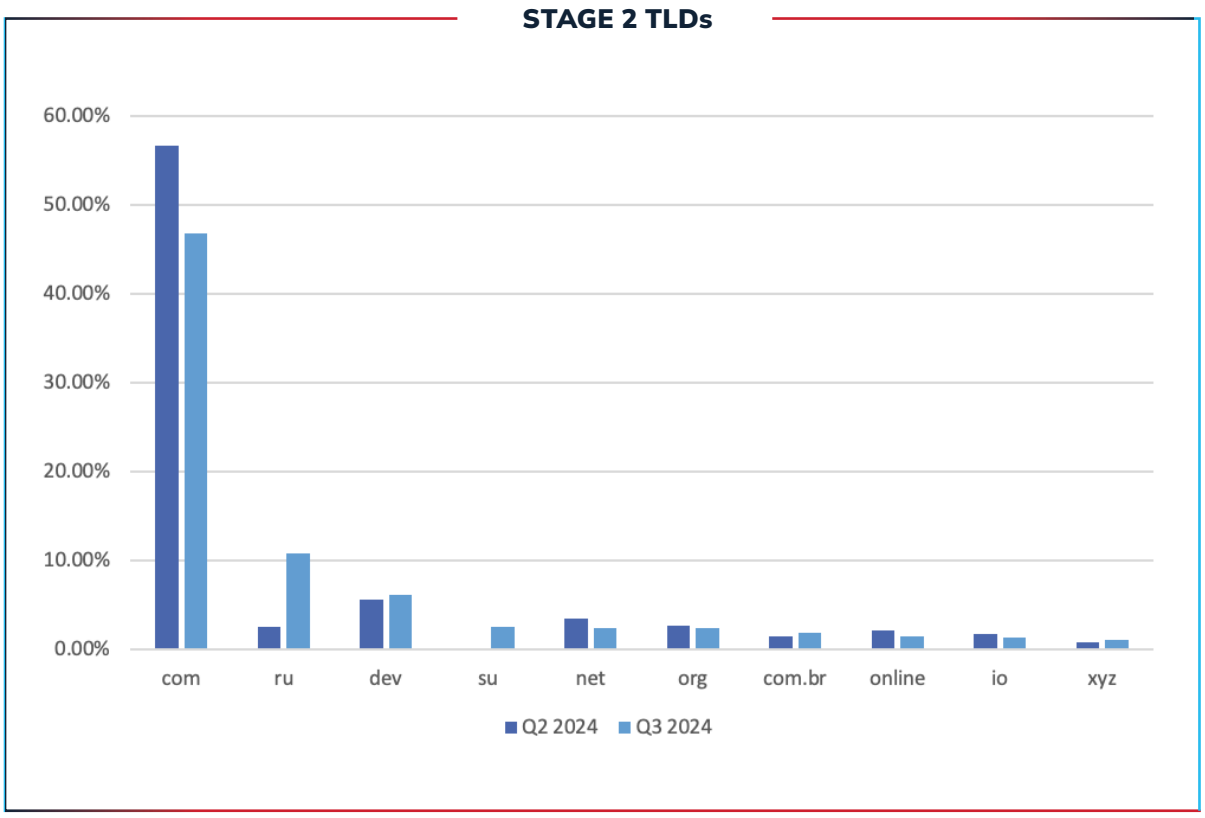


*Figure 8: The top ten Stage 2 TLDs in Q3 2024, with Q2 2024 totals for comparison.*

TLDs used in Stage 2 saw more significant changes with the .ru TLD increasing by more than 4 times in volume and the .su TLD increasing more than 12 times in volume. This is a direct result of increasing use of the .su and .ru TLDs for data exfiltration.

# File Extensions of Attachments

The appearance of .html and .htm file extensions as the 1st and 3rd place respectively comes as a surprise to few. File attachments with these extensions have become increasingly common. They bypass SEGs at an alarming rate and typically deliver credential phishing that is either directly embedded in the HTML file or is accessed via a link in the HTML file. The 2nd place .docx extension reflects the growing popularity of attached Office documents that contain links or QR codes leading to credential phishing pages. QR codes in particular have become increasingly common as they easily bypass most SEGs when embedded in an attached document. In some cases, .docx files have been used to deliver malware such as KrBanker or Loki Bot but this is typically via an embedded link rather than a QR code. Files with the .pdf file extension are used similarly to .docx files to deliver credential phishing or, in rare cases, malware. However, it seems that SEGs are becoming increasingly better at scanning their contents and they are declining in popularity. The .rtf, .doc, and .xlsx file extensions are all used for the same purposes as the .docx file extension, containing either embedded links or QR codes. Some .xlsx files have been used to deliver malware such as jRAT but this is a relatively rare occurrence. Lastly, .svg files are used similarly to HTML files, containing embedded links, and are consistently used to deliver Async RAT.

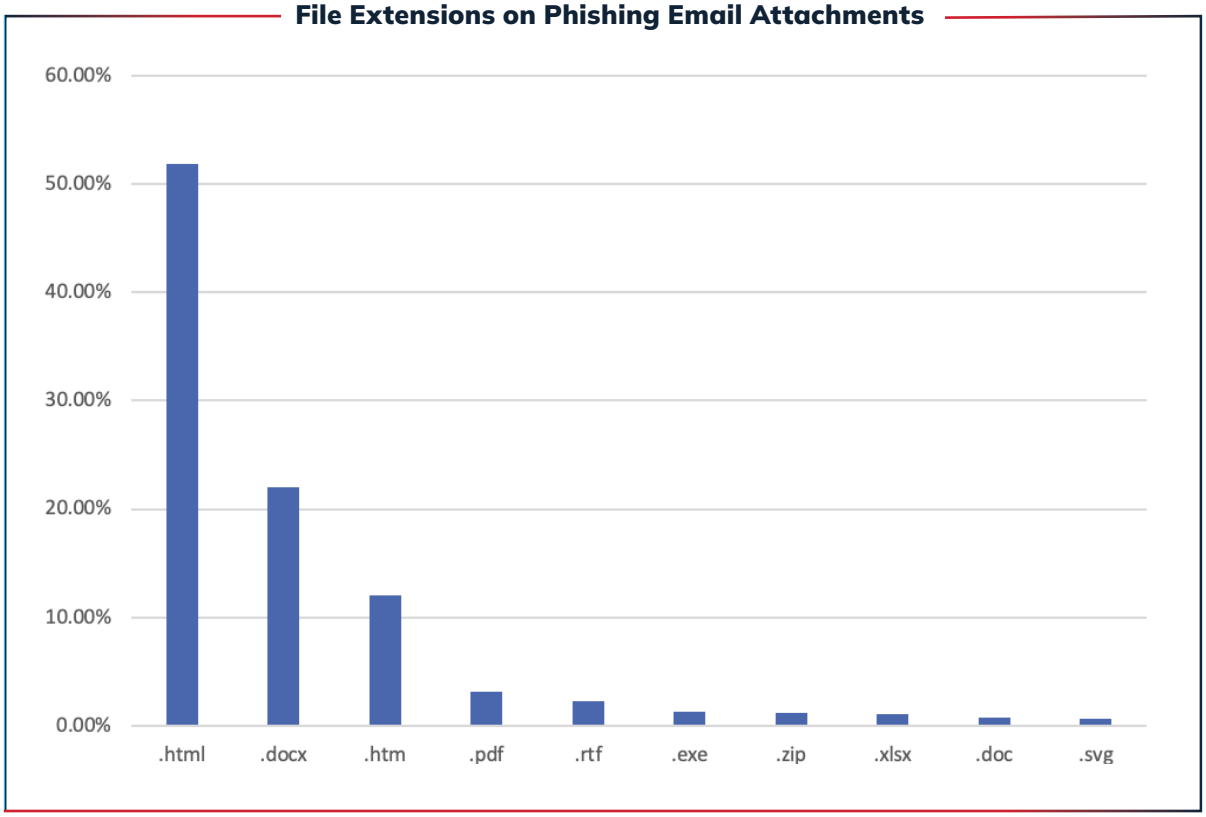


*Figure 9: Top 10 most-common attachment file extensions found in environments protected by SEGs in Q3 2024.*

# Command and Control Server Locations

| Q2 2024 | | Q3 2024 | |
|---|---|---|---|
| COUNTRY | PERCENTAGE | COUNTRY | PERCENTAGE |
| United States | 76.72% | United States | 80.94% |
| Germany | 4.07% | Germany | 2.96% |
| Canada | 1.48% | Canada | 1.64% |
| United Kingdom | 1.47% | United Kingdom | 1.31% |
| Russia | 1.44% | Netherlands | 1.07% |

*Table 3: Q2 2024 and Q3 2024 percentages for C2 sources by IP address geolocation.*

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. Surprisingly, this quarter saw little change from the previous quarter.

Typically, all C2 sources but the United States will change in ranking or be completely replaced by those previously below the top 5. Although there were some changes to the exact makeup, with Germany losing an entire percent and the United States gaining a whopping 4%, the top 4 positions saw no change. Russia being replaced by the Netherlands is also a surprise as Russia has been in the top 5 for the last 3 quarters. This overall lack of major change is likely driven by the same causes as those in Q2, namely a lack of large-scale botnets using a large number of distributed C2 IPs to make takedowns more difficult.

*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.*

# Projections for Q4 2024 and Beyond

## 5 PROJECTIONS

1. GitHub to be used more as a SEG delivery bypass mechanism.
2. Holiday-themed phishing emails will increase this year.
3. As interest rates are lowered, focus on US brokerages such as Fidelity, Vanguard, and Charles Schwab will likely increase – credential phishing emails spoofing those brands to increase.
4. Q4 2024 and much of 2025 will see an uptick in federal services spoofing campaigns as changes to the political landscape keep federal services on the minds of many.
5. Multi-factor authentication-themed campaigns will continue to decrease as focus shifts around Q4 events.

# FINISHED INTELLIGENCE: TOPICS AND TRENDS

**Strategic Analysis: Threat Actors Bypass SEGs With Ease Using SEG Technology Against Itself**

This report looks over encoded URLs by SEGs which allowed threat actors to bypass other SEGs during Q2 2024. There are 4 major SEGs threat actors leveraged against other SEGs, and although this is a common tactic, Q2 had a notably higher volume compared to other quarters.

**Strategic Analysis: Malware Exploit Bypasses SEGs Leaving Organizations at Risk**

This report analyzes a SEG bypass method used by threat actors to deliver malware. When the archive is opened outside of the Outlook client and analyzed by SEGs, the archive appears to contain a .Mpeg video which does not play and does not act malicious. However, when the archive is opened inside the Outlook client or the Windows Explorer Archive Manager, the .Mpeg file is (correctly) seen as a .html and allows the victim to execute the embedded FormBook malware.

**Strategic Analysis: Ransomware in 2024 - Top 5 Delivery Methods and Threats to Know**

This report looks over the main delivery methods of ransomware. The different delivery mechanisms include RATs staging for ransomware and Initial Access Brokers (IABs) directly downloading ransomware. This report also contains the top 5 threat actor groups which are notorious for delivering ransomware.

**Strategic Analysis: Research Identifies Prevalence of Brand Impersonation in Three-Year Cross-Industry Analysis**

This report covers a wide variety of brand impersonation and which brands are typically seen being spoofed in 10 different industries. In total, 14 different brands were spoofed across all 10 industries, which include finance and insurance, manufacturing, mining, retail, real estate, healthcare, utilities, transportation, professional services, and information industries.

**Strategic Analysis: Decoding Credential Phishing: A Step-by-Step Breakdown Using the Cyber Kill Chain**

This report reviews the Cyber Kill Chain, which contains the step-by-step methods threat actors typically use to create their campaigns and send their malware to users. The Cyber Kill Chain contains seven steps: reconnaissance, weaponization, delivery, exploitation, installation, C2, and actions on objectives. This report goes more in depth regarding each of these steps, along with examples of each.

**Strategic Analysis: Async RAT – Phishing Malware Baseline**

This report details Async Remote Access Trojan (RAT), which is a widely used RAT throughout the threat landscape. This malware was created in 2019 with very few updates since its release. A few of its capabilities include keylogging, screen viewing, password stealing, and clipboard monitoring.

# FINISHED INTELLIGENCE: TOPICS AND TRENDS

**Flash Alert: Amarok Ransomware Reappears**

A legal-themed ransomware campaign targeting Dutch speakers of an international law firm kicked off on Friday, July 5. The ransomware is known as Amarok Locker and was last seen in February targeting Italy. This multi-lingual ransomware is known for both encrypting files and exfiltrating files to be used in additional ransom demands.

**Flash Alert: Xsam Xadoo RAT**

An email campaign delivering the newly distributed Xsam Xadoo RAT was seen shortly before this Flash Alert was released. Xsam Xadoo RAT is self-named and is primarily known for stealing information. In fact, "Xadoo" means "steal" in Somali. Xsam Xadoo RAT appears to be currently focused on cryptocurrency and credential stealing. It was also seen deploying the XMRig cryptocurrency miner.