COFENSE

Q4 2021 Cofense Phishing Review

Strategic Analysis provided by Cofense Intelligence | cofense.com

Executive Summary

Malicious phishing campaigns rose in Q4, mainly due to the return of Emotet in early November. Campaigns delivering malware preferred keyloggers, with information stealers remaining a close second within the quarter. The most common malware families selected Office documents as a delivery mechanism, with CVE-2017-11882 also heavily chosen. SquirrelWaffle campaigns delivering Qakbot were common, making Qakbot a malware family to watch closely in Q1 of 2022. Patterns in threat actors' use of credential phishing domains and malicious attachment file types were generally consistent with Q3.

In our Q4 Strategic Analysis reports, we reported how threat actors could manipulate HTML files that would help them be delivered to an end-user within a secure email gateway (SEG) protected environment. We've shown trends within the SquirrelWaffle payload infrastructure to assist in remediation and mitigation, and discussed a surge of phishing campaigns using XLL files to deliver malware. We also reported on the changes within the newly re-emergent Emotet after delivering two Flash Alerts that warned customers of Emotet's return and significant changes.

At the time of the Emotet takedown in January 2021, Cofense Intelligence predicted its return.

In 2022, malicious botnet takedowns will probably occur, but it should not be assumed that such takedowns are final. Building on its Q4 2021 return, Emotet campaigns are likely to increase in volume, and evolve with the cyber defenses deployed.

Phishing Activity Levels

Emotet's return was the most significant change to the phishing threat landscape within Q4 of 2021. This return resulted in a higher overall volume for this quarter on a year-over-year basis, as well as a significant spike in malware campaigns for the month of November.

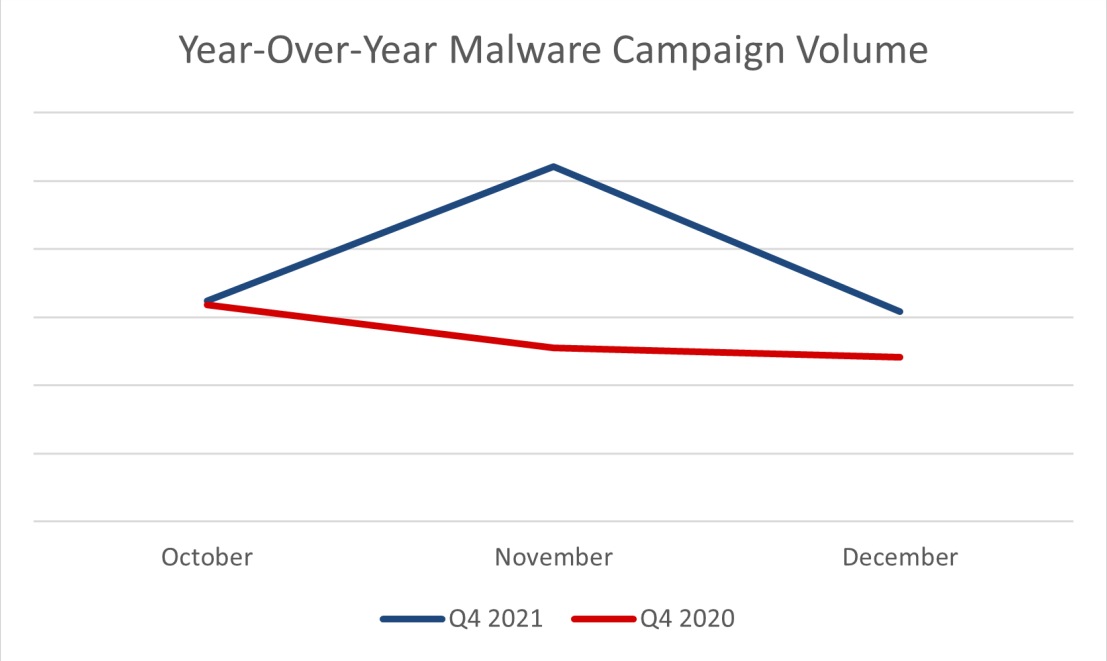
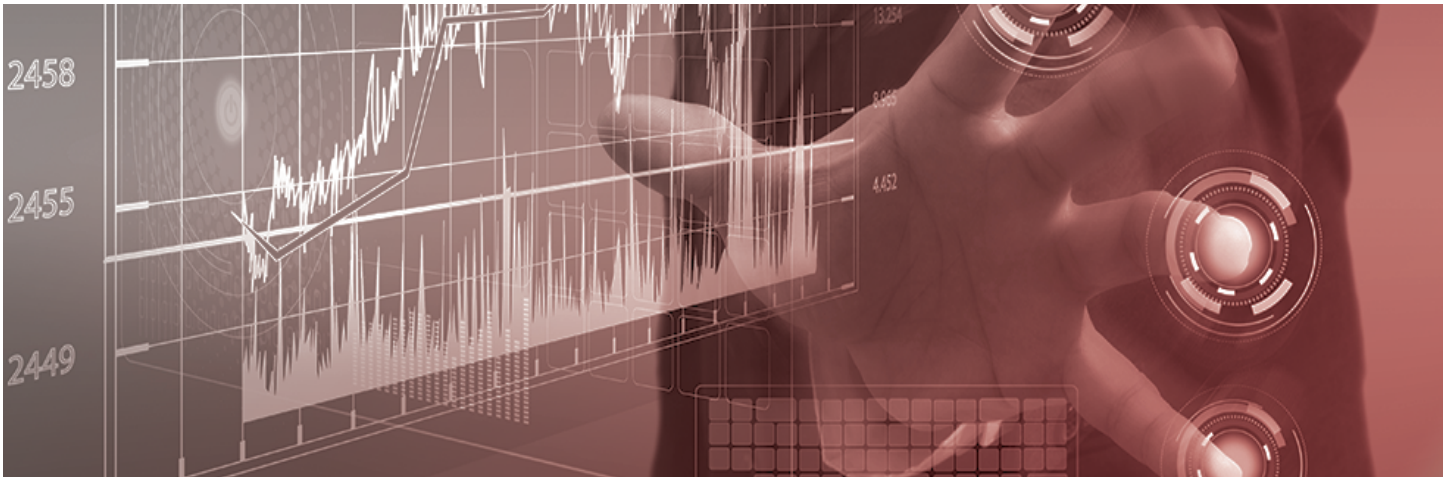


Figure 1: Volume of phishing campaigns delivering malware in Q4 2021 compared to Q4 2020



Prevalent Malware in Q4

The five most common malware types remained the same from Q3 to Q4 of this year, although their order differed and some of the top families by type changed.

Top Five Malware Type	Top Family in Type
Loader	Emotet
Keylogger	Agent Tesla
Information Stealer	FormGrabber
Remote Access Trojan	Remcos RAT
Banker	QakBot

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

The return of Emotet significantly impacted the volume of Loaders, which affected this quarter's overall metrics. SquirrelWaffle also moved those metrics, as it was used to deliver large volumes of QakBot, which replaced TrickBot as the top malware family in the Banker category.

Agent Tesla remained the most heavily distributed keylogger throughout Q4. Like Q3, FormGrabber was the most common information stealer. Remcos was once again the most actively seen Remote Access Trojan within the phishing threat landscape.

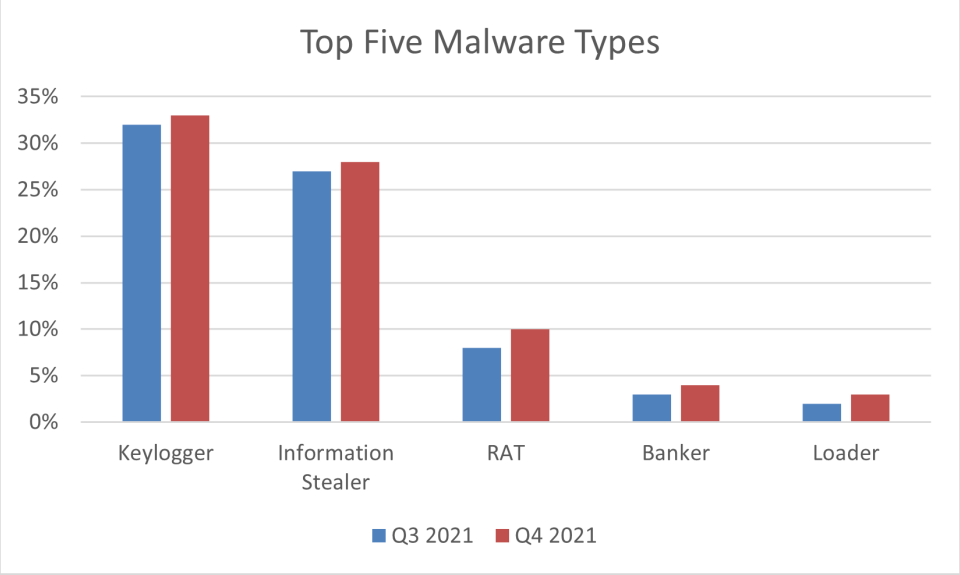


Figure 2: Top five malware types in Q3 2021 and Q4 2021, as a percentage of total campaigns.

Finished Intelligence: Topics and Trends

Throughout Q4 2021, Cofense Intelligence performed an 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.

Testing a Threat Actor's Methods for Encoding Malicious HTML Attachments

Threat actors regularly weaponize HTML files to deliver credential phishing to victims' email inboxes. To bypass SEGs, threat actors may encode (or partially encode) HTML files in any of multiple ways. This report characterizes some of the more common methods used to encode HTML files and investigates the conditions under which encoding a malicious HTML file increases the chances that attachments will reach inboxes in SEG-protected environments.

Footprinting SquirrelWaffle's Payload Infrastructure

While analyzing phishing campaigns that deliver SquirrelWaffle (SW), Cofense Intelligence linked patterns within SW email campaigns and the infrastructure hosting these payloads. A sampling of over 400 unique domains confirmed hosting samples of SW were analyzed. These hosting domains were found to have multiple shared commonalities. Phishing campaigns delivering SW, which acts as a loader for additional malware, have steadily increased since the late third quarter/ early fourth quarter of 2021. By analyzing and detecting patterns in SW's hosted infrastructure, Cofense Intelligence can provide insights and indicators that help protect organizations at an earlier point in the cyber threat kill chain.

Drastic Increase in Excel-DNA use for Malware Delivery

The Excel-DNA (Excel DotNET for Applications) is an open-source project to create XLL files as add-ins for Microsoft Excel. It has recently become a more prolific method for malware delivery. An XLL file is a Microsoft Excel add-in with many legitimate workplace uses. Threat actors have taken these add-ins and configured their files to reach out to Discord's content delivery network (CDN) to download and run malicious payloads. This delivery method was first observed in June and has surged in volume during October and November. We anticipate this tactic becoming more common within the phishing threat landscape as more threat actors discover and modify new uses for Excel-DNA.

Emotet Combines Past Success and New Tactics

Emotet built itself into a significant part of the phishing threat landscape over several years, combining innovative tactics with an enormous volume of malicious emails. A law enforcement operation in January shut the botnet down, but as we predicted at the time, it returned to operation in November. This report examines what has changed and what has stayed the same about its behavior.

Emotet Installs Cobalt Strick

Cofense researchers detected Emotet loading other malware today for the first time since it resumed operations. For the last three weeks, Emotet has only spread itself, limiting its activity to sending malicious emails and expanding its installation base. Today, some infected computers received a command to install Cobalt Strike, a popular post-exploitation tool.

Emotet Showing Signs of Life

Nearly a year ago, law enforcement agencies in several countries cooperated in taking down the Emotet botnet. When we reported on it, we predicted that Emotet would return. We cited its operators' close ties with the operators of other malware families such as TrickBot as a likely vector for Emotet to rebuild. Starting yesterday, TrickBot has indeed begun to drop a new variant of Emotet. Several new Emotet command and control (C2) servers have also been brought online. We view this as a precursor to a total return to action by the Emotet botnet.

Delivery Mechanism Rundown

In line with projections from our Q3 Quarterly Trends Review, another commodity loader, DBatLoader, rose to prominence within the phishing threat landscape. CVE-2017-11882 increased its share of delivery mechanisms, rose to the top for this quarter, and often delivered DBatLoader. In turn, DBatLoader was used to deliver a variety of malware families. OfficeMacro laden documents were second in volume analyzed with Emotets return contributing to the volume. DotNET Loaders rounded out the top three delivery mechanisms for the 4th quarter and were commonly seen delivering Agent Tesla keylogger.

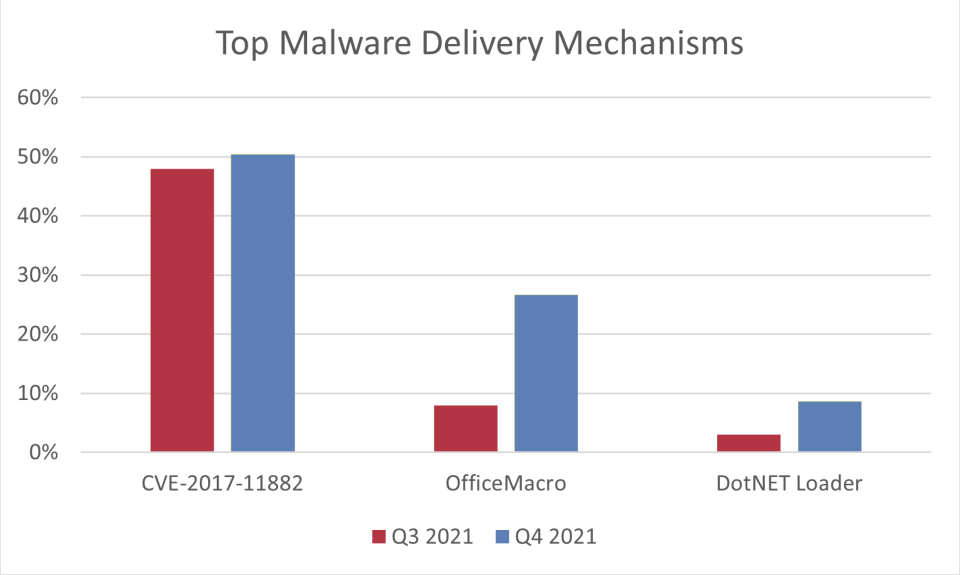


Figure 3: Comparison of malware delivery mechanisms as a percentage of the total in Q3 2021 and Q4 2021.

TLDs and Domains Used in Credential Phishing

In our Strategic Analysis, The Top TLDs Used in Credential Phishing, we analyzed Q2 data to determine which top-level domains (TLDs) and domains were most prominent in credential phishing emails that reached SEG-protected users. We ran the same analysis on Q4 data as we did in Q3 to establish a trend analysis for this report. We categorized URLs as Stage 1 if they were embedded in the emails and Stage 2 if the victim would have to take action (such as clicking a link) to reach them.

In both stages combined, most top TLDs were the same as in Q3. Domains using the .com TLD still account for approximately half of the total. Q4 showed more use of .ru, .app, and .ms due to a more significant number of URLs used within the credential harvesting campaigns.

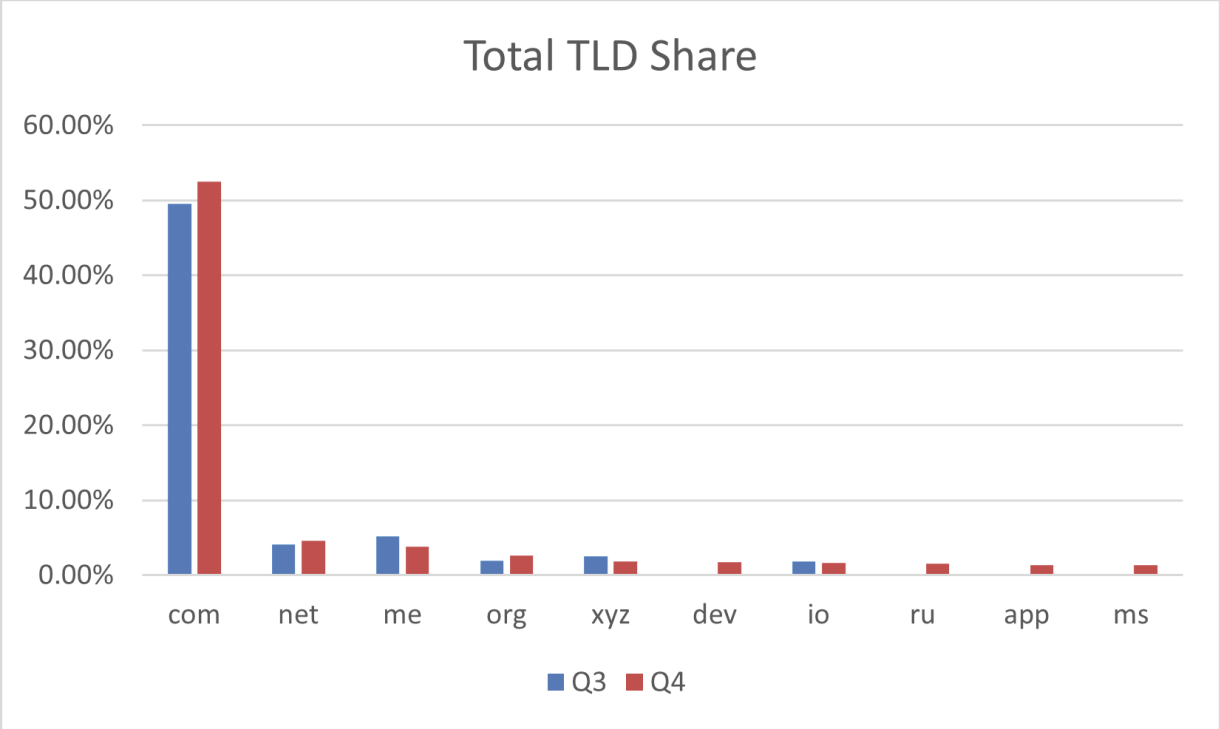


Figure 4: Top ten TLDs in Q4 compared with Q3.

Stage 1 URLs used .com for a more significant percentage of domains in Q4 than Q3, as shown in Table 2 below. From Q3 to Q4, the TLDs .xyz and .br, were replaced by .co and .app.

Stage 1 TLD	Q3 2021	Q4 2021
com	54.8%	55.3%
net	4.8%	6.1%
ms	5.5%	3.1%
io	3.2%	2.4%
org	1.3%	2.2%
ly	1.9%	2.1%
co	0.6%	1.9%
app	1.9%	1.6%
me	1.3%	1.5%
in	1.9%	1.4%

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

The share of .com domains increased substantially (by almost 5%) among Stage 2 URLs, as shown in Table 3. This is almost entirely attributable to a high volume of credential harvesting campaigns using .com. Between Q3 and Q4, the TLDs .cloud and .app, were replaced by .dev and .online.

Stage 2 TLD	Q3 2021	Q4 2021
com	45.5%	50.2%
me	8.3%	5.6%
net	3.6%	3.5%
org	2.5%	3.0%
dev	0.5%	2.7%
xyz	3.3%	2.5%
ru	1.5%	2.0%
uk	1.3%	1.6%
online	1.1%	1.5%
br	1.6%	1.4%

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

The ten most common .com domains in both stages were consistent with Q3, showing widespread abuse of trusted platforms:

- sharepoint
- live
- amazonaws
- google
- myportfolio
- digitaloceanspaces
- weebly
- oraclecloud
- backblazeb2
- eventscloud

Seven out of the ten most common domains using the .com TLD were the same as Q3. Adobe, WeTransfer, and GoogleAPIs were replaced by MyPortfolio, OracleCloud, and EventsCloud, respectively. Even with this change, we can see that cloud services are still being abused heavily within the phishing threat landscape during Q4.

File Extensions of Attachments

Our quarterly analysis revealed significant changes from Q3 to Q4 in the distribution of filename extensions on email attachments that reached users in SEG-protected environments. Overall, .pdf attachments were the top extension analyzed, at 33%. Attachments with .htm or .html extensions were still heavily used, and together accounted for 55% of the total. Most of these attachments delivered credential phishing attacks, either embedded in the files or with links to malicious pages.

PDF files continue to increase, rising 14% from last quarter. Archive files fell back to levels previously seen in Q2, a dip from Q3. Office files, .docx and .xlsx, remain within the top ten file extensions seen within the phishing threat landscape but have dipped in Q4 overall.

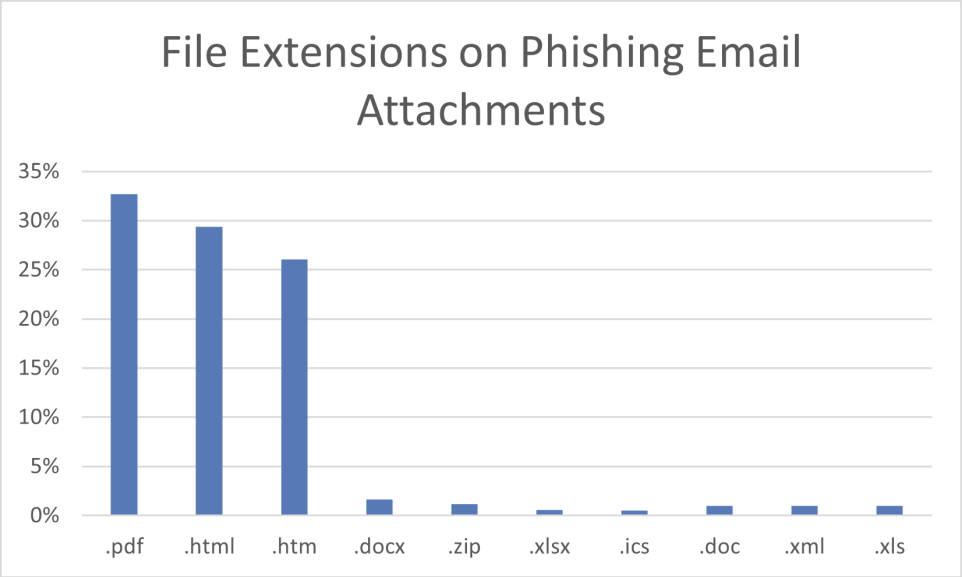


Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs

Command and Control Server Locations

Tracking Command and Control (C2) servers provide 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 United States maintained the largest share of the C2 locations worldwide. Servers in Germany decreased, but it was still the second most common location. Canada's share increased and helped to displace Russia from the top five. Great Britain returns to the top five from its Q3 ousting. 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.

Country	Percentage	Country	Percentage
United States	58.36%	United States	59.99%
Germany	4.76%	Germany	4.67%
Russia	2.95%	Canada	2.73%
Netherlands	2.65%	Great Britain	2.40%
Canada	2.63%	Netherlands	2.36%

Table 4: Q3 2021 and Q4 2021 percentages for C2 sources by IP address geolocation

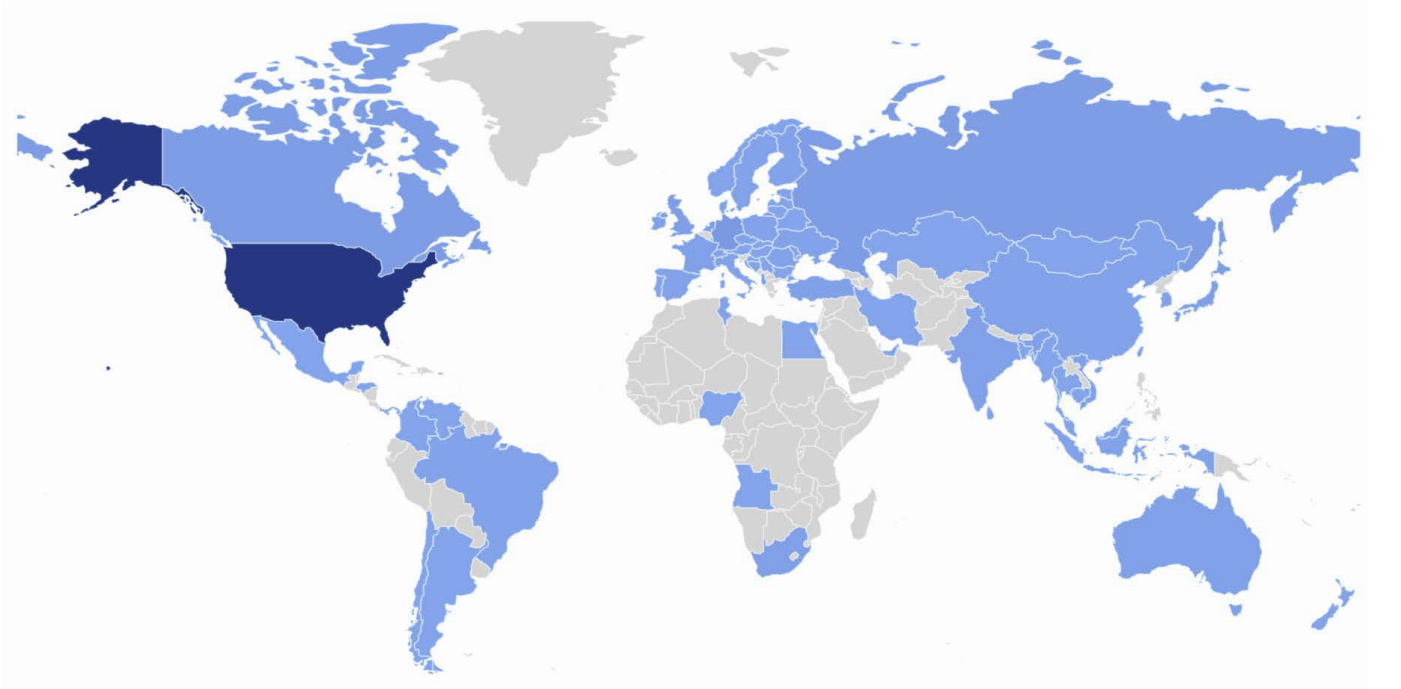
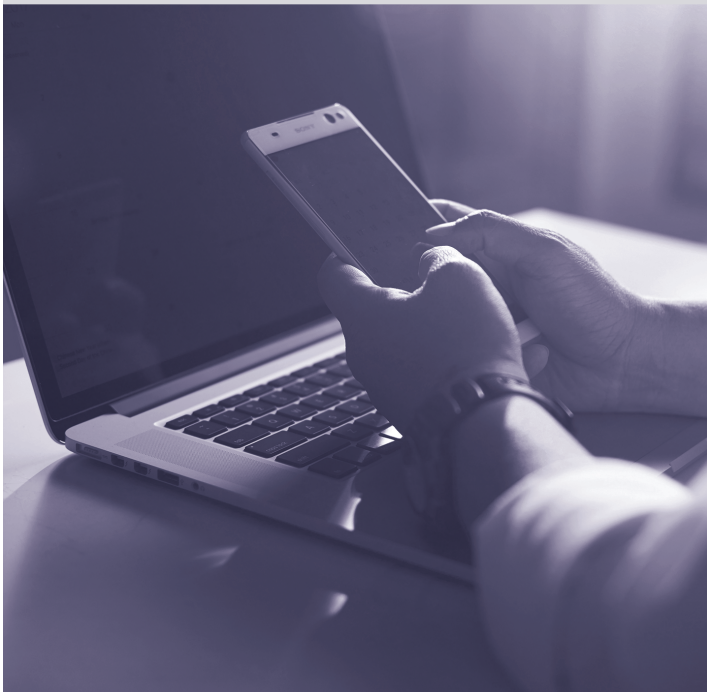


Figure 6: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Predictions for Q1 2022 and Beyond

Another Take-Down and Another Assumption

In light of the trend of global efforts to combat the cyber threat landscape, including the Emotet takedown in 2021 and the Trickbot takedown in 2020, we expect similar takedowns to occur in 2022. Such takedowns may lead organizations to wrongly assume that the targeted botnet will not re-emerge as a threat in the future.



In a January 2021 Flash Alert, Cofense Intelligence predicted that Emotet was likely to return after being disrupted by Operation LadyBird. Cofense Intelligence correctly predicted in Q3 2020, TrickBot did survive the attempted take-down and found new methods to deliver its payload. Botnet takedowns should be considered on a case-by-case basis, to assess whether they were successful in their aim.

Emotet to Expand and Experiment

Emotet activity has been intermittent but demonstrates significant efforts toward rebuilding its pre-takedown capacity. While Emotet has largely relied on tried and true TTPs for payload delivery since its return, Cofense Intelligence expects the botnet to gather steam heading into 2022, and to experiment with new methods. As the threat actors of Emotet re-emerge, they face the challenge of regaining the status they once had, which may lead them to experiment with new delivery mechanisms for their payload.