



Q2 2022

Cofense Phishing Intelligence Trends Review



Executive Summary

The phishing threat landscape experienced several changes throughout Q2 2022. Emotet and QakBot operators have introduced new delivery mechanisms into their phishing campaigns, likely due to Microsoft's changes to the default settings of Office macros. As a result of their adoption by Emotet, LNK downloaders have become the top delivery mechanism for this quarter. Myportfolio.com, Evernote.com, Live.com, and Canva.com joined the top 10 .com domains most abused in evasive credential phishing. All of the top malware families for this quarter saw an increase in volume except for Emotet, which has come down from record highs seen in Q1 but still dominates the landscape. QakBot has become the top malware family reaching enterprise users, which has led to a spike in volume for the banker malware type. Bumblebee, a new highly sophisticated malware loader has been seen reaching inboxes to spread Cobalt Strike.

This quarter brings added focus on Business Email Compromise (BEC), the costliest email threat. A new addition to **ThreatHQ** provides valuable insight and even email examples of active BEC campaigns reaching users' inboxes. We also cover some of the tactics and trends of recent BEC campaigns in a **Strategic Analysis** published on June 23rd.

During this quarter, our Strategic Analysis gave readers a look into the tactics and trends of BEC, how QakBot excels at reaching inboxes, an advanced DcRAT phishing campaign, and other key topics within the phishing threat landscape. We also published several Flash Alerts updating others on important and time-sensitive matters such as Bumblebee phishing campaigns reaching inboxes to deliver Cobalt Strike, and new delivery methods used by QakBot like the Follina vulnerability and Microsoft Windows Installers (MSI files).



Overall Activity

The overall observed phishing activity for this quarter decreased compared to Q1, mostly due to Emotet volume dropping. Not including Emotet, the volume of phishing emails delivering other malware families saw an overall increase. The volume for Q2 remained steady after dropping from a large spike in March.

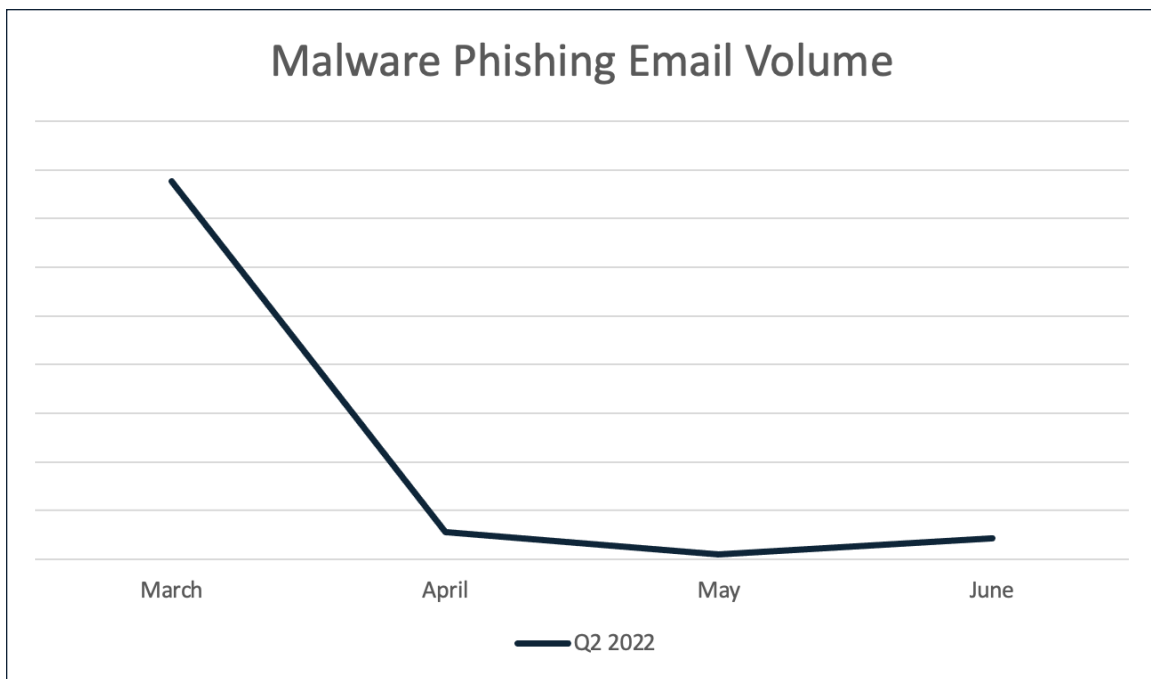


Figure 1: Volume of phishing emails delivering malware in Q2 2022.



Prevalent Malware in Q2

The five most common malware types and the top family for each type remained the same from Q1 to Q2, but the order of the malware types differed slightly due to changes in volume.

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

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

The Top Five Malware Types chart (Figure 2) saw a few changes this quarter. The loader volume continues to eclipse any other malware type, due to Emotet returning to full functionality in Q1 of this year. The chart below has been capped in order to show distinguishable volumes of other phishing activity.

Compared to Q1, all malware types aside from loader saw an increase in volume. Information stealers saw the largest increase with malware families like FormBook and Loki Bot being high commodities in the phishing threat landscape. Agent Tesla and Snake keyloggers contribute to a high percentage of the keylogger volume. The banker malware type passed Remote Access Trojans (RATs) due to a high volume of QakBot phishing emails. Remcos RAT continues to be the top RAT; it is followed by another popular alternative for threat actors, the NanoCore RAT.

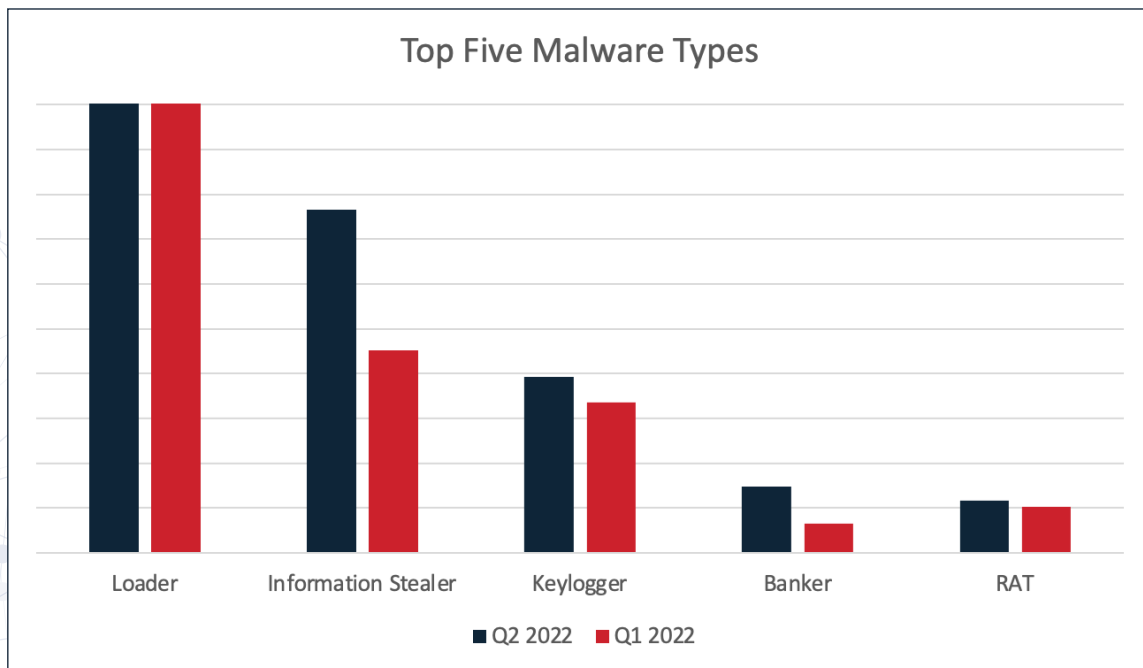


Figure 2: Top five malware types in Q2 2022 and Q1 2022, by volume of emails.

Finished Intelligence: Topics and Trends

Throughout Q2 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 and flash alerts that Cofense Intelligence produced on notable topics and trends identified during this period.

Tracking An Advanced DcRAT Campaign

Cofense Intelligence has uncovered what we judge to be a continuous campaign stretching across 7 months from late September 2021 to late April 2022. The campaign targeted multiple sectors but focused on the Energy and Financial sectors. The campaign used either compromised email accounts or spoofed real accounts belonging to aerospace or chemical supply companies in order to send the phishing emails. Each email in the campaign abused Google Drive links and used the same malware delivery chain to deliver DcRAT malware. Among the DcRAT command and control (C2) locations observed, one C2 was seen in use across a 6-month time period. Although the end goal of the campaign is not certain, the advanced tactics, techniques, and procedures (TTPs), as well as the carefully crafted nature of the campaign indicates a threat actor or threat actor group with capabilities beyond that of the average threat actor.

Evolving Threat – Why QakBot Excels at Reaching Inboxes

The QakBot banking trojan, also known as QBot or Pinkslipbot, was first released in 2007 and is currently reaching users' inboxes at a high volume compared to other malware families. QakBot campaigns go to extensive lengths to bypass security measures, avoid detection, and obstruct analysis tactics. The phishing emails are disseminated by the QakBot botnet at a high rate, utilizing the tactic of hijacked email threads and embedded links to spread the infection. The combination of these two tactics is most likely the primary reason QakBot is leading all other malware families in reaching inboxes. QakBot operators have been seen making major changes to tactics, techniques, and procedures (TTPs) within the infection chain. In this report, we will cover the history of QakBot, why security operators should be aware of the threat that it poses, the phishing emails disseminated by the botnet, and the configurations to avoid analysis and detection within the campaigns. Additionally, this report covers the TTPs used and observed changes like the addition of the Follina exploit in a recent campaign.

BEC: Tactics and Trends of the Most Costly Email Threat

Business email compromise (BEC) causes more financial losses than any other form of cyber threat activity. More than ransomware? A lot more if we go by **statistics from the FBI**. But what does BEC actually look like? In this report, we bring the realities of BEC to life by interacting with real threat actors, becoming familiar with the stories they present, and examining trends in real-world BEC campaigns. We also consider BEC impacts and the potential for recovery of assets, along with mitigation strategies.

Finished Intelligence: Topics and Trends

QakBot Delivered Via Follina Vulnerability

On June 8th, 2022, Cofense Intelligence uncovered a QakBot malware campaign that displays several major TTP changes from other QakBot campaigns, while still reaching corporate inboxes. This new campaign employs the “Follina” vulnerability (CVE-2022-30190) and uses .HTML attachments rather than the chain of embedded links into Office Macros that QakBot is known to use.

BumbleBee Campaign Reaches Inboxes to deliver Cobalt Strike

Cofense Intelligence observed the new BumbleBee loader using advanced techniques to deliver Cobalt Strike. The campaign uses reply chain emails in order to appear more legitimate. These emails were found in multiple corporate environments protected by a variety of prominent Secure Email Gateways (SEGs).

QakBot Campaigns Using MSI Files Reach Inboxes

Phishing campaigns delivering QakBot changed to a new delivery tactic. The new campaigns included an MSI file as a delivery mechanism. At the time of this report, this was the first major change in delivery tactics for QakBot since June 2020. Cofense analysts found that the new campaigns were reaching inboxes in SEG-protected environments.

FormBook - Phishing Malware Baseline

FormBook has consistently placed in the top 5 malware families most commonly seen by Cofense Intelligence in recent quarters, and was accordingly included in our Feb. 2022 report **Malware Primer: Prominent Families in Phishing 2021**. In this report, we specifically take an in-depth look at FormBook, including background information, FormBook’s capabilities, its behavior observed in the wild, and some characteristics that can help with mitigation.

RedLine Stealer - Phishing Malware Baseline

RedLine Stealer is an information stealer that was first released in early 2020 and sold in Russian underground markets. Threat actors have used a variety of social engineering approaches to distribute it, including many well-crafted phishing campaigns. In this Strategic Analysis, we discuss RedLine’s capabilities, real-world usage, and characteristics that are useful for detection and mitigation.

Delivery Mechanism Rundown

Compared to Q1, the Top Malware Delivery Mechanisms chart for Q2 saw a few changes. The top two delivery mechanisms for this quarter are heavily influenced by Emotet volume, and their volumes shown graph below (Figure 3) have accordingly been capped, in order to make other mechanisms perceptible. LNK Downloaders have become the top delivery mechanism as malware families like Emotet and QakBot look to replace Office macros. Consequently, the volume for Office macros dropped significantly for this reporting period, but still remains significantly above the graph's cap. The CVE-2017-11882 vulnerability has been a very popular option for delivering a variety of malware families. The volume for CVE-2017-11882 and other popular delivery mechanisms appears minute when compared to those using Emotet (i.e. LNK downloader and OfficeMacro), but they still pose a credible threat, and in fact, experienced an increase in absolute volume compared to the previous quarter. Other noteworthy delivery mechanisms seen delivering malware in Q2 are DBatLoader, GuLoader, and DotNETLoaders.

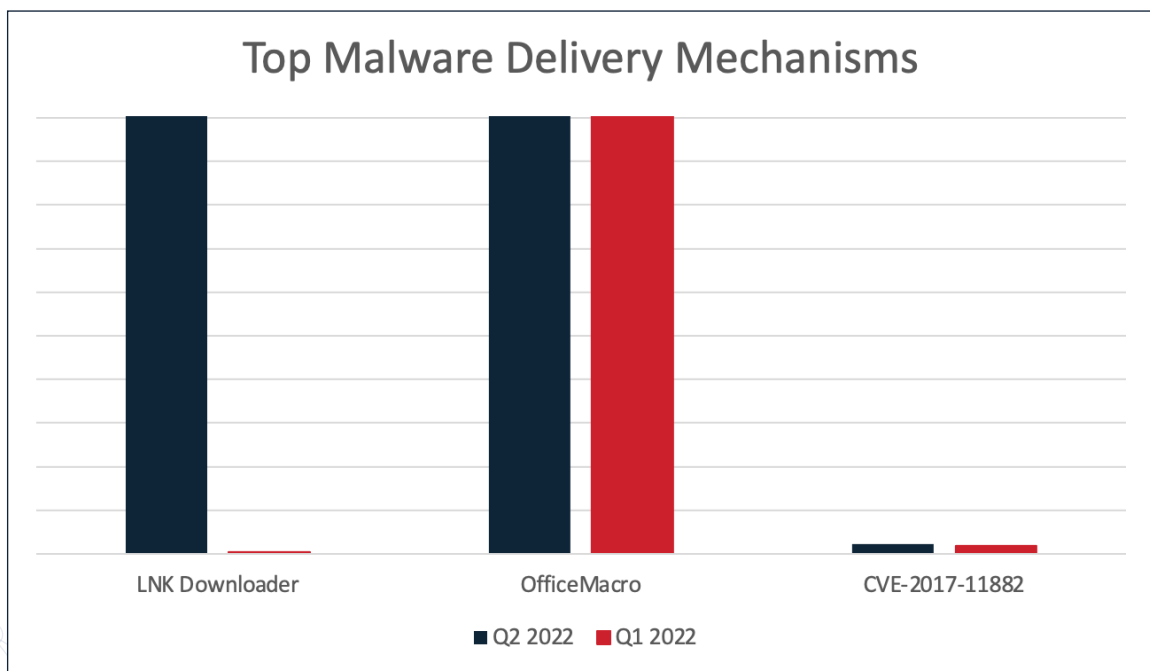


Figure 3: Top Malware Delivery Mechanisms by Email Volume in Q2 2022 and Q1 2022.

TLDs and Domains Used in Credential Phishing

In this section, we analyze URLs used in credential phishing emails that reached users in environments protected by SEGs, to identify the top-level domains (TLDs) and domains 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 takes action with the embedded URL.

When both stages are combined, the order of the top 10 TLDs varied compared to that seen in Q1. Domains using the .com TLD accounted for approximately 50% of the total, a decrease from Q1. The .net TLD increased to around 6.5%. Other notable TLDs that were also top 10 for Q1 are .co, .me, .org, .io, .br, .xyz, and .in. The only new addition for this quarter was the .app TLD.

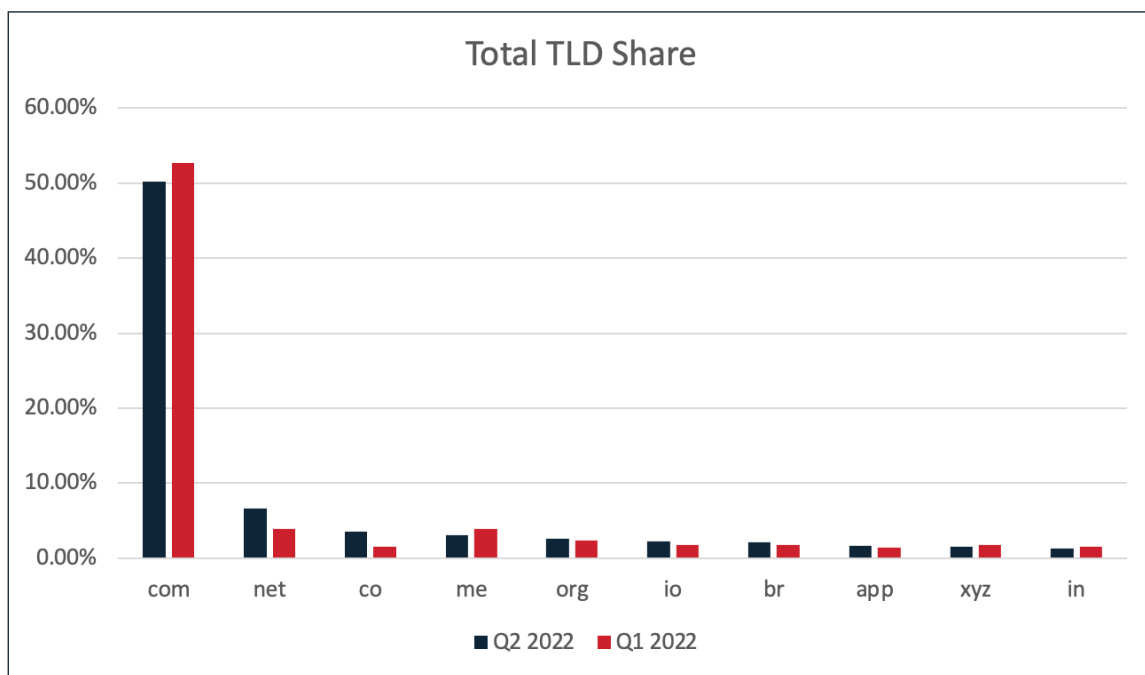


Figure 4: Top 10 TLDs in Q2 2022 compared with Q1 2022.

TLDs and Domains Used in Credential Phishing

The percentage of Stage 1 URLs represented by .com was larger than that of Stage 2. The top 10 TLDs for Stage 1 URLs remained largely consistent with those of Q4, except for some changes in order and the replacement of .ly by .id.

STAGE 1 TLD	Q2 2022	Q1 2022
com	54.41%	55.80%
net	8.90%	3.70%
br	2.65%	1.05%
co	2.64%	1.80%
io	2.52%	2.90%
org	2.17%	2.30%
in	1.58%	1.90%
ms	1.56%	2.50%
app	1.35%	1.90%
me	1.35%	1.80%

Table 2: Stage 1 TLDs in Q2 2022 compared with Q1 2022.


The top 10 Stage 2 TLDs for this quarter saw multiple changes outside of the top three. The top three Stage 2 TLDs remain consistent with the largest change being the volume of .me domains decreasing. The number of URLs with the .app, .co, and .io TLDs increased this quarter replacing .dev, .online, and .id for this chart.

STAGE 2 TLD	Q2 2022	Q1 2022
com	48.78%	49.60%
me	4.96%	6.00%
net	4.92%	4.10%
co	4.64%	1.36%
org	3.05%	2.30%
xyz	2.52%	2.40%
app	2.12%	1.11%
io	2.06%	0.89%
br	1.79%	2.50%
ru	1.56%	1.50%

Table 3: Stage 2 TLDs in Q2 2022 compared with Q1 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, a number of trusted cloud platforms can be identified, showing a continued use for credential phishing threat actors.



- Adobe
- Google
- Myportfolio
- Backblazeb2
- Weebly
- Sharepoint
- Evernote
- Live
- Digitaloceanspaces
- Canva

Compared to the previous quarter, the top 10 most common .com domains had multiple changes. Adobe.com took over the top spot for this quarter, while the Myportfolio, Evernote, Live, and Canva .com domains increased in volume to join the top 10. The .com domains replaced by these new additions were Oraclecloud, Amazonaws, Atdmt, and Axshare.



File Extensions of Attachments

Our quarterly analysis revealed some changes from Q1 to Q2 in the distribution of filename extensions on email attachments that reached users in SEG-protected environments. .pdf attachments remained the top extension analyzed and saw a large increase compared to the previous quarter, making up over 40%. This is more than the combined 35% that .html and .htm files make up. These file extensions are more commonly associated with credential phishing attacks, and we continue to see that for this quarter.

Office files like .docx, .xlsx, .xls, and .doc continue to be top 10 file extensions on phishing email attachments. These files are used for a variety of purposes such as delivering credential phishing, malicious Office macros, and exploit vulnerabilities. The .lz file extension replaced .shtml for this quarter, and it is an archive like .zip that is primarily used to deliver malware campaigns.

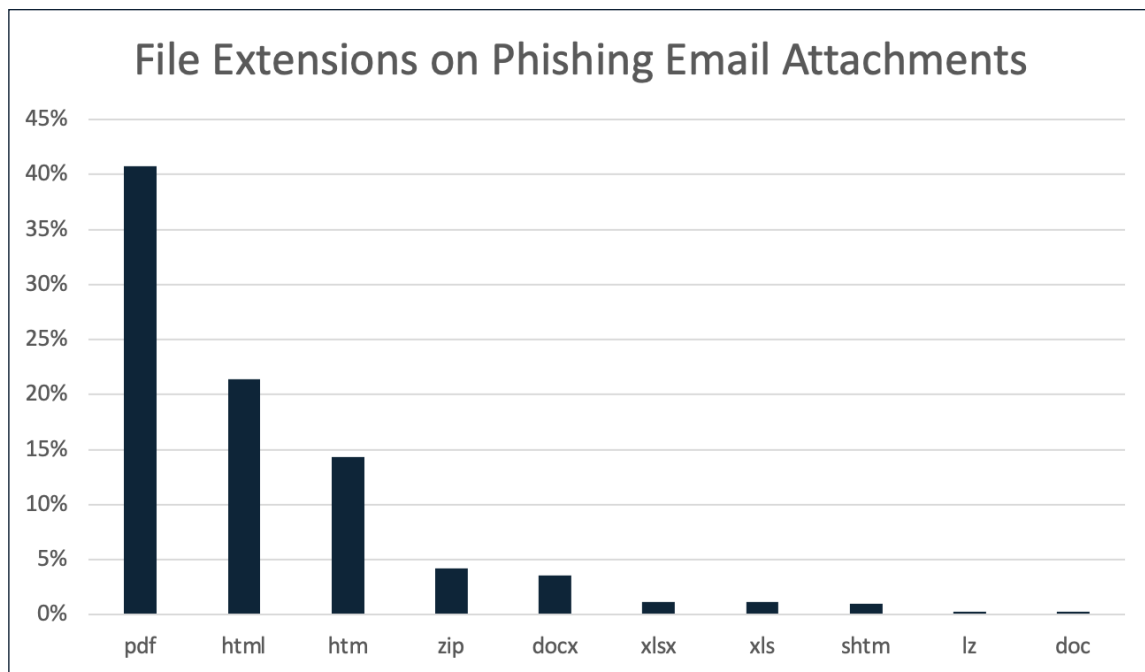


Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs

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. The top five locations for this quarter were very similar to that of Q1, except that servers in Hong Kong replaced Great Britain. The other four countries remained the same and even held similar percentages. 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 2022		Q2 2022	
Country	Percentage	Country	Percentage
United States	59.92%	United States	59.76%
Germany	4.73%	Germany	4.61%
Canada	2.78%	Canada	2.60%
Great Britain	2.00%	Hong Kong	2.31%
Netherlands	1.92%	Netherlands	2.08%

Table 4: Q1 2022 and Q2 2022 percentages for C2 sources by IP address geolocation.

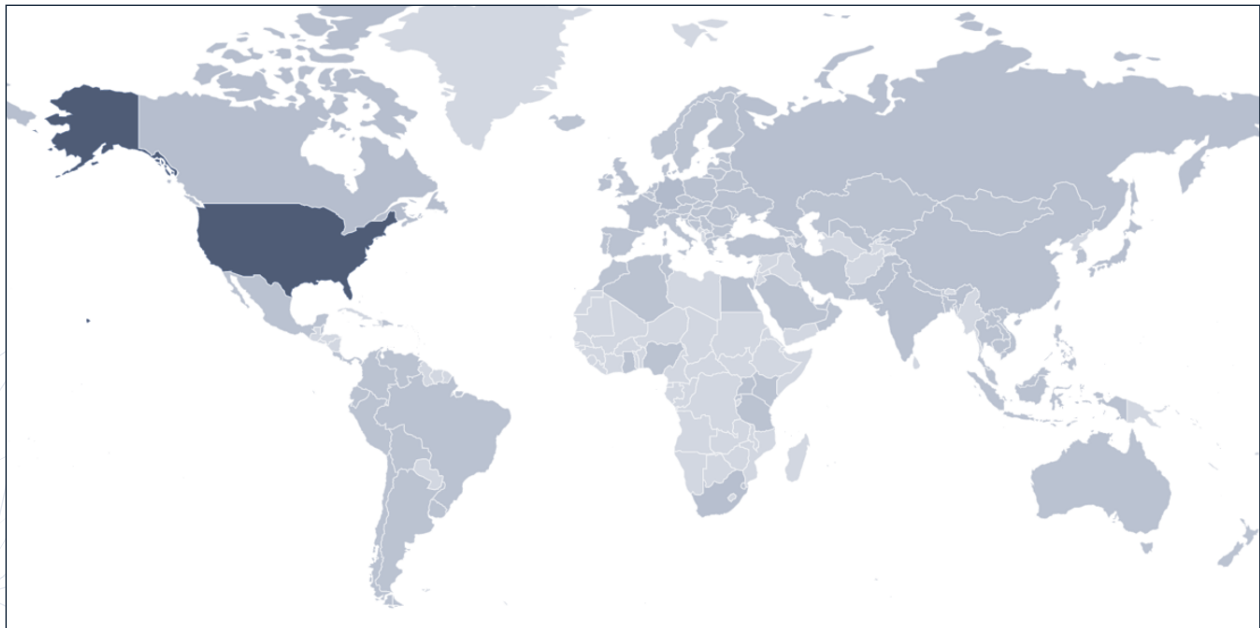


Figure 6: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Projections for Q3 2022 and Beyond

Microsoft Updates to VBA Macros Embedded in Malicious Office Documents Will Continue to Impact the Phishing Threat Landscape

Earlier this year, Microsoft announced that they will be changing the default Office setting to block VBA macros from files downloaded from the internet. Since this announcement, we have seen malware families known to heavily abuse the use of malicious Office macros make changes within their campaigns to incorporate new delivery mechanisms. The delivery mechanism data from Q2 has reflected this change as LNK Downloaders became the top delivery mechanism displacing Office macros. In early July, this default change to VBA macros was rolled back with some comments saying the roll back is temporary. Microsoft's next steps in regard to the VBA macros update is very likely to impact the phishing threat landscape throughout the remainder of the year.

Qakbot is the Malware Family to Watch for Q3 2022

Qakbot is currently the top malware family seen in phishing emails reported to the Cofense Phishing Defense Center from users in environments protected by SEGs. The success rate of the phishing emails reaching enterprise inboxes is attributed to the use of hijacked email threads from compromised emails and the use of TTPs within phishing emails, which are known to aid in bypassing security. In recent months, threat actors using Qakbot have been seen making several changes to their phishing tactics. These changes primarily include seeking alternative delivery mechanisms like LNK downloaders and the Follina vulnerability to replace Office macros. With such a high volume of Qakbot phishing emails successfully reaching inboxes, this makes Qakbot the malware family to watch as we enter Q3 2022, especially since a successful Qakbot infection can lead to more costly threats like ransomware.

Less Common Hosting Providers Will be Abused More Frequently to Host Malware

The abuse of hosting providers to deliver malicious files has become a popular method for threat actors to bypass security and deliver malware. It is common to see trusted cloud providers like OneDrive, Google, SharePoint, and other well-known organizations be abused by threat actors. Lately, more less-common hosting providers have been seen and, in some cases, fake providers have been created by threat actors. As we enter Q3, we anticipate a more frequent use of these less-common and even fake hosting providers to deliver malicious payloads.

Economic Uncertainty May Increase Overall Phishing Volume

Overall volume in the phishing threat landscape has been known to fluctuate as economic changes occur. This was seen during the early to mid-pandemic period which created conditions that were ripe for new threat actors to enter the field or existing ones to ramp up operations. The overall phishing volume is likely to see this ramp-up again as countries face new unpredictable changes to the economy.