COFENSE

Q3 2021 Cofense Phishing Review

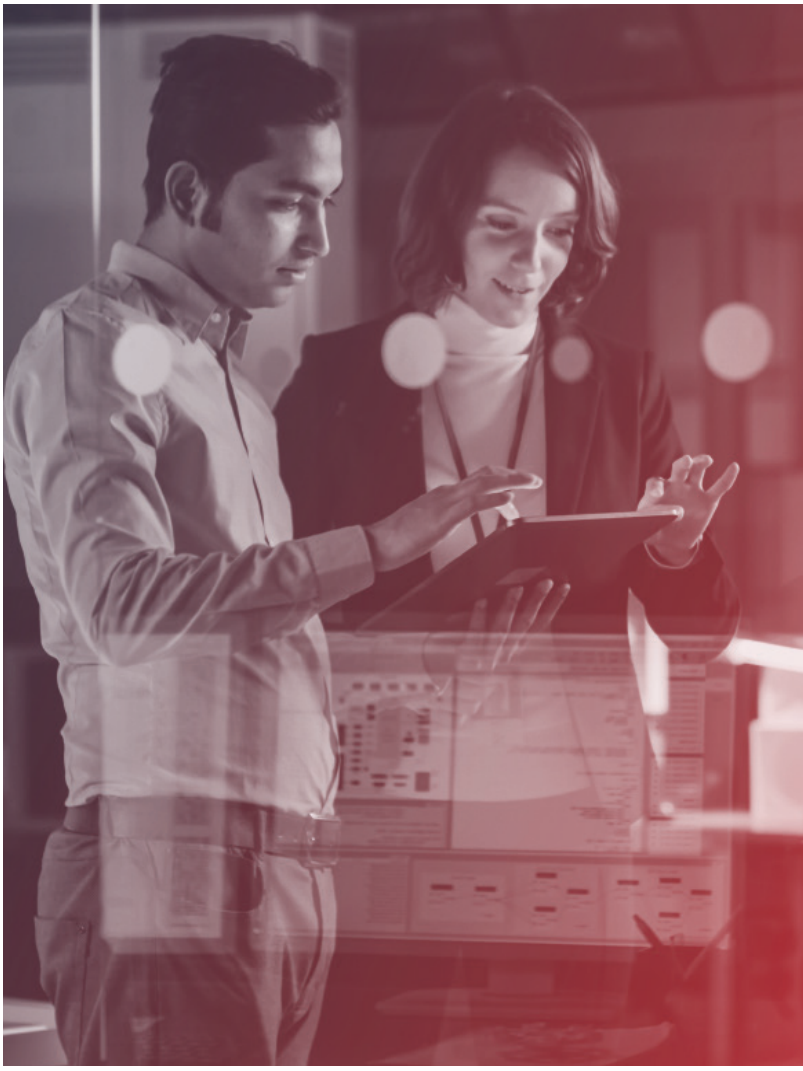
Strategic Analysis provided by Cofense Intelligence | cofense.com

Executive Summary

Despite a slight decline in July and August, phishing remained at high levels through Q3 2021, echoing the sustained summer activity we observed for the first time in 2020. Campaigns delivering malware continued to favor keyloggers, although information stealers began a steady climb in volume late in the quarter. The most common malware families continued to favor Office documents as a delivery mechanism, while simple downloaders written in Delphi were also used frequently. TrickBot campaigns used a remarkable variety of new delivery mechanisms, making it a malware family to watch closely in Q4. Patterns in threat actors' use of credential phishing domains and malicious attachment file types were generally consistent with Q2.

In our Q3 Strategic Analysis reports, we reported on the ways threat actors can use multiple layers of established tactics to take advantage of the inherent limitations of secure email gateways (SEGs). We also analyzed the relationship between phishing and ransomware attacks, and the use of current events in Afghanistan as phishing lures. In a Flash Alert, we warned customers of an emergent phishing campaign that primarily targeted executives, likely based on keywords in their publicly visible job titles.

In Q4, we believe conditions will be favorable for a new subscription-based malware



downloader to join the phishing threat landscape. Based on recent testing of new tactics, TrickBot campaigns will likely increase in volume and in breadth of targeting. Many of the economic pressures that emerged during the COVID-19 pandemic last year remain in place now, so we expect overall phishing activity to continue to follow the patterns set in 2020, staying high through the fall and only decreasing in mid to late December.

Overall Activity

As we predicted in our Q1 2021 review, overall phishing volume stayed elevated during the summer, with higher volume in Q3 2021 than Q3 2020. Activity declined gradually following a Q2 peak in June, but then picked up again in September, ending the quarter above the June high. No significant malware families emerged or disappeared during Q3. Instead, the trend lines reflect the ebb and flow of campaigns delivering the most common families. The acceleration of volume in late summer was a novel development last year and may repeat again this year.

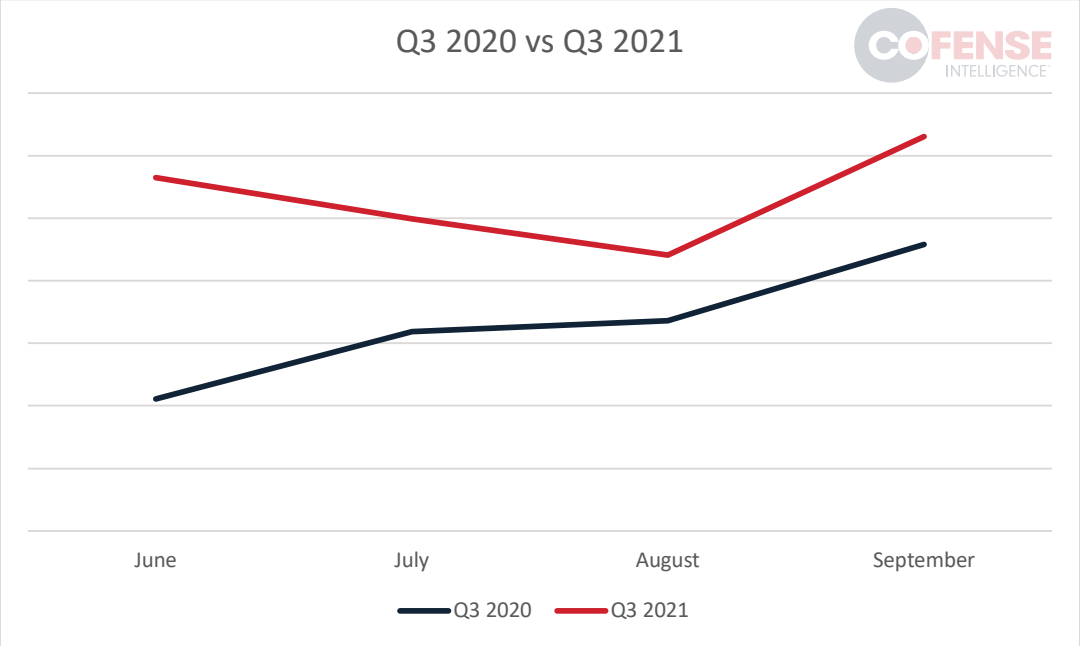


Figure 1: Overall phishing activity from Q3 2020 compared to Q3 2021

Prevalent Malware in Q3

The five most common malware types remained the same in Q3 as in Q2. Some of the most common malware families within each type did change, however.

Top Five Malware Type	Top Family in Type
Keylogger	Agent Tesla
Information Stealer	FormGrabber
Remote Access Trojan	Remcos
Banker	TrickBot
Loader	Chanitor

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

Agent Tesla remained the most heavily distributed keylogger throughout Q3. FormGrabber surpassed Loki Bot as the most common information stealer. Likewise, Remcos topped NanoCore as the top RAT. Q3 saw new versions and a rise in volume for TrickBot, which may be the start of a longer trend of increased activity by the banking trojan. Chanitor remained the most common loader, as it was in Q2.

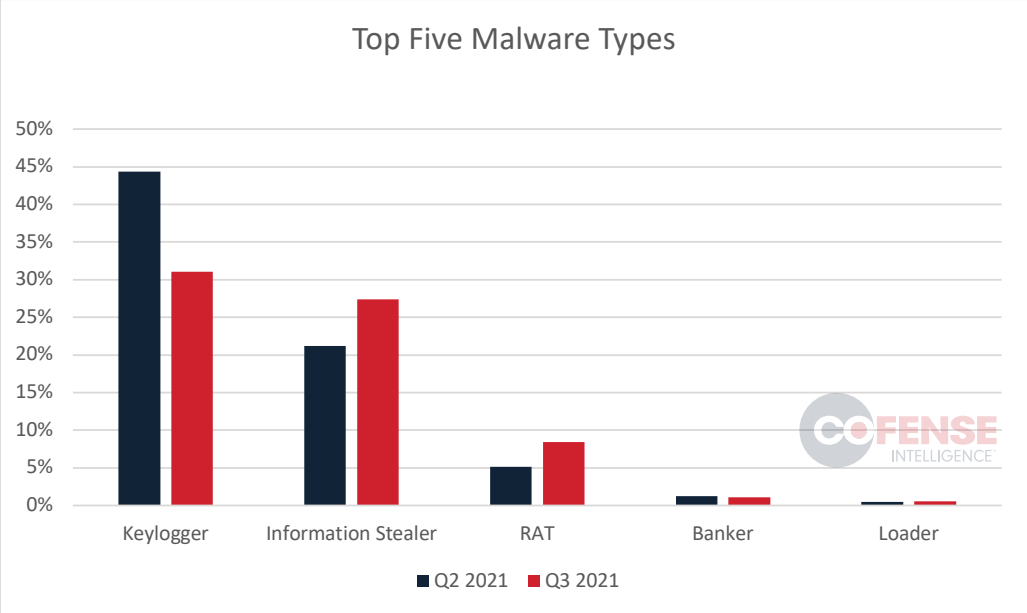


Figure 2: Top five malware types in Q2 2021 and Q3 2021, as a percentage of total campaigns.

Finished Intelligence: Topics and Trends

Throughout Q3 2021, Cofense Intelligence performed in-depth analysis on a variety of threats, to provide you with a strategic understanding of the phishing threat landscape, and to 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.

Threat Actors Exploit SEG Limitations to Help Phishing Threats Reach End Users

Cofense Intelligence observed three techniques in phishing campaigns that are likely used to help with secure email gateway evasion. The use of multi-layered links and redirection, multi-layered compression, and multi-layered encoding have each steadily increased within the phishing threat landscape. Chaining redirecting links together is a common technique used, while adding trusted platforms as the infrastructure further helps to circumvent analysis. Archives have always added a layer of obfuscation, but multiple compression layers of different compression types make detection less likely. Furthermore, we frequently observe multiple layers of encoding surrounding a malicious attachment found within SEG protected environments. Iteration limitations within SEGs may provide success to threat actors who simply add multiple layers to a known technique.

The Top TLDs Used in Credential Phishing

Customers asked us to find out which top-level domains (TLDs) are most commonly used in credential phishing emails. We analyzed malicious URLs reported by Cofense users during Q2 2021. Surprisingly, no individual TLDs stood out as a statistically significant indicator of malicious intent. Instead, our analysis shows that threat actors frequently use trusted third-party services to deliver, redirect to, or host their credential phishing pages. Based on our findings, TLD- or domain-centered threat mitigation measures are less likely to be effective than human-centered measures such as user education and human-vetted threat intelligence.

Password-Expiration-Themed Campaign Targets Executives

We analyzed a sizable credential phishing campaign that uses a password expiration notice lure targeting executive-level employees. The emails bypassed SEGs with the use of URL redirection, an increasingly popular tactic by threat actors. The campaign targeted individuals at multiple organizations across the finance, insurance, construction, and retail sectors.

Phishing as a Ransomware Precursor

In the context of cyber threats and security responses, ransomware has taken on a life of its own, and has become a major focus of media attention around the world. A large variety of other threat types exist, but many of those are broadly labeled simply as “malware” and “cyber attacks” in media coverage, while ransomware is specifically named. Although (self-evidently) using ransomware to acquire a ransom is the final objective of any ransomware operation, the process through which threat actors compromise and prepare victim networks for ransomware deployment involves an initial entry vector, as well as a host of other tools, malware, and infrastructure. In light of this, an excessive focus on the ransomware itself is counterproductive. By the time an actual ransomware binary is detectable within a targeted organization’s network, it may be too late to mitigate the impact. Thus, it is more important than ever to catch a ransomware operation at the phishing stage, before it is even identifiable as a ransomware attack.

Adversaries Could Evolve an XSS Phishing TTP for Greater Success

A widely-reported phishing campaign spoofing the UPS brand and using cross-site scripting (XSS) to deliver malware has reaffirmed that the end user is the last line of defense. This extensive campaign rendered a malicious download within the body of the UPS website, adding a sense of legitimacy to the phishing campaign. Cofense Intelligence identified that these reported campaigns successfully reached enterprise end users. Thus, these tactics, techniques and procedures (TTPs) clearly were effective for threat actors in getting the phishing email to the user inbox. However, we must think beyond defense of this TTP alone, as it would be easy for threat actors to iterate upon this campaign with URL redirects to further increase the effectiveness of their campaigns. This is a proof-of-concept report to demonstrate how easily small tweaks can result in more dangerous and effective phishing campaigns.

Taliban Takeover in Afghanistan Provides Fodder for Advance-Fee Phishing Lures

Threat actors are well known for developing campaigns based on world events; the Taliban takeover in Afghanistan is no exception. Cofense Intelligence observed a steady stream of Afghanistan-themed phishing emails in the wild during Q3, with a more limited selection actually observed reaching email inboxes within enterprise environments. We analyzed an assortment of advance-fee and inheritance scams using the news-worthy events in Afghanistan as a means for targeting victim’s emotions and financial interests. Common themes included CEOs of Afghan companies needing to liquidate assets before funds are taken, emails attempting to exploit religious and humanitarian tendencies, and various other proposals.

Delivery Mechanism Rundown

Office documents remained the most common delivery mechanisms in Q3. Specifically, CVE-2017-11882 increased in its share of delivery mechanisms. It was used to deliver a variety of malware families, most commonly Agent Tesla. Delphi loaders, primarily delivering Remcos, surged in August and September. Malicious Office macros decreased almost by half, but did remain in the top three as well. They delivered less-common malware families like Chanitor, BazarBackdoor, and StormKitty.

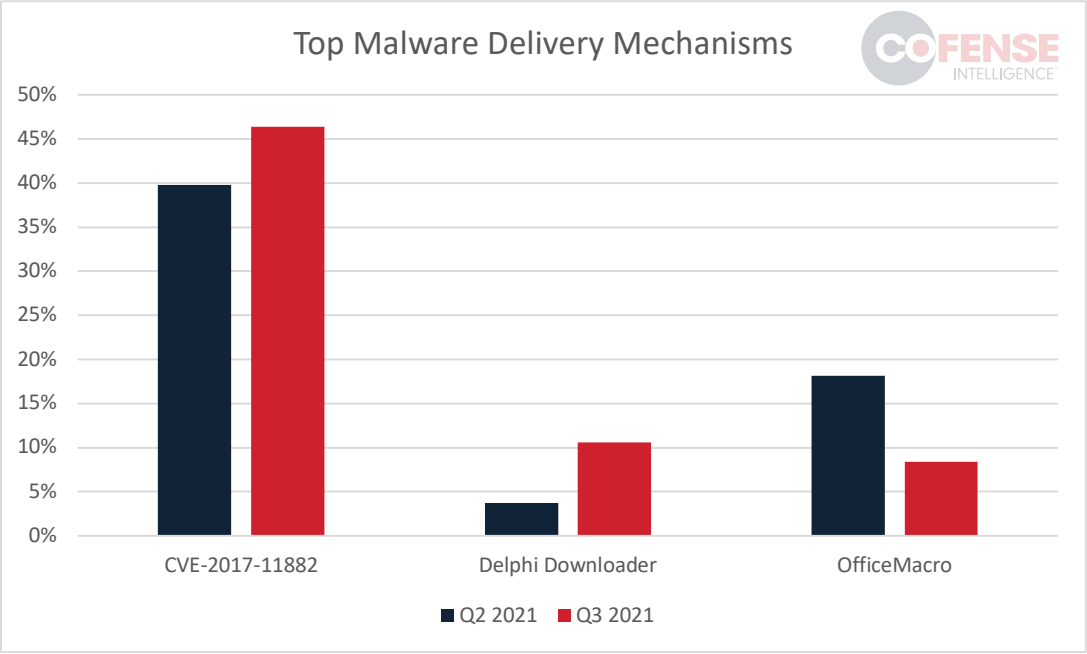


Figure 3: Comparison of malware delivery mechanisms as a percentage of the total in Q2 2021 and Q3 2021.

TLDs and Domains Used in Credential Phishing

In our Strategic Analysis, The Top TLDs Used in Credential Phishing, we analyzed Q2 data to find out which top-level domains (TLDs) and domains were most prominent in credential phishing emails that reached SEG-protected users. For this report, we ran the same analysis on Q3 data. 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, the top TLDs were consistent with Q2. Domains using the .com TLD still account for roughly half of the total. Q3 saw more use of .me than .net, due to a larger number of URLs from the code collaboration site Glitch, which uses the domain glitch.me to share projects.

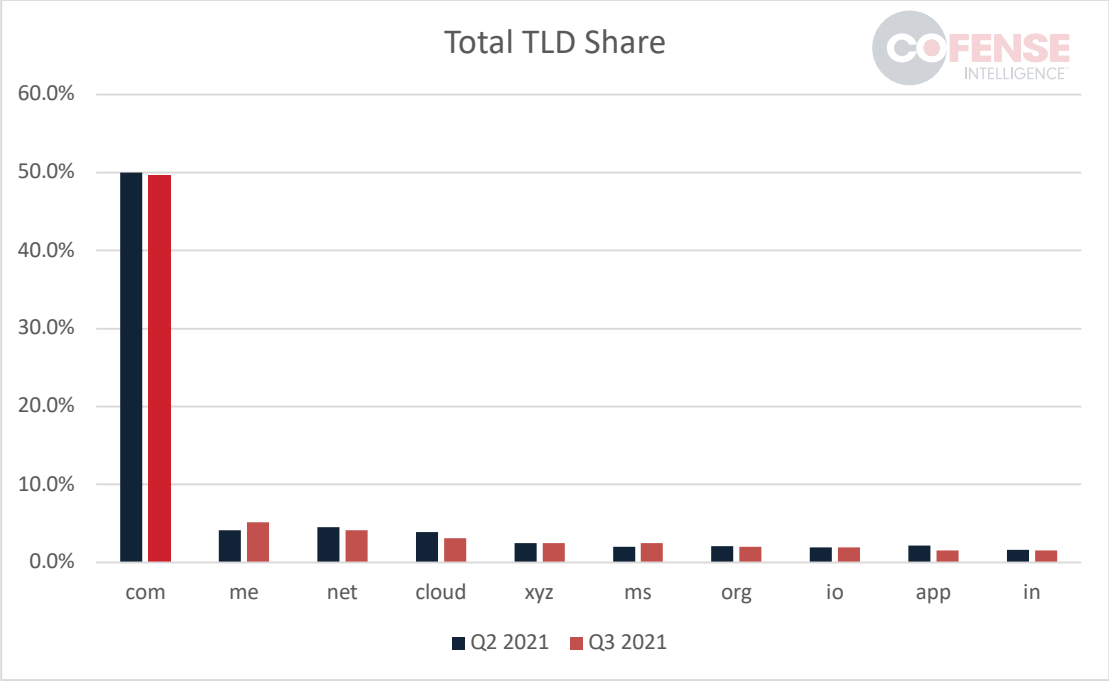


Figure 4: Top ten TLDs in Q3 compared with Q2.

Stage 1 URLs used fewer .com domains in Q3, as shown in Table 2 below. Two other TLDs made up most of the difference: .ms, primarily included in 1drv.ms links sent from compromised Microsoft accounts, and .io, used by a few code collaboration websites.

Stage 1 TLD	Q2 2021	Q3 2021
com	58.4%	54.8%
ms	2.3%	5.5%
net	5.0%	4.8%
io	2.0%	3.2%
in	1.4%	1.9%
ly	2.6%	1.9%
xyz	1.6%	1.5%
org	1.6%	1.3%
me	1.6%	1.3%
br	1.3%	1.2%

Table 2: Stage 1 TLDs in Q3 compared with Q2.

The share of .com domains also decreased slightly among Stage 2 URLs, as shown in Table 3. This is almost entirely attributable to the heavy use of glitch.me URLs.

Stage 2 TLD	Q2 2021	Q3 2021
com	48.2%	45.5%
me	3.4%	8.3%
cloud	6.9%	5.2%
net	3.7%	3.6%
xyz	3.0%	3.3%
org	2.2%	2.5%
app	2.0%	1.9%
br	1.3%	1.6%
ru	1.1%	1.5%
uk	1.4%	1.3%

Table 3: Stage 2 TLDs in Q3 compared with Q2.

The ten most common .com domains in both stages were consistent with Q2, showing widespread abuse of trusted platforms:

- sharepoint
- live
- amazonaws
- google
- adobe
- digitaloceanspaces
- weebly
- googleapis
- backblazeb2
- wetransfer

Threat actors used two website building services, Jimdo and Simplesite, so much during Q2 that their domains appeared in the list. However, those campaigns only lasted a few weeks. In the Q3 analysis, backup service Backblaze and file sharing service WeTransfer have taken their places in the top ten.

File Extensions of Attachments

Our quarterly analysis showed little significant change from Q2 in the distribution of filename extensions on attachments that reached users in SEG-protected environments. Attachments with .htm or .html extensions were still the most common by far, together accounting for 37% of the total. The majority of these attachments delivered credential phishing attacks, either embedded in the files or with links to malicious pages.

PDF files increased by 4% compared to the second quarter. .zip and .rar archive files also bounced back slightly from low Q2 levels, primarily targeting energy, healthcare, and construction organizations. Office files, .docx and .xlsx, rose as well, corresponding with the high use of CVE-2017-11882 and Office macros discussed above.

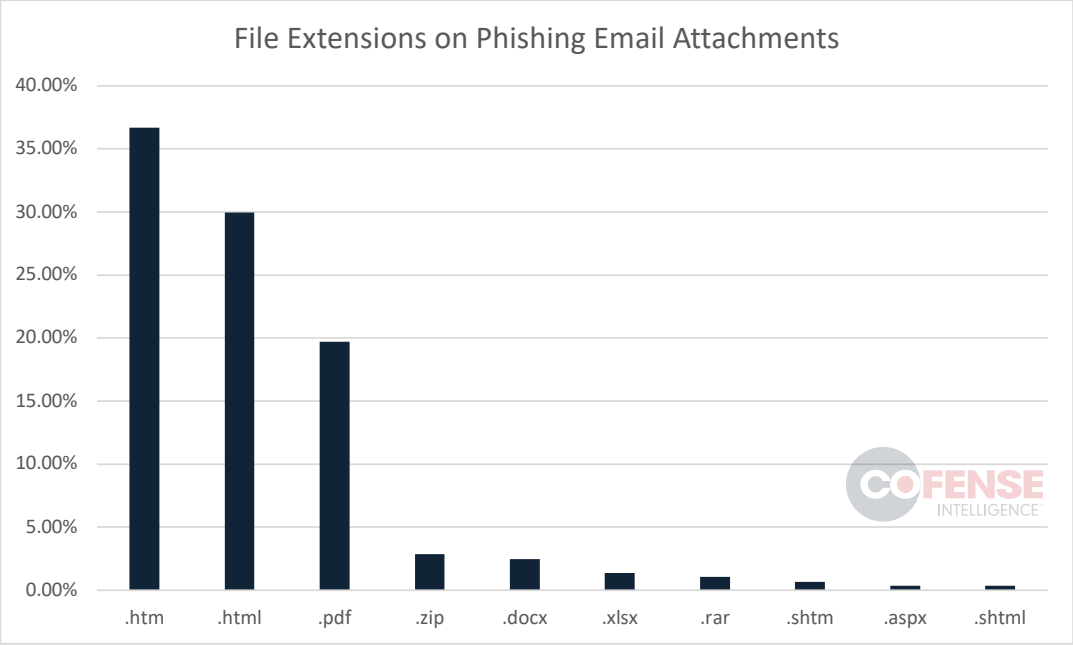


Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs

Command and Control Server Locations

Tracking Command and Control (C2) servers provides insight into a range of malicious cyber activity across the globe. These C2 nodes can deliver phishing campaigns or command malware and will 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. Hong Kong's share dropped slightly, enough to be replaced by Russia 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 location rather than where operations are originating.

Q2 2021		Q3 2021	
Country	**Percentage**	**Country**	**Percentage**
United States	58.87%	United States	58.36%
Germany	5.30%	Germany	4.76%
Hong Kong	2.94%	Russia	2.95%
Canada	2.57%	Netherlands	2.65%
Netherlands	2.54%	Canada	2.63%

Table 4: Q2 2021 and Q3 2021 percentages for C2 sources by IP address geolocation

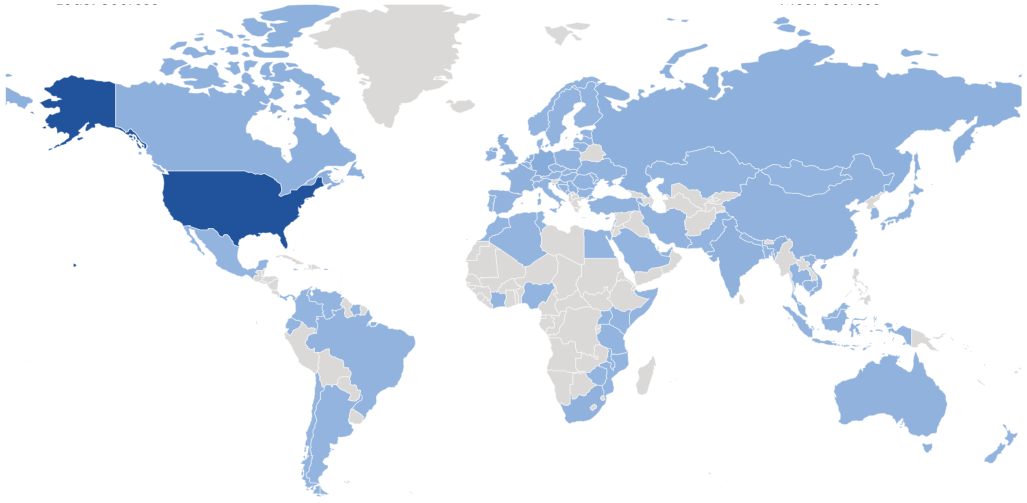


Figure 6: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Predictions for Q4 2021 and Beyond

Emergence of a new commodity malware downloader

GuLoader, a subscription-based downloader, has been steadily declining in volume during the last few quarters. Meanwhile, we've tracked an increase in one-off downloaders written in DotNET and Delphi. With advertised fees for GuLoader (operating as CloudEyE) ranging from $100 to $750 per month, the price may be too high for some threat actors. We think that the threat landscape is primed for a new commodity downloader to compete with GuLoader as a delivery mechanism.

Modification and increase in TrickBot activity

Having survived a takedown operation in October 2020, TrickBot has remained active in the phishing threat landscape. We recently identified campaigns testing new delivery methods for it, including LNK and CHM downloaders. This kind of testing is often a precursor to broader behavior changes. We also tracked TrickBot targeting multiple companies with one campaign. We believe that TrickBot will expand these broad-targeted campaigns, while also deploying improvements in the rest of its attack chain.

Novel activity trends from 2020 to be realized again in 2021

Earlier in this report we discussed high overall activity during the summer, with a further increase as we move into fall. Last year, this was a novelty that we attributed to the COVID-19 pandemic. Since the majority contributing factors we identified in 2020 are still in effect, we expect that overall threat activity throughout the rest of 2021 will follow 2020 trends. It will likely remain elevated through the fall, only starting to decrease during the holiday season.