Q1 2023

Cofense Phishing Intelligence Trends Review

Executive Summary

Q1 2023 was filled with many updates and changes to the major malware families used in phishing as well as several notable deviations in tactics, techniques, and procedures (TTPs). Cofense Intelligence issues Active Threat Reports based on observed malicious email threats. In Q1 we had a 20% increase in Active Threat Reports compared to last quarter, and 34% increase compared to Q1 of last year. This quarterly phishing intelligence report will outline key trends we saw in Q1.

The key highlights for Q1 2023 include:

- Credential phishing volume for this quarter was volatile and increased significantly throughout the quarter by 527%. Overall, credential phishing threats increased 40% year-over-year from Q1 2022.
- Qakbot remained the most successful malware family reaching inboxes, 185% more often than Emotet, despite Emotet's extremely high dissemination volume.
- Evasive malicious campaigns abusing Telegram bots continued to rise tremendously in Q1 2023, outstripping Q4 2022 volume by 397% and surpassing all of 2022 volume by 310%.
- Threat actors experimented with a variety of delivery mechanism combinations, including the notable introduction of OneNote files as a common mechanism for threat during Q1.
- YouTube was an unexpected addition to the Top 10 .com domains being employed by threat actors, who used open redirects at youtube.com to point to phishing pages.

In Q1 we had a 20% increase in Active Threat Reports compared to last quarter, and 34% increase compared to Q1 of last year.

Evasive malicious campaigns abusing Telegram bots continued to rise tremendously in Q1 2023, outstripping Q4 2022 volume by 397% and surpassing all of 2022 volume by 310%.

Each quarter, Cofense Intelligence has analyzed credential phishing emails that reaches user environments protected by SEGs. Throughout Q1, Cofense Intelligence observed several changes within the phishing threat landscape. This includes changes in threat actor's tactics, techniques, and procedures (TTPs), as well as data trends such as volume. In addition, Cofense Intelligence Strategic Analyses gave readers more insight into credential phishing, such as abuse to OneNote, how threat actors have specifically tailored subdomains to their targets, and that phishing URLs are four times more likely than phishing attachments to reach users. Malware tactics and techniques were also covered, as we provided a deep dive into the Agent Tesla keylogger, which is consistently one of the top malware families by volume. Another topic covered was the rising abuse of Telegram bots for credential exfiltration in both credential phishing and malware campaigns.

Credential Phishing Activity

Credential phishing volume for this quarter was volatile but increased significantly throughout the quarter by 527%. Q1 2023 had an approximately 40% increase in credential phishing volume compared to that of Q1 2022. The highest credential phishing volume in Q1 occurred during the month of March, with a surge that greatly outpaced the earlier months.

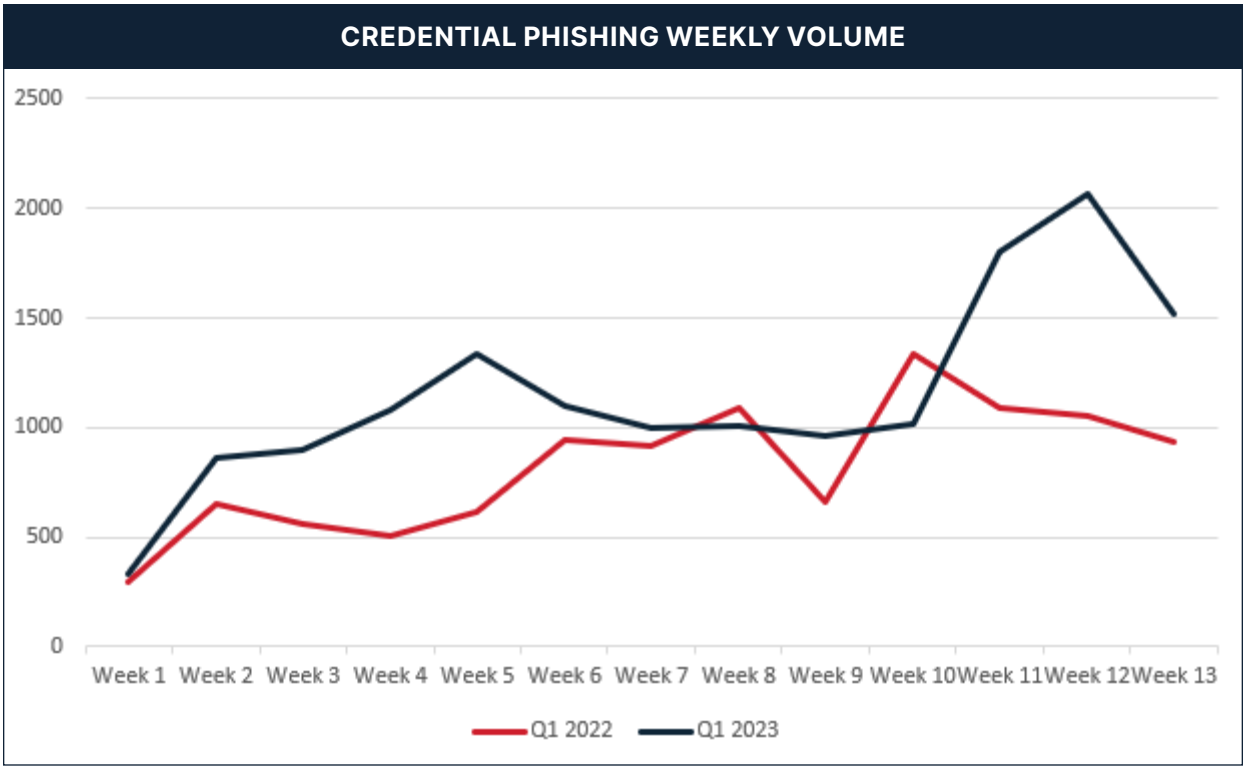


Figure 1: Comparison of volume of credential phishing emails observed in Q1 2022 and Q1 2023.

Credential phishing volume for this quarter was volatile but increased significantly throughout the quarter by 527%.

Prevalent Malware in Q1

The five most common malware families for each malware type remained consistent from Q4 to Q1. The only change was that there was a higher volume of Remote Access Trojans (RATs) than Bankers this quarter.

TOP FIVE MALWARE TYPES	TOP FAMILY IN TYPE
Loader	Emotet
Keylogger	Agent Tesla
Information Stealer	FormBook
Remote Access Trojan	Remcos RAT
Banker	QakBot

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

The overall volume of malware sent throughout each quarter is heavily influenced by the high volume of emails that Emotet disseminates. This leads to a continuous dominance by loaders compared to other malware types. The top malware families and types remained mostly consistent to that of Q4. However, the most significant change in malware types was a 38% increase in the use of keyloggers. The top malware family for each malware type remained consistent from Q4. RATs succeeded Bankers in volume for this quarter, but both types had relatively similar volumes to each other. QakBot was very active throughout Q4 before going inactive for the first half of Q1, which led to a lower banker volume than the previous quarter. The loader malware type continued to hold the top position despite a 44% decrease in volume.

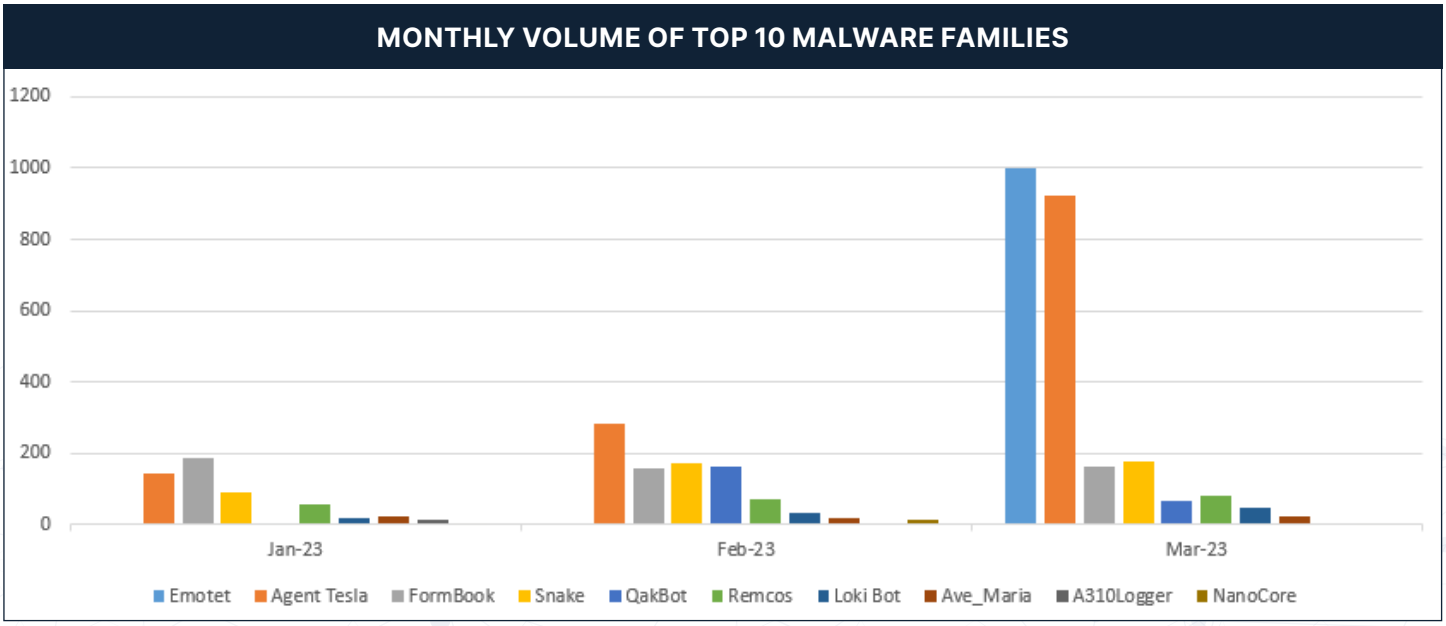


Figure 2: Monthly volume of top ten malware families in each type (this chart is capped for legibility, and does not show the full height of Emotet volume in March)

Prevalent Malware in Q1

Throughout all three months we see a pattern in malware activity. This pattern begins in January, where Agent Tesla led in volume, followed by FormBook and Remcos, respectively. During the rest of the Q1, those three families consistently fall in that order, although they are also joined by Emotet and Qakbot. Emotet was quiet the first two months of the quarter yet made its return in March. Although Emotet was not sending, on January 17th Cofense researchers observed .dll file updates being sent to the Emotet epochs, which was reported on in a Flash Alert. When active, Emotet's dissemination capacity far outpaces that of the other malware families. Qakbot on the other hand, was the most successful during Q1 2023. Qakbot was discovered in inboxes 185% more often than Emotet, despite only being active during February and March.

Qakbot was discovered in inboxes 185% more often than Emotet, despite only being active during February and March.

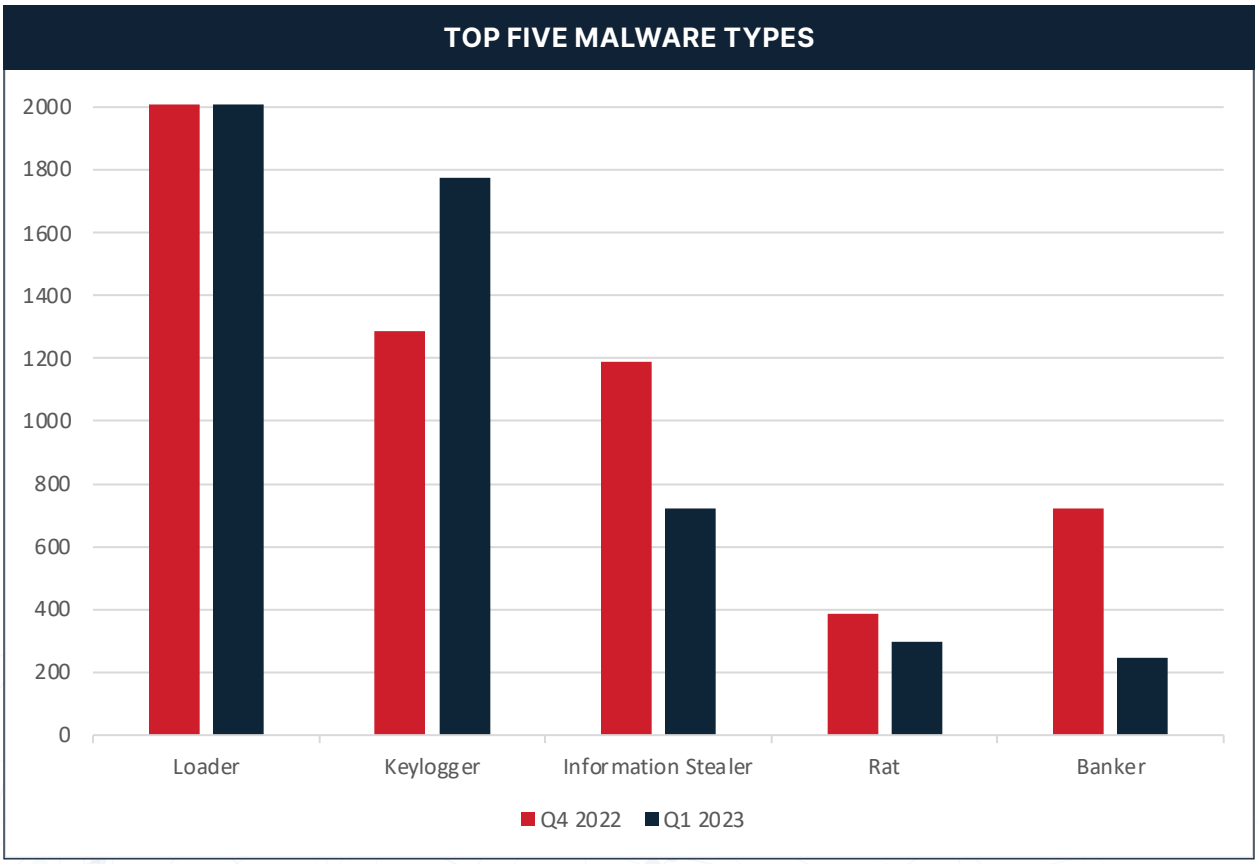


Figure 3: Top five malware types in Q4 2022 and Q1 2023, by volume of emails. The maximum value for this chart has been capped and does not show the full proportion of the Loader malware type.

2023 Annual Report Projections – Web3 Technologies and Telegram Bots

In the **Cofense 2023 Annual State of Email Security Report**, we highlighted major growth in several phishing tactics seen in 2022. Cofense Intelligence Analysts identified continued trends from 2022 that includes:

- Telegram bots used as exfiltration destinations for stolen credentials
- Malicious use of Web3 technologies as a link-crafting tool for phishing campaigns

Telegram bot API usage continued to rise tremendously in Q1, already surpassing all of 2022 by 310%.

When compared to the previous year, both of these tactics saw a substantial increase in usage in phishing campaigns. This trend has continued into Q1 2023 and doesn't appear to be going away anytime soon. Telegram bot increases 397% for Q1 compared to Q4. Further, Telegram bot API usage continued to rise tremendously in Q1, already surpassing all of 2022 by 310%. The use of Telegram bots has already reached new highs this quarter compared to all of last year and is expected to hold these levels or even go beyond. In Figure 4, we saw substantial percent increases quarter over quarter, and reaching new highs of 397% in Q1 2023.

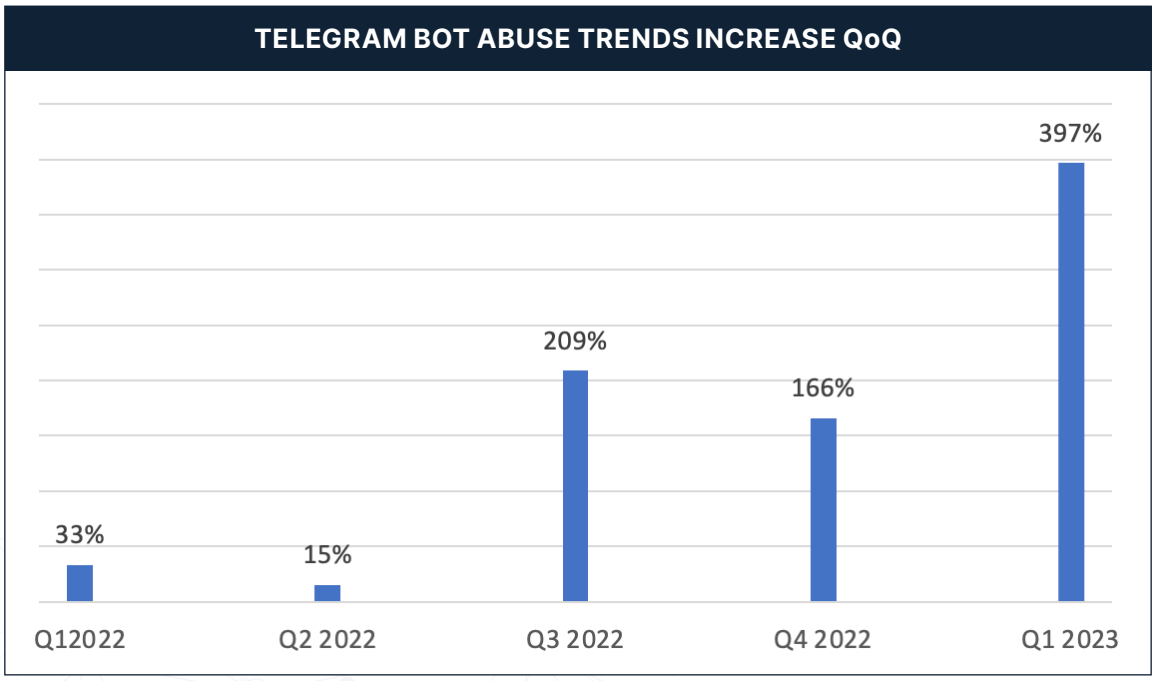


Figure 4: Shows the increases in Telegram Bots Abuse by quarter.

Web3 Technologies have seen large spikes in 2022. The abuse of Web3 technologies has increased 353% compared to Q1 of 2022. The use of Web3 technologies has maintained the high volume we saw towards the end of 2022, which is significantly higher than what we saw in Q1 2022.

The abuse of Web3 technologies has increased 353% compared to Q1 of 2022.

Delivery Mechanism Rundown

In Q1, Cofense Intelligence saw threat actors use more sophisticated tactics by introducing a new delivery mechanism within their phishing emails. The use of OneNote files as a delivery mechanism took off this quarter, replacing Office macros as a top delivery mechanism while adding OLE Package and WSF Downloader respectively as they are used within the new infection chain. The Top Malware Delivery Mechanisms chart for Q1 includes two new delivery mechanisms heavily used in this quarter that were not seen in previous quarters. These two mechanisms, OLE Packages and WSF Downloader, are largely due to a new malware delivery method used primarily by threat actors operating Emotet and QakBot malware. The use of OneNote files (.ONE files), which are referred to as OLE Packages, contain an encoded Windows Script File (WSF) that downloads and runs the malware. This new combination of delivery mechanisms quickly moved to the top of malware delivery mechanisms due to the high volume of Emotet and QakBot emails that are disseminated into the wild. This change in tactics resulted in malicious Office macros and DotNETLoader not making it as a top delivery mechanism for this quarter, but they were both still very relevant across the phishing threat landscape. When Emotet is excluded, CVE-2017-11882 continues to be the top delivery mechanism for other malware families. CVE-2017-11882 is primarily used to deliver Agent Tesla keylogger, but it is extremely common to see it delivering other malware families as well.

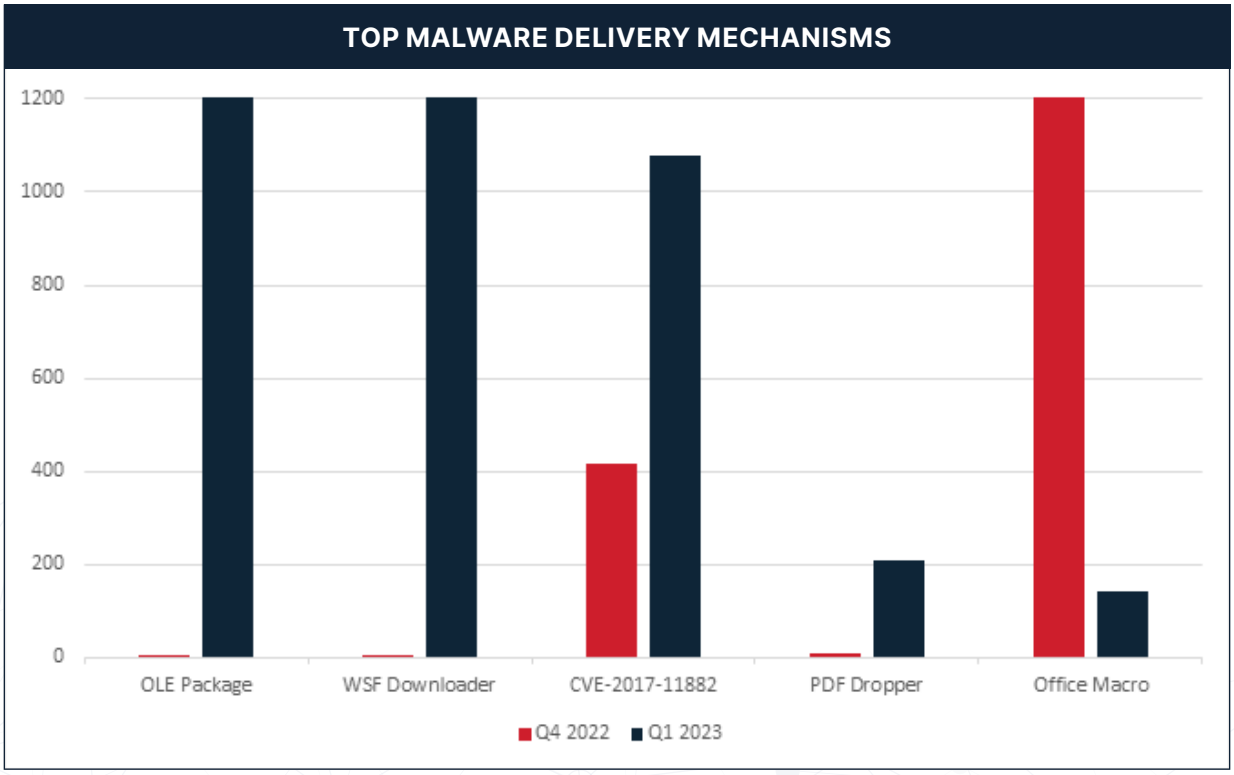


Figure 5: Top Malware Delivery Mechanisms by Email Volume in Q4 2022 and Q1 2023. The maximum values for the chart are capped, and do not show the full volume of mechanisms associated with Emotet.

Domains and TLDs Used in Credential Phishing

Each quarter, Cofense Intelligence has analyzed credential phishing emails that reached users in environments protected by SEGs, to identify the top-level domains (TLDs) and individual domain names that were most prominent. 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 for credential phishing threat actors.

RANK	Q4 2022	Q1 2023
1	Sharepoint.com	Amazonaws.com
2	Adobe.com	Sharepoint.com
3	Google.com	Google.com
4	Microsoft.com	Backblazeb2.com
5	Box.com	Microsoft.com
6	Canva.com	Dropbox.com
7	Myhuaweicloud.com	Adobe.com
8	Herokuapp.com	Youtube.com
9	amazonaws.com	Box.com
10	embluemail.com	Myportfolio.com

Table 2: Q4 2022 and Q1 2023 ten most common .com domains used in credential phishing campaigns.

Compared to Q4, this quarter saw several changes amongst the top ten most common .com domains. Sharepoint was bumped down from the top by Amazonaws, however Google remained in the top three. Several .com domains were replaced in the list by Backblazeb2, Dropbox, Youtube, and Myportfolio. These new additions replaced Canva, Myhuaweicloud, Heokuapp, and Embluemail. Overall, these changes are not surprising as all of these .com domains are popular for threat actors to use and abuse, and the volume often fluctuates. However, Youtube making the list was unexpected compared to the others. Most of the .com domains that make up this list are trusted platforms abused to host phishing sites, but lately Youtube's domain has become a popular location for threat actors to abuse an open redirect to redirect to their phishing sites.

The URLs analyzed are split into two categories: Stage 1 and Stage 2. Stage 1 URLs are embedded in the phishing emails and are the first step in the infection chain, whereas Stage 2 URLs can only be reached if the user acts with the embedded URL in Stage 1. When both stages are combined, the order and makeup of the top ten TLDs varied compared to that seen in Q4. Domains using the .com TLD accounted for approximately 48.13% of the total, a decrease from Q4. The .ru TLD had an approximate 7.5% increase compared to the previous quarter, even overtaking the .net TLD, which is an unexpected change for this quarter. The .ms and .xyz TLDs were replaced by the .me and .online TLDs, both of which saw a significant increase compared to the previous quarter.

Domains and TLDs Used in Credential Phishing

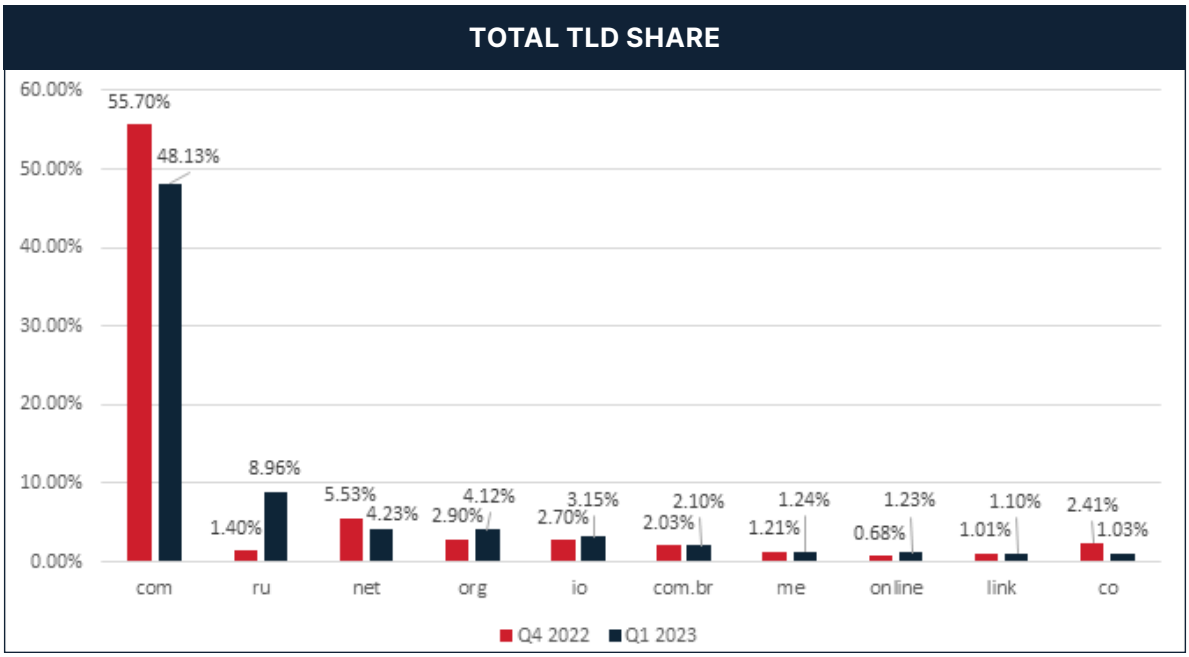


Figure 6: Top 10 TLDs in Q4 2022 compared with Q1 2023.

The Top ten TLDs specific to Stage 1 URLs only saw minor changes from those of Q4. The main changes were in volume as only 2 of the TLDs were replaced out of the top ten. The TLDs .me and .ru replaced .com.br and .app from Q4. The .com TLD continues to be the top TLD by a significant margin and increased by approximately 3% this quarter. While .com increased in volume, other TLDs like .net, .co, and .ms saw a decrease for this quarter.

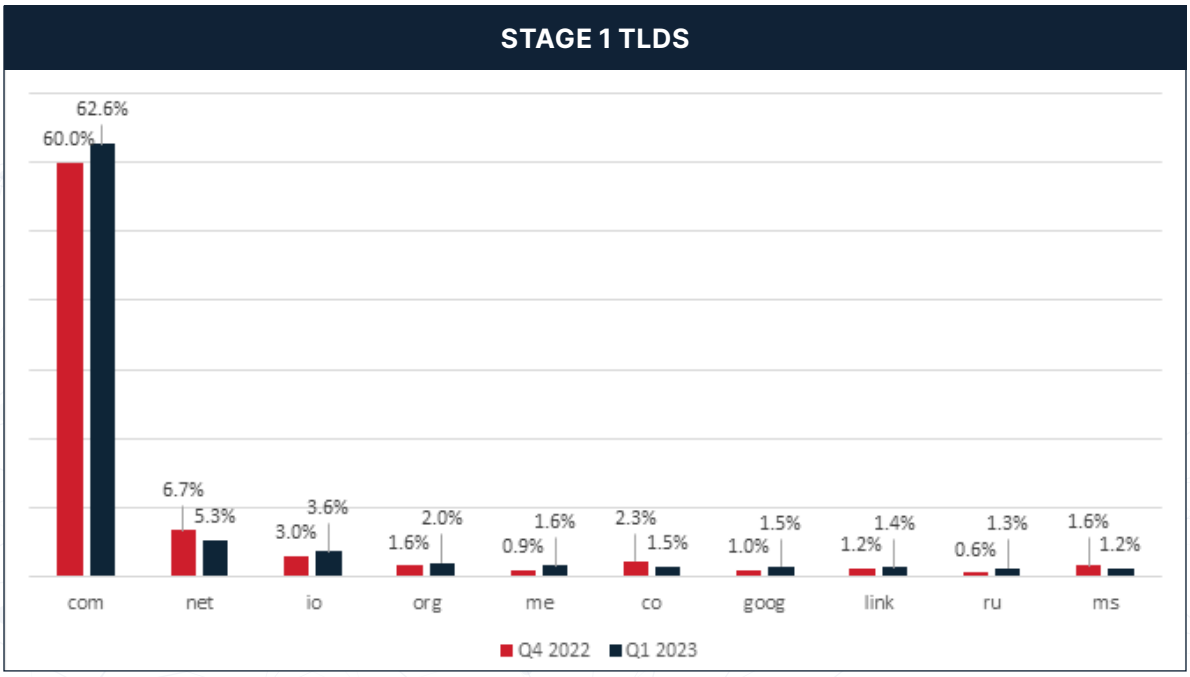


Figure 7: Stage 1 TLDs in Q4 2022 compared with Q1 2023.

Domains and TLDs Used in Credential Phishing

The top ten Stage 2 TLDs for this quarter saw multiple changes within the top ten TLDs. The TLDs .online, .tk, and .me replaced .xyz, .click, and .co as top TLDs for this quarter. The .com TLD dropped by approximately 6%, yet this was not the only TLD that dropped in volume. These other TLDs include .org, .com.br, and .me. There was a drastic increase in the use of .ru the TLD as a Stage 2 TLD for this quarter, jumping almost 10% compared to Q4.

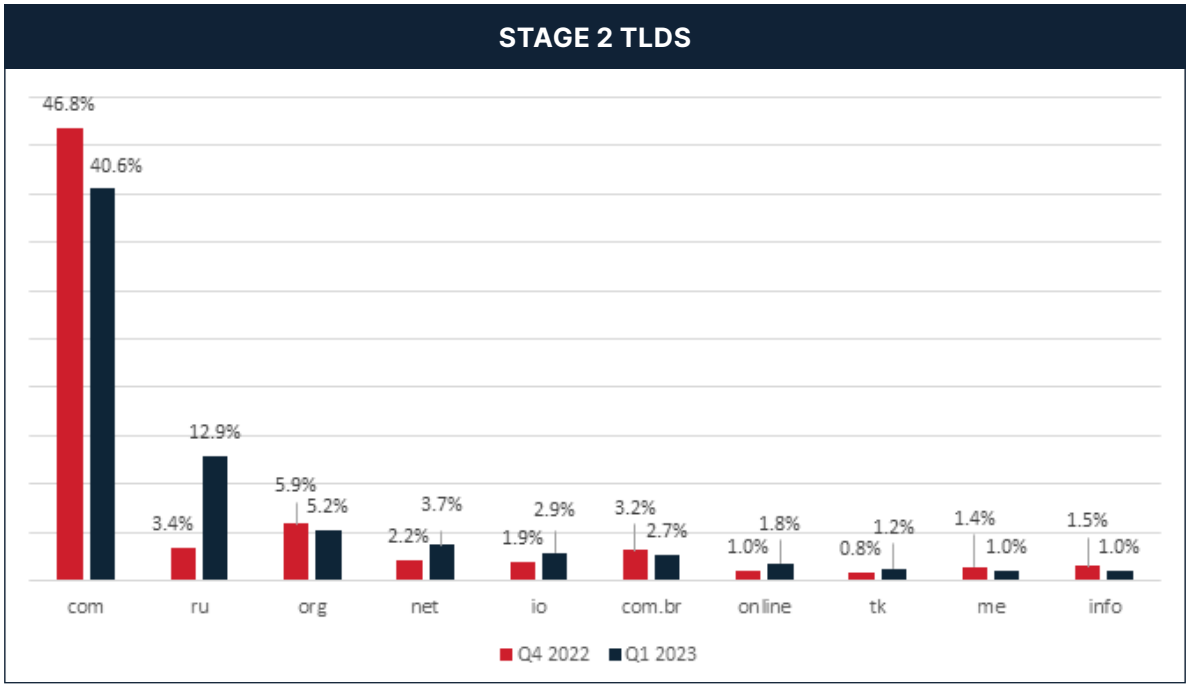
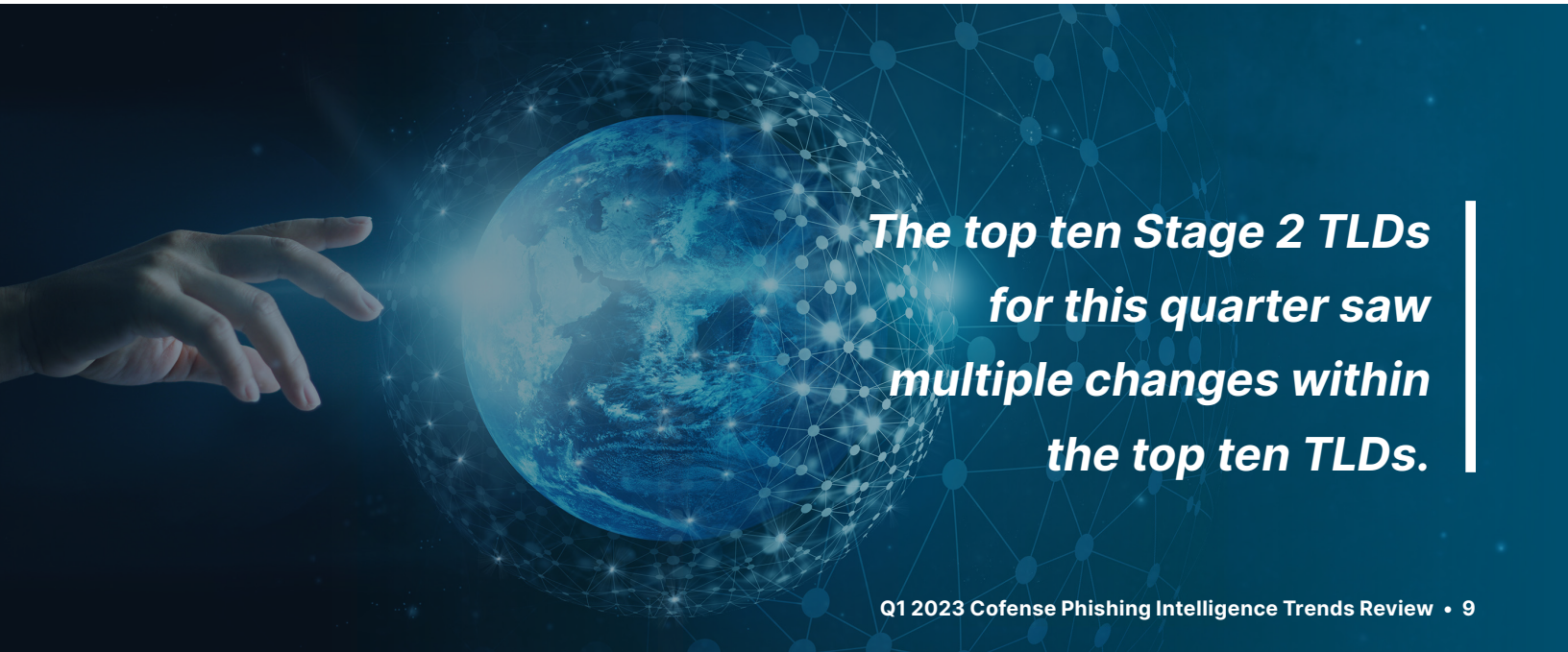


Figure 8: Stage 1 TLDs in Q4 2022 compared with Q1 2023.



The top ten Stage 2 TLDs for this quarter saw multiple changes within the top ten TLDs.

File Extensions of Attachments

Our quarterly analysis revealed threat actors are being consistent from Q4 to Q1 with the use of filename extensions on email attachments that reached users in SEG-protected environments. Out of the top ten file extensions, only one new file extension made the chart, and there was only one other change in the order. The .shtm file extension replaced .rar as a top ten for this quarter. The positions for the other file extensions remained the same except that the .shtml file extension passed .docx in volume. The overall HTML attachment usage dropped compared to the last quarter, with just over 38% for this quarter which is less than the use of .pdf attachments. The file extensions of .pdf, .html, .htm, .shtml, and increasingly .xlsx are typically used for credential phishing. File extensions that contain links to credential phishing pages include .pdf and .xlsx, while .html, .htm, and .shtml will either present a credential phishing page when opened or automatically redirect to one. The .zip file extension is currently the only archive in the top ten, as it is still a popular way of delivering a wide variety of malware and phishing resources. Several Office files can be seen across the list such as .doc and .xls, these are most associated with CVE-2017-11882, a very common delivery mechanism for delivering malware.

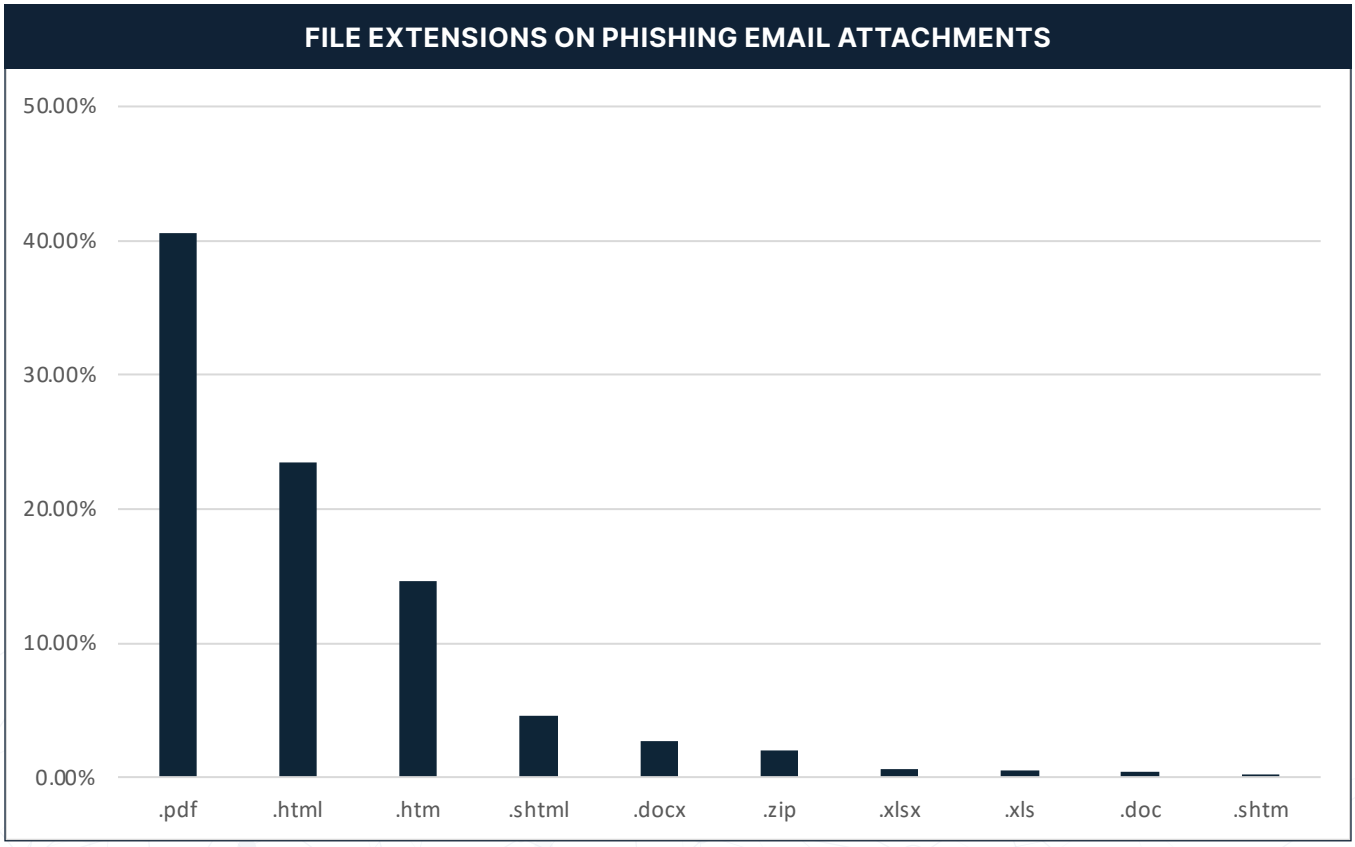


Figure 9: Top 10 most common attachment file extensions found in environments protected by SEGs.

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. For this quarter, four out of the top five locations were the same as last quarter but in a slightly different order. France made the top five list replacing Australia in the fifth spot. The United States remains the top location with a very small change in percentage. Great Britain and Canada changed positions compared to Q4. Great Britain had a substantial increase of nearly 6% in volume, double the previous quarter.

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 2022		Q1 2023	
Country	**Percentage**	**Country**	**Percentage**
United States	68.90%	United States	68.60%
Great Britain	4.40%	Great Britain	10.30%
Canada	7.83%	Canada	6.97%
Germany	3.99%	Germany	2.95%
France	1.60%	France	1.61%

Table 3: Q4 2022 and Q1 2023 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.

Projections for Q2 2023 and Beyond

Microsoft Updates to OneNote Files will Impact the Phishing Threat Landscape

Microsoft has announced that they will implement new security measures within OneNote files to help prevent the spread of advanced malware families like Emotet and QakBot that have taken advantage of these files. The announcement mentions adding a notification to alert users when a OneNote file is used to download a file that is deemed malicious, adding that they will be blocking files with known malicious file extensions. The list of file extensions can be found **here**. The file extension list contains .wsf and .hta, both are file extensions that we have seen within QakBot and Emotet campaigns throughout this quarter. These changes are expected to roll out towards the end of April, and although these changes seem to be an overall benefit, we can almost certainly expect malware families like Emotet and QakBot to change their delivery tactics if these updates impact their phishing campaigns. We saw this same scenario last year when Microsoft announced the default disabling of Macros, which led to Emotet, QakBot, and Iced-ID exploring alternative techniques.

Open Redirects to Further Spread Across Credential Phishing Campaigns

Threat actors have been taking advantage of benign URLs hosted on legitimate domains and hiding phishing URLs within them. This capability is not new but has become a popular tactic for credential phishing threat actors. URLs can contain information that tells a website to redirect the visitor to a new location. Threat actors are able to take advantage of this by abusing websites designed to allow users to redirect web traffic, and especially those that contain open redirect vulnerabilities. Phishing campaigns abusing these open redirects continue to successfully bypass secure email gateways (SEGs) and reach intended targets. As we have seen many times before, more threat actors adopt tactics once they have proven to be successful.

With Summer Months Comes Summer Volume

Compared to Q4 2022, this quarter saw an overall decrease in volume. The volume within the phishing threat landscape is often heavily swayed by malware families like Emotet that go inactive for periods of times, but when active disseminate a large number of emails. Emotet aside, during each of the past three years the overall volume from Q2 has surpassed that of Q1. If this trend continues, we can expect to see a similar occurrence this year, with an overall increase in phishing volume as we enter the summer months.

Projections for Q2 2023 and Beyond

The Fight Against Ransomware

In March, the FBI issued their 2022 IC3 report that states that phishing email is the top crime for ransomware that targets organizations around the world. Phishing emails has been the top crime on the FBI's list for 2 years now in a row. It is important to look upstream at the chain of events that led to the ransomware and determine the payloads delivered within the email. Cofense Intelligence analyzes these threats at great lengths and provides unique human-vetted expertise and analysis with actionable insights. We treat each malware infection as a potential vector for future ransomware attacks, reverse engineer the payloads and trace the steps that led to the infection to enable our customers to determine the flaws in their defenses and prevent phishing attacks.

In Q1, we saw the continuation of the takedown of ransomware gangs such as the Hive in Jan, but then saw an uptick in phishing threats in Feb. Despite the takedown measures in early of the quarter, we don't see these threats taking a break as seen in the volumes in Q1. As long as we continue to see a rise in phishing threats as threat actors get more sophisticated, we will see a continuation of these ransomware attacks 2023 and beyond.

Finished Intelligence: Topics and Trends

Throughout Q1 2023, Cofense Intelligence performed in-depth analyses on various threats to provide readers with a strategic understanding of the phishing threat landscape and notify readers of sudden or upcoming developments. Below, we summarize finished intelligence reports that Cofense Intelligence produced on notable topics and trends identified during this period.

Strategic Analysis – How Threat Actors Embed Files in OneNote Documents

Beginning in December 2022, Microsoft Office OneNote (.one) files have been used in malicious emails to deliver multiple malware families, including the well-known QakBot and Emotet. Threat actors have likely been experimenting with .one files as an alternative to Office macros, which as of this report have become less common. Word and Excel documents with Office macros were some of the most popular methods for delivering malware before Microsoft disabled Office macros by default from untrusted online sources in April 2022. Now that Office macros are disabled by default, along with CVE-2017-11882 (another extremely common delivery mechanism) being around long enough for many organizations to patch, threat actors have been looking for alternatives. This is particularly the case with QakBot, which has been delivered by a variety of experimental mechanisms since Office macros in documents from the internet were initially disabled by Microsoft.

Flash Alert – Emotet Sending Malicious Emails After Three-Month Hiatus

On Mar 7th, after several months of inactivity, the Emotet botnet resumed email activity. Malicious emails seem to be replying to already existing email chains, with the addition of an attached .zip file, which is not password protected. The attached .zip files were finance and invoice themed.

Strategic Analysis – Tailored Subdomains in Credential Phishing Campaigns

In 2022, over two thirds of campaigns reported to the Cofense Phishing Defense center involved URLs with subdomains. In about 5% of campaigns, threat actors chose subdomains tailored specifically to the targeted organization or user. Tailored subdomains may be more convincing than generic phishing URLs, but fortunately they are also likely to be more detectable. In this report, we explore credential phishing threat actors' use of subdomains in general and tailored subdomains, as well as methods network defenders can use to counteract them.

Strategic Analysis – URLs 4X More Likely than Phishing Attachments to Reach Users

The first steps in traditional phishing emails have remained the same for decades; the email will contain either a malicious URL or attachment. In recent years, however, URLs embedded in phishing emails as an initial means of engaging the intended victim have reached those intended victims at a much higher rate than attachments used for the same purpose. Our data from 2022 shows that the dominance of URLs over attachments continued throughout the year for several reasons, including abusable trusted domains, free services on the web that provide phishing infrastructure, and the evasive effects of redirects.

Finished Intelligence: Topics and Trends

Strategic Analysis – Agent Tesla Keylogger – Phishing Malware Baseline

Agent Tesla is a keylogger written in .NET. It can monitor keystrokes, take screenshots, steal passwords from a variety of applications, and exfiltrate this data back to the threat actor through common protocols. Though it has been regularly used by threat actors over the past eight years, its usage soared in late 2020 and early 2021. Aside from Emotet, we observed Agent Tesla being sent at a higher volume than any other malware family in Q1 2023. Due to its relatively low price compared to other malware families, and the high functionality it possesses, we have no reason to believe it will be going away any time soon.

Flash Alert – Botnet Updates Suggest Emotet Activity on the Horizon

On January 17th, after nearly a two-month hiatus, Cofense researchers observed new activity in Emotet epochs 4 and 5. Emotet uses several botnets called epochs, each of which are assigned their own command and control (C2) infrastructure. Prior to this, Cofense observed .dll file updates being sent to each epoch, almost certainly configuring bots to contact new infrastructure. If activity follows previous Emotet trends, these epochs will likely begin sending malicious emails again in the coming weeks, if not days.

Strategic Analysis – Rising Abuse of Telegram Bots for Credential Exfiltration

Among phishing emails reaching inboxes over the course of 2022, the utilization of Telegram bots as exfiltration destinations for phished information increased gradually but significantly, resulting in a year-over-year increase of more than 800% between 2021 and 2022. The increase is largely associated with the now popular tactic of using HTML attachments as delivery mechanisms in credential phishing. While Telegram bots being used by threat actors to exfiltrate information is not new, it has not been commonly known for its use in credential phishing. Telegram bots have become a popular choice for threat actors, since they are low-cost or free, as well as a single-pane-of-glass solution. Threat actors appreciate the ease of setting up bots in a private or group chat, the bots' compatibility with a wide range of programming languages, and the ease of integration into malicious mediums such as malware or credential phishing kits. Coupling the ease of Telegram bot setup and use with the popular and successful tactic of attaching an HTML credential phishing file to an email, a threat actor can quickly and efficiently reach inboxes while exfiltrating credentials to a single point, using an often-trusted service.