COFENSE

Q1 2022

Cofense Phishing Intelligence Trends Review

Executive Summary

The phishing threat landscape was impacted by several factors in Q1 of 2022, such as Emotet volume reaching new highs since the return, and scam-based threats arising from the conflict between Russia and Ukraine. Overall, the volume of phishing emails did increase with some noteworthy changes in malware types and delivery mechanisms. The information stealer malware type increased in volume passing keylogger for the first time in several reports. This was due to an increase in volume for FormGrabber malware. Other changes include the high volume of Emotet controlling the top delivery mechanisms chart for this period.

Emotet returned in November of 2021 but didn't quite reach the volume we saw prior to the takedown in January of that year. As the first quarter of 2022 has unraveled, we have seen a significant increase in Emotet volume, which appears to have returned to full operation for the first time since the law enforcement takedown in January 2021.

During this quarter, our Strategic Analysis gave readers a look into the top malware families from 2021, phishing takeaways from the Conti ransomware leaks, the cryptocurrency and NFT threat landscape, the Ofux cybercrime shops, and other key topics within the phishing threat landscape. We also published several Flash Alerts updating users on important and time-sensitive matters such as the Russia and Ukraine conflict, as well as changes made by Emotet threat actors.

Overall Activity

The overall phishing activity for this quarter is greatly impacted by the Emotet botnet returning to full functionality. Although Emotet did return in Q4 2021, the volume was not back to the full potential like we have seen this quarter. The overall volume remained steady with a slight decrease from January into February; however, due to Emotet, there was a spike in volume from February to March.

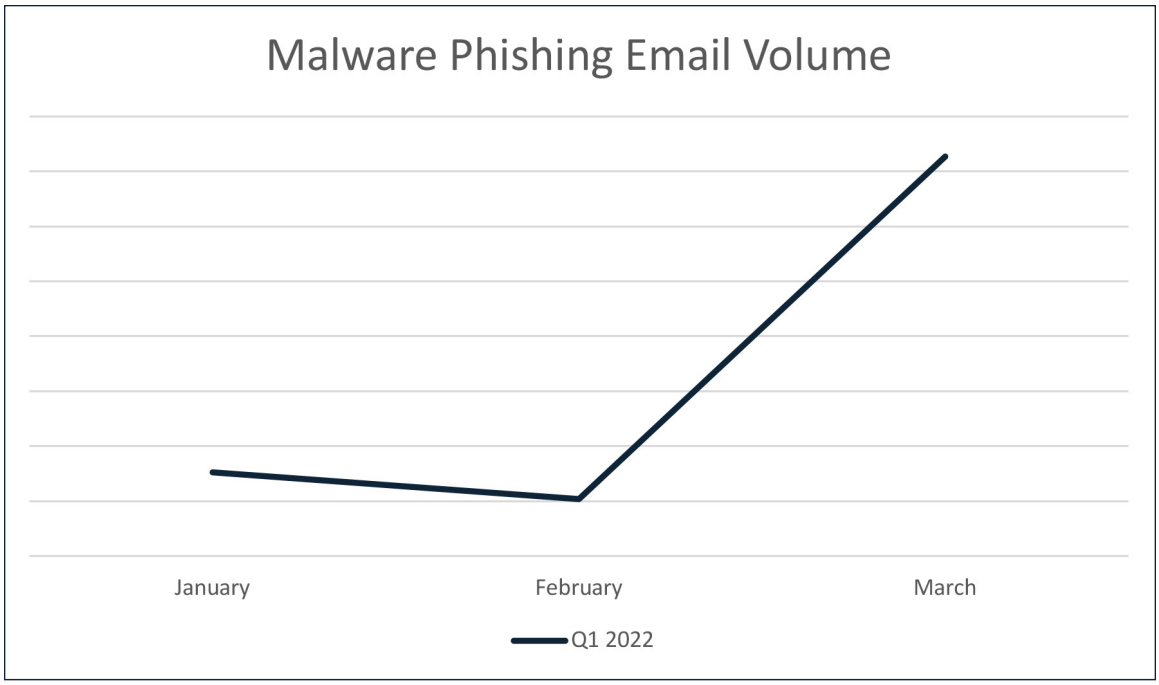

Figure 1: Volume of phishing emails delivering malware in Q1 2022.

Prevalent Malware in Q1

The five most common malware types and the top family for each type remained the same from Q4 to Q1, but the order of the malware types differed due to changes in volume.

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

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

The Top Five Malware Types chart saw a few changes this quarter. The loader volume goes way beyond any other malware type due to Emotet returning to full functionality. This chart has been capped in total volume; this is because of the Emotet botnet's ability to disseminate a very high volume of emails, which goes well beyond that of other malware types.

Compared to Q4, information stealer passed keylogger due to a high volume of FormGrabber and Loki Bot information stealers. Keyloggers still remain a very popular option for threat actors, with Agent Tesla contributing to a high percentage of that volume. Remcos was the most commonly seen Remote Access Trojan (RAT), but the NanoCore RAT trailed very close in volume. QakBot makes up the top banker for this quarter, however, the overall volume of bankers has dropped, which is attributable to TrickBot being inactive for several months.

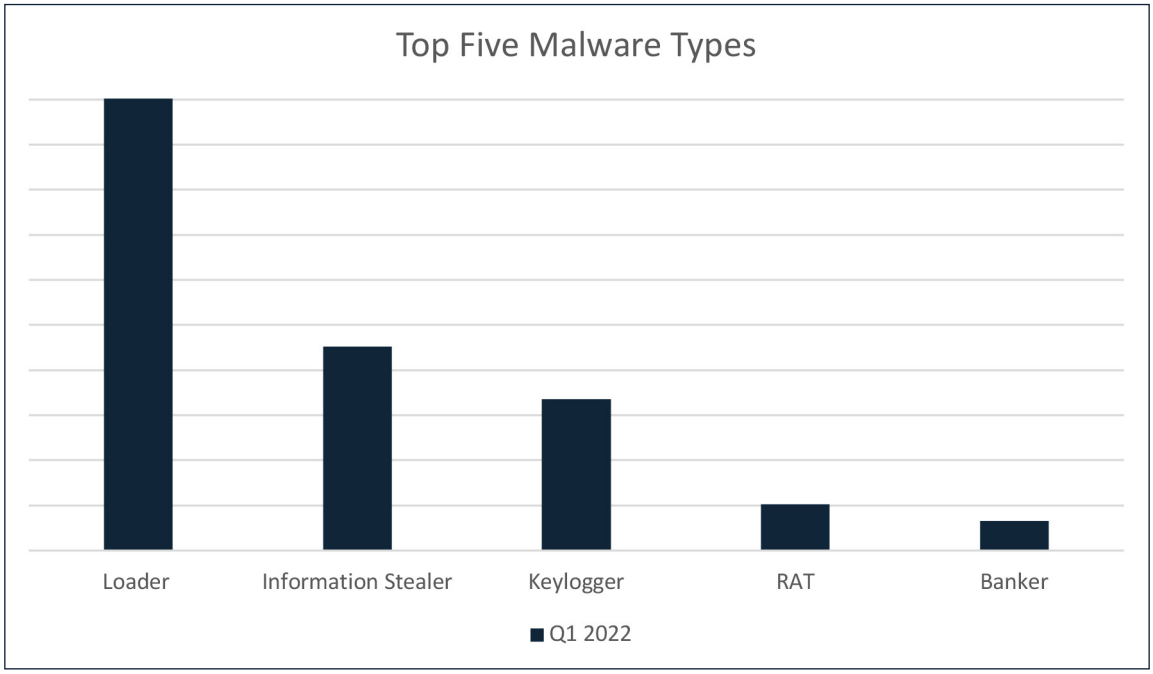

Figure 2: Top five malware types in Q1 2022 and Q4 2021, by volume of emails.

Finished Intelligence: Topics and Trends

Throughout Q1 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.

Malware Primer Prominent Families in Phishing 2021

Cofense assesses a wide range of malware families in producing Active Threat Reports throughout the year, but in this report, we aim to provide a quick reference guide for understanding the families that make up the highest volume of phishing campaigns disseminated in 2021. There are several characteristics that can make a malware family appealing to threat actors, such as the malware features, cost, and complexity. In combination, these properties determine how well malware aligns to a threat actor's agenda for a phishing campaign. Figure 1 shows the most common characteristics of each malware family that we observe in phishing campaigns.

Ofux Cybercrime Shops Facilitate Phishing Attacks

Threat actors frequently use compromised email accounts and websites to conduct phishing campaigns. Several publicly-available online shops, running a platform named "Ofux,"allow threat actors to buy and sell access to compromised accounts and servers for that purpose. Sellers offer everything a phishing threat actor might need: email sending capability, access to websites for hosting malicious content, and access to hacked individual email accounts. Phishing campaigns that use legitimate but compromised assets are more likely to reach targeted users, highlighting the need for robust email defenses and user education.

NanoCore RAT – Malware Baseline

The NanoCore RAT has consistently placed in the top 5 malware families most commonly seen by Cofense Intelligence™ in recent quarters and was accordingly included in our report "Malware Primer: Prominent Families in Phishing 2021." In this report, we take an in-depth look at NanoCore RAT, including background information, NanoCore's capabilities, its behavior observed in the wild, and some characteristics that can help with mitigation. NanoCore is a .NET based RAT which has been around for almost 10 years and is well known both for its widespread usage and for the highly publicized arrest and guilty plea of its developer. It is simple and easy to use, with many plugins that enable it to perform a variety of malicious activities.

Phishing Takeaways from the Conti Ransomware Leaks

Conti is one of the most prolific ransomware operations in the threat landscape today. In a recent act of retaliation against Conti's leaders for their support of Russia, an anonymous person leaked documentation and internal chat logs from the group. This report covers several phishing-related takeaways from the leaks.

Finished Intelligence: Topics and Trends

Phishing for Tokens: Cryptocurrency and NFT Phishing

Cryptocurrency (crypto) and non-fungible tokens (NFTs) have become a popular topic for the general media, and consequently, a target for threat actors seeking financial gain. A months-long spike in well-crafted phishing campaigns has coincided with this public interest, targeting login credentials for cryptocurrency trading platforms and NFT marketplaces, digital crypto wallet keys, and several other methods that allow access to a user's cryptocurrency. Cofense has identified cryptocurrency-and NFT-related phishing campaigns that were reported to the Cofense Phishing Defense Center (PDC) by users in environments that are protected by secure email gateways (SEGs). In this report, we examine two examples of these phishing emails: a phishing email that uses the current Russia and Ukraine conflict as a lure to steal Bitcoin wallet data, and a phishing email spoofing OpenSea just days before they report a successful attack that impacted 17 users to steal over $1.7 million worth of NFTs. While early investment in cryptographic assets was largely limited to private individuals, recent increases in corporate use and investment also increase the potential breadth of impact from threat activity targeting these assets.

Russia Ukraine Conflict in Phishing Themes

As the conflict in Ukraine unfolds, Cofense Intelligence continues to monitor for phishing threats related to the conflict and has identified malicious campaigns that are using the current event as a lure to target end users. These campaigns are almost certainly opportunistic, as threat actors are weaponizing the conflict for financial gain by creating well-crafted credential phishing campaigns and donation scams. Threat actors using current events as themes within their email campaigns is quite common, and users should be universally vigilant against these threats. A variety of emails using this particular conflict as a lure have been reported to the Cofense Phishing Defense Center directly from enterprise users' inboxes. We have no evidence to suggest—based on IOCs, tactics, or campaign sophistication—that any of these campaigns were conducted by nation states directly involved in the war in Ukraine.

Emotet Phishing Emails Exploit US Tax Season Spoofing IRS

Emotet has consistently employed financial themes in its phishing emails and has exploited the arrival of the US tax season to construct emails targeting users who need to file tax returns. The 2022 tax season is no different. On March 14, 2022, Cofense Intelligence observed phishing emails using W-9 tax form lures to deliver Emotet payloads. In past years, Cofense Intelligence has reported on Emotet taking advantage of tax season to deliver W-9 themed malicious documents, but this year the tactic has been improved. Emotet operators have upped their game in this most recent campaign, now including the IRS logo, a specific mention of the organization employing individual recipients, and a password with which to extract the attached password protected archives. When the Office-macro-laden spreadsheets enclosed in the password protected archives are opened, they request that macros be enabled. If macros are enabled, Emotet .dll files are delivered to the victim's computer.

Emotet Reinstates Embedded URLs Reaching Inboxes

Since its rebirth in November 2021, Emotet's phishing emails have focused on using attached Office-macro-laden Excel files as a delivery mechanism for their payload. However, Emotet has recently reinstated another delivery method, sometimes providing embedded URLs linking to downloadable malicious documents, rather than directly attaching these documents to emails. Instances of Emotet campaigns using this delivery method have now been discovered by the Cofense Phishing Defense Center in corporate inboxes protected by secure email gateways.

Delivery Mechanism Rundown

The Top Malware Delivery Mechanisms chart for Q1 differs greatly from that of Q4 2021 and is heavily influenced by Emotet volume. Office-macro-laden documents, malicious PowerShell scripts, and Microsoft HTA files had drastic volume increases due to their immense use in widespread Emotet campaigns. The use of Office macros towers above the rest, since it is the primary delivery mechanism used by Emotet phishing campaigns analyzed during this quarter and is also a very common delivery mechanism among several malware families. Malicious powershell scripts were also used by Emotet, although to a lesser degree, making them the second most common delivery mechanism.

Taking a step back from Emotet to shed light on other delivery mechanisms, some notable mentions are CVE-2017-11882, DotNET loaders, and DBatLoader. These three delivery mechanisms make up a respectable volume, deliver a wide variety of different malware families, and still maintain their popularity amongst threat actors. However, the email volume for these delivery mechanisms is minuscule compared to that of the Emotet botnet.

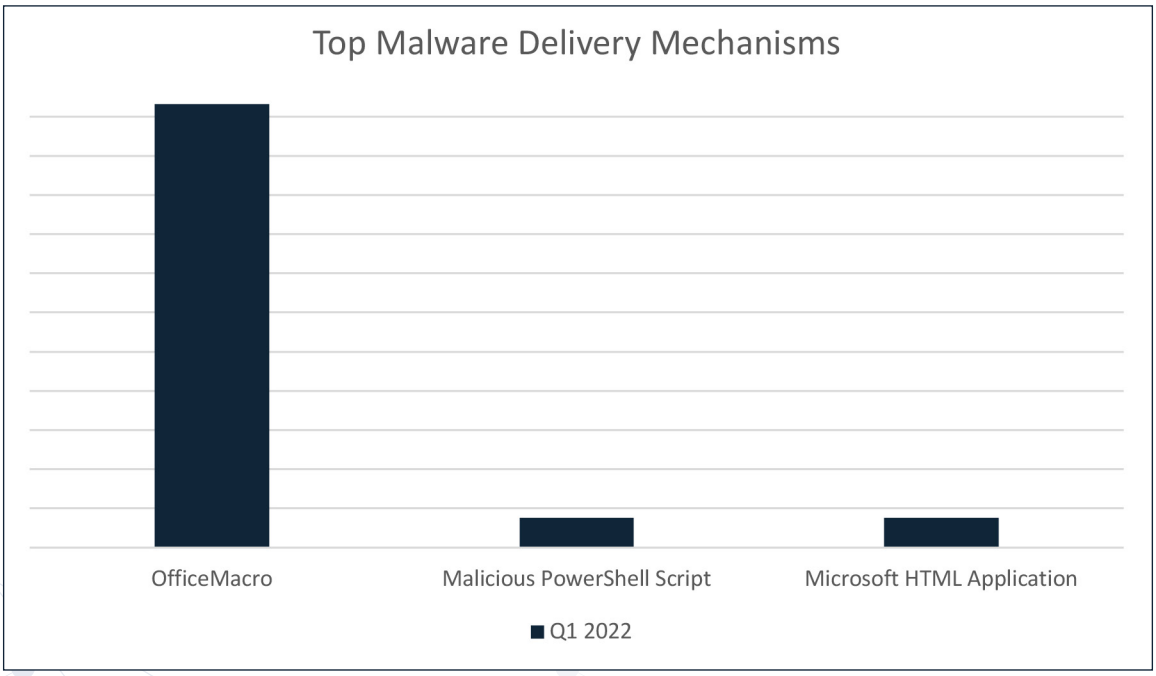

Figure 3: Top Malware Delivery Mechanisms by Email Volume in Q1 2022.

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 top four TLDs remain consistent to that seen in Q4. Domains using the .com TLD accounted for approximately 53% of the total, an increase from Q4. Other notable TLDs are .net, .me, and .org which held the top four spots in the previous quarter. New additions to the top 10 TLDs for this quarter are .br, .in, .co, and .id. which have all increased in volume compared to Q4.

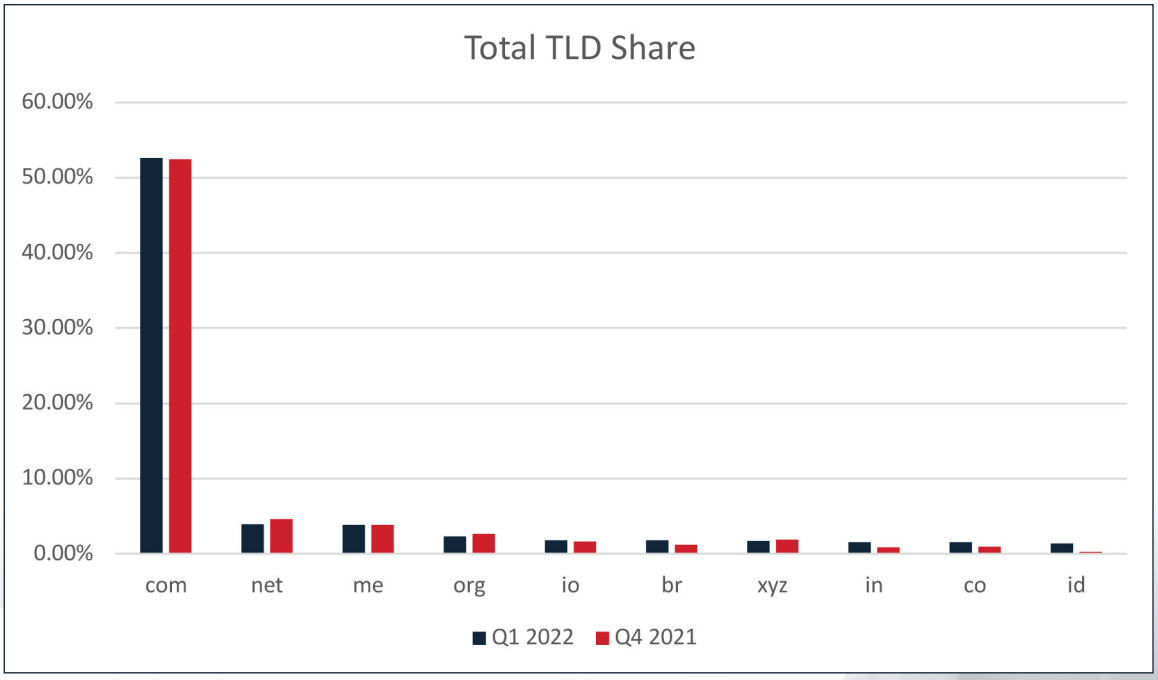

Figure 4: Top 10 TLDs in Q1 2022 compared with Q4 2021.

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	Q1 2022	Q4 2021
com	55.8%	55.3%
net	3.7%	6.1%
io	2.9%	2.4%
ms	2.5%	3.1%
org	2.3%	2.2%
in	1.9%	1.4%
co	1.9%	1.9%
app	1.9%	1.6%
me	1.8%	1.5%
id	1.5%	0.3%

Table 2: Stage 1 TLDs in Q1 2022 compared with Q4 2021.

A few notable changes can be seen when comparing the top 10 stage 2 TLDs of this quarter to those of Q4 2021. An increase in share for the .br, .online, and .id TLDs caused several changes in positions and resulted in .uk not making it as a top 10 TLD for this quarter.

STAGE 2 TLD	Q1 2022	Q4 2021
com	49.6%	50.2%
me	6.0%	5.6%
net	4.1%	3.5%
br	2.5%	1.4%
xyz	2.4%	2.5%
org	2.3%	3.0%
dev	2.0%	2.7%
online	1.7%	1.5%
ru	1.5%	2.0%
id	1.3%	0.18%

Table 3: Stage 2 TLDs in Q1 2022 compared with Q4 2021.

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.

- Backblazeb2
- Google
- Oraclecloud
- Weebly
- Adobe
- Sharepoint
- Amazonaws
- Digitaloceanspaces
- Atdmt
- Axshare

Of the top 10 most common domains using the .com TLD, only three were replaced from the previous quarter. An increase in the volume of URLs using the domains atdmt, axshare, and adobe brought them to the top 10. Although some of the volume was very close, this new addition removed myportfolio, eventscloud, and live which was number eleven on the list.

File Extensions of Attachments

Our quarterly analysis revealed some changes from Q4 to Q1 in the distribution of filename extensions on email attachments that reached users in SEG-protected environments. Overall, .pdf attachments remained the top extension analyzed, making up 32%. Jointly, attachments with .htm or .html made up approximately 50% of the total. Like the previous quarter, most of these attachments delivered credential phishing attacks, either embedded in the files or with links to malicious pages.

There was a notable increase in .zip attachments, likely attributable to password protected zip archives in malware campaigns. Office files like docx, .doc, xlsx, and .xls made it in the top 10 file extensions seen and have had an overall increase in volume for Q1 compared to Q4.

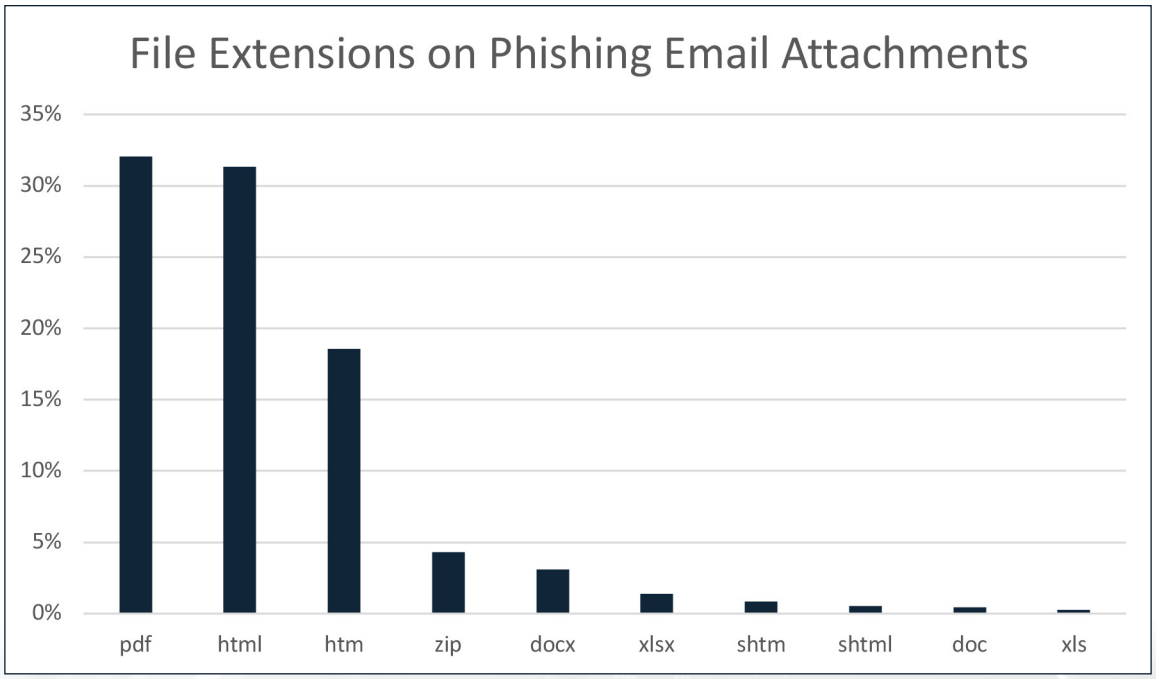

Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs.

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 remained consistent to those from Q4 of last year. The United States maintained the largest share of the C2 locations worldwide. Servers in Germany had a slight increase and remained the second most common location. Canada's share has increased the past two quarters. Both Great Britain and Netherlands decreased this quarter but remained in the top five. 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 2021		Q1 2022	
Country	**Percentage**	**Country**	**Percentage**
United States	59.99%	United States	59.92%
Germany	4.67%	Germany	4.73%
Canada	2.73%	Canada	2.78%
Great Britain	2.40%	Great Britain	2.00%
Netherlands	2.36%	Netherlands	1.92%

Table 4: Q4 2021 and Q1 2022 percentages for C2 sources by IP address geolocation.

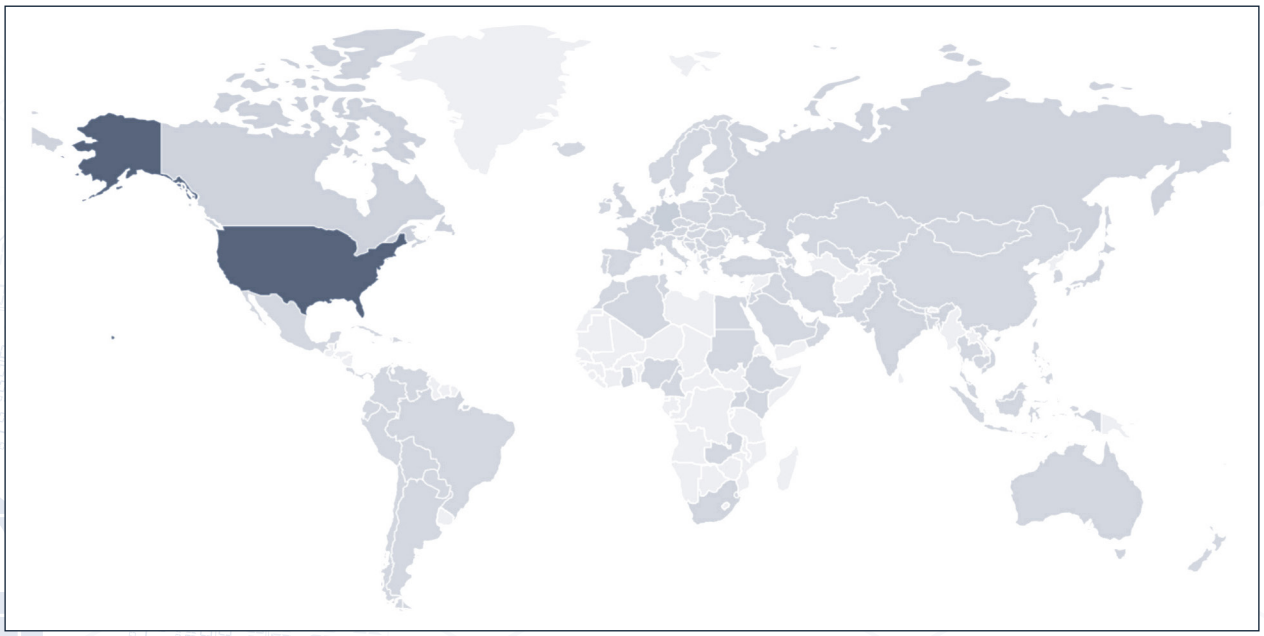

Figure 6: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Projections for Q2 2022 and Beyond

Russia-Ukraine Conflict Likely to Continue Being Reflected in Landscape, Although not in Ways Many Expected
The conflict between Russia and Ukraine has unfolded throughout Q1, and many broadly-voiced expectations regarding its impact on the cyber threat landscape have not materialized. Although targeted cyber attacks against both Ukraine and Russia have been planned and in some cases executed, there has been little evidence of general malware-based phishing threats using the conflict as a lure, and no major cyber attacks from Russia targeting critical industries in Western Europe or the Americas. However, there have been a considerable number of donation scam email campaigns targeting cryptocurrency holders, as well as generic advance fee fraud, using the conflict as a lure to achieve financial gain. As the conflict continues into Q2, there is no indication that this impact of the conflict on the phishing threat landscape will decrease. An escalated cyberthreat fully depends on how the conflict evolves, how engaged other countries become, and how Russia responds to Western engagement if it intensifies. There are several unknown factors in play, and organizations should remain vigilant as the terrain shifts.

After Reaching 2020 Volumes, Emotet Now More Likely to Incorporate Evasion Tactics
In our quarterly report for Q4 2021, we projected Emotet's expansion, indicating that it would gather steam in Q1 2022. In accordance with this projection, the volume of Emotet phishing campaigns increased massively, in many cases reaching tens of thousands of emails per day. However, Emotet's operators did not experiment to the extent that we anticipated. During the resurrection of the Emotet botnet, its phishing campaigns have mostly remained consistent, typically involving a password protected ZIP archive that contains an Office macro laden document to deliver the Emotet binaries. Prior to the law enforcement takedown of Emotet in January 2021, it was a common occurrence for the botnet to go dormant for varied periods, during which the operators developed methods to disrupt analysis or make successful infections less obvious. Going forward, as Emotet phishing volume reaches critical mass and the security community makes significant efforts to impede it, we are likely to see more experimentation, as Emotet makes changes in an effort to bypass security measures.

Conti Ransomware Gang Leaks May Inspire/Augment Other Ransomware Operations
As seen in our Strategic Analysis Phishing Takeaways from the Conti Ransomware Leaks, the Conti ransomware leaks have become a valuable resource for security researchers. This resource can also be used by threat actors with a desire to emulate Conti activity. Seeing the strategies, tactics, resources, profits, and daily discussions of a premier ransomware group may demystify their activities and convince others that a similar operation is feasible. This could motivate new ransomware operators to enter the landscape, improve the operations of existing low-level ransomware operators, or entice recruits to join phishing operations that support ransomware. The leaks may also cause existing threat actors to become more concerned with the security of their operations.

Potential Future Increase in Phishing Campaigns That Use CAPTCHA
We have observed a noticeable uptick in the tactic of adding CAPTCHAs, or challenge-responses, within phishing campaigns. Security professionals and end users should be aware of its presence, as the tactic may become more popular if threat actors deem it to be effective. While we cannot be certain of the intended impact of the tactic, it is most likely intended to impede the automated analysis of phishing URLs. A second, less likely intent is to add more interaction from end users, in order to create a stronger sense of legitimacy.