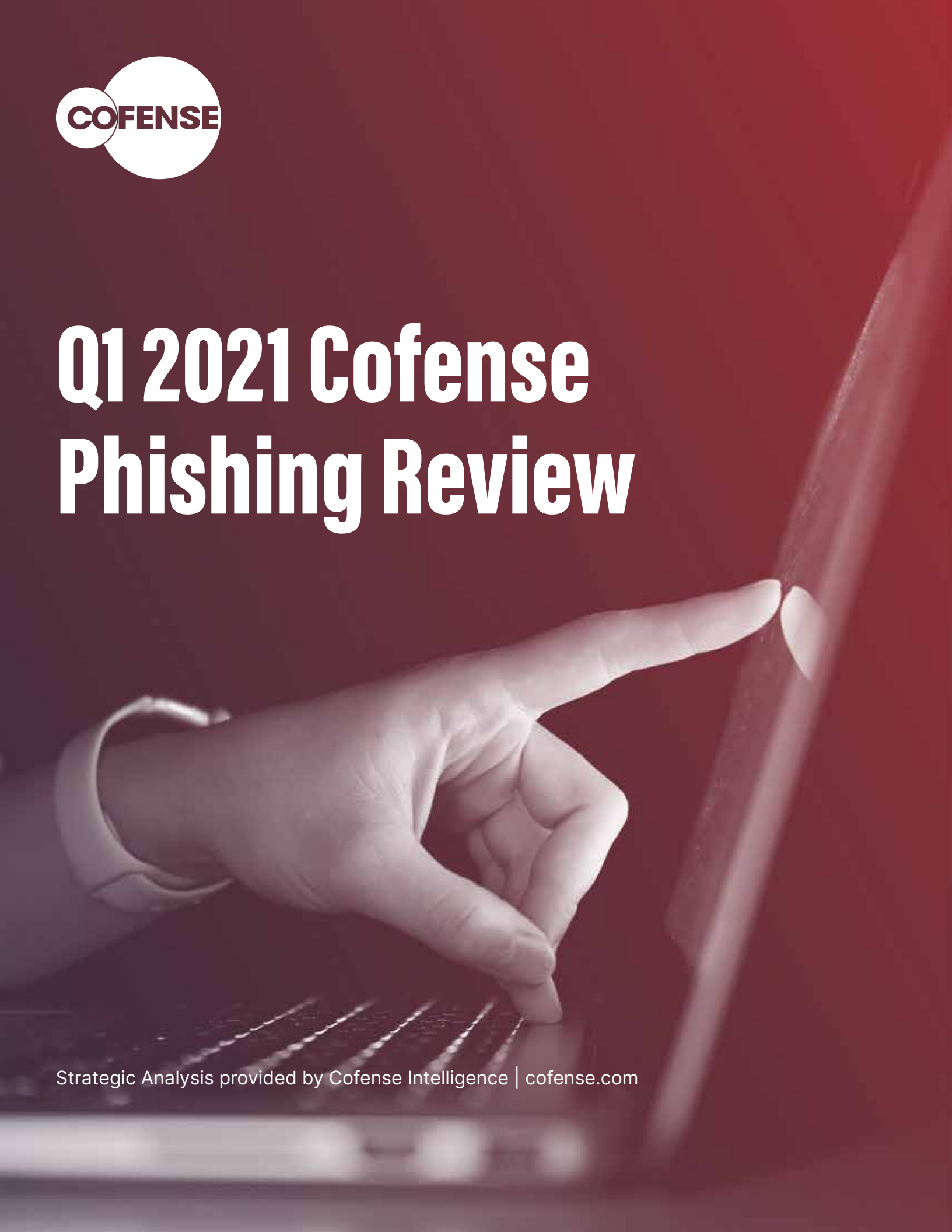


Q1 2021 Cofense Phishing Review

Strategic Analysis provided by Cofense Intelligence | cofense.com

Executive Summary

Q1 2021 was marked by a few notable changes and innovations in an otherwise-steady phishing threat landscape. Despite a slight dip in January, the most prominent malware families identified in this report increased overall campaign volume from the previous quarter. Emotet was the only exception, as it appears to have been completely disabled by its takedown by authorities in late January. HTML attachments and malicious Office documents remained the most common delivery mechanisms, but DotNET Loaders also increased sharply.

We did not see the same emergence of new malware families during Q1 as we did during each of the last few quarters. Instead, threat actors updated existing tactics, techniques, and procedures (TTPs), possibly adapting to environmental factors. We analyzed new campaigns delivering BazarBackdoor using uncommon lures and infrastructure that rely more on exploitation of victims' initiative than on technical efforts to evade protections. IcedID gained characteristics of other sophisticated banking trojans, including the email-reply-chain tactic, as well as a new delivery mechanism using corrupted payloads to avoid detection. Phishing campaigns attempting to install multiple malware families continue to increase.

The major disruptions of 2020 make it difficult to know what to expect going forward, but we're making three predictions for Q2 2021:

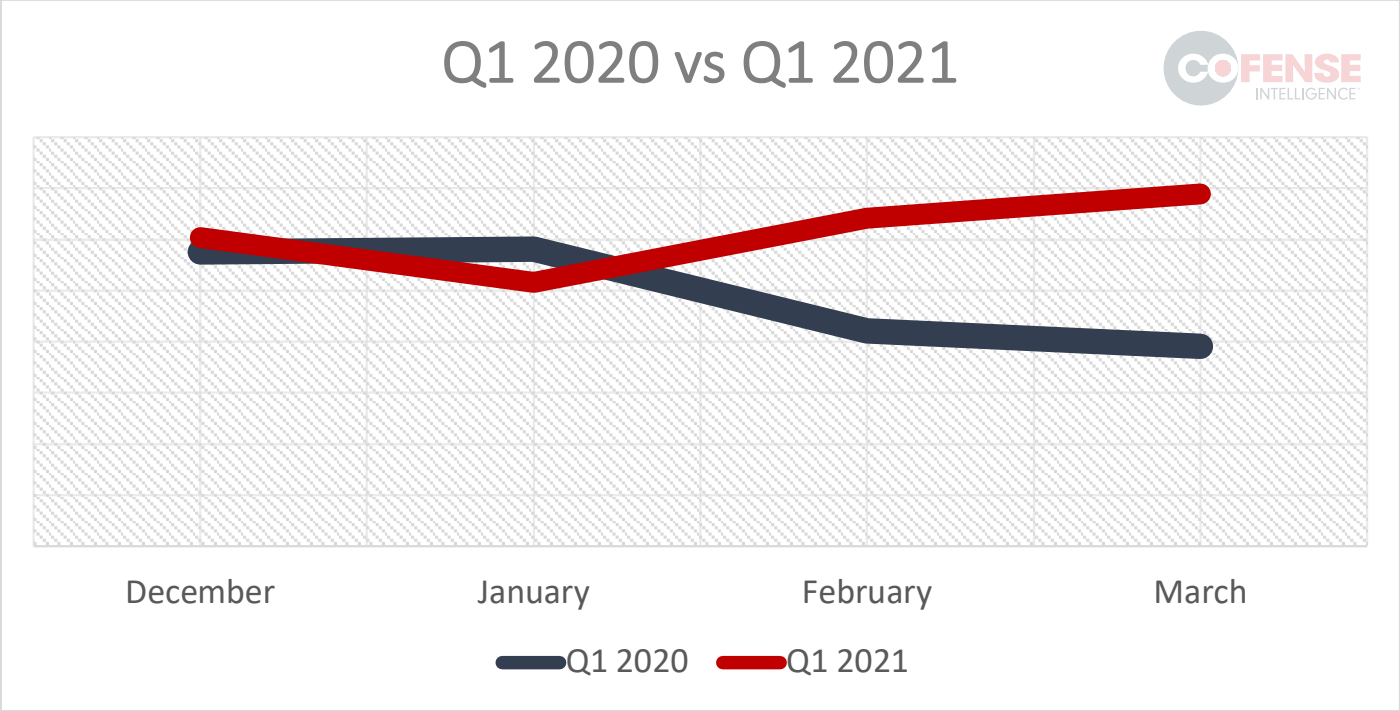
- Law enforcement action will drive innovation among malware operators.
- Threat activity will increase during the summer.
- The reply-chain tactic will continue to rise.

Overall Activity

Cofense Intelligence noticed an interesting change in overall phishing activity in Q1 2021 compared to the Q1 2020. Campaign volume held steady in January 2020, and then fell in February and March. But this year, volume dropped in January, then rose sharply in February and March, as shown in Table 1:

The dropoff at the start of 2021 represented only a brief return to normality from the unusually high campaign volume we saw in December 2020 and discussed in **our last quarterly review**. The decrease occurred across all malware families except Emotet, although Emotet's production also stopped after the law enforcement takedown in late January. The increases in the rest of Q1 are likewise broad: campaigns distributing all of the top malware families simply ramped up in February and kept volume high in March. The operators of Emotet are known to collaborate with other major malware operators, so an attempt to recover from the Emotet takedown may explain part of this spike.

2020 represented a notable increase in overall phishing activity, especially after the start of the COVID-19 pandemic. We will be tracking 2021 activity closely, as we expect the higher volume to continue throughout the coming months.



Prevalent Malware in Q1

The top five most common malware types, as well as the top five malware families within each malware type, remained unchanged from Q4 2020, except that loaders and Emotet dropped to third place:

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

Table 2: Top five malware types with the top family of each type.

Keyloggers led the way in the first quarter, as Agent Tesla and FormGrabber represented much of the higher volume during February and March. We also saw delivery of the Snake keylogger increase later in the quarter. Loki Bot was responsible for most of the information stealer volume, while RATs such as Remcos and Nanocore were also common. Bankers followed distantly in fifth place. Emotet was active enough in January to put loaders into the top five for Q1, but we do not expect it to return for many months, if ever.

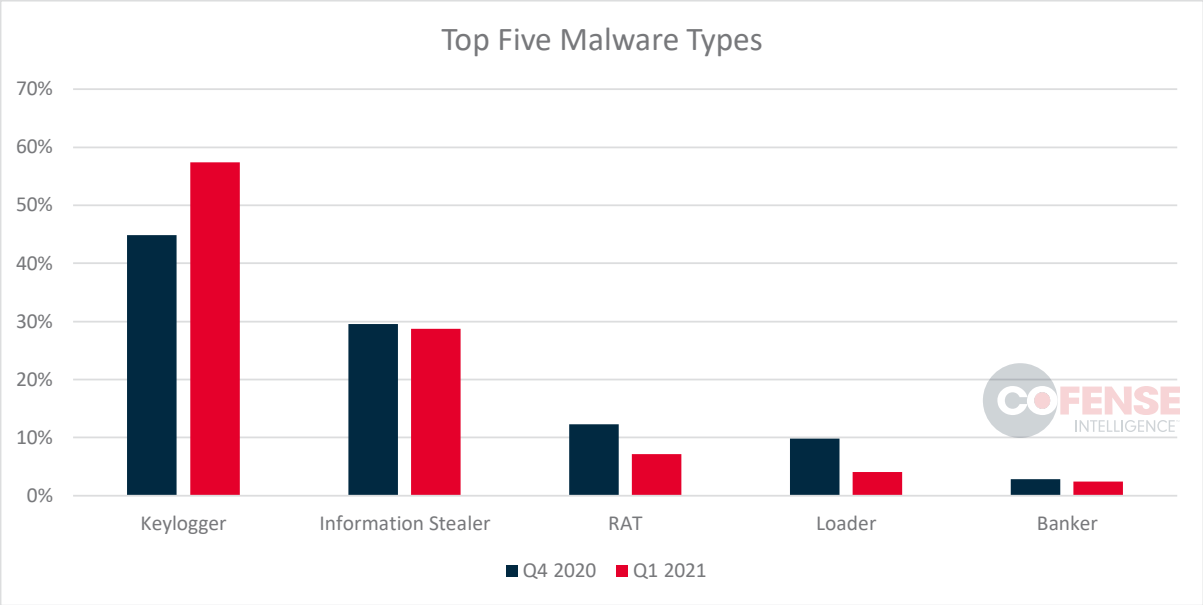


Figure 1: Top five malware types in Q4 2020 and Q1 2021, as a percentage of total campaigns.

New Developments

The Emotet takedown on January 27 had a major impact on the phishing threat landscape. During the rest of the quarter, we noticed some interesting developments in other malware families, which suggested an effort to adapt to the sudden loss of the Emotet botnet.

BazarBackdoor Innovations

During this quarter, we analyzed two campaigns using an unusual new set of lures, techniques, and infrastructure to disseminate BazarBackdoor. These campaigns avoid detection by foregoing common tactics such as embedded links or malicious attachments. Instead, they rely on the victims' own initiative to open the phishing sites and install the malware.

The first of the campaigns used lures based on order confirmations. Some of them were likely based on current events, such as fake order confirmations for flowers or lingerie around Valentine's Day. They did not include any malicious payloads or links, only a non-clickable version of the website corresponding to the orders. To be infected, users had to manually type the URL into their browser and enter their order number. The website would give them a malicious Office document and instructions to enable macros in it. The second campaign was similar, but did not even include a URL. Instead, it listed a phone number, as shown in Figure 1 below. Users calling the number reach a call center, where a live human operator talks them through the rest of the infection process.

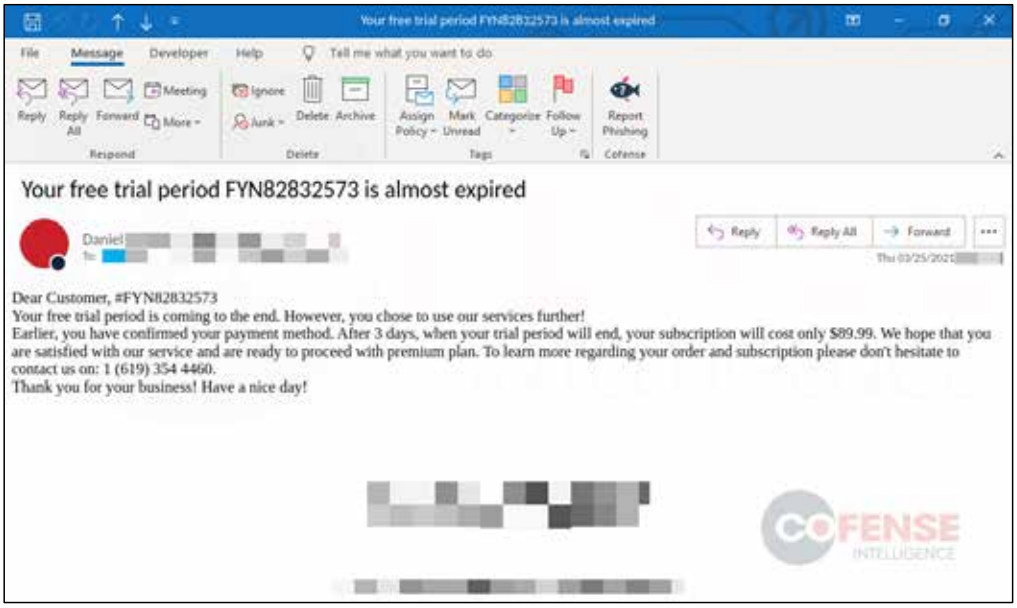


Figure 2: A campaign delivering BazarBackdoor using the subscription lure to direct users to a call center.

Phishing emails from both campaigns successfully reached intended victims in environments protected by secure email gateways (SEGs). The phishing emails from both campaigns require significant effort for victims to reach out to and engage with threat actors or their infrastructure. The addition of what seems to be a fully functional BazarBackdoor call center shows just how far threat actors are willing to go for a successful infection. See **BazarBackdoor Campaigns Exploit Victims' Initiative to Avoid Detection** for a full analysis of both campaigns.

IcedID Innovations

The banking trojan known as IcedID or Bokbot also went through new developments during the first quarter. Its authors implemented new TTPs that mimic other malware families, as well as a newer delivery mechanism. One of IcedID's newly-adopted TTPs is the use of the email reply-chain tactic. Threat actors use existing infections to scrape emails of compromised users. They weaponize these by resending the scraped emails to contacts within the email chains, which makes recipients more likely to trust and open the message. Other prominent malware families have enjoyed success with this technique, including Emotet and QakBot.

The delivery mechanism used in this campaign also changed, moving to a malicious Excel version 4.0 document as the first stage. The use of version 4.0 macros in an infection chain is a **growing trend** within the phishing threat landscape. For example, it is often seen as the first-stage loader for TrickBot. Once the macro is enabled, it attempts to connect to up to three different locations in order to download a sample of Gziploader, a relatively new delivery mechanism.

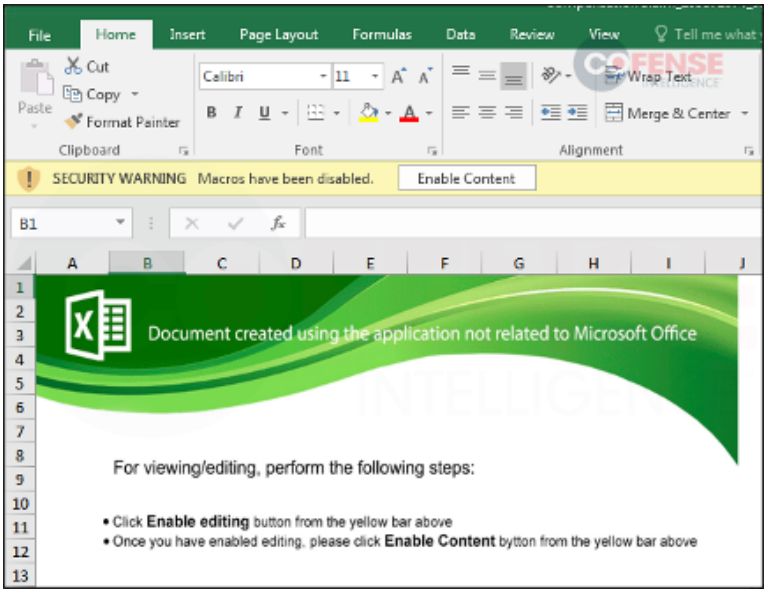


Figure 3: An Excel 4.0 document delivering IcedID.

In addition to the email content and delivery mechanisms, IcedID itself also underwent some significant changes. We discussed all of these changes in more detail our April 1 **Strategic Analysis**. The operators of IcedID have known relationships with operators of Emotet and TrickBot, both of which have seen success using similar TTPs. We are watching to see if further merging of TTPs takes place between IcedID and other families.

Multi-malware Campaigns

A longer-term, growing trend that we also observed in Q1 is the delivery of multiple malware families in one campaign. Since even the most sophisticated campaigns yield a limited number of infections, installing multiple families is a good way for threat actors to get the most out of their phishing attempts.

Q1 2021 in particular saw a high number of these campaigns. Keyloggers are often included as one of the malware families. This quarter, we saw Agent Tesla delivered alongside Snake and Matiex keyloggers, as well as FormGrabber, Remcos RAT, Loki Bot, and Lime RAT. These campaigns are unusual because the malware families were delivered as either multiple attachments to one email or as part of a predetermined download order. Most multi-family campaigns use a first stage loader to establish persistence and perform some reconnaissance. A command-and-control server determines which payloads, if any, will be delivered next. In these cases, the payloads are often customized according to the compromised environment.

The distinction between predetermined versus customized malware delivery is important, as it may offer some insight into the threat actors' purpose. Many of the families delivered via the predetermined method are commercially available malware such as Agent Tesla and the others mentioned above. Meanwhile, the malware being delivered based on infected environments is often more customized, such as PowerShell scripts that are used for in-depth reconnaissance.

Delivery Mechanism Rundown

The top two delivery mechanisms for malware in Q1 2021 were malicious Office documents. Office macros continue to rank highest, likely because they still work well, and are easy to use in targeting a part of nearly every organization's attack surface. Similarly, CVE-2017-11882 can be mitigated by disabling the Equation Editor in Office. However, because of the need for the feature within some organizations, it continues to be abused by threat actors.

DotNET Loaders also surged as malware delivery mechanisms during the first quarter, most commonly delivering Agent Tesla. These loaders are simple DotNET executables, included as attachments. They often contact one or more benign-looking websites which contain hidden encoded binary data. The loaders are able to decode and assemble the data into a malicious payload, then execute it.

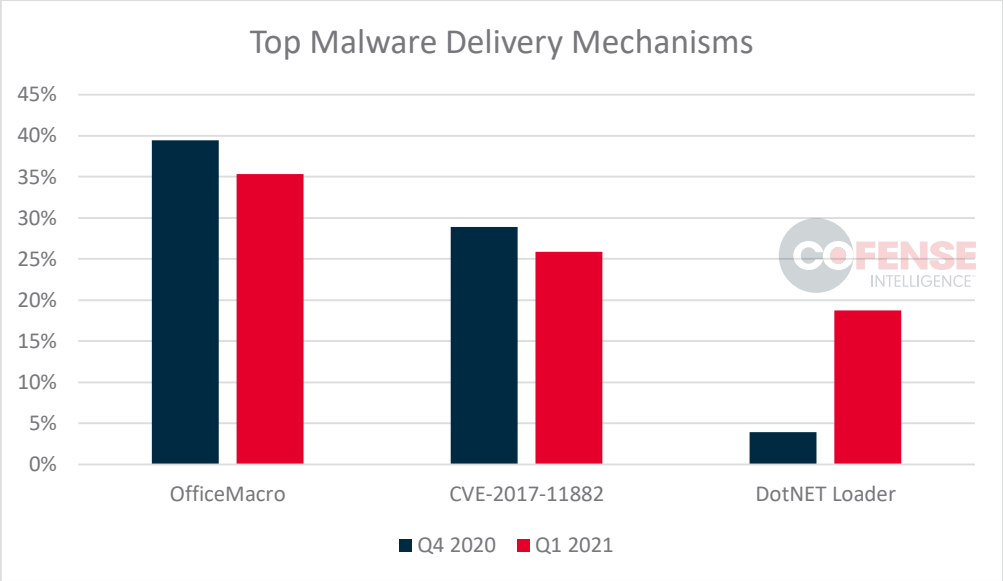


Figure 4: Comparison of malware delivery mechanisms as a percentage of the total in Q4 2020 and Q1 2021.

Embedded links were the most common delivery mechanism for credential phishing. HTML attachments were also prominent for credential phishing, along with a smaller amount of malware delivery. These attached HTML files are typically small and only contain a script that redirects to a malicious site when opened in the browser. The payloads on the malicious landing pages vary, from malware downloads to credential phishing pages. Some of the HTML attachments we analyzed during this quarter were encoded in multiple ways in order to thwart detection or analysis.

As discussed above, we analyzed a new delivery mechanism named Gziploader delivering IcedID during this quarter. Gziploader replaces PhotoLoader, bringing a new way of evading analysis of its payloads. After fingerprinting the infected machine, it calls out to a configured benign site and saves the response. This response and fingerprint information is then used within the HTTP get request for a payload—in this case, IcedID.

Gziploader gets its name from downloading a gzip archive as the payload. However, the gzip archive is intentionally corrupted, and Gziploader fixes it to then decompress and extract the desired payload. This intentionally broken aspect of the payload helps it to evade analysis and be seen as benign. Gziploader is also more likely to pass an initial analysis as benign since it only calls out to legitimate websites. If the right information is not supplied, it terminates itself. This delivery mechanism was one of the many items that are new to IcedID's TTPs.

File Extensions of Attachments

Continuing analysis from our most recent quarterly reports, we examined filename extensions on email attachments that reached users in SEG-protected environments during this quarter. Compared to Q4 2020, the top file extensions remained unchanged, although the order was shifted. As expected, the primary credential phishing vectors of .pdf, .htm, and .html files continued to maintain the lead. However, .pdf volume in particular declined, allowing a more balanced representation among the other top file extensions.

An unusual aspect of this is that .pdf files have been used in new campaign types, such as the BazarBackdoor campaigns discussed earlier, without containing any detectable malicious content or links—yet they still decreased in overall volume. Previously, a small number of sectors received a majority of the .pdf files delivered. During Q1, however, .pdf file delivery was more distributed, with the top five recipient sectors all being within a few percentage points of each other.

The outliers in this quarter's analysis were .zip attachments, of which the real estate sector received almost 50%, and .xls attachments of which the energy sector received over 55%. The remaining major change to the file extensions of phishing email attachments was the disappearance of .bat files in favor of .jnlp files. This is not surprising as the .bat file extension is often used to disguise malicious executables which should be easily stopped. The .jnlp file extension is also a surprise as its contents are easily read, however, several campaigns delivering these files were seen across multiple sectors.

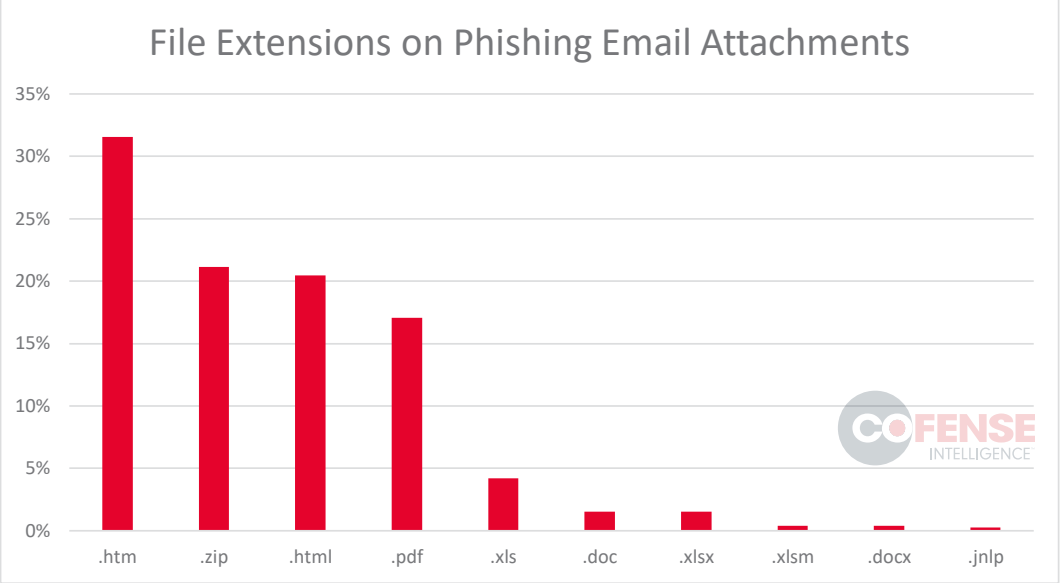


Figure 5: Top 10 most common attachment file extensions found in environments protected by SEGs.

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, command malware, and often will receive information and exfiltrated data from infected hosts. The United States accounts for the majority of C2 locations worldwide, and has gradually increased since Q3 2020. The Netherlands and Hong Kong replaced France and Canada as top five C2 locations for this quarter compared to last. The overall share held by the top five locations increased by a total of 3.85%. 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.

Q4 2020		Q1 2020	
Country	**Percentage**	**Country**	**Percentage**
United States	52.19%	United States	55.30%
Germany	4.50%	Germany	4.40%
France	2.67%	Netherlands	2.94%
Great Britain	2.50%	Great Britain	2.79%
Canada	2.27%	Hong Kong	2.55%

Table 3: Q4 2020 and Q1 2021 percentages for C2 sources by IP address geolocation.

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

COVID-19 Theme Continuation

The COVID-19 pandemic remained a significant issue through the first quarter, with relief spending, virus variants and surges, and vaccine rollouts keeping it in the news. Although COVID-19-themed campaigns appeared to be waning in late 2020, threat actors did continue to take advantage of the subject in Q1. Lures included testing, vaccination, and relief funds. Campaign volume stayed consistent through the quarter. The majority of the campaigns we analyzed delivered credential phishing.

Predictions for Q2 2021

Law Enforcement Action Will Drive Innovation Among Malware Operators

Developments and adaptations are a constant in phishing threat activity, but many of the changes particular to Q1 of this year may represent a recognition by malware operators that they can suddenly lose a significant portion of their infrastructure to law enforcement. Addressing this risk may involve branching out into lower-sophistication efforts like the BazarBackdoor call centers, adapting malware to fill a vacuum like IcedID, or squeezing every bit of value possible out of successful infections with multiple-malware installations. We believe we will continue to see creative new innovations from the major malware operators as the year progresses.

Threat Activity Will Increase During Summer

Summer has been the busiest season for phishing threat actors for the last several years. We believe this trend will continue, especially given the strong start in Q1. We attributed much of the increase last year to the COVID-19 pandemic. While the pandemic may finally recede as vaccinations increase, the negative economic effects will almost certainly linger, making sustained threat activity much more likely.

Reply-Chain Tactic Will Continue to Rise

We've analyzed various campaigns, which include multiple different malware families, using the reply-chain tactic to make users more likely to trust malicious emails. Banking trojans, in particular, have made use of this tactic. Emotet enjoyed success with it throughout 2020, and now IcedID is using it. We expect that its use will increase over the course of 2021, especially among established malware operators with access to more users' email content.