COFENSE™

Q3 2020

PHISHING REVIEW

Strategic Analysis provided by Cofense Intelligence | COFENSE.COM

Executive Summary

Phishing threat activity remained high in volume during the third quarter of 2020, breaking with a trend of summer lulls in previous years. Threat actors created new malware families—particularly in the Remote Access Trojan (RAT) and ransomware phenotypes—and brought older ones back in phishing campaigns. Emotet contributed to the busy summer after months of inactivity, bringing new campaigns and adjusted tactics. All of this added variety on top of consistent trends such as the use of Agent Tesla keylogger.

The top delivery mechanisms in Q3 remained consistent with Q2, although changes in threat activity caused their relative volume to change. C2 server locations largely stayed consistent from Q2 as well, with Russia being a notable exception in falling from the top five. Threat actors used a variety of attachment types to successfully evade secure email gateways (SEGs) and ensure delivery of their phishing emails to users' inboxes, which we detail in this report.

Campaigns using COVID-19 as a theme continued to fade into the background of the phishing threat landscape but may return later in the year if another wave of outbreaks occurs. Though such campaigns have dropped in volume significantly since their April peak, they have certainly not disappeared completely.

Prevalent Malware in Q3

Due to the lack of the usual summertime lull in phishing activity, overall threat activity in Q3 of this year was significantly higher than Q3 in previous years.[1] This is likely due to economic hardships and new opportunities brought on by the COVID-19 pandemic. We observed campaigns using a wider variety of malware, higher volume of emails, and broader targeting than in past summers.

Since Q2, we have continued to see a mix of new malware families and returning older families. Ransomware was the most common phenotype in newly-analyzed Q3 threats, with four new families emerging during this reporting period. RATs made for the highest total of newly created and returning malware families seen within the phishing threat landscape over the last quarter. Emotet became active in July after five months of dormancy, leading to an overall increase in phishing volume.

Following the trend established in Q2 2020,[2] keyloggers remained by far the most prevalent phenotype analyzed. The volume of the other phenotypes in this past quarter is similar to that of Q2 as well. The combination of newly-created and returning RAT malware families explains the slight increase in the RAT phenotype volume this quarter. The chart below shows the top five malware phenotypes by volume.

[1] Cofense Intelligence customers can find more details in the following Strategic Analysis: "Strategic Analysis – Busy Summer Indicates Active Fall to Come" published September 17, 2020.
[2] Cofense Intelligence: "Quarterly Trends Review – Q2 2020" published July 9, 2020.

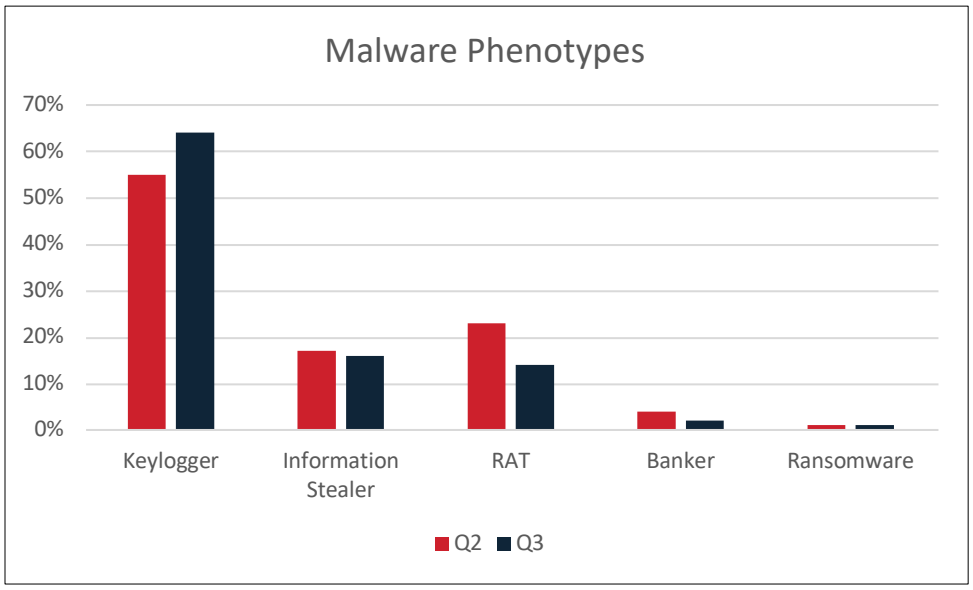

Figure 1: Q2 2020 (red) phenotype trends compared with Q3 2020 (navy) as a percentage of total volume.

Ransomware phishing volume increased this quarter, with an unusually high number of new families: LolKek, Phobos, Exorcist, and OniChan. A few of these new ransomware families include data exfiltration capabilities, adding to the increasingly popular tactic employed by threat actors to increase leverage for ransom payment by threatening to and/or leaking sensitive data. These four new families join Avaddon as popular ransomware families identified in phishing campaigns this quarter.

Some older malware families, shown in the table below, have returned to the phishing threat landscape in Q3 after being absent last quarter.

Malware Family	Phenotype
Amadey	Information Stealer
Async RAT	RAT
BetaBot	Information Stealer
Client Maximus	Banking Trojan
Ratty RAT	RAT
RedLine Stealer	Information Stealer
WebMonitor RAT	RAT

Figure 2: Older malware families that returned in Q3.

The continuing economic hardship caused by the COVID-19 pandemic is likely pushing more people into cybercrime or the creation of tools to support cybercrime. For example, Avaddon ransomware and Agent Tesla keylogger are both designed to be easy to purchase and deploy, lowering the barrier to entry for new and unsophisticated cybercriminals. This low barrier and an influx of new threat actors are likely contributing factors to the popularity of these malware families. Cofense Intelligence™ customers can refer to our Strategic Analysis reports on Agent Tesla keylogger and Avaddon ransomware for more details.[3, 4]

Emotet/Geodo's Expanding Reach

We observed several important changes in Emotet's capabilities when it resumed activity in July. Early in Q2, its operators added the ability to steal email attachments from victims' mailboxes along with the emails themselves. These attachments were used in Q3 to make Emotet's spoofed reply chains more credible.

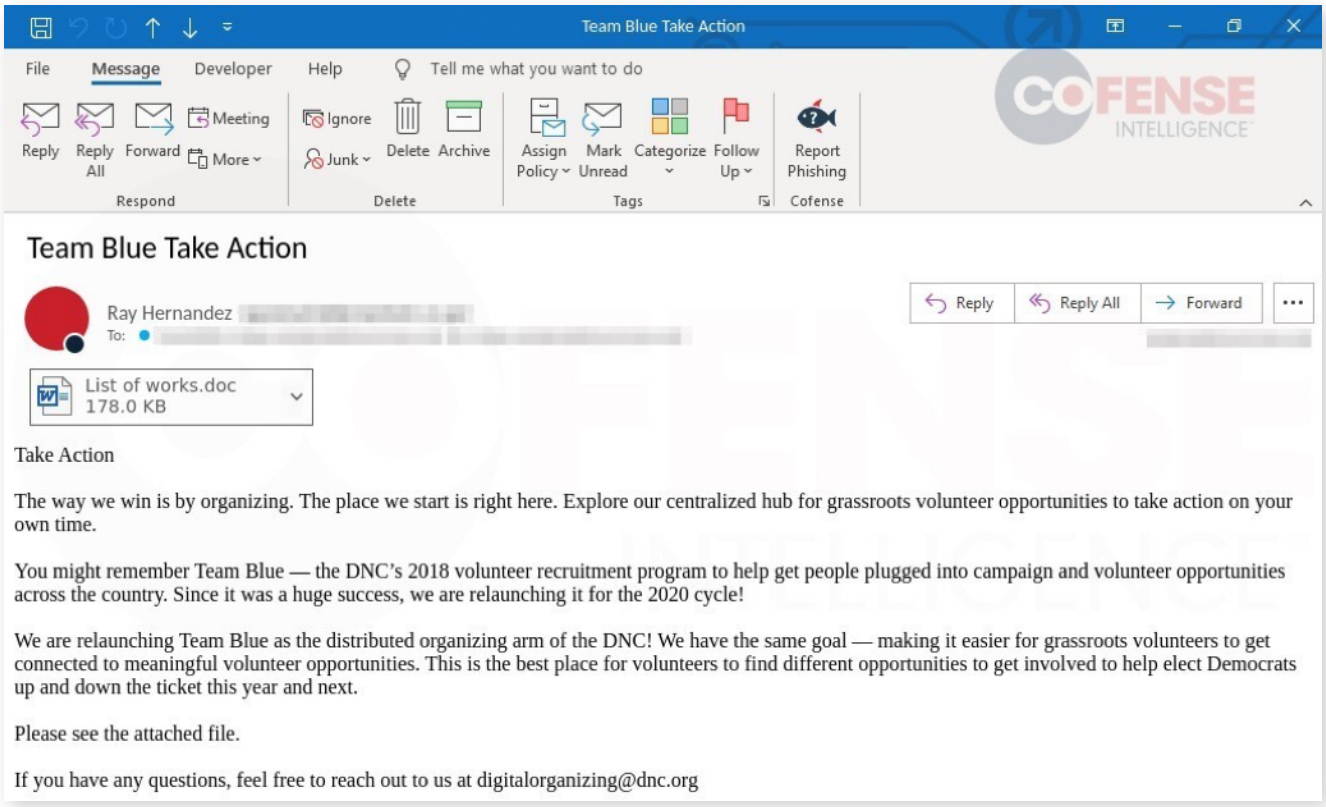

Figure 3: An Emotet phishing email with an election theme.

[3] Cofense Intelligence Strategic Analysis: "The Prominent Agent Tesla Keylogger Reaches End Users" published October 1, 2020.
[4] Cofense Intelligence Strategic Analysis: "Avaddon Ransomware Joins Data Exfiltration Trend" published August 20, 2020.

Emotet has also continued to widen its target base, expanding the number of languages used in its templates and the variety of top level domains (TLDs) it uses as senders and targets. This language expansion started in late 2019 with highly effective Japanese-language phishing emails. The number of unique sender TLDs observed in August 2020 was 337, up from a previous high of 259 in late 2019

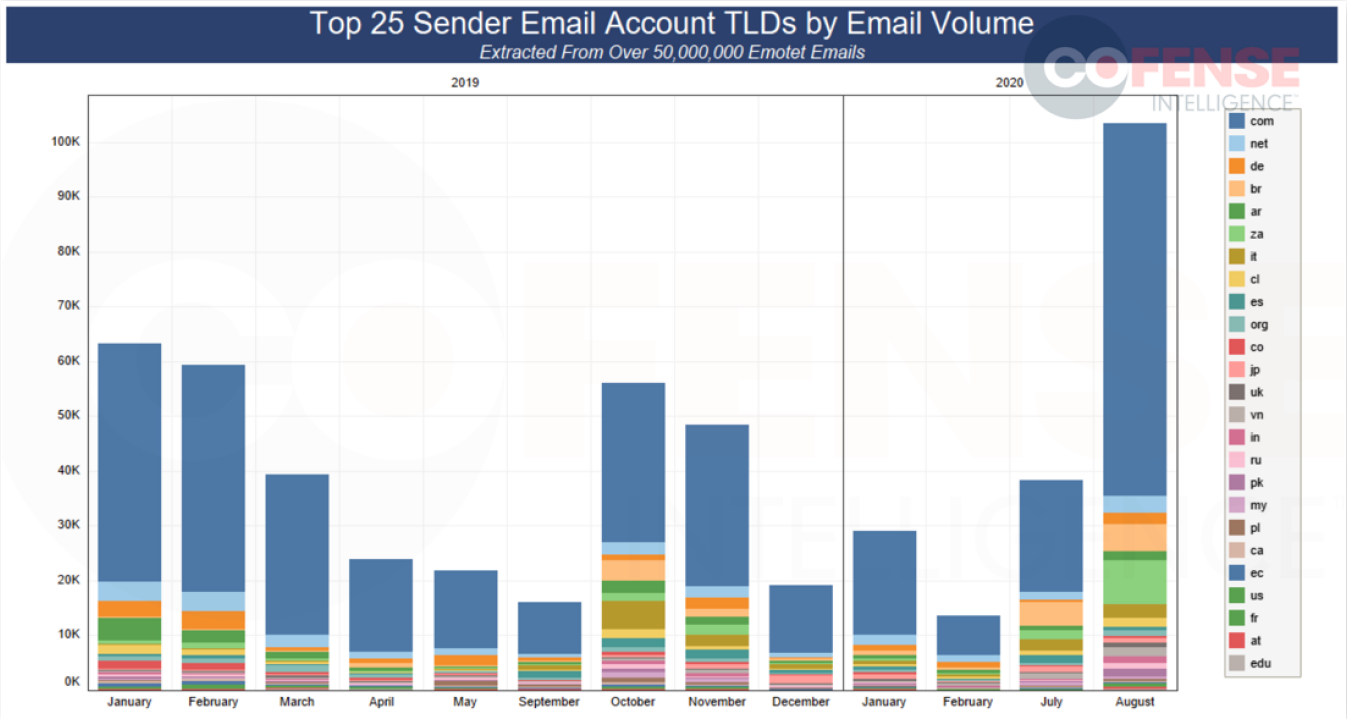

Figure 4: Variety of Emotet sender TLDs increased dramatically in August.

These efforts, along with technical improvements such as hash manipulation to avoid detection, appear to have been effective. Cofense observed 120,500 unique sender addresses in August 2020, almost double the previous record from 2019. Since Emotet uses compromised accounts as senders, this explosive growth represents massive success for the botnet and illustrates the potency of well-crafted phishing attacks. Though future lulls are expected, Emotet is very likely to remain a significant threat in the future.

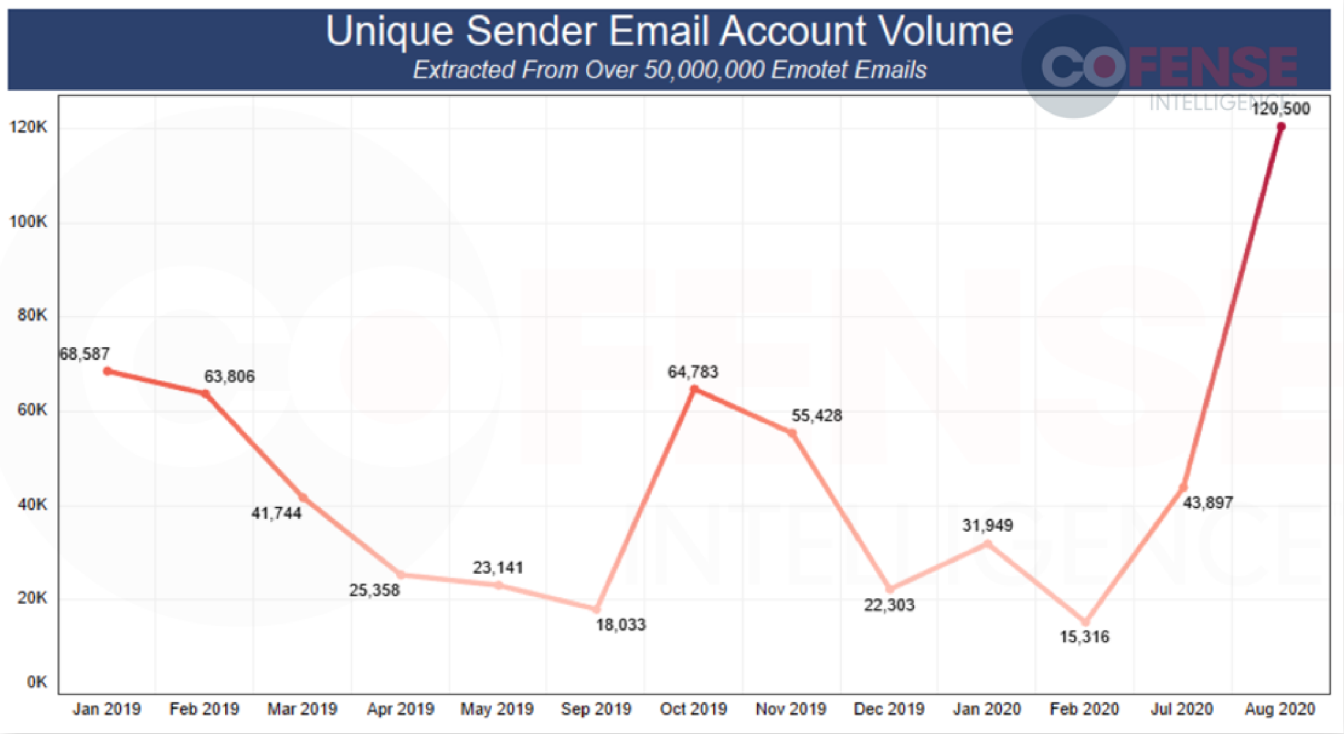

Figure 5: Emotet's unique sender address base rose sharply in August.

Agent Tesla Remained a Keylogging Fixture

Agent Tesla keylogger has established itself as a popular and effective malware, targeting users across a wide variety of industries. It has maintained prominence in the phishing threat landscape since its release in 2014 and has been the highest-volume keylogger observed by Cofense Intelligence for this quarter and year. Agent Tesla is consistently evolving to better serve its threat actor clients and evade security measures. It combines novel tactics, techniques, and procedures (TTPs) with well-established ones to reach users protected by leading SEGs[5].

Ease of use, a competitive price tag, and advanced features are likely contributing to Agent Tesla's popularity with threat actors. With multiple exfiltration channels available, it can easily integrate into any C2 infrastructure. When combined with the TTPs that allow it to evade SEGs, this robust keylogger with RAT capabilities is a significant threat to organizations today and will very likely continue to be a prolific part of the phishing threat landscape for the foreseeable future.

[5] Cofense Intelligence Strategic Analysis: "The Prominent Agent Tesla Keylogger Reaches End Users" published October 01, 2020.

Delivery Mechanisms Rundown

Continuing the trend established early in Q1, the top three delivery mechanisms remained the same through Q3: Office macros, CVE-2017-11882, and GuLoader. Emotet primarily uses Office macros, so its spike in activity this summer put Office macros into the top spot. Malicious documents exploiting of CVE-2017-11882 have consistently been a top delivery mechanism in 2020, a trend that continued through Q3. GuLoader established itself early in the year as a top delivery mechanism as well. However, it did decline in volume after scrutiny by security researchers and a suspension of sales early in the summer,[6] and has not returned to the levels seen in late spring.

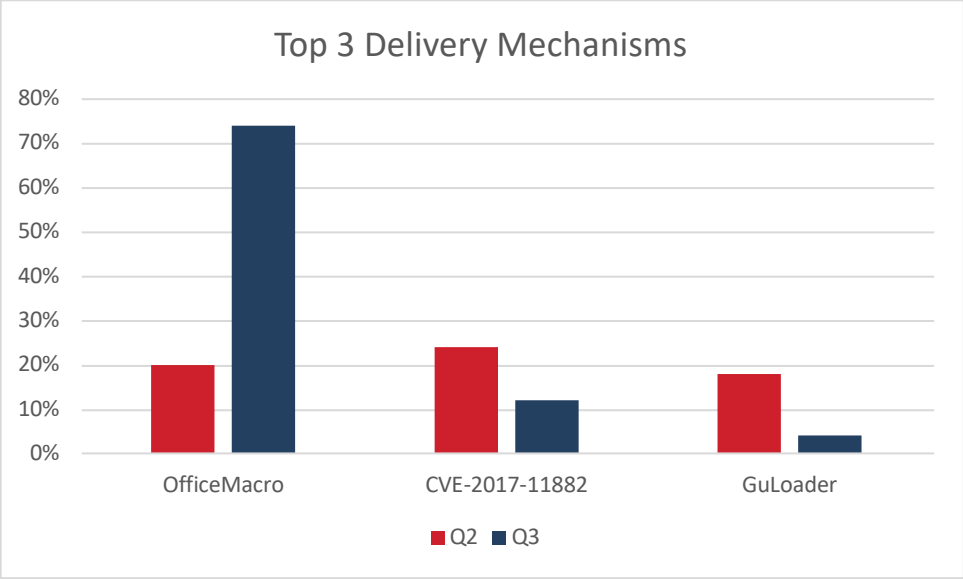

Figure 6: Top three delivery mechanisms in Q2 (red) compared with Q3 (navy) as a percentage of total volume.

Command and Control Servers Geolocations

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, although its share declined slightly for the first time since Q3 2019. Germany remains as home to second-highest number of C2 server locations, and the Netherlands in third place—even with an overall decrease from both countries.

Russia has dropped out of the top five countries hosting C2 nodes and lands in ninth, almost completely out of the top 10. The decline in Russian-hosted C2 servers may be attributed to the countrywide network implementations

[6] Cofense Intelligence Strategic Analysis: "GuLoader Rises as Top Delivery Mechanism" published July 23, 2020.

continually rolled out by the Russian government, with the latest being consideration for a law that would criminalize specific internet protocols including TLS 1.3, DNS over HTTPS (DoH), and DNS over TLS (DoT).[7]

These statistics do not directly correlate with the full range of infrastructure threat actors use and should only be interpreted as C2 location, and not where operations are originating. That said, security teams may see a C2 server (often as part of a server-hosting farm like AWS or Azure) located in one of these top C2 hosting nations.

Country	Percentage	Country	Percentage
Q2 2020		Q3 2020	
United States	49.71%	United States	45.87%
Germany	6.48%	Germany	5.74%
Netherlands	5.39%	Netherlands	2.96%
Russia	4.16%	Great Britain	2.91%
Romania	4.11%	Canada / China	2.48%

Figure 7: Q2 and Q3 percentages for C2 sources by IP address geolocation.

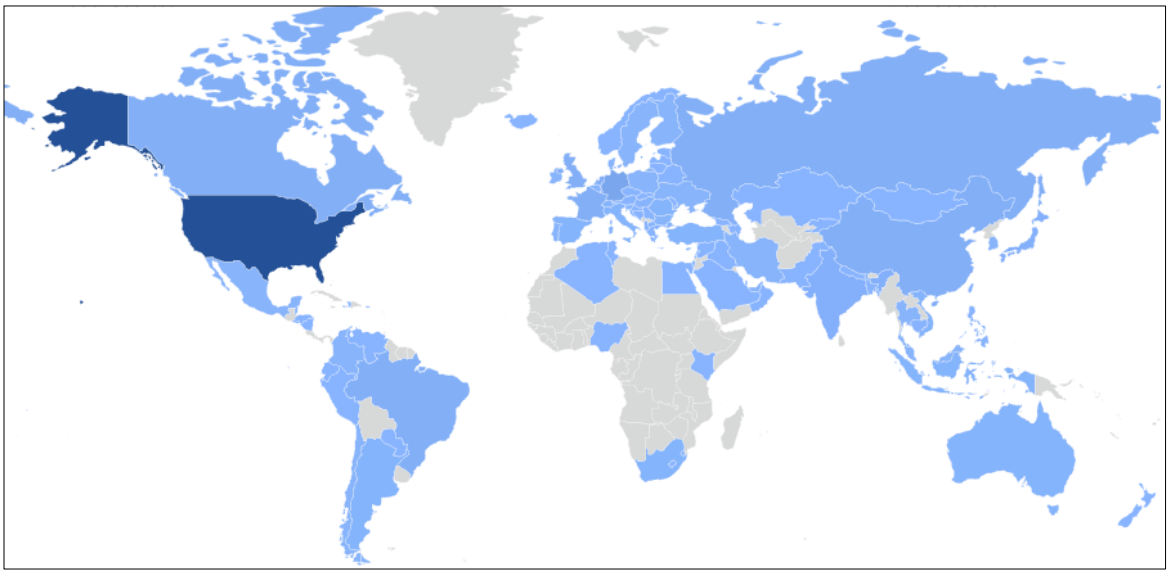

Figure 8: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

[7] Russia Is Trying Something New to Isolate Its Internet from the Rest of the World: https://slate.com/technology/2020/09/russia-internet-encryption-protocol-ban.html, published September 25, 2020.

SEG Evasion Trends: A Closer Look at Attachment Types

During Q3 2020, Cofense Intelligence identified a major trend in the filename extensions of email attachments that reached users in SEG-protected environments. The most popular extensions were .pdf attachments. Such .pdf files were used to deliver links which most frequently led to credential phishing pages but were also seen downloading AZORult Stealer. The insurance and manufacturing sectors saw more of these .pdf attachments than any other sector.

The next most commonly identified file extensions, .htm and .html, were most often used to deliver credential phish as well. The sectors that saw the most of these were again insurance and manufacturing. These files continue to evade SEGs despite an observed lack of .html files being used for legitimate purposes, which should encourage SEGs to be more suspicious of such attachments.

Microsoft Office documents containing malicious macros or exploits were also common in Q3. Archive files, sometimes using false filename extensions, appeared frequently as well. In an upcoming strategic analysis, we will dive deeper into trends in phishing email attachment file types, and explore some rarer and less-often leveraged extensions. Furthermore, we will explain how these attachments are evading SEGs and which industries they are targeting.

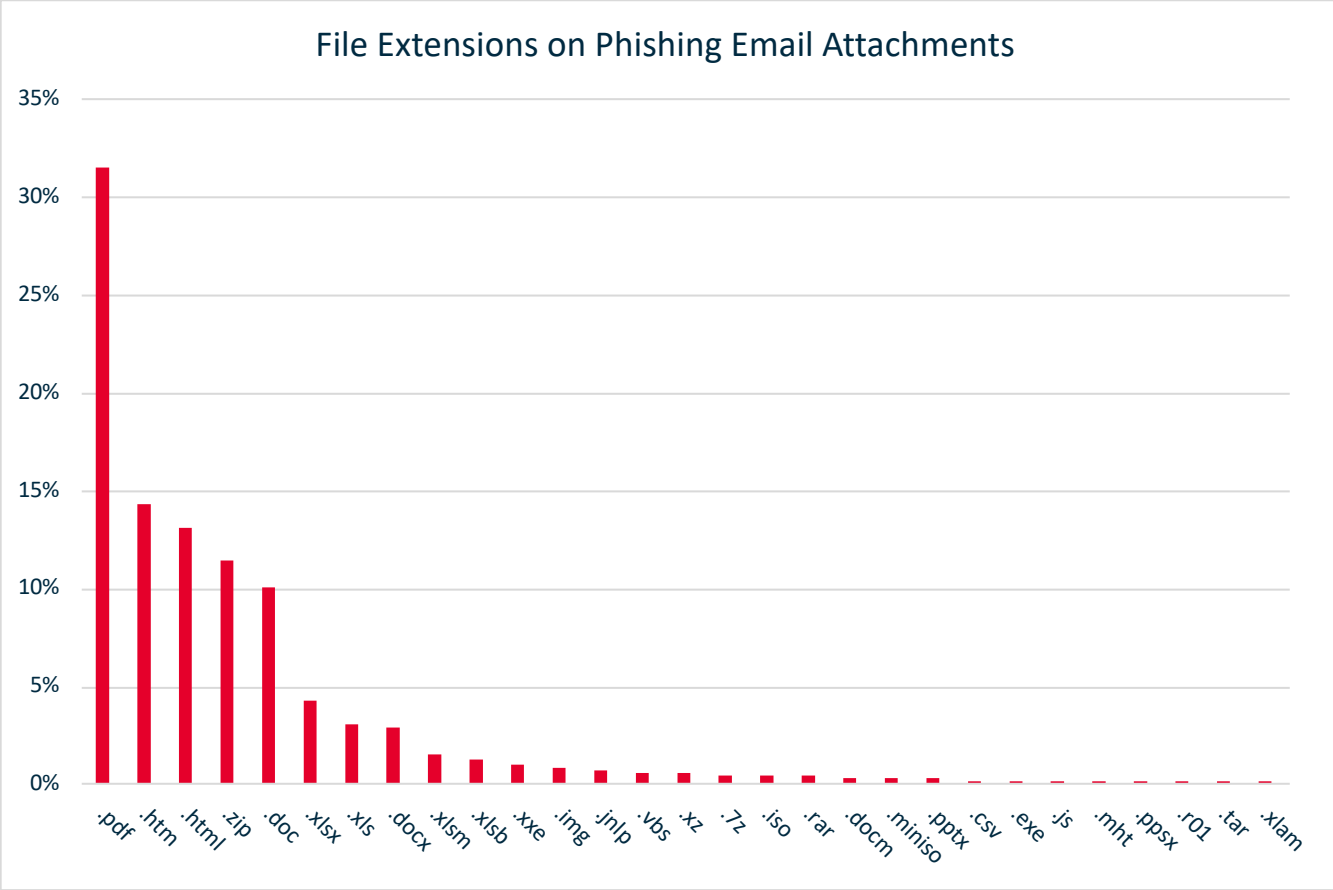

Figure 9: Frequency of filename extensions of phishing email attachments in Q3.

COVID-19 Threat Landscape

COVID-19 continues to disrupt daily life, but its presence in the phishing threat landscape has steadily faded. Since its peak in April, the volume of COVID-themed campaigns has slowly decreased. During the peak, these phishing emails predominately delivered credential phishing attacks and Agent Tesla payloads. The remaining emails delivered an assortment of keyloggers, RATs, and information stealers. As the volume of COVID-themed phishing emails declined through Q2 and Q3, threat actors using the pandemic theme gradually shifted away from the use of malicious links or attachments. More recent COVID-themed campaigns have attempted business email compromise or other criminal mischief focused on pandemic-related subjects, such as financial assistance or shipping services.

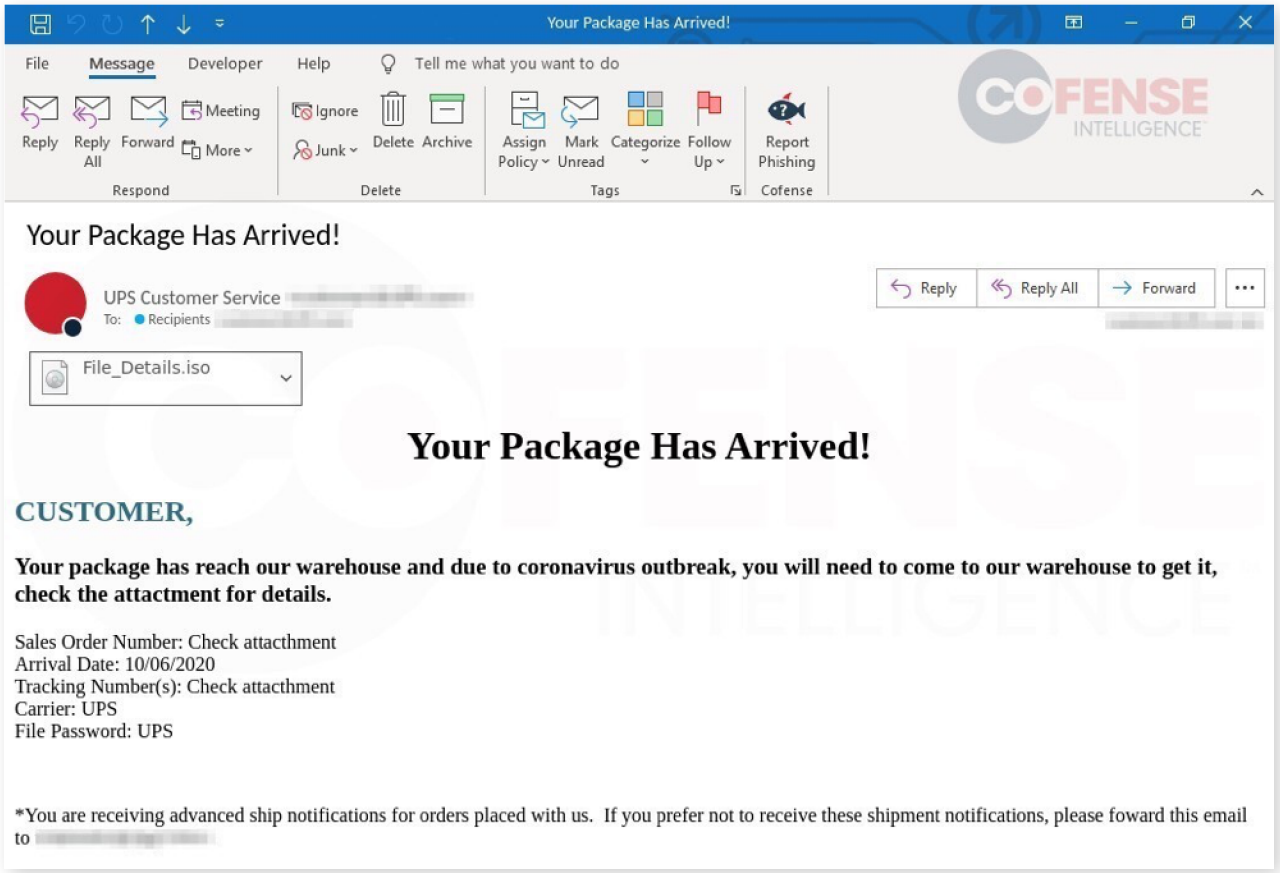

Figure 10: A COVID-19-themed phishing email.

Health officials have warned of a possible second-wave outbreak of COVID-19 to come during winter in the northern hemisphere. This wave could lead to a resurgence in COVID-related campaigns. As the pandemic continues to disrupt the economy, business operations, and travel arrangements, we assess that threat actors will likely continue to exploit users with themes related to the financial sector, shipping and delivery services, and remote working.

Phishing Predictions for Q4 and Q1 2021

Healthcare and supporting industries will become the most targeted industry.

Healthcare organizations have long been a popular target for phishing threat actors. The COVID-19 crisis has likely increased adversaries' focus on healthcare targets—several healthcare providers have suffered compromises this year, at a time when continuity of operations is especially critical. If there is another wave of outbreaks as winter arrives, threat actors will very likely increase their targeting of healthcare organizations.

We have already seen devastating effects on healthcare providers, such as when Universal Health Services suffered a significant outage from what is assessed to be a Ryuk ransomware variant on its systems.[8] We have also seen what can happen when cloud services are not accessible for healthcare services, as when September's Microsoft 365 outages were possibly tied to 911 call center disruptions.[9] These examples illustrate the grave real-world consequences of compromise or outage in healthcare services. Threat actors will likely perceive this as an opportunity for leverage for payment and increase their targeting of healthcare organizations in the future.

Cloud computing will bring about new vulnerabilities and tactics used within phishing.

The COVID-19 pandemic has contributed to an acceleration in adoption of cloud computing and storage this year, building on a preexisting trend of moving to cloud solutions.[10] Vulnerabilities in cloud-based infrastructure have already yielded great results for threat actors, especially when those vulnerabilities are based on misconfigurations of cloud security features by data owners. Businesses shifting to the cloud often miss crucial steps to fully secure their new environment. This is likely to lead to more data breaches involving cloud infrastructure in Q4 2020 and into 2021.

Given these opportunities, threat actors are likely to continue targeting cloud services or take advantage of organizations' trust in them with phishing, as we have already reported multiple times this year. For example, in Q2, threat actors abused SSO infrastructure to obtain access to a victim's data without a password.[11] In Q3, we reported repeatedly on threat actors' use of embedded links to cloud file sharing services[12] to get credential phishing emails to users in secure environments. Delivery mechanisms such as GuLoader can also use cloud services to fetch malicious payloads undetected.

---

[8] UHS Health System Confirms All US Sites Affected by Ransomware Attack: https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack, published October 5, 2020.
[9] 911 Services Down in Multiple US States: https://www.zdnet.com/article/911-services-down-in-multiple-us-states/, published September 29, 2020.
[10] Study Confirms COVID-19 Impact on Cloud Adoption, Permanent Work-from-Home: https://virtualizationreview.com/articles/2020/06/03/mariadb-survey.aspx, published June 3, 2020.
[11] MFA Bypass Phish Caught: OAuth2 Grants Access to User Data Without a Password: https://cofense.com/mfa-bypass-phish-caught-oauth2-grants-access-user-data-without-password/, published May 18, 2020.
[12] Cofense Intelligence Strategic Analysis: "Credential Phishing in Secure Environments" published August 6, 2020.

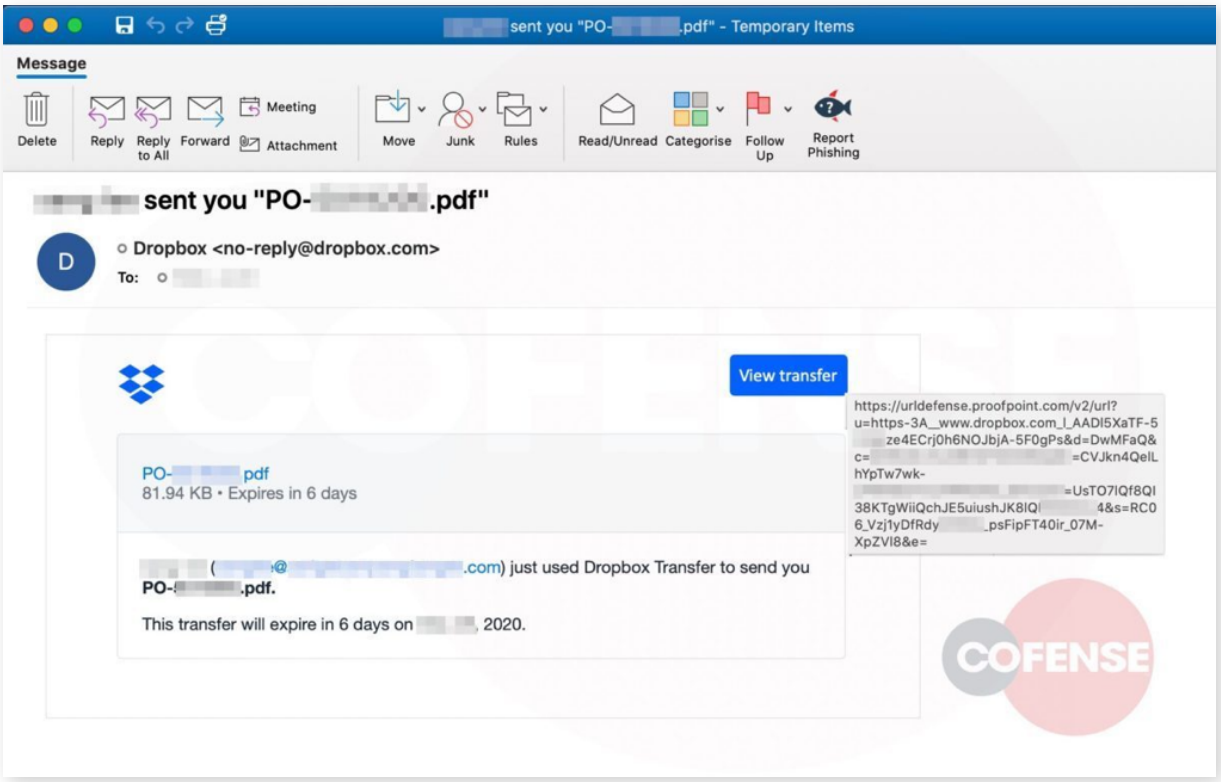

Figure 11: A phishing email using an embedded link to Dropbox to evade SEGs.

Due to the opportunities afforded by growing cloud adoption and the considerable success of cloud-related threat activity, we assess that threat actors will likely increasingly capitalize on cloud infrastructure to either host malicious content or to launch malicious campaigns.

Elections remain in the crosshairs, though election-themed phish are notably absent.

The 2020 presidential elections are happening at a volatile time, both politically and on the cyber security frontier. This particular mix has provided an enticing target for foreign groups who in the past used direct cyber-attacks initiated by phishing.[13] Cofense Intelligence assesses that it is highly probable that some organizations with ties to the elections or to software or hardware used in voting centers will be the targets of spearphishing. However, companies that are more tangentially related to the elections should also be concerned, as they could be targeted and used as part of a supply chain attack. For example, government service provider Tyler Technologies suffered a major ransomware attack in September.[14]

[13] TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election, published June 5, 2017.
[14] Govt. Services Firm Tyler Technologies Hit in Apparent Ransomware Attack: https://krebsonsecurity.com/2020/09/govt-services-firm-tyler-technologies-hit-in-apparent-ransomware-attack/, published September 23, 2020.

In many states, early voting has already started, and a large number of people have already voted. Despite this, there has not been a major increase in election relating phishing themes. This unpredicted lack of volume indicates that threat actors may not be as interested in using election themes to deliver phishing as originally predicted.

ABOUT COFENSE

Cofense is uniting humanity against phishing. Everyday phishing attacks evade perimeter defenses, including secure email gateways, to reach employee inboxes. Cofense gives incident responders the tools they need to analyze, identify, and stop attacks in minutes, while conditioning employees to recognize and report phishing threats, thereby turning soft targets into active human sensors. By combining human intelligence and advanced technology, our solutions enable organizations to prevent breaches, loss of funds, data theft, and reputational damage. No one delivers a more complete, end-to-end phishing defense. Cofense has thousands of enterprise customers worldwide, spanning every major vertical including defense, energy, financial services, healthcare, retail, and manufacturing. Learn more at https://cofense.com