Q4 2022

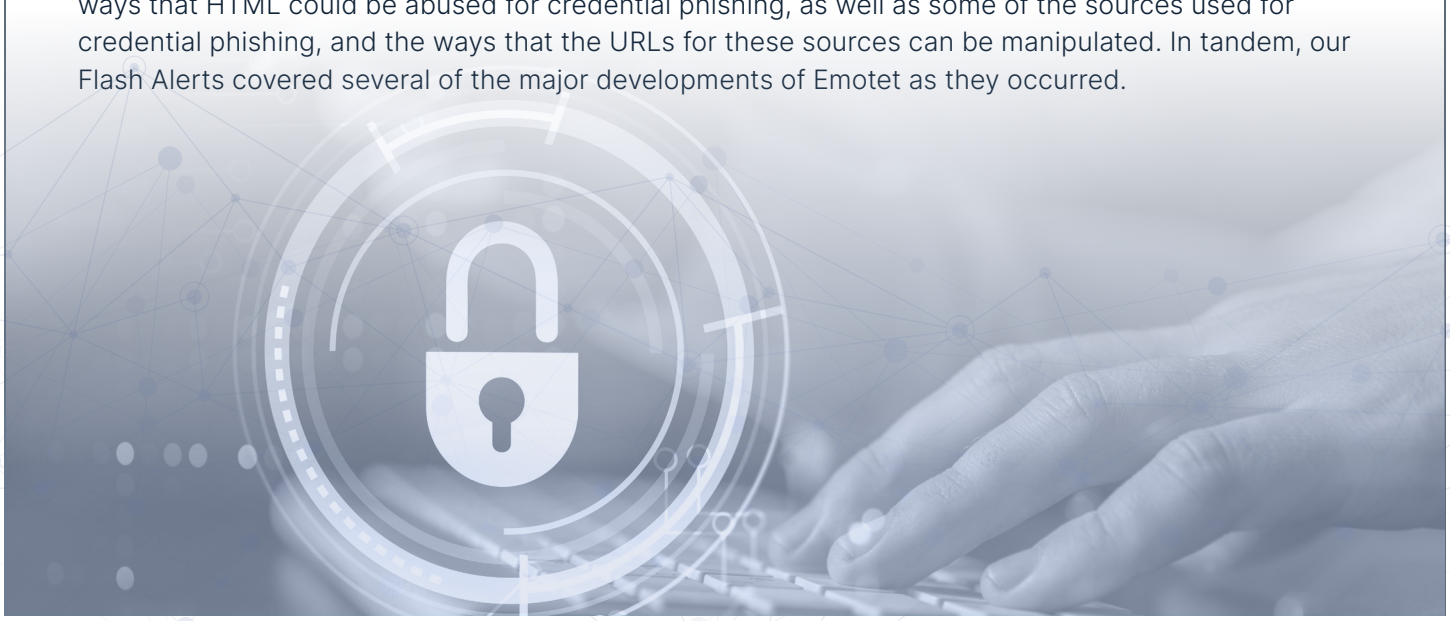
Cofense Phishing Intelligence Trends Review

Executive Summary

The phishing threat landscape in Q4 2022 saw a number of small scale but impactful changes, but less of the sweeping changes seen in previous quarters. As usual, several of the significant changes in Q4 were due to Emotet. This includes a phishing volume spike in November, the prominence of Office macros as a delivery trend, and the continued dominance of the Loader malware type. There was little change within malware types other than RAT and Banker swapping places, but both had volume low enough to make the change negligible. The most common TLDs used in evasive credential phishing stayed mostly the same, with the only activities of note being that the stage 2 TLD .ru went from not being in the top 10 in Q3 to taking 3rd place in Q4. The other notable change is that Microsoft reappeared in the top 10 .com domains, likely due to an increase in phishing campaigns using services such as customervoice[.]microsoft[.]com to link to credential phishing pages. Command and control server locations showed little overall change, but did see an increased concentration of sources within the top 5 with lower overall volume for less common locations. Our previous highlighting of QakBot continued to be accurate, as Q4 saw several improvements in QakBot's delivery.

In Q4, Cofense observed several expected events and trends, as well as some surprising new ones. Some of the expected ones, such as QakBot's forays into new techniques and other malware families using the same HTML delivery method as QakBot, were predicted in our last quarterly report. Although the timing of Emotet's spikes can never be predicted, we anticipated a return to activity was possible in Q4. However, Emotet's high-volume return in November was surprisingly brief. A separate unexpected trend was uncovered in our Strategic Analysis Report on the use of Web3 technology for evasive credential phishing. While the use of certain Web3 technologies was evident in credential phishing campaigns we were processing, our study showed that overall use between multiple technologies had surprisingly increased by 482% from Q1 to Q3.

During this quarter, other Cofense Intelligence Strategic Analyses gave readers a look into the different ways that HTML could be abused for credential phishing, as well as some of the sources used for credential phishing, and the ways that the URLs for these sources can be manipulated. In tandem, our Flash Alerts covered several of the major developments of Emotet as they occurred.



Overall Activity

The overall observed phishing activity for this quarter was, on average, lower than that of Q3. The spike in volume in November due to Emotet was not enough to offset the typically low volume of phishing activity in December.

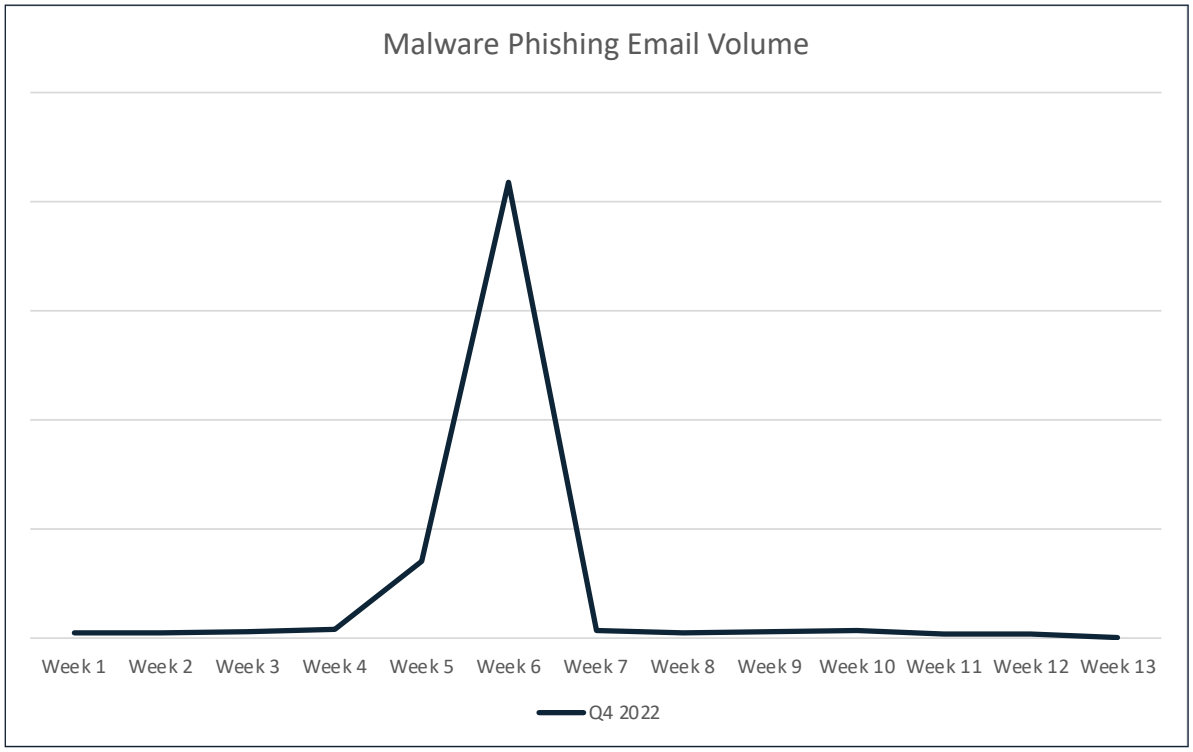


Figure 1: Volume of phishing emails delivering malware in Q4 2022.

Prevalent Malware in Q4

The five most common malware types and the top family for each type remained the same from Q3 to Q4, with only the ranking of Bankers and Remote Access Trojans swapping.

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

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

The top malware families within each malware type were consistent with Q3. Compared to Q3, the Information Stealer and Keylogger malware types saw a slight decrease in volume. The Loader malware type, led by Emotet, continued to maintain its top position but also saw a decrease in volume, due to Emotet being largely inactive. In contrast, the Banker malware type doubled in volume. In fact, the Banker malware type became more popular than the RAT malware type. This was due almost exclusively to an increase in QakBot campaigns over the course of Q4, which we predicted in our Q3 Phishing Intelligence Trends Report. These QakBot campaigns utilized either embedded URLs or attached HTML files.

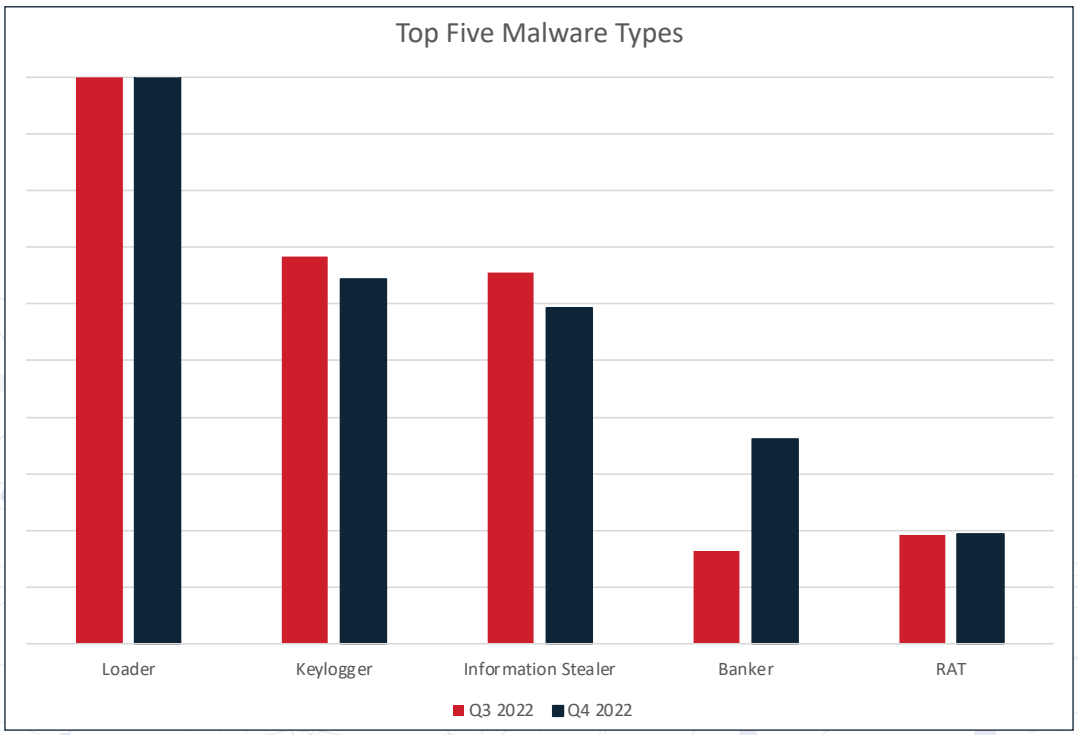


Figure 2: Top five malware types in Q3 2022 and Q4 2022, by volume of emails. The maximum value for this chart has been capped and does not show the full proportion of the Loader malware type.

Finished Intelligence: Topics and Trends

Throughout Q4 2022, Cofense Intelligence performed in-depth analysis on various threats to provide you with a strategic understanding of the phishing threat landscape and notify you of sudden or upcoming developments. Below, we summarize finished intelligence reports that Cofense Intelligence produced on notable topics and trends identified during this period.

Sudden Increase in Emotet C2 Traffic

Emotet botnet command and control traffic spiked on the morning of Oct. 10, 2022, following a code deployment. The intent of Emotet operators beyond this deployment was unclear. However, it was plausible that Emotet would begin sending malicious emails again following Oct. 10, after nearly three months of relative inactivity.

Emotet is Back and Reaching Inboxes

After being inactive since July of this year, Emotet went back to sending emails containing malicious documents. The Cofense Phishing Defense Center began to analyze new Emotet phishing emails reaching enterprise inboxes the morning of Nov. 2nd, with the first being received at 08:24 UTC.

Emotet Uses Fake Alert to Deceive Recipients Drops IcedID

Since resuming malicious email activity on Nov. 2, the Emotet botnet has largely been using attached malicious Excel spreadsheets to deliver Emotet malware. These malicious spreadsheets are currently displaying a fake Microsoft security banner within the first row of the spreadsheet, telling intended victims to place the document in a specific Microsoft Office Templates folder and open it from there. Successful Emotet infections have also been observed delivering IcedID as a secondary payload.

Cost-Effective Service Abused in HTML Credential Phishing

Threat actors have found a new cost-effective way to exfiltrate stolen credentials from malicious HTML files. Formspark is a service that allows users to submit information from sites and HTML forms for low cost, or even free. By abusing this service, threat actors can create phishing campaigns that use HTML files for a cheaper cost than usual, which is very appealing to most threat actors. This tactic can be seen when HTML files post credentials to the Formspark domain submit-form[.]com. The tactic of using submit-form URLs to exfiltrate stolen credentials is not new but has started to grow in popularity throughout the later months of 2022. Phishing emails using this tactic have been seen successfully reaching enterprise users in environments protected by secure email gateways (SEGs), and in a wide range of industry sectors.

Finished Intelligence: Topics and Trends

The Art of The URL Redirect

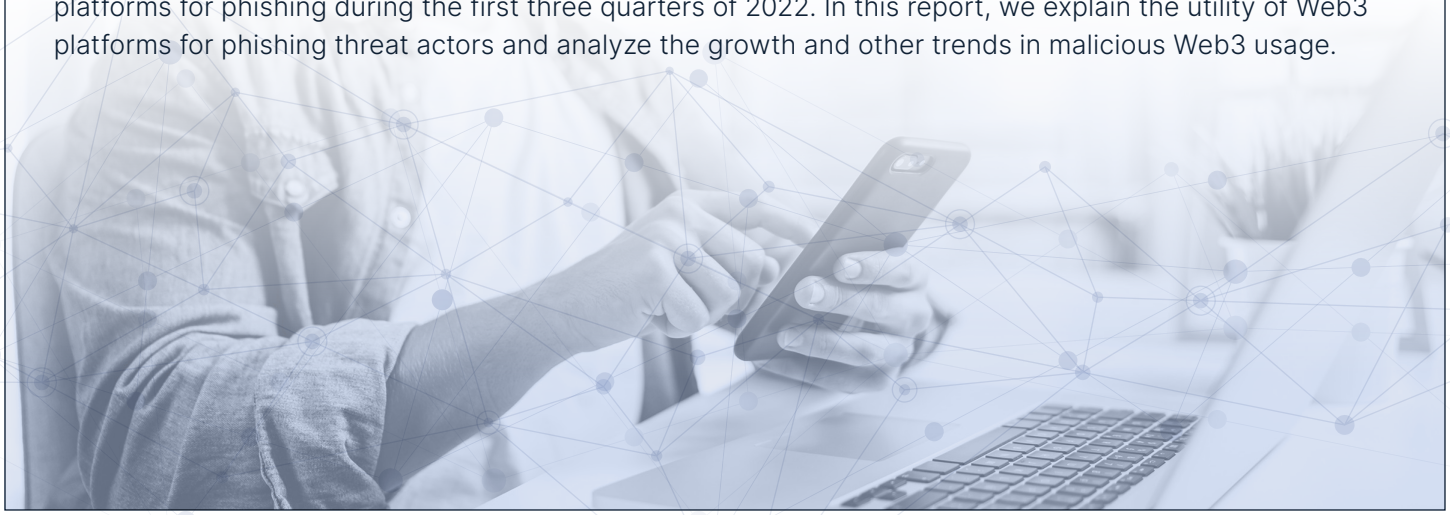
It is one thing to place a phishing URL directly in an email, and another thing to take a benign URL and hide a phishing URL inside it. URLs can contain information that tells a website to redirect the visitor to a new location. This capability is not new, and there are many legitimate uses for it. But as is often the case, threat actors use the capability for their own purposes. In this report, we review a recent campaign that relied entirely on URL redirects like this. This campaign illustrates how threat actors abuse legitimate websites designed to allow customers to redirect web traffic, and especially those that contain open redirect vulnerabilities. This abuse allows threat actors to bypass email security and makes it more likely for a phish to end up in the inbox.

HTML Smuggling of Malware and QakBot

HTML smuggling has been used for some time to deliver malware because it enables threat actors to hide malicious files inside of innocuous-looking HTML attachments. In recent times, it has been used in various ways to deliver the well-known malware QakBot. HTML smuggling takes advantage of how Secure Email Gateways (SEGs) treat attached HTML files, as opposed to attached document or .exe files, to deliver malware in a way that can bypass many SEGs. This is likely the reason that threat actors use complex versions of the technique in advanced phishing campaigns, as well as in the delivery of advanced malware, such as QakBot.

Abuse of Web3 Technology for Evasive Phishing Grows Massively in 2022

The term “Web3” refers to a set of technologies intended to decentralize common internet and computing activity. Proponents of decentralization tout the ability to host content without the need for large technology companies. In short, anybody can publish any content, avoiding technical problems like server management as well as legal problems or censorship. Unfortunately, these features make the technologies attractive to threat actors seeking easy, robust hosting for malicious content. Analyzing credential phishing campaigns that reached inboxes during the first three quarters of 2022, we found massive growth in the abuse of Web3 platforms for phishing during the first three quarters of 2022. In this report, we explain the utility of Web3 platforms for phishing threat actors and analyze the growth and other trends in malicious Web3 usage.



Delivery Mechanism Rundown

Compared to Q3, the Top Malware Delivery Mechanisms for Q4 saw little change. OfficeMacros, CVE-2017-11882, and DotNETLoaders remained in the top 3 with the only change being that CVE-2017-11882 swapped rankings with DotNETLoaders. Similar to last quarter, the top delivery mechanisms were heavily affected by Emotet. Specifically, OfficeMacros had a significant lead on all other delivery mechanisms. In this case, the top value of the chart is capped at roughly twice the highest value of other delivery mechanisms. In this quarter, OfficeMacros were used primarily to deliver Emotet, CVE-2017-11882 was primarily used to deliver Agent Tesla Keylogger, and DotNETLoaders were also primarily used to deliver Agent Tesla Keylogger. Although not a delivery mechanism itself, one of the interesting and increasingly popular ways that malware has been delivered this quarter is via .iso, .img, .vhd, and other similar archive files containing a .dll and a script file used to run the .dll.

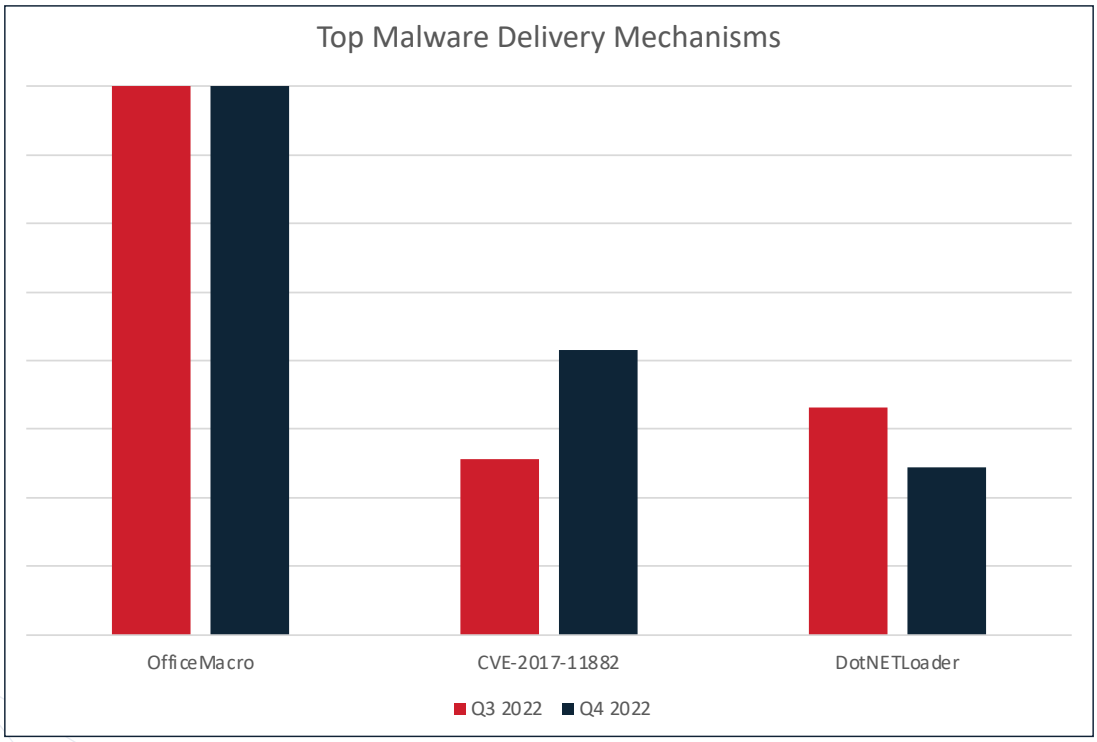


Figure 3: Top Malware Delivery Mechanisms by Email Volume in Q3 2022 and Q4 2022. Maximum values are capped at roughly twice the highest volume for other mechanisms.

TLDs and Domains Used in Credential Phishing

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

When both stages are combined, the order and makeup of the top 10 TLDs varied compared to that seen in Q3. Domains using the .com TLD accounted for approximately 56% of the total, a slight increase from Q3. The .net TLD decreased significantly from around 10% to around 5%. The new additions for this quarter were the .ru, .ms, and .link TLDs, while notable holdovers from Q3 include .com.br, .org, .io, .co, and .xyz.

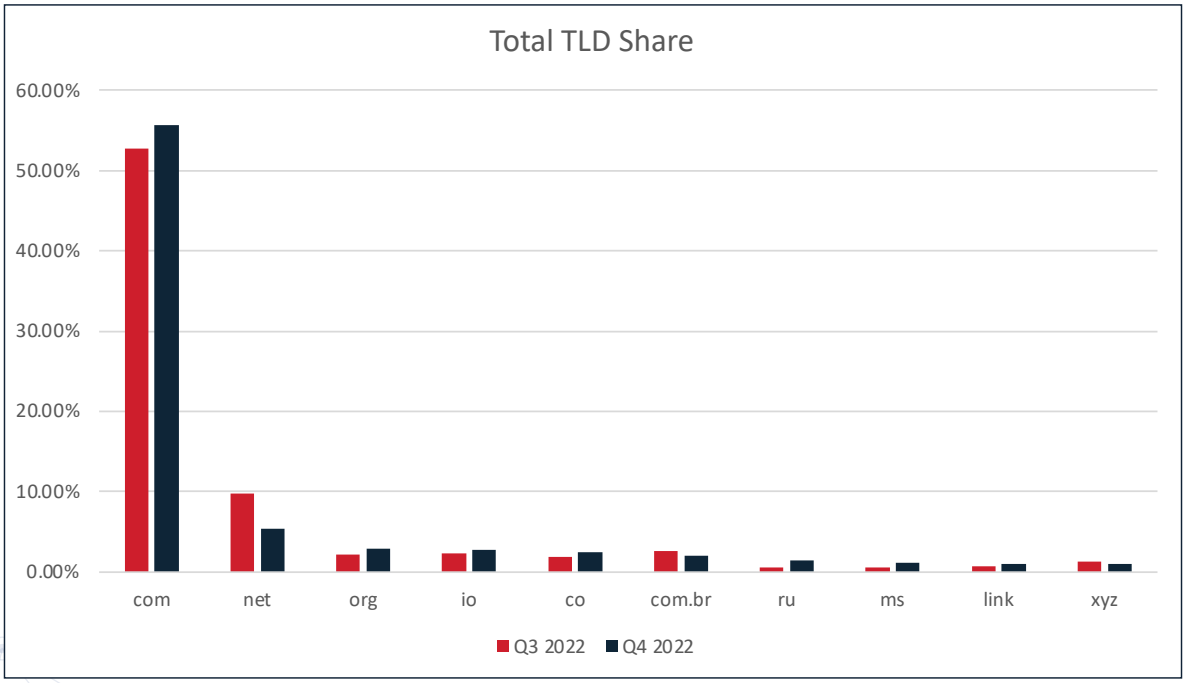


Figure 4: Top 10 TLDs in Q3 2022 compared with Q4 2022.

TLDs and Domains Used in Credential Phishing

The Top 10 TLDs specific to Stage 1 URLs changed significantly from those of Q3, with the main difference being changes in volume and the addition of 4 new TLDs. The TLDs .ms, .link, .app, and .goog replaced the lowest four of the Top 10 TLDs from Q3. The differences in volume were also notable, with .com increasing by 5%, and .net decreasing by 5% from Q3.

STAGE 1 TLD	Q4 2022	Q3 2022
com	59.95%	54.85%
net	6.70%	10.96%
io	3.03%	2.65%
co	2.27%	1.81%
org	1.62%	1.76%
ms	1.55%	0.72%
com.br	1.54%	2.49%
link	1.17%	0.76%
app	1.14%	0.87%
goog	1.01%	0.52%

Table 2: Stage 1 TLDs in Q3 2022 compared with Q4 2022.

The top 10 Stage 2 TLDs for this quarter saw multiple changes including within the top three. The .ru and .io TLDs returned from Q2 after being absent in Q3, with .ru taking third place. These, along with the .click and .info TLDs, replaced the .page, .online, .live and .co.uk TLDs from Q3.

STAGE 2 TLD	Q4 2022	Q3 2022
com	46.79%	45.60%
org	5.92%	4.04%
ru	3.42%	0.99%
com.br	3.19%	3.53%
co	2.76%	2.35%
xyz	2.39%	3.87%
net	2.16%	4.70%
io	1.90%	0.67%
click	1.70%	0.09%
info	1.54%	0.79%

Table 3: Stage 2 TLDs in Q3 2022 compared with Q4 2022.

TLDs and Domains Used in Credential Phishing

The 10 most common .com domains used in both stages combined are represented below. Of the domains, several trusted cloud platforms can be identified, showing a continued use for credential phishing threat actors.

Compared to the previous quarter, the top 10 most common .com domains had multiple changes. Sharepoint became the most common domain, more than doubling Adobe.com, which had been the leader for several quarters. Evernote, Myportfolio, Petanitest, Axshare, and Clickfunnels were replaced by Box, Huawei Cloud, emBlue, Microsoft, and Herokuapp. While the majority of these changes were not unusual, Evernote completely disappeared from the list and was replaced by Microsoft.com, which rose due the usage of Microsoft.com subdomains such as customervoice[.]microsoft[.]com to redirect to credential phishing pages.

File Extensions of Attachments

Our quarterly analysis revealed a few changes from Q3 to Q4 in the distribution of filename extensions on email attachments that reached users in SEG-protected environments. The top 3 file extensions (.pdf, .html, and .htm) remained the same, but beyond that, almost all other extensions shifted position. The file extensions .shtm and .rpmsg completely disappeared from the top 10 whereas .xls and .rar reappeared. For the first time in quite a while, .pdf no longer made up more than .htm and .html files combined, as overall HTML attachment usage rose to 44.97% of the total. The file extensions of .pdf, .html, .htm, .shtml, and increasingly .xlsx are typically used for credential phishing. .pdf and .xlsx files will contain links to credential phishing pages while .html, .htm, and .shtml will either present a credential phishing page when opened or automatically redirect to one. The archives currently in the top 10 (.zip and .rar) are used to deliver such a wide variety of malware and phishing that it is impossible to narrow them down to a single most commonly delivered threat. The remaining file extensions in the top 10 (.doc and .xls) are most often used to deliver malware via CVE-2017-11882 but have also been seen delivering small volumes of credential phishing via embedded URLs.

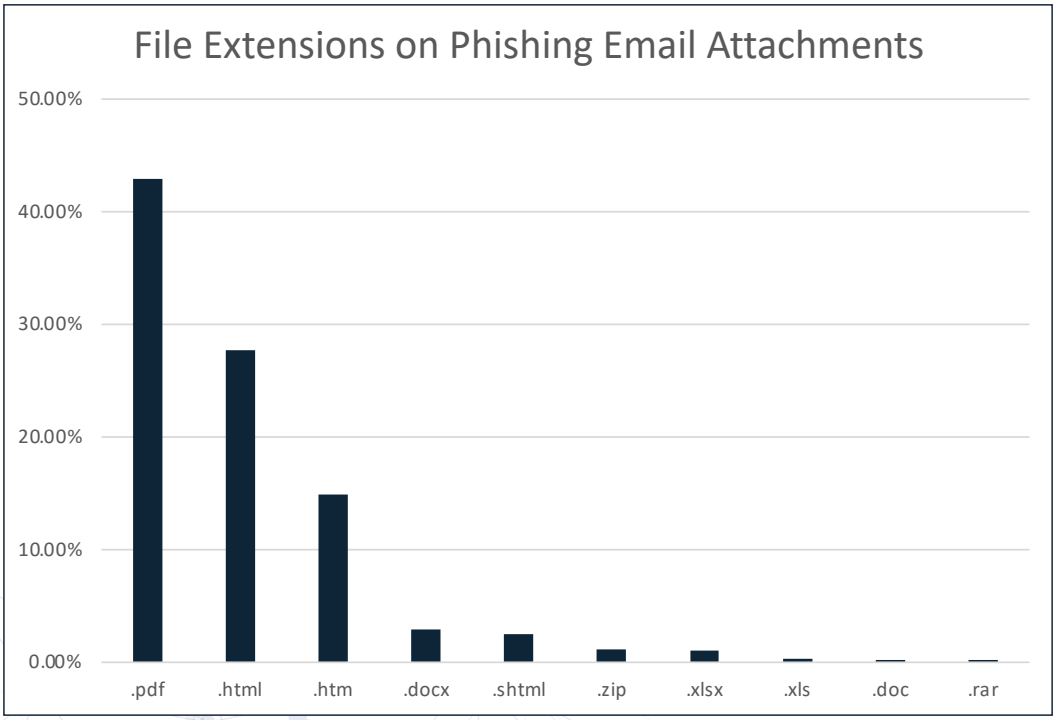


Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs

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, and often receive information and exfiltrated data from infected hosts. In this quarter, four out of the top five locations were the same as last quarter but in a slightly different order. The only change in country was that Hong Kong was replaced by Australia. An unusual and interesting change for this quarter was that 2nd through 4th place had almost double the percentage of sources from the last several quarters. It is unusual for any country other than the United States to have more than 5% share and even more rare for multiple countries to have more than 3% share. *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.*

Q3 2022		Q4 2022	
Country	**Percentage**	**Country**	**Percentage**
United States	60.78%	United States	68.90%
Germany	4.91%	Canada	7.83%
Canada	2.62%	Great Britain	4.40%
Hong Kong	2.60%	Germany	3.99%
Great Britain	2.12%	Australia	2.48%

Table 4: Q3 2022 and Q4 2022 percentages for C2 sources by IP address geolocation

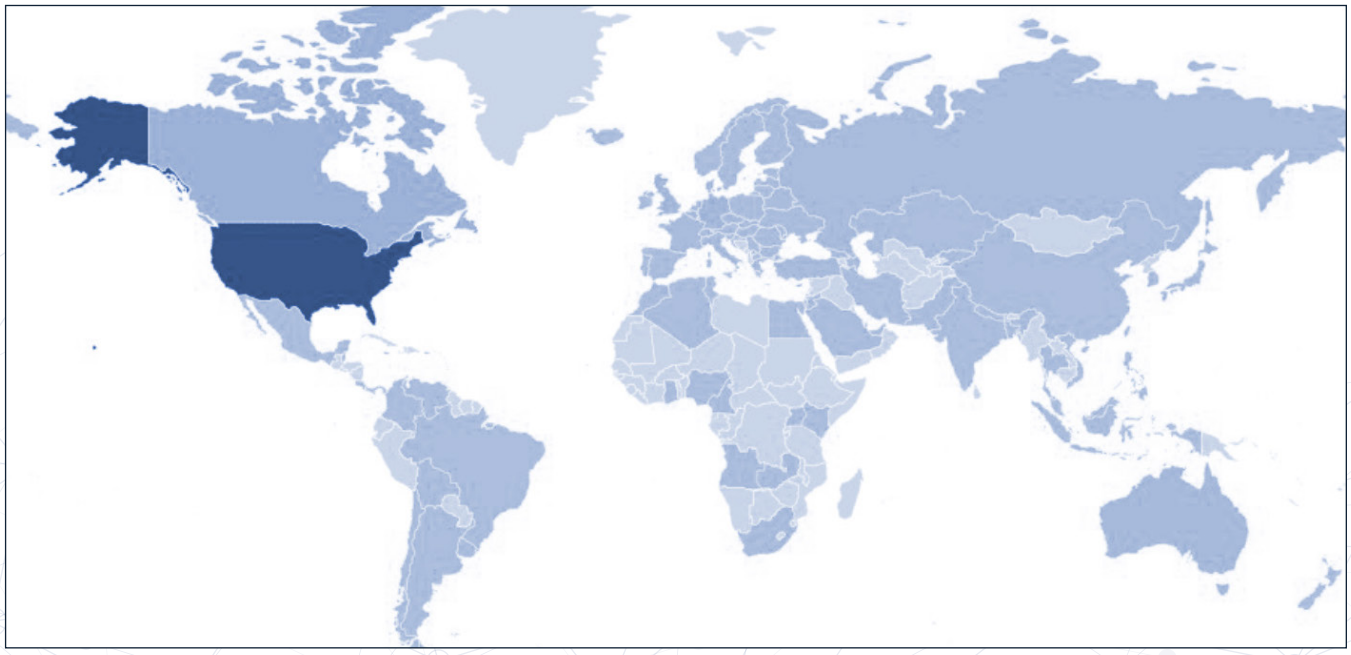


Figure 6: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Projections for Q1 2023 and Beyond

Rise of HTML Attachments Continues

In our Q3 Quarterly Intelligence trends report, we correctly predicted that other malware would imitate QakBot campaigns unusual delivery techniques involving HTML files. Since that prediction, we have seen several malware families, such as Iced-ID and NetSupport Manager RAT, being delivered using similar HTML file delivery methods. We expect this trend to continue and gain popularity, as it seems to be particularly effective. The increasingly popular technique of using of Telegram bots for exfiltration in credential phishing has also employed HTML attachments as lures or credential entry forms, further boosting their presence.

Blockchain Technology to Grow in Phishing Usage

As mentioned above, we saw a 482% growth in the usage of Web3 platforms (blockchain technology intended to decentralize and improve computing and internet activity) for phishing from Q1 to Q3. While we do not expect quite such explosive growth, we still expect that number to increase as time goes on. We expect to see both more abuse of existing Web3 platforms and the creation of even more new Web3 platforms. The only potential impediment to this growth is content moderation which is inherently opposed to the concept of Web3.

Password Protected Archives to Spread to Other Malware

Password protected archives are a common trick of more advanced malware distributors such as those delivering Emotet and more recently QakBot. This trick is often used in combination with other techniques such as having the password protected archive embedded in an HTML file. We have recently seen campaigns delivering less complex malware such as Async RAT and NanoCore RAT using password protected archives. We expect this trend to slowly continue and grow over time as threat actors recognize its effectiveness as compared to archives without password protection.

Unpredictable Emotet Spikes not as Effective as QakBot, But Changes Possible

In the months since its return, Emotet has popped up for short periods, sent emails at high volume, and then disappeared for some time. This is likely to continue. It is difficult to determine how long the current suspension of activity will last, but it is likely that Emotet will return and quickly work itself up to high volume yet again. This behavior, which includes significant downtime, gives competitors like QakBot room to improve and grow. Further, while Emotet receives significant attention for its hard-to-predict spikes, it is important to note that over the past year, despite its massive volume, Emotet malware has not been the most successful in bypassing email gateways to actually reach inboxes. That award has continued to go to Qakbot, which we've affectionately designated as our "Malware Family to Watch" over the past few quarters. Although we have no direct indications of activity, it is possible that Emotet authors are using the current downtime to make significant changes intended to improve the effectiveness of their malware delivery campaigns. In the past, Emotet authors have been known to make significant changes to the malware's delivery methods after coming back from long hiatus.