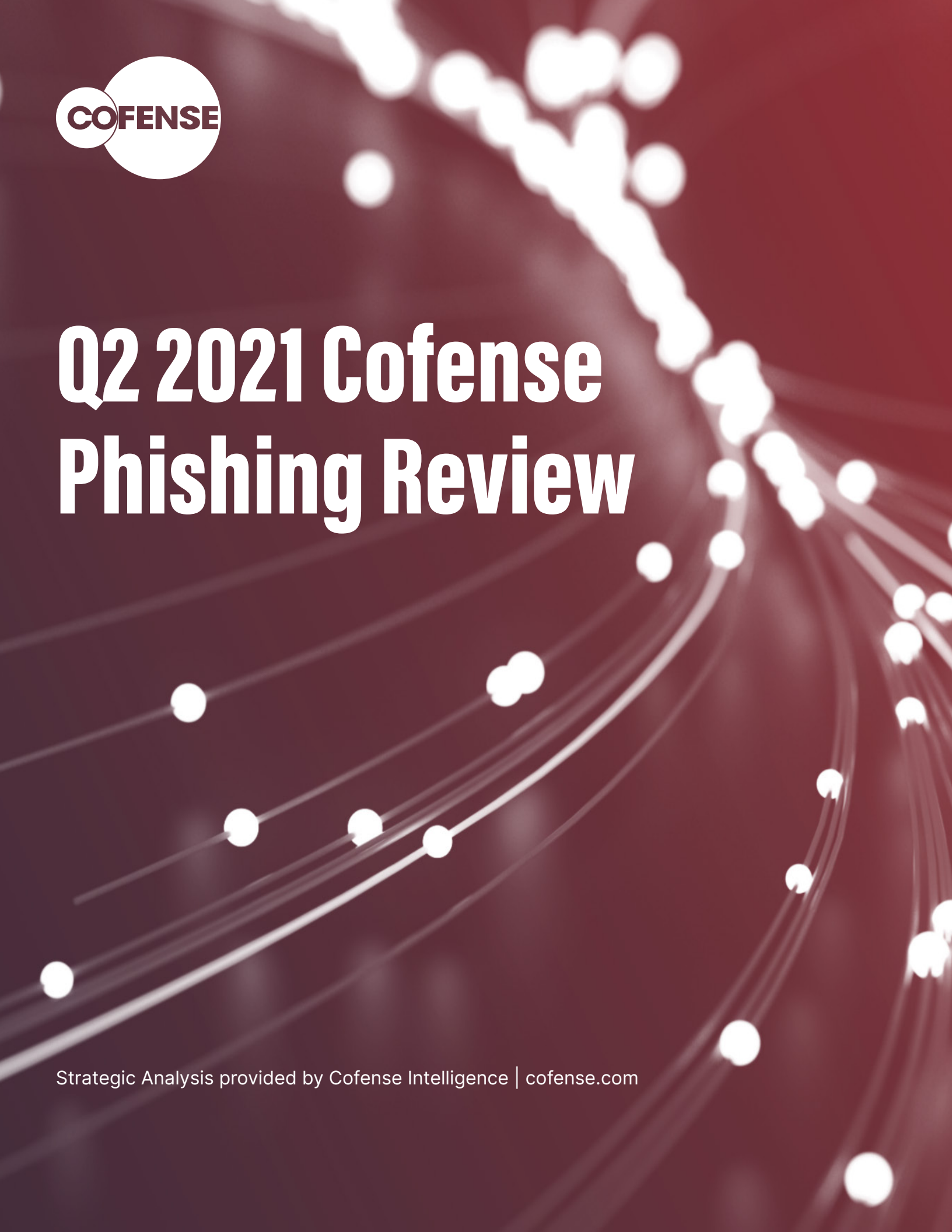

Q2 2021 Cofense Phishing Review

Strategic Analysis provided by Cofense Intelligence | cofense.com

Executive Summary

Q2 2021 showed a clear increase in overall phishing volume. The monthly phishing activity was largely duplicative of the Q2 2020 volume, following the same trends with higher fluctuations in the volume changes per month. Compared to Q1 2021, the top delivery mechanisms used to deliver malware-based phishing attacks stayed the same. CVE-2017-11882 and malicious Office documents remain the most common delivery mechanisms as threat actors can use these to target nearly every organization's attack surface. This is the first quarter following the Q1 Emotet takedown by law enforcement. The absence of Emotet resulted in a significant decrease in the volume for the Loader malware type.

Threat actors continue to utilize tried-and-true methods to bypass security. During this quarter, several phishing campaigns reaching enterprise users protected by secure email gateways (SEGs) were reported on in the form of Active Threat Reports (ATRs). Protecting against these campaigns is an essential part of a security operations center since a successful malware-based attack can be disastrous for an organization. Even though some malware attacks can be very profitable for threat actors, the cheaper prices and evasiveness associated with credential phishing remain attractive. A high percentage of phishing emails reported to the Cofense Phishing Defense Center (PDC) during Q2 2021 employed credential phishing rather than malware.

Going into Q3 2021, Cofense Intelligence anticipates an increase in overall threat activity. We also expect credential phishing attacks to continue to outpace malware-based attacks. Fluctuating COVID-19 situations around the globe will likely affect the volume of phishing emails using COVID themes, as well as overall participation in threat activity.

Overall Activity

The overall phishing volume during Q2 2021 increased compared to that of Q2 2020, but the volume pattern remained the same. Comparing monthly volume, both years showed an increase during April and June, and a decrease during the month of May.

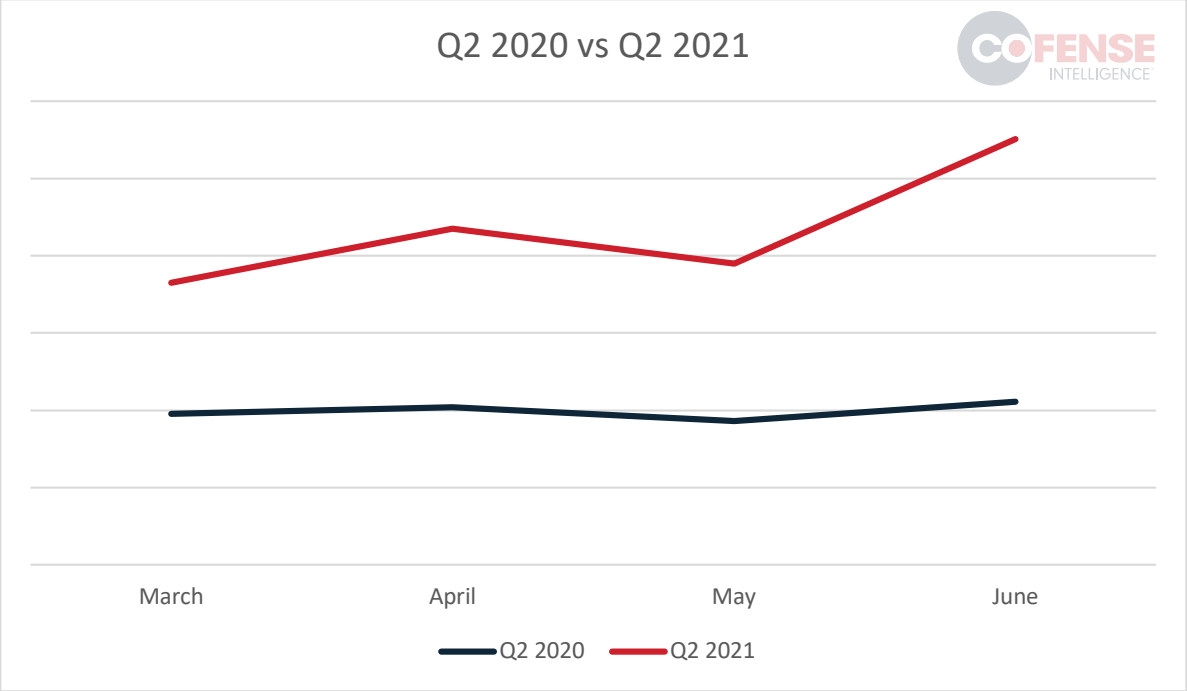

Figure 1: Overall phishing activity from Q2 2020 compared to Q2 2021

The monthly volume changes during Q2 2021 showed sharper percentage shifts than the previous year, however the changes did follow the same trends. Both years showed an increase in volume for April, a decrease in May, and a significant increase in June compared to the other months. The percentage changes were mostly driven by the volume of phishing emails that were dissemenated during the month. Overall, the changes were broad and the top malware families each month remained the same. Compared to Q2 2020 and Q1 2021, the overall volume during this years Q2 increased for each month. We will be tracking 2021 activity closely, as we expect the higher volume to continue throughout the coming months.

Prevalent Malware in Q2

The top five most common malware types, as well as the top five malware families within each malware type, had a few changes from Q1 2021.

Top Five Malware Type	Top Family in Type
Keylogger	Agent Tesla
Information Stealer	Loki Bot
Remote Access Trojan	NanoCore RAT
Banker	Dridex
Loader	Chanitor

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

The top five malware types remained the same with the bottom three changing positions. The Emotet takedown in Q1 resulted in the loader malware type dropping to the lowest spot on the chart, with Chanitor taking Emotet's place as the top malware family for that type. Keyloggers continue to hold the top spot among malware types, being represented by popular malware families like Agent Tesla, FormGrabber, and Snake keylogger. Nanocore was the top remote access trojan during this quarter, but Remcos RAT was still very common. Loki Bot and Dridex both held their positions from the previous quarter.

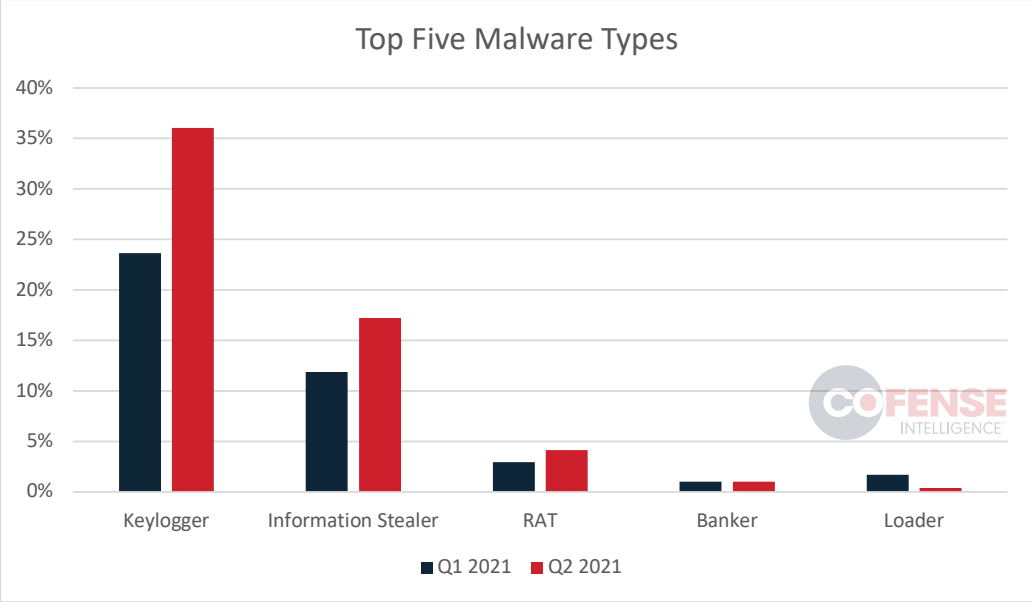

Figure 2: Top five malware types in Q1 2021 and Q2 2021, as a percentage of total campaigns.

Q2 2021 Credential Phishing Trends

Since late 2020, credential phishing has comprised an increasing percentage of campaigns reaching user inboxes. During Q2 2021, 78% of phishing campaigns reported by the Cofense PDC were credential phishing campaigns. Threat actors continue to prefer the cheaper prices and effectiveness associated with credential phishing, even though a successful malware-based attack can be disastrous for an organization. Cofense Intelligence reported on several trends seen within these campaigns, including the abuse of trusted cloud services and a multi-stage campaign that has used both open redirects and compromised domains to reach enterprise users.

Malware Campaigns Compared to Credential Phishing

Credential phishing typically harvests only what the victim can be tricked into divulging, and the interaction generally ends after the information is harvested. Credential phishing is cheap to deploy and can require minimal direct interaction from the threat actor after it is deployed. Stolen information can be sold or used by threat actors but, if done quickly, changing passwords is often enough to stave off serious harm.

In contrast, malware, once in place on the victim's machine, can continually harvest information and credentials, making password changes ineffective. Ransomware and other methods can even be used to extort victims for additional financial gain. However, malware is generally more expensive to deploy, and organizations are often better equipped to detect and prevent malware making it harder for threat actors to successfully deploy many forms of malware. Malware also typically requires more knowledge and more frequent direct interaction from the threat actor.

The largest overlap between these two methods of collecting information is the infrastructure used. One of the ways that threat actors get malicious emails into inboxes is by hosting malicious content on legitimate domains, such as docs[.]google[.]com. The malicious content can be anything from credential phishing landing pages to remote access trojan executables or other malicious files. Of all the legitimate domains abused to host malicious content, Google Docs was abused the most for both credential phishing and malware. The overlap was significant, with 13% of credential phishing and over 20% of hosted malware that abuses legitimate domains relying on docs[.]google[.]com for some of its infrastructure. This shows just how effective abusing legitimate cloud services can be for delivering almost any kind of malicious content.

Openly Advertised Commercial Phishing Services Reach End Users

During this quarter, Cofense Intelligence conducted a case study on a common thread linking credential phishing campaigns identified in many ATRs, hitting an unusually broad set of targets. We found that they are the product of a commercial phishing service operating in the open, with apparently little fear of reprisal. Despite operating openly and being reported by Cofense and other researchers, these campaigns have successfully reached numerous inboxes protected by several popular SEGs across a wide variety of industries. This allows for low-skilled threat actors to pay a modest amount of money for a effective attack that could potentially compromise accounts in any organization.

The campaigns we studied shared the same basic components. Lures were generic business-related topics such as shared files, requests for proposals, or notifications of new messages. The embedded links in the emails used a variety of trusted platforms, open redirects, or legitimate websites that had been hacked. Some of the common platforms included. The credential phishing page uses a smaller set of trusted platforms for hosting. These seem to be limited to cloud storage services. The most common ones in our analysis were Amazon S3, IBM Cloud Object Storage, and Backblaze B2.

The exfiltration destinations include a limited, persistent set of domains that have been established for months. The pages we examined exfiltrated data to two domains: first to apidatacss[.]com, and secondly to a rotating assortment of other domains. Based on the long-running malicious domains and servers, and the blatant, open sale of the phishing services, BulletProftLink is probably not a high priority target for coordinated action by tech organizations or law enforcement. But they've developed a very effective method to make sure credential phishing emails reach end users. The pages exfiltrated data to two domains: first to apidatacss[.]com, and secondly to a rotating assortment of other domains, shown in Table 2 below. We used passive DNS data to estimate how long the domains have been in operation.

Domain	First Seen	Origin Server
apidatacss[.]com	2020-01-03	31[.]28[.]168[.]4
smtpro101[.]com	2021-04-23	62[.]149[.]20[.]91
smtptemp[.]site	2021-02-19	62[.]149[.]20[.]91
plutosmto[.]com	2020-11-01	Unknown

Table 2: Exfiltration domains used in the campaigns we analyzed.

Trusted Cloud Services Abused in Credential Phishing

Popular cloud services such as Google Docs and Microsoft OneDrive are often abused because of their "trusted" status. Something that is considered "trusted" typically undergoes less scrutiny from SEGs than unknown content. This can be in the form of a URL embedded in an email which is ignored by a SEG because it is "trusted" or in the form of antivirus (AV) allowing a process to run because it is perceived as "trusted". Threat actors even take advantage of victim's "trust" in brands by spoofing well-known companies in emails.

Abusing cloud service companies like Dropbox allows threat actors to take advantage of the trusted status of Dropbox links to avoid some SEGs, spoof a known and trusted brand to take advantage of victim's trust, and potentially avoid network environmental controls. In the recent **Strategic Analyses** "The Trusted Cloud Services Abused Most in Evasive Credential Phishing" the statistics on cloud service abuse were examined and the top 5 cloud services most often abused for credential phishing were backblazeb2[.]com, googleapis[.]com, digitaloceanspaces[.]com, docs[.]google[.]com, and onedrive[.]live[.]com.

The Strategic Analysis "Google Docs Domain Abused Most as Multipurpose Tool" compared these to the legitimate domains used to host malicious payloads downloaded by malware, as well as the legitimate domains used to host payloads directly interacted with by victimes.
As can be seen in Table 3, the domains with the most overlap were docs[.]google[.]com and onedrive[.]com.

Domain	Victim Interaction %	Malware Payload %	Credential Phishing %
archive[.]org		3.59%	
backblazeb2[.]com	0.28%		33.00%
blogspot[.]com		7.17%	
cdn[.]discordapp[.]com	1.42%	12.11%	
digitaloceanspaces[.]com			15.00%
docs[.]google[.]com	20.74%	65.47%	13.00%
drive[.]google[.]com	31.53%	1.35%	
dropbox[.]com	2.84%		3.00%
feedproxy[.]google[.]com	9.94%		
googleapis[.]com	0.85%	0.45%	22.00%
onedrive[.]com	22.44%	5.83%	7.00%

Table 3: Comparison of Legitimate Domains Used to Host and Deliver Malware and Credential Phishing

Delivery Mechanism Rundown

The top three malware delivery mechanisms for this reporting period did not change from Q1 2021. CVE-2017-11882 and malicious Office macros remain the top two delivery mechanisms, since both can be used to target nearly every organization's attack surface. During this quarter, DotNETLoaders continue to be a popular delivery mechanism, often used in multi-stage malware campaigns.

- CVE-2017-11882 increased in volume and passed Office macros for the top position. This delivery mechanism is most commonly used for the delivery of Agent Tesla keylogger, FormGrabber, and various RATs. The vulnerability can be mitigated by disabling the Equation Editor in Office, but this is a necessary feature within some organizations.

- Malicious Office macros are a popular method to deliver a wide range of malware. The general use of Office within organizations makes this an effective delivery mechanism for threat actors. Time sensitive matters are often a popular theme for these campaigns by disguising the Office macros as financial inquiries, important notices, and other time sensitive documents. IT admins can set the default setting for macros to disabled, but this is another feature organizations find appealing.

- DotNETLoaders often contact URLs that contain hidden encoded binaries, the loader then encodes and assembles the data into a malicious payload that is then executed. We saw a slight decrease in DotNETLoaders for Q2 2021, in contrast to the surge we saw in Q1; however, DotNETLoaders still make up a large portion of the delivery mechanisms seen. The most common malware families disseminated by this loader during this quarter were Agent Tesla keylogger, Snake keylogger, and Async RAT.

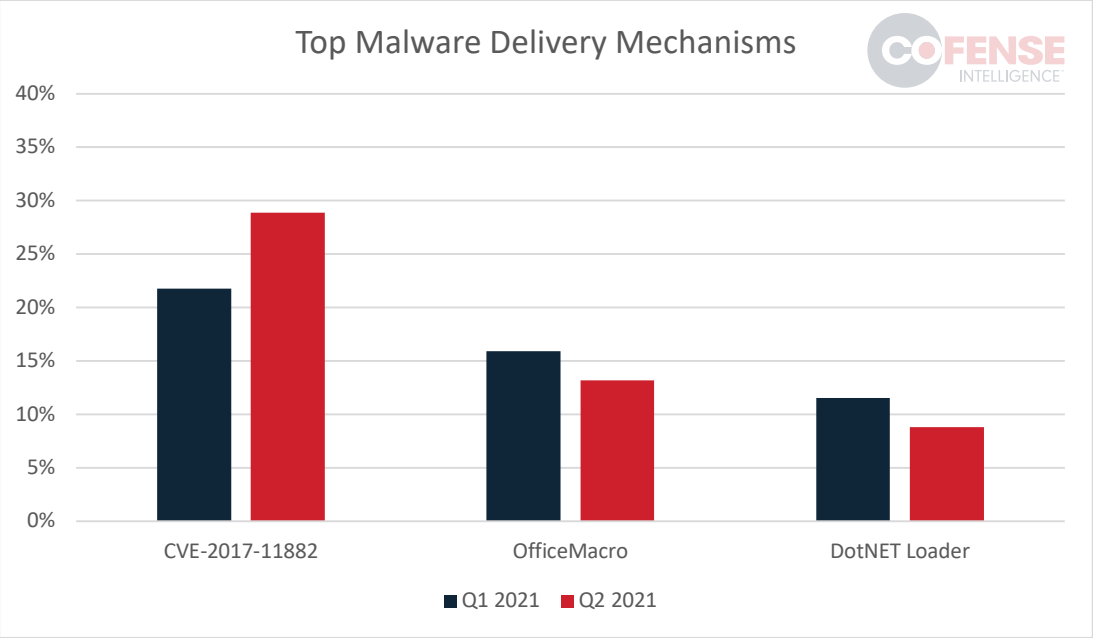

Figure 3: Comparison of malware delivery mechanisms as a percentage of the total in Q1 2021 and Q2 2021.

The chart shows the top three malware delivery mechanisms for this quarter in terms of volume. The following is a breakdown of other loaders and droppers that also made up a significant amount of volume, but did not make the top three:

- Malicious HTML and PDF files are more commonly associated with credential phishing campaigns but are also used for malware delivery. Both file types generally contain scripts to redirect to malicious sites opened in a web browser. These sites often contain malware downloads or credential phishing landing pages.

- VBS downloaders were seen delivering a variety of different malware families. These downloaders leverage Visual Basic runtime applications that are usually available within Windows environments to carry out the download and execution of additional malware binaries. Success of campaigns using this method of distributing malware relies on the presence of these runtime applications which are most commonly associated with a Microsoft Office installation being present on affected machines.

- Although not large enough to merit placement in the top three, the volume of GuLoader and Delphi loaders each spiked during this quarter. GuLoader is a portable executable that is written in Visual Basic, whereas Delphi loader is a more basic loader written in the Delphi programming language. Both delivery mechanisms were most used to deliver FormGrabber.

File Extensions of Attachments

As in previous quarterly reports, we examined the file extensions labeled on attachments that reached users in SEG-protected environments. In this quarter the prevalence of .zip archives decreased significantly from that of Q1 2021 and returned to levels seen in other previous quarters. This likely indicates a shift towards directly attached files as a corresponding uptick in other archive types was not present.

File extensions often used for delivering credential phishing, such as .htm, .html, and .pdf, continued to be popular with the mining and energy sectors combined making up over 50% of the volume for each of the three file extensions. Files with the .html file extension in particular saw increased volume as compared to the last several quarters. Not only did they overtake .htm files but they also increased in volume to account for almost 40% of the file extensions on phishing email attachments seen this quarter. These files were often customized with the name of the receiving company or individual contained in the file name. In contrast, .pdf files appear to have taken a drop as compared to previous quarters, however, their volume has remained steady while .htm and .html files have fluctuated. The presence of PowerPoint .ppt files was a surprise as they are typically rarer. In this case the files were seen as part of complex infection chains utilizing blogspot[.]com to deliver malware.

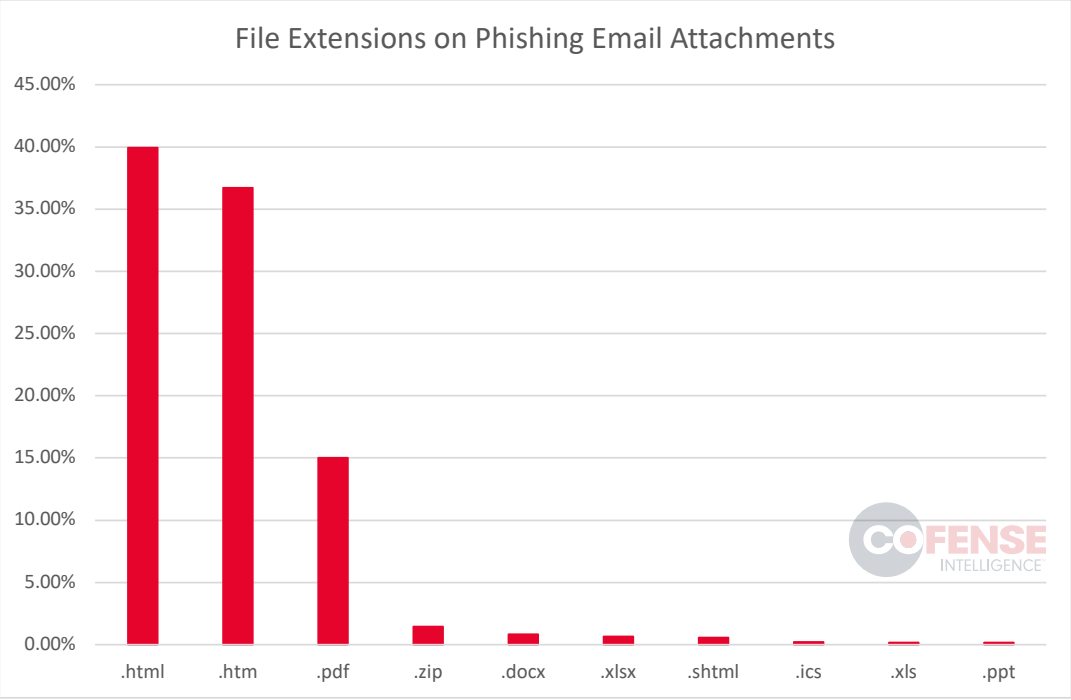

Figure 4: Top 10 most common attachment file extensions found in environments protected by SEGs.

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' share has gradually increased since Q3 2020, and accounts for the majority of C2 locations worldwide. Great Britain was replaced by Canada as a top five C2 location for this quarter in comparison to last. All the top locations for this quarter, except for the Netherlands, increased their overall share during this quarter. These statistics do not directly correlate with the full range of infrastructure threat actors use, and should only be interpreted as C2 location rather than where operations are originating.

Q1 2021		Q2 2021	
Country	**Percentage**	**Country**	**Percentage**
United States	55.30%	United States	58.87%
Germany	4.40%	Germany	5.30%
Netherlands	2.94%	Hong Kong	2.94%
Great Britain	2.79%	Canada	2.57%
Hong Kong	2.55%	Netherlands	2.54%

Table 4: Q1 2021 and Q2 2021 percentages for C2 sources by IP address geolocation.

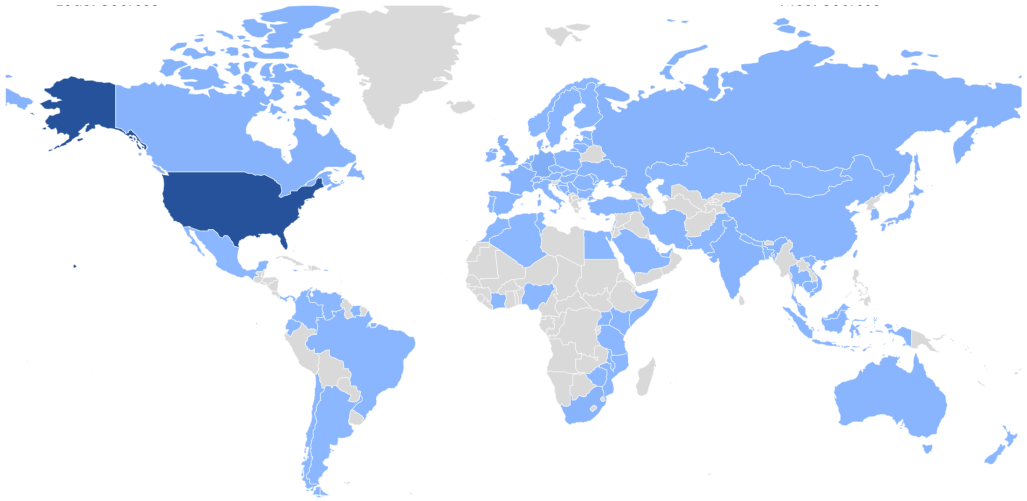

Figure 5: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

Predictions for Q3 2021

Fluctuating COVID-19 situations around the globe will impact overall phishing volume

With the ongoing global pandemic varying situation, it is likely that overall phishing volume will be impacted, along with the volume of phishing campaigns using COVID-19 themes. We expect to see an increase in overall phishing volume if COVID-19 situations continue to worsen. This could include a new wave of regional phishing campaigns that use specific COVID-19-related information to target end users, or just an increase in more generic phishing emails that target users who continue to work from home due to the pandemic. Previously, changes in new government relief and local government policies have been used as lures within phishing campaigns. Other possible themes are delta variant, business office re-opening notifications, and vaccinations. Further, the economic impact of COVID-related lockdowns may prompt increased participation in threat activity from economically stressed regions. As the global situation of the pandemic continues, expect threat actors to take advantage of the chaotic news cycle, as well as ongoing adjustments to new work environments.

An increase in password protected archives with passwords displayed in image form

SEGs have been able to open and analyze malicious password-protected attachments by scraping the password text offered in the email body. Threat actors have found a way to bypass this by displaying the password in an image, and using the image as the email body. When this image-based technique is used, it forces an end user to manually input the password in order to access the attachement. This tactic is more efficient at bypassing SEGs and could to lead to a higher infection rate. We expect that the use of this tactic will increase in the coming months.

The use of credential phishing will continue to outpace malware-based attacks

Credential phishing remains a prevalent attack vector and is very popular among threat actors. We have also seen that it is an effective method of bypassing security infrastructure. We expect that the percentage of threat actors using credential phishing will grow compared to that of malware-based attacks. The first stages of credential phishing can change entirely dependent upon the goals of the campaign, this often determines the campaigns' ability to bypass security. The volume of credential phishing we have seen successfully reaching end users compared to that of malware indicates a possible transition from malware, since a phishing attack that does not reach the inbox has essentially failed.