PHISHME
COFENSE
EMAIL SECURITY

CATCH MORE PHISH

Q2 2024 | Phishing Intelligence Trends Review

PHISHME
COFENSE
EMAIL SECURITY

Contents

Executive Summary:

In Q2 2024, Cofense Intelligence saw threats bypassing secure email gateways (SEGs) and landing in inboxes and saw previous trends reappear such as the utilization of various Remote Access Trojans (RATs) and Loader malware. RATs have been a popular choice over the last decade and the reappearance is due to modernizing their capability to reach targets in various ways, changing their techniques and tactics to advance their campaigns in a more targeted way. Of note was the substantial increase in volume for jRAT, njRAT, and Ghost RAT, while other variants such as STRRAT saw a precipitous drop. Additionally, we saw increases in those targeted campaigns themed around taxes and policy. Cofense Intelligence observed a slowdown in past malware families and credential phishing threats due to the takedown efforts from Operation Endgame. However, we don't see the threats slowing down for long as most of the threat actors use this time to regroup and reposition themselves to come back with more sophisticated strategies.

In the *Q1 2024 Cofense Phishing Intelligence Trends Review* report, our predictions for Q2 were spot-on. We predicted more small-scale and highly targeted campaigns and more law enforcement takedowns leading to more diverse ransomware delivery for Q2 2024 and beyond. We were right. When it comes to phishing detection and response, it only takes one threat to bypass your SEG and compromise your security. Perhaps more targeted and sophisticated attacks are on the horizon versus the wide-cast net we traditionally have seen in Lockbit ransomware. Our intelligence with our Vision solution can auto-quarantine these threats, mitigate the risks to your organization, and improve your overall security posture.

The Key Highlights for Q2 2024 Include:

- **RAT family increased overall by 68%, most notably emails delivering njRAT went up 152%, typically legal themed and in Spanish language.**
- Active threats increased significantly in these two themes:
  - Policy theme went up 566% in Q2, primarily from HR policy adjustments requiring some kind of interaction.
  - Upward trend of ATRs with a tax theme went up 238% from Q1.
- HTA delivery mechanism (Microsoft HTML file extension) increased to 2% of all delivery mechanisms, an 88% increase in ATRs with HTA, and it mostly delivered the Mispadu banking trojan.
- Stage 2 TLD .ru usage decreased from 10% to 3%, indicating threat actors made a significant shift away from hosting in Russia.
- Coordinated Worldwide Law Enforcement named operations continue to disrupt threat actors (Operation Endgame 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

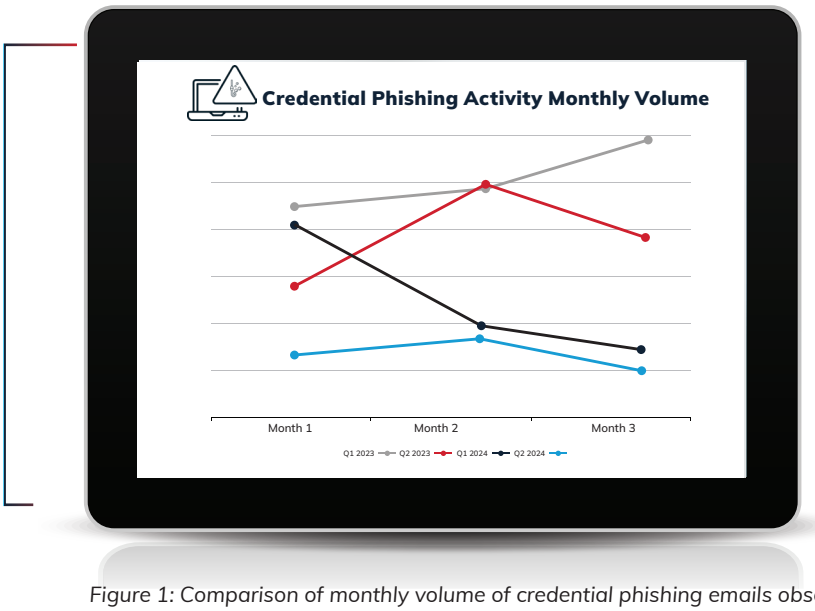


Figure 1: Comparison of monthly volume of credential phishing emails observed in Q1 and Q2 during 2023 and 2024.

In Figure 1, credential phishing activity went down almost 25% from Q1 2024 to Q2 2024. This is in keeping with past trends from 2023 when Q2 was roughly 22% lower in volume than Q1. Looking at the first two quarters of 2024, Q2 saw much more consistent volumes than Q1 with only a slight spike halfway through the quarter. This makes sense as there were fewer notable threat campaign events with increased phishing volumes associated to them.

Figure 2: Comparison of weekly volume of credential phishing emails observed in Q1 2024 and Q2 2024.

Prevalent Malware in Q2 2024

Despite June's low numbers, Agent Tesla Keylogger remained the top family type in Table 1. Thanks in part to Operation Endgame, a multinational coordinated cyber operation that dismantled the infrastructure of at least 4 malware groups: IcedID, Smokeloader, PikaBot, and Bumblebee. Of particular note, alongside DarkGate, PikaBot was one of the two malwares that came to prominence in the wake of last year's Qakbot takedown. Separately, we saw a re-entrance of Banker and Ransomware in the top five malware types in Table 1.

More importantly, Operation Endgame takedown had an impact on malware volumes towards the end of Q2; however, we don't see the threats slowing down anytime soon. Most of the threat actors use this time to regroup to come back with more sophisticated strategies. When it comes to phishing detection and response, it only takes one threat to compromise your security.

TOP 05 Malware Types	TOP FAMILY Family in Type
Keylogger	Agent Tesla Keylogger
RAT	Remcos RAT
Information Stealer	FormBook
Banker	Mispadu
Ransomware	LockBit Ransomware

Table 1: Top five malware types with the top family of each type in Q2 2024.

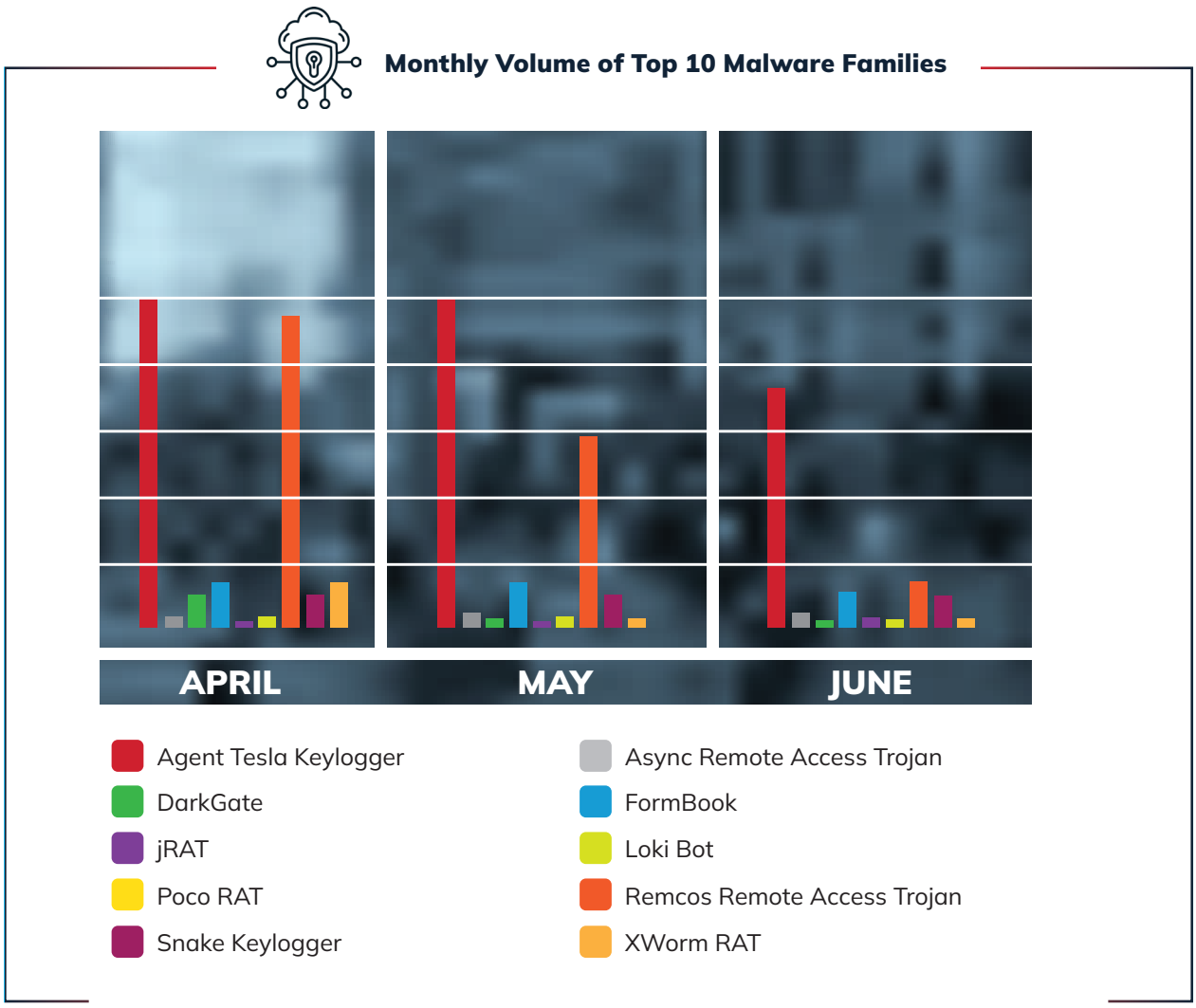
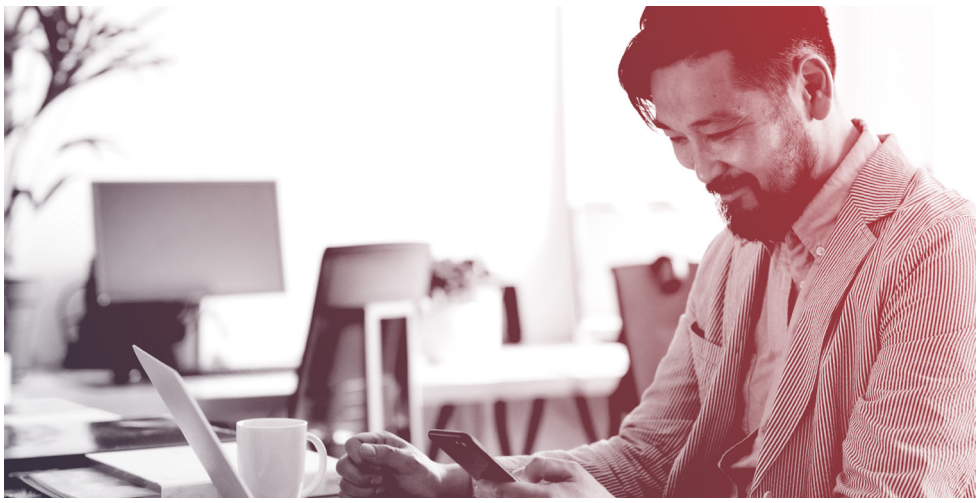


Figure 3: Monthly volume of top ten malware families in each type in Q1 2024. Agent Tesla Keylogger is truncated at 9-16% of total value for April and May so that differences in the other families can be seen.



In Q1 2024, Agent Tesla remains the most popular malware family this quarter as shown in Figure 3. However, as highlighted in the *Q1 2024 Cofense Phishing Intelligence Trends Review* report, Cofense Intelligence identified and continued to monitor a noticeable increase in activity for STR Remote Access Trojan in March. This brief surge in activity was replaced by Remcos RAT (alongside Poco RAT, XWorm RAT, and jRAT), which appeared strongly through April and continued into May before resuming more historically normal levels in June. This activity is consistent with a typical malware campaign, usually lasting around three months, and the quick shift in RAT types shows threat actors' ability to quickly pivot. **Similar to the RAT resurgence in March/April, PikaBot began showing strong activity in the second half of Q1, but this was supplanted by DarkGate in Q2, undoubtedly due to the dismantling of PikaBot's infrastructure in May.** Unique to this quarter though is an uncharacteristic increase in Banker type malware, specifically **Mispadu, which has not seen much popularity until now, appearing in 88% more active threats this quarter. Mispadu is a banking trojan that uses .hta file extensions as the delivery mechanism. HTA is an HTML application that uses a Microsoft Windows program whose source code includes one or more scripting languages. HTA executes without the constraints of an internet browser security model and is executed as a "fully trusted" application.** Finally, after remaining relatively under the radar in Q1, FormBook reappeared with consistent activity throughout Q2.

LockBit ransomware reappeared in the top five, but this doesn't appear targeted as the threat actors use a wide net. In Q1 2024, we saw international takedown initiatives to disrupt this Ransomware as a Service (RaaS) such as dismantling of their website, infrastructure, and data. Considering no arrests were made, we see the reappearance of this threat. Since 2019, we have seen an uptick and growth with LockBit regardless of the attempts to disrupt and dismantle these threat actors. Despite this disruption, LockBit v3.0 was released in June of 2024, while the Lockbit Black ransomware was seen often being delivered by the Phorpiex botnet.

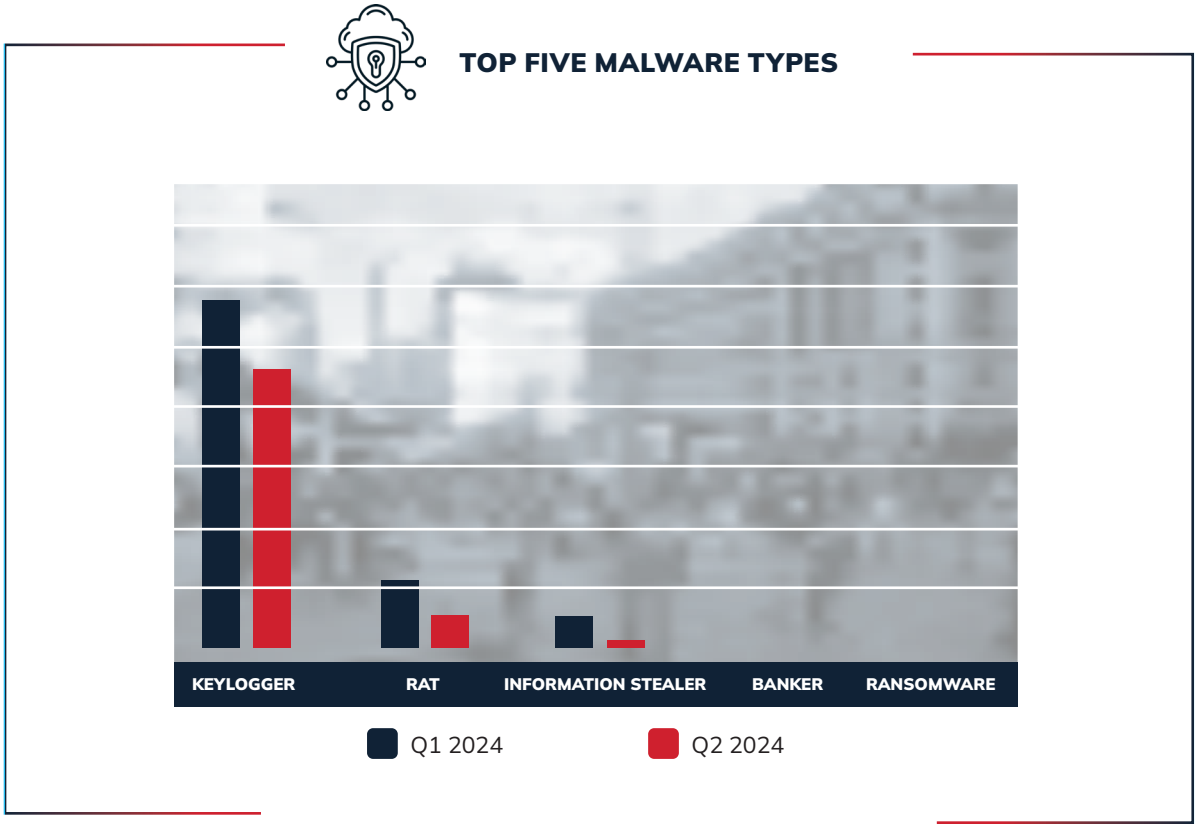


Figure 4: Top five malware types in Q1 2024 and Q2 2024 by volume of emails.

Delivery Mechanism Rundown

Q2 2024 saw a marked decrease in overall activity across the entire threat landscape, though it should be restated that Q1 2024 saw a major increase in activity over Q4 2023. However, there was a shift in popularity amongst the top five most popular delivery mechanisms. In Figure 5, as previously reported, the ubiquitous CVE-2017-11882 continued to maintain the top spot for this quarter and directly contributed to several of the top malware families noted in the previous section, as well as below. **CVE-2017-11882 is nothing new, the Microsoft Office Flaw has been around for almost 17 years and is still being widely used today as the top delivery mechanism for malware.** VBS Downloader and PDF Dropper saw a minor uptick in volume but remained consistent for the most part. However, the most notable deviation from last quarter is that DotNET Loader dropped from second place in Q1 down to fourth place in Q2, a drop of nearly 85% by activity volume. Office Document maintains the fifth place this quarter after jumping JSDroppers in Q1, showing a steady continuity in its use as an attack vector.

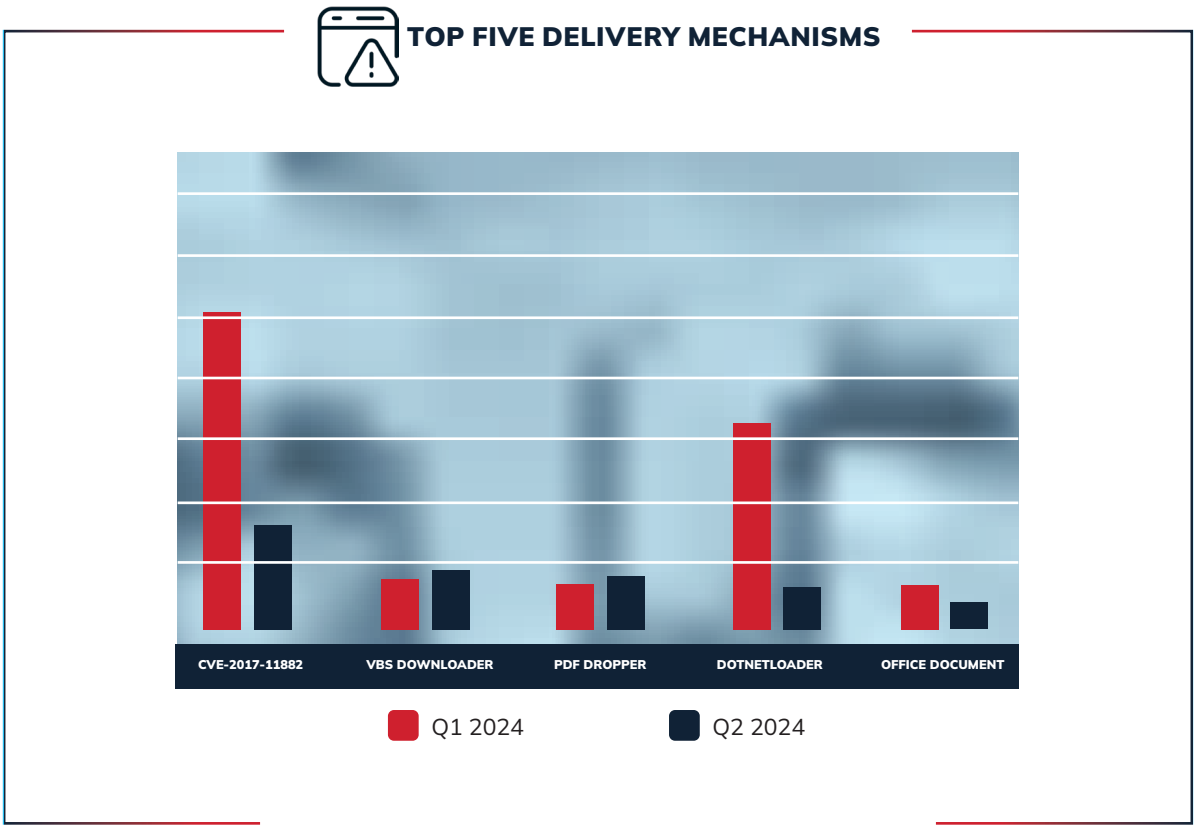


Figure 5: Top five malware delivery mechanisms by email volume in Q1 2024, with Q4 2023 totals for comparison.

The pie chart in Figure 6 shows the **top malware families delivered via CVE-2017-11882. Agent Tesla Keylogger continues to be the most used malware family by almost 41%,** while Remcos RAT maintains its second-place position. FormBook overtook Loki Bot for third place this quarter with approximately three times as much activity. Of note is the absence of NanoCore RAT in Q2, with its utilization volume being too low to include.

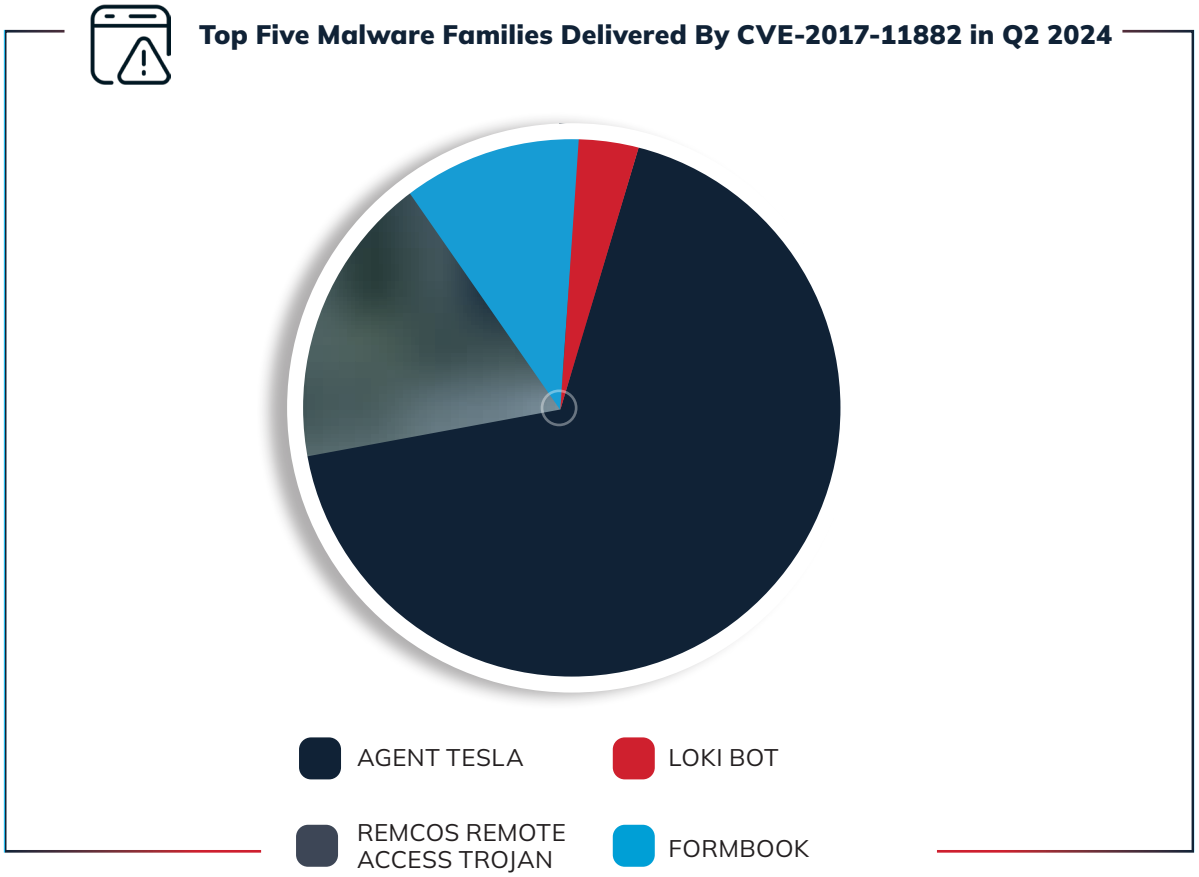


Figure 6: Top five malware families delivered by CVE-2017-11882 in Q2 2024.

Domains and TLDs Used in Credential Phishing

Each quarter, Cofense Intelligence analyzes credential phishing emails that reached users in environments protected by 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	Q1 2024	Q2 2024
1	Cloudfare-ipfs	Dropbox
2	Adobe	Sharepoint
3	Google	Cloudflare-ipfs
4	Linode Objects	Google
5	Sharepoint	Dynamics
6	Beehiiv	Adobe
7	DropBox	Linode Objects
8	Dynamics	Beehiiv
9	Microsoft	Amazon AWS
10	Myqcloud	Exactag

Table 2: Q1 2024 and Q2 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, which propelled it to the top position. However, in Q2 it sank to the third position in favor of file hosting services Dropbox and Sharepoint,** which took first and second respectively. All other abuse remained somewhat consistent with the notable reappearance of Amazon AWS, which fell out of the top 10 last quarter.

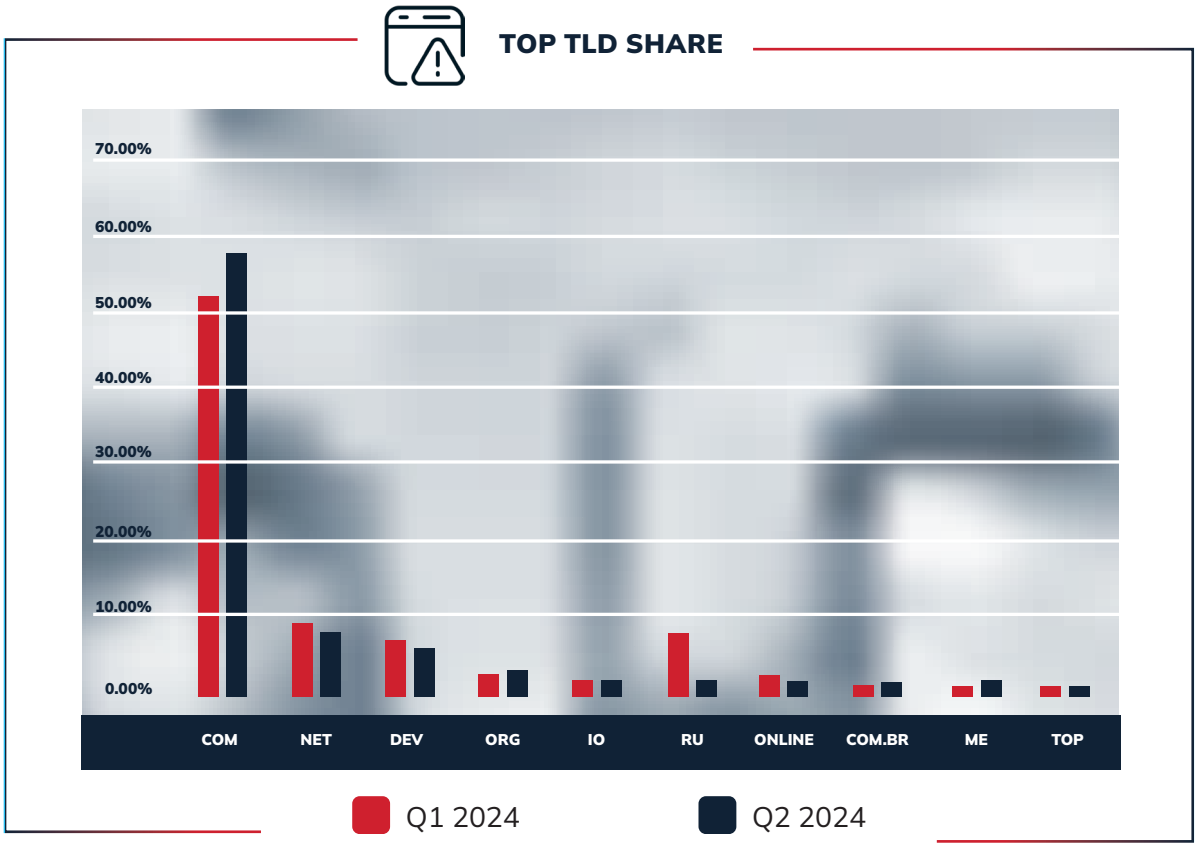
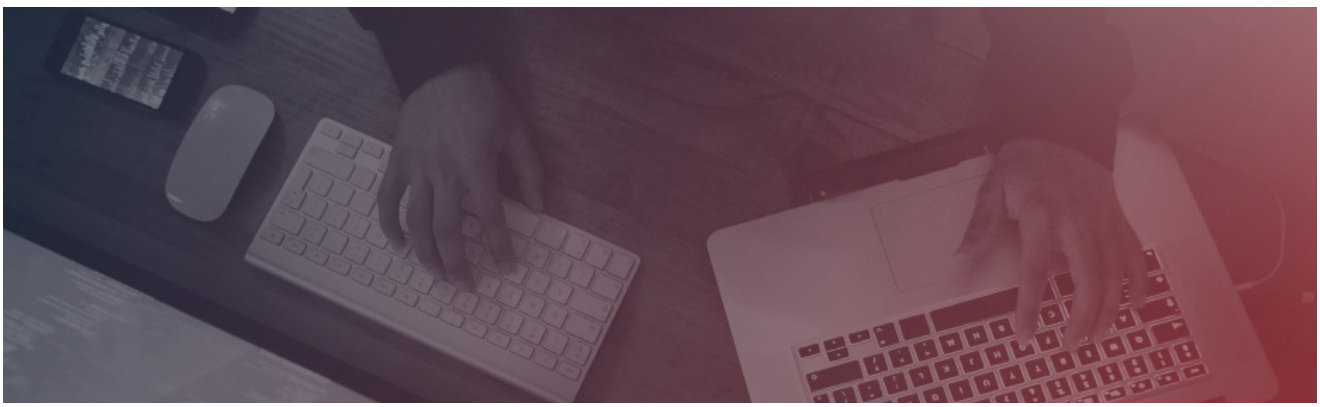


Figure 7: The top ten TLDs for both stages in Q2 2024, with Q1 2024 totals for comparison.

Between Q1 and Q2 of 2024, most TLDs remained at similar levels. As mentioned previously, the .com TLD continues to be the most heavily used, while .dev and .ru saw a substantial decrease. The .ru TLD in particular continued its downward trend from Q4 2023, only appearing at about one-third of Q1 2024's volume.



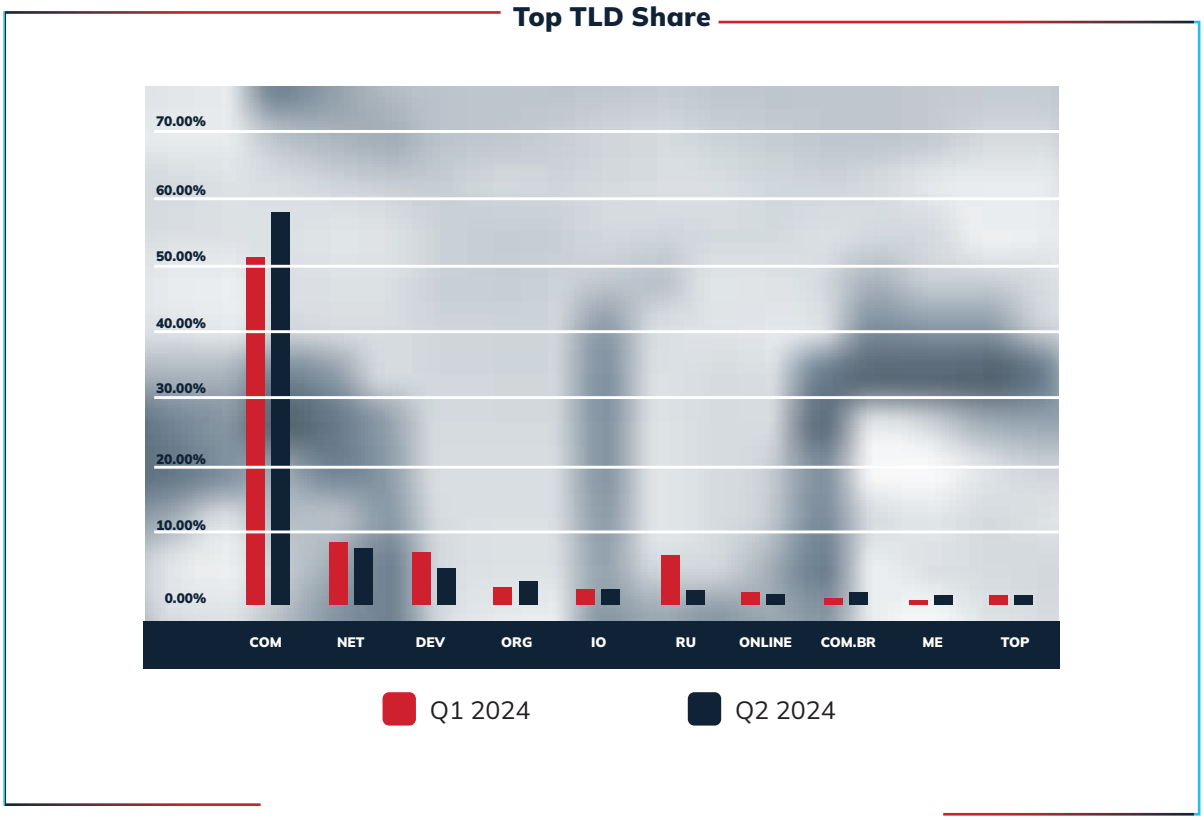


Figure 8: The top ten Stage 1 TLDs in Q2 2024, with Q1 2024 totals for comparison.

Q2 2024 saw a marked increase in the prevalence of the .com TLD amongst stage 1 TLDs. This was accompanied by minor increases in .me and .com.br, both of which nearly doubled but still remain at lower volumes overall. Interestingly, Q1 2024 saw the .app, .to, and .co.uk TLDs replace .ru, .org, and .com.br TLDs. This was attributed to a Meta spoofing campaign which looks to have subsided, resulting in the later three reappearing in the top ten Stage 1 TLDs.

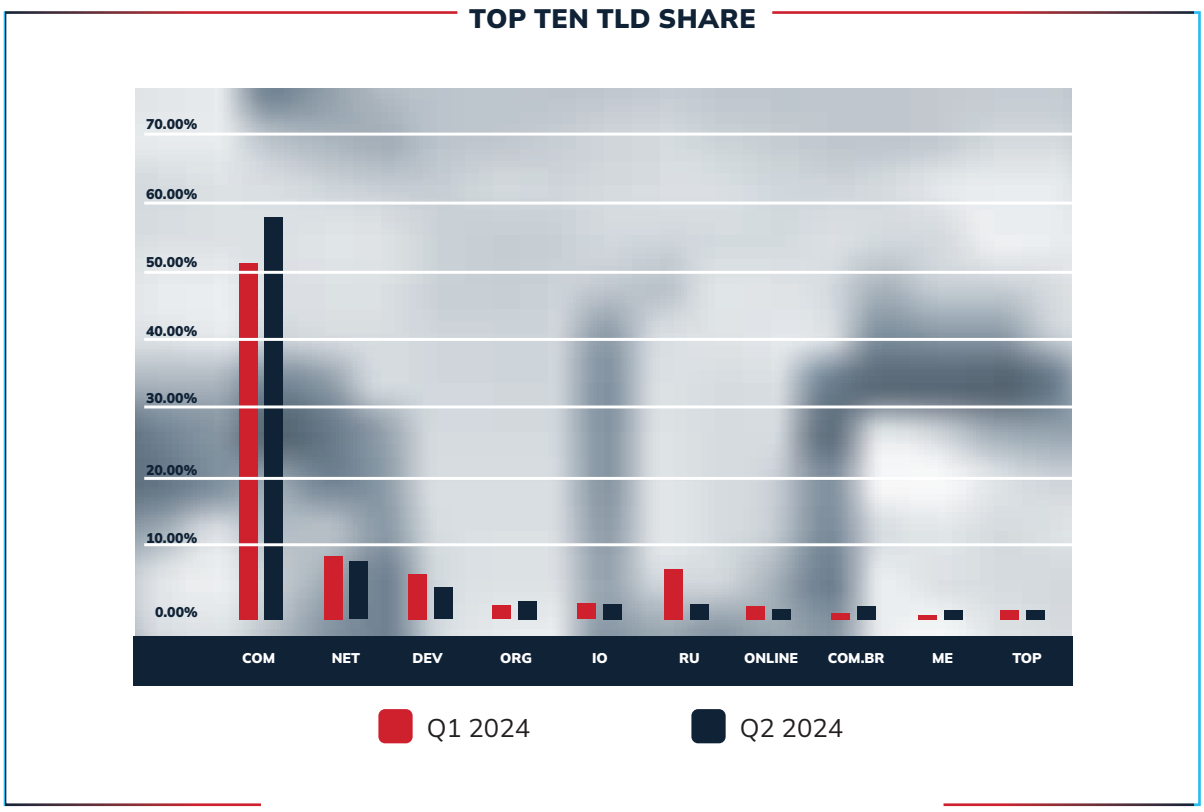
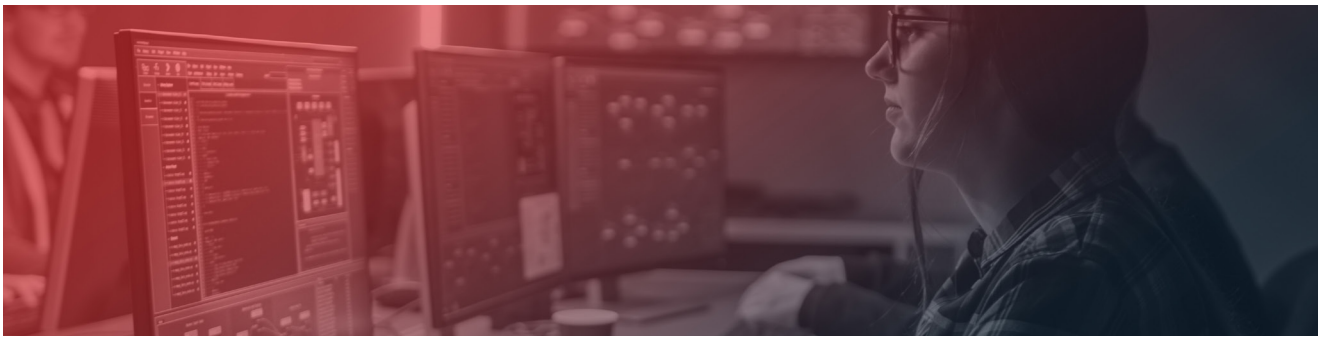


Figure 9: The top ten Stage 2 TLDs in Q2 2024, with Q1 2024 totals for comparison.

TLDs used in Stage 2 saw some shifts in activity, primarily away from the .dev TLD, which increased in Q1, and .ru TLD, continuing its decline from the previous two quarters. Q2 2024 saw the .com TLD increase in popularity for both Stage 1 and 2, maintaining its dominance atop the abuse TLD charts. Despite its small share, the .com.br TLD almost doubled in usage from Q1 to Q2 in all measured cases. There is no prevailing trend in its usage beyond the fact that credential phishing using the .com.br TLD was some of the most varied in terms of the spoofed brand. This may be indicative of it being adopted by a wider audience of threat actors.



File Extensions of Attachments

The previous quarter saw PDFs maintaining the top spot for the most-seen file extension on email attachments that bypassed SEGs. While PDFs continued to be a commonly used file type in Q2 2024, Cofense Intelligence monitored several other extensions that increased greatly in popularity, namely .zip, .html, and .txt. All these extensions are commonly used formats for email attached files, but the shift of the most-used types this quarter highlights a change in the attempted attack vector. Archive files like .zip and .tar can easily hide any type of file within them including malware such as the RATs that were identified in greater numbers this quarter. The files contained within archives can be difficult to catch with automated security scanners, likely contributing to their increased use by threat actors. Much like .pdf and .txt files, archive files like .zip are often legitimately sent as email attachments, thus increasing the likelihood of them reaching users' inboxes. However, while not necessarily always suspicious, executables (.exe extensions) should be treated with a higher degree of suspicion and it is of particular interest that so many of them are bypassing SEGs still in Q2 2024.

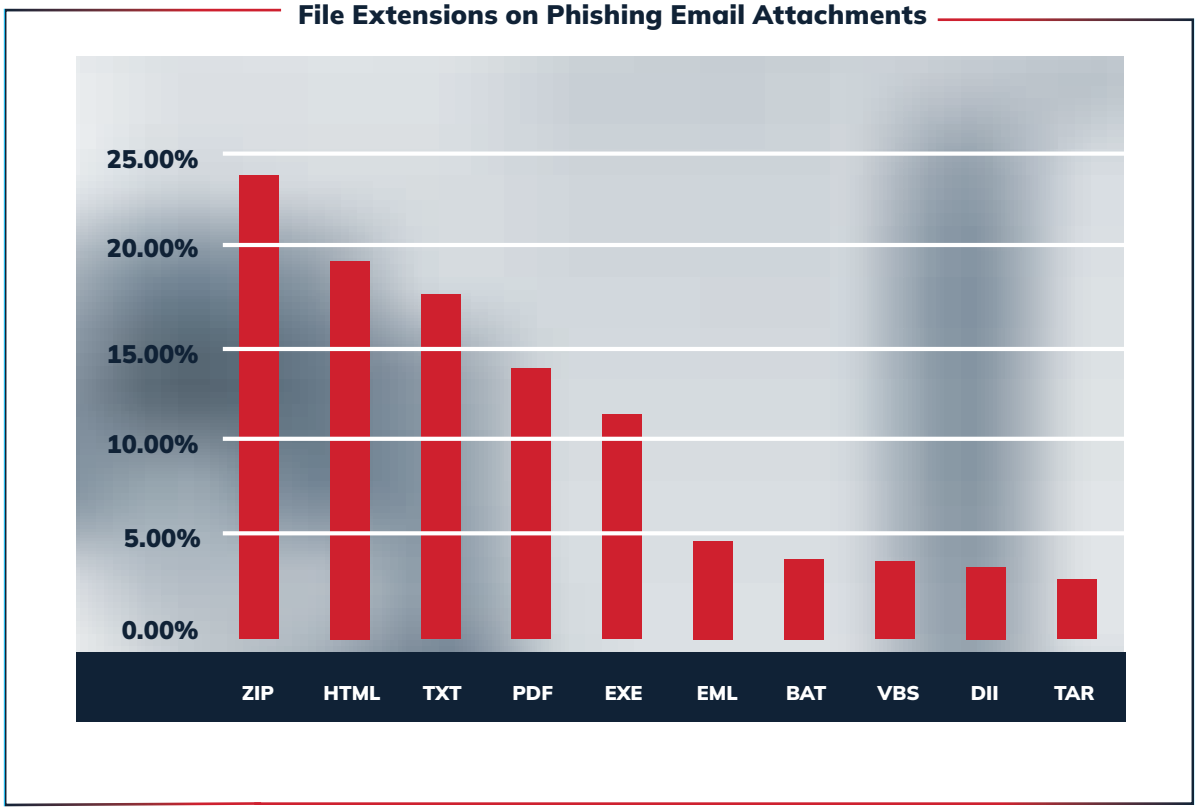


Figure 10: Top ten most common attachment file extensions found in environments protected by SEGs in Q2 2024

Command and Control Server Locations

Tracking Command and Control (C2) servers provide 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 several differences between Q1 and Q2 2024, but the volume share remained mostly the same overall. Bulgaria, which appeared in the top five last quarter, dropped and was replaced by the United Kingdom, which had not entered the top five in the previous two quarters. Germany also lost some share of the total C2 hosting volume, while the United States unsurprisingly maintained the number one spot.

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.

Q1 2024		Q2 2024	
COUNTRY	PERCENTAGE	COUNTRY	PERCENTAGE
United States	75.27 %	United States	76.72%
Germany	4.59 %	Germany	4.07%
Russia	1.45 %	Canada	1.48%
Canada	1.45 %	United Kingdom	1.47%
Bulgaria	1.33 %	Russia	1.44%

Table 3: Q1 2024 and Q2 2024 percentages for C2 sources by IP address geolocation.

Projections for Q3 2024 and Beyond

In the *Q1 2024 Cofense Phishing Intelligence Trends Review* report, predictions for Q2 were correct. Cofense Intelligence predicted small-scale and highly targeted campaigns and law enforcement takedown leading to more diverse ransomware delivery for Q2 2024 and beyond. Our Intelligence was accurate that campaigns are indicative of threat actors more frequently using small, timebound, but advanced campaigns to deliver malware. Threat actors will likely seek to employ new methods of ransomware delivery and new types of malware loaders in their campaigns. Here are our projections for Q3 2024 and beyond.

5 PROJECTIONS

EMBEDDED LINKS IN PDFS TO INCREASE

PDFs are a widely used file format for legitimate communication, especially within business environments. They are also extensible, specifically meaning that malicious content can be embedded within them. Additionally, links to URLs can be easily contained within these files, directing users to credential harvesting domains or the delivery of stage 2 malware.

FILENAMES WITH UNICODE RIGHT TO LEFT SO THE FILENAME DOES NOT APPEAR TO END IN .EXE WILL INCREASE.

Threat actors have made use of the ability to add a special character to file names that reverses how the file name is read for some time. When done correctly, a file with the .exe extension could appear to have a .pdf file extension. This can confound even experienced individuals. Cofense has seen an increase from Q1 to Q2 and we expect to see the trend continue if it continues to be effective.

AUTHENTICATION-THEMED EMAILS WILL INCREASE.

Authentication, especially multi-factor authentication-themed credential phishing has been around for some time. As enterprises continue to shift over to mandatory multi-factor authentication, we expect to see an increase in campaigns themed around it.

INCREASE IN CRYPTO WALLET TARGETED CREDENTIAL PHISHING

The crypto market has been in a trough for the first half of this year but could see a rebound in the second half. Historically, positive activity like this makes it a target for threat actors looking to pilfer credentials for crypto theft.

DUE TO BRAZILIAN BANKERS, THE BANKER MALWARE TYPE WILL CONTINUE TO INCREASE.

Brazilian bankers have consistently made up a majority of malware specialized for banking seen by Cofense. With bankers like Mispadu becoming increasingly common, we expect to see other Brazilian bankers, such as Grandoreiro and Mekotio, following the trend.

FINISHED INTELLIGENCE: TOPICS AND TRENDS

Strategic Analysis: Agent Tesla: The Punches Keep Coming

This report is a five-year historical overview of Agent Tesla Keylogger. A quick overview of the trend analysis suggests that Agent Tesla email campaigns continue to rise yearly, with Q3 and Q4 being notably higher in email volume.

Strategic Analysis: Meta Business Accounts at Risk of Cyber Threat

This report explores the inner workings of an advanced phishing campaign capable of bypassing multi-factor authentication (MFA) to target Meta business accounts. Cofense has discovered a comprehensive toolkit enabling threat actors to create malicious links, verify if they are active threats, generate emails, and other additional tasks. As it stands, this campaign proficiently crafts phishing emails directed at users in 19 countries and across various languages. These emails, appearing to originate from Meta, claim that the account violated a policy or infringed on a copyright. Should this campaign succeed, followers of the compromised Facebook business account are likely to be at risk of additional, potentially targeted, attacks using unexpected attack vectors, such as malicious ad campaigns.

Strategic Analysis: Threats That Hide in Your Microsoft Office Documents

This report covers the many malicious uses of Office 365 software suite-based documents and spreadsheets. This includes Office macros, CVE-2017-11882, CVE-2017-0199, embedded URLs, and QR codes.

Strategic Analysis: STR RAT – Phishing Malware Baseline

This report covers the basics of STR RAT including its capabilities, origin, and behavior. STR RAT is a remote access trojan (RAT) first seen in 2020 that is capable of keylogging, stealing credentials, and even delivering additional malicious payloads.

Strategic Analysis: PDF Dropper - Delivery Mechanism Baseline

This report covers Portable Document Format (PDF) files, their malicious uses, where they appear, and their various features. The report especially focuses on their ability to bypass many SEGs. It is important to note that not all the PDFs in these SEG-protected environments are malicious, although a fair number of them are.

Strategic Analysis: New Malware Campaign Targeting Spanish Language Victims

This report covers a malware family that Cofense recently identified and named Poco RAT, which is a simple RAT that targets Spanish language victims. It was first observed in early 2024, mainly focusing on companies in the mining sector and was delivered via embedded links to seven zip archives containing executables hosted on Google Drive. The campaigns are ongoing and continue to exhibit the same TTPs.