COFENSE™

Q2 2020

# PHISHING REVIEW

Strategic Analysis provided by Cofense Intelligence | COFENSE.COM

# Executive Summary

Phishing threat actors shifted tactics slightly in the second quarter of 2020, leveraging a combination of well-established malware and some creative new delivery mechanisms to reach end users. Keyloggers surged to become the most popular malware phenotype, while information stealers and banking trojans (also known as bankers) faded, and other malware types remained steady. A few entirely new malware families emerged, but threat actors also brought back older, mostly dormant families.

The two most popular delivery mechanisms during this quarter both use Microsoft Office documents, and the more direct GuLoader continues to establish itself as a popular choice. Threat actors are still leveraging trusted platforms such as cloud hosting providers and have added a few creative secure email gateway (SEG) evasion techniques as well. These techniques take advantage of older, overlooked features in trusted software such as Java and Microsoft Excel.

Campaigns related to COVID-19 reached their height in April, then tapered off throughout May and June. The majority of them carried credential phishing attacks, while the rest delivered malware, most predominantly Agent Tesla. Predictably, messages from government and health organizations remain popular phishing themes. As COVID-19 circumstances continue to evolve, threat actors can be expected to take advantage of every related opportunity.

Ransomware campaigns shifted focus as well. During Q1 2020, they continued to target specific industries that were more likely to pay. However, a new campaign in Q2 went to a wide set of users not affiliated with each other or any specific industry. This may signal that broadly-targeted ransomware is again becoming profitable to threat actors.

## Prevalent Malware in Q2: Keyloggers Reign, New Families Emerge

Phishing campaigns in Q2 included many different types of malware, including a number of newly emerging families. Moreover, several older malware families that have been relatively dormant for years have reemerged, featuring minor updates or tweaks, and often with COVID-related themes. The overall volume of activity from non-Emotet related threat actors increased slightly in Q2, likely due to the economic and lifestyle impacts of the ongoing pandemic.

The highest volume of unique campaigns in Q2 2020, in terms of malware phenotypes (or malware type), was keyloggers, with no close second place. This was an abrupt shift from the previous leading information stealer and banker phenotypes of recent quarters. The recent economic downturn is likely pushing more people into criminal activity. This may account for the increase in keyloggers, which are lightweight and easily purchased. The chart below identifies our top five malware phenotypes delivered via phishing in Q2 2020.

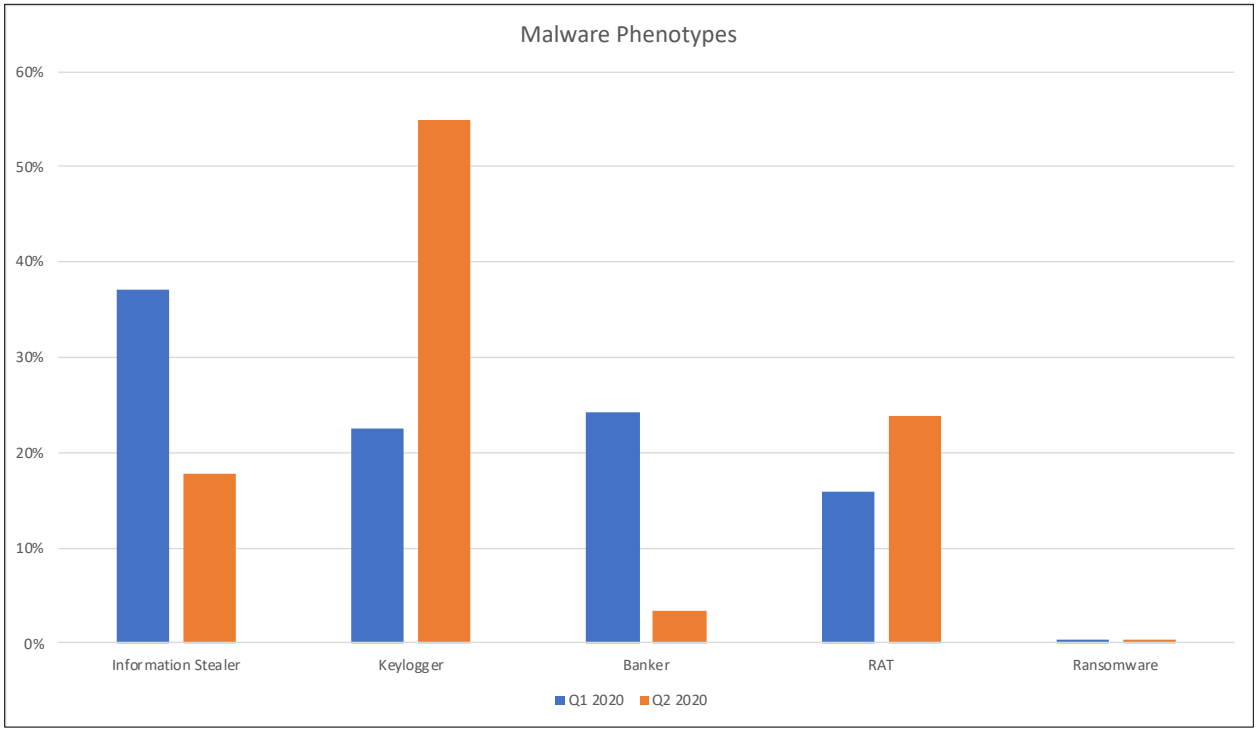


*Figure 1: Q1 2020 (blue) phenotype trends compared with Q2 2020 (orange) as a percentage of total volume*

New malware is created and released fairly often, but these malware families do not typically sustain high levels of dissemination. This is likely due to a combination of factors including price, provided capabilities, and lack of ability to avoid detection or bypass defenses. Some malware, such as WSHRAT, maintains market share by giving up stealth in favor of low price and ease of use. This last quarter has been marked by an unusual number of newly developed or adapted malware and the re-emergence of time-tested classic malware. Some of these updated malware families have been capable of evading SEGs, indicating that they are more highly prioritizing detection evasion.

Two newly-emergent malware families stand out in Q2: Mass Logger and Avaddon Ransomware. Mass Logger is the new creation of an advanced threat actor with significant experience and has been successful in quickly gaining and maintaining popularity in the competitive Keylogger market. Avaddon is the newest ransomware family delivered by the Trik/Phorpiex botnet and has a much larger target base than usual. Cofense Intelligence™ customers can refer to our Strategic Analysis reports on both malware for more details.[1,2]

[1] Cofense Intelligence customers can find more details in the following Strategic Analysis: "*Mass Logger Enters the Phishing Threat Landscape*" published May 28, 2020

[2] Cofense Intelligence customers can find more details in the following Strategic Analysis: "*Avaddon Ransomware Signals Possible Return to Broad-Targeting Ransomware Campaigns*" published June 11, 2020

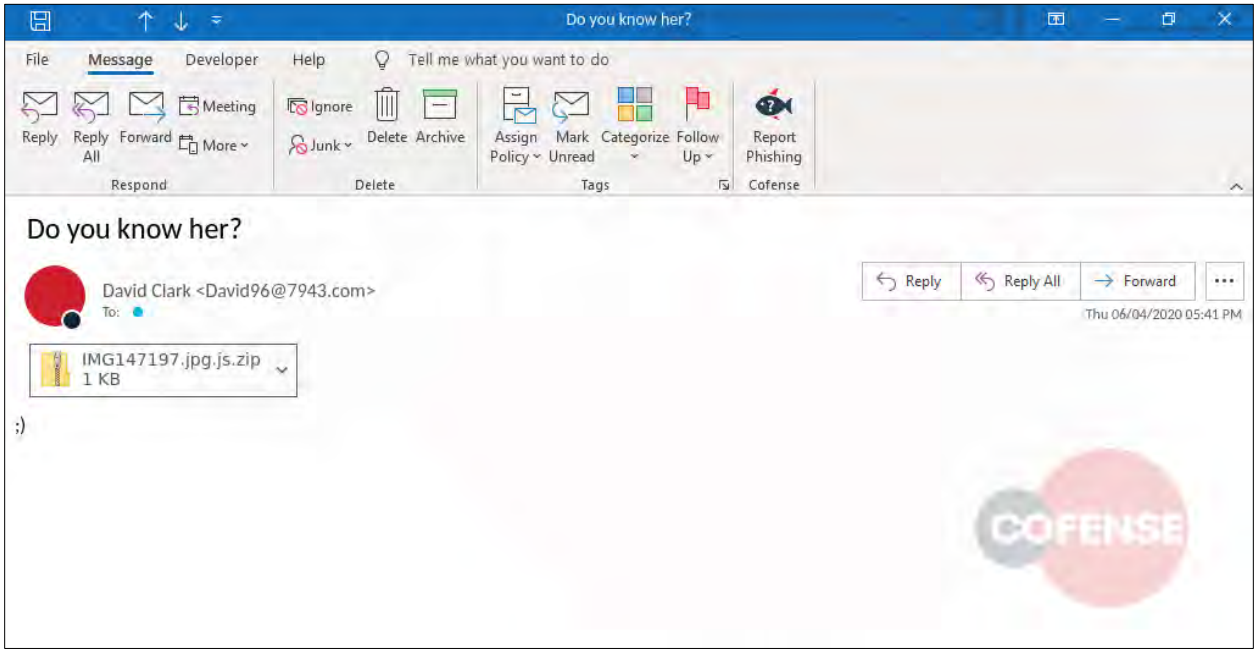


*Figure 2: An email sent by the Trik botnet delivering a script which downloads Avaddon ransomware*

As mentioned before, long existing malware have reemerged in Q2, some with newer variants. This continues a trend that began in Q1, especially as the pandemic emerged. Below are the malware families that emerged or reemerged thus far in 2020 in phishing campaigns identified by Cofense Intelligence. Those in bold are new, while the others have returned to the phishing landscape. These malware families include:

- **Avaddon Ransomware**
- BetaBot
- Chanitor/Hancitor
- Cobian RAT
- Dharma Ransomware
- Expiro
- **Gamorrah Bot**
- **Hive RAT** (modified version of Firebird RAT)
- IcedID
- KPOT
- Kutaki
- LatentBot
- Loda
- **Mass Logger**
- Proyecto
- Pyrogenic Stealer
- Remote Manipulator System
- **STRRAT** (modified version of WSHRAT)
- Sality
- Vidar

## Delivery Mechanisms: New Techniques to Evade Detection

Threat actors implemented new ways to evade detection and reach enterprise end users by abusing overlooked software features and continuing to weaponize trusted platforms. In a particularly crafty technique, threat actors delivered malware using a version of Microsoft Excel macros introduced in 1992. That version was deprecated within a year, and the way macros were written was changed soon after this version (version 4.0) was rolled out. However, Excel has maintained compatibility with version 4.0 macros in all subsequent releases. Threat actors

recognized this as an opportunity to use a relatively unknown delivery mechanism, and this tactic has recently been used to successfully evade SEG[3].

A TrickBot campaign from early June provides another example of adversaries abusing older software features. The campaign delivered Java Network Launch Protocol (JNLP) files, which allowed Java to load and run code files from remote sources. Oracle removed support for this feature in late 2018 with Java version 11, but many users still run older versions. Despite its simplicity, this delivery mechanism managed to evade multiple SEGs[4].

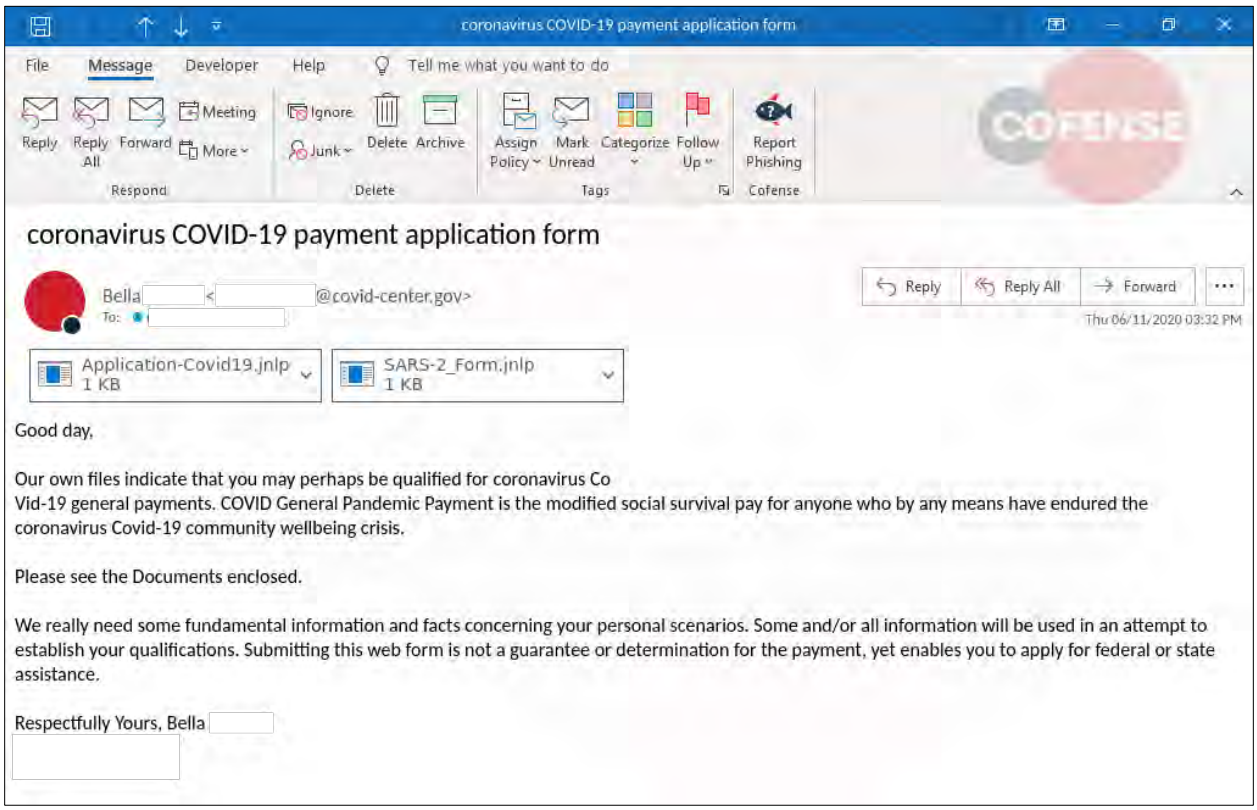


*Figure 3: An example of a Coronavirus themed phishing email delivering a JNLP file which downloads TrickBot*

While threat actors have had continued success with abusing explicit trust in services like cloud hosting providers, these new campaigns represent an interesting new trend. In both cases, they take advantage of organizations' implicit trust in their software. Though the software is well-supported by trusted technology companies, the campaigns abused features that most organizations likely did not even know about. As threat actors identify these vectors, they find more ways to ensure their phishing emails evade SEGs and reach users' inboxes.

[3] Cofense Intelligence customers can find more details in the following Strategic Analysis: "*Old Excel Macros v4.0 Used in New Phishing Trend*" published June 25, 2020

[4] Cofense Intelligence customers can find more details in the following Flash Alert: "*Novel TrickBot Delivery Method Successfully Evades SEGs*" published June 12, 2020


Dive into the latest trends in phishing awareness and incident response.

**LEARN MORE**

Interested in presenting at Virtual Submerge?
**Submit a topic for consideration!**

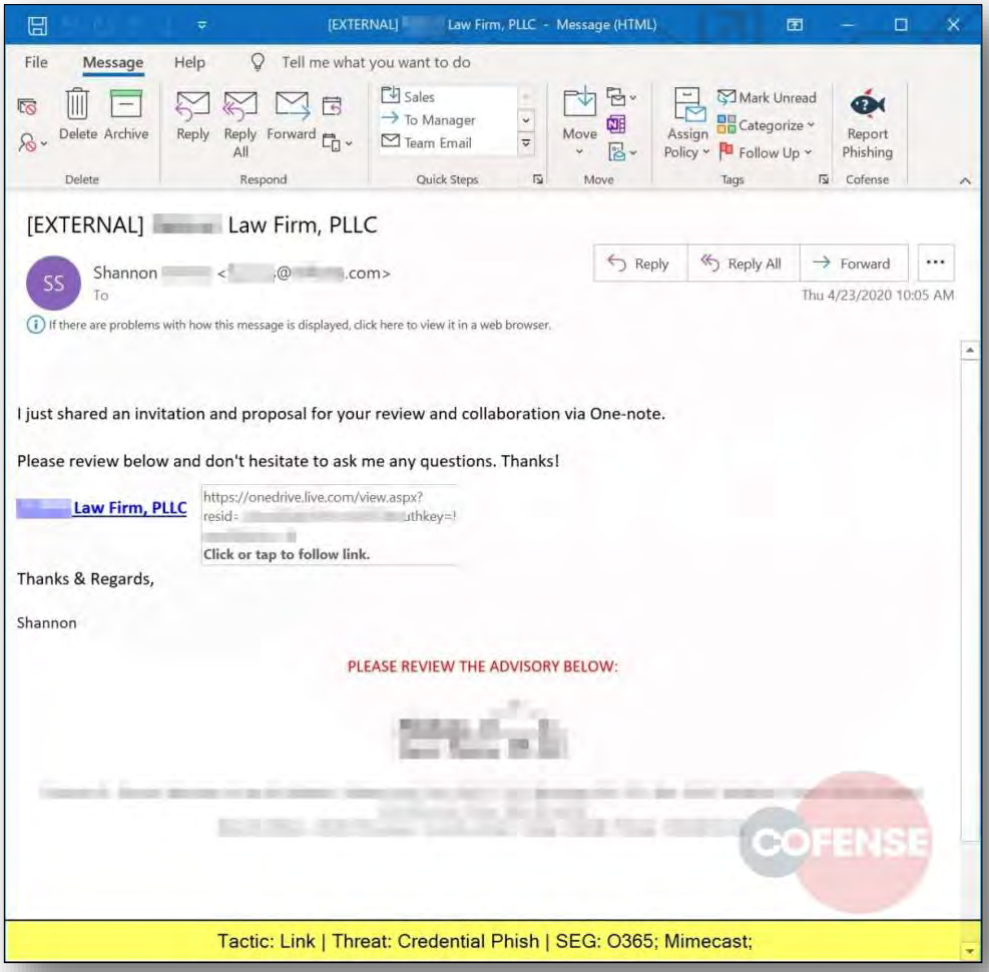


*Figure 4: Example of an email utilizing a trusted source URL to carry out a credential phish*

Threat actors continue to use trusted platforms, such as cloud file sharing services, to deliver malware and host credential phish. Above is one such example, wherein OneDrive was used to execute a credential phishing attack.

This exploitation of trust was also a factor in a sophisticated credential phishing campaign in May. Threat actors used compromised accounts to create detailed and trustworthy-looking emails, with customized images, messaging, and signatures from the initial victim's actual emails. The phishing emails were sent directly from the compromised victim's account to their contacts, so recipients were more likely to find the messages credible. We watched as this campaign spread from the energy sector to the financial sector in the Middle East. Other techniques, like randomization of links and use of URLs with valid TLS certificates, helped these emails evade

detection. The effort to increase credibility makes it likely that this type of campaign will continue to spread to other high-value target industries[5].

## The Continued Dominance of Malicious Macros and CVE-2017-11882

Over the course of Q2 2020, CVE-2017-11882—also known as the Equation Editor vulnerability—and Office macro-enabled documents continued to dominate as the most popular delivery mechanisms for malware overall in phishing campaigns. CVE-2017-11882 is often used to download malware like information stealers and keyloggers, such as the prevalent Agent Tesla Keylogger.

The third most seen delivery mechanism in Q2 was GuLoader, which first emerged in Q1 and surged during Q2. GuLoader is most often seen being used to deliver RATs. Its increasing use may be due to its abuse of legitimate file sharing platforms to host malicious content, which makes its network activity harder to detect than most other delivery mechanisms.

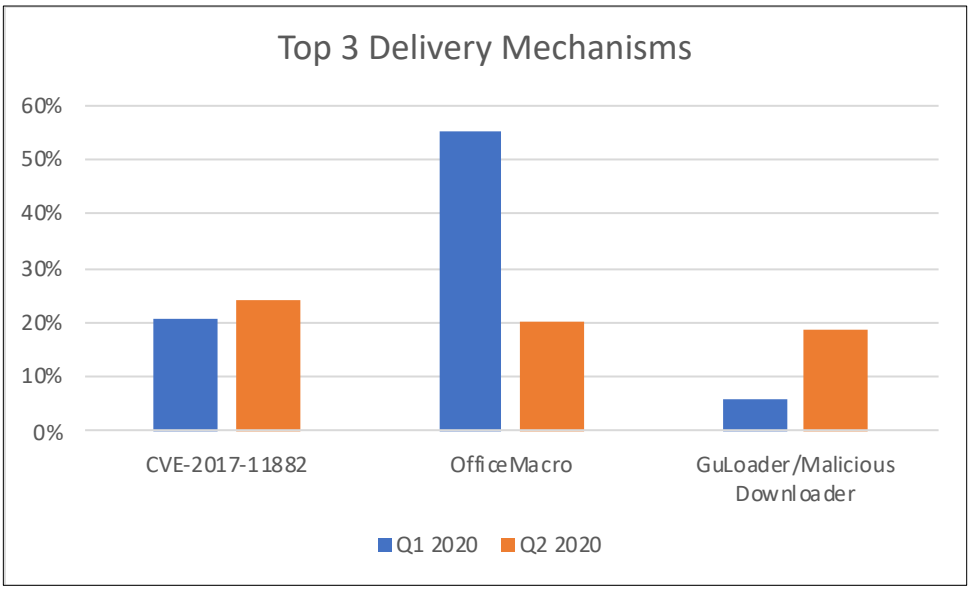


*Figure 5: Top 3 delivery mechanisms in Q1 2020 (blue) compared with Q2 2020 (orange) as a percentage of total volume.*

[5] Cofense Intelligence customers can find more details in the following Flash Alert: "*Energy and Financial Sectors Targeted in Sophisticated Credential Phishing Campaign*" published June 12, 2020

## Where in the World?

### Directing the Malware from the United States: Command and Control Servers Locations

Tracking Command and Control (C2) servers reveals a full range of activity across the globe. These nodes can deliver or command malware delivered via phishing campaigns, and they often receive information from infected hosts. Maintaining its consistent lead, the United States accounts for almost 50% of C2 locations worldwide during Q2 2020. The top four countries from Q1 have maintained their positions, and each has increased the number of hosted C2 servers. The final position in the top five, previously held by France or Great Britain, is now held by Romania. Although these statistics do not directly correlate with the infrastructure threat actors use, security teams may see a malicious C2 server (likely as part of a server-hosting farm like AWS or Azure) originating from one of these top nations.

| Country | Percentage | Country | Percentage |
|---|---|---|---|
| Q1 2020 | | Q2 2020 | |
| United States | 45.10% | United States | 49.71% |
| Germany | 4.78% | Germany | 6.48% |
| Netherlands | 4.02% | Netherlands | 5.39% |
| Russia | 3.82% | Russia | 4.16% |
| France | 2.84% | Romania | 4.11% |

*Table 1: Q1 2020 and Q2 2020 percentages for C2 sources by IP address geolocation*

## Malware Phenotypes Differ by Language

Cofense Intelligence tracks large numbers of phishing campaigns globally. While many different languages and spoofed brands are represented in phishing campaigns, common themes and malware types are shared across regions and languages. The most common themes globally are finance, purchase order, and shipping related. The financed-themed emails often spoof a bank such as Santander or Halkbank or refer to a supposed invoice. Purchase order emails are generally industry related.

Shown below are the percentages of malware phenotypes delivered in the most commonly seen non-English emails, though there are some differences in the specific malware family delivered within each phenotype depending on the region. For example, NanoCore RATs are more commonly delivered in Chinese language emails, whereas Remcos RATs are more prevalent in Turkish language emails.

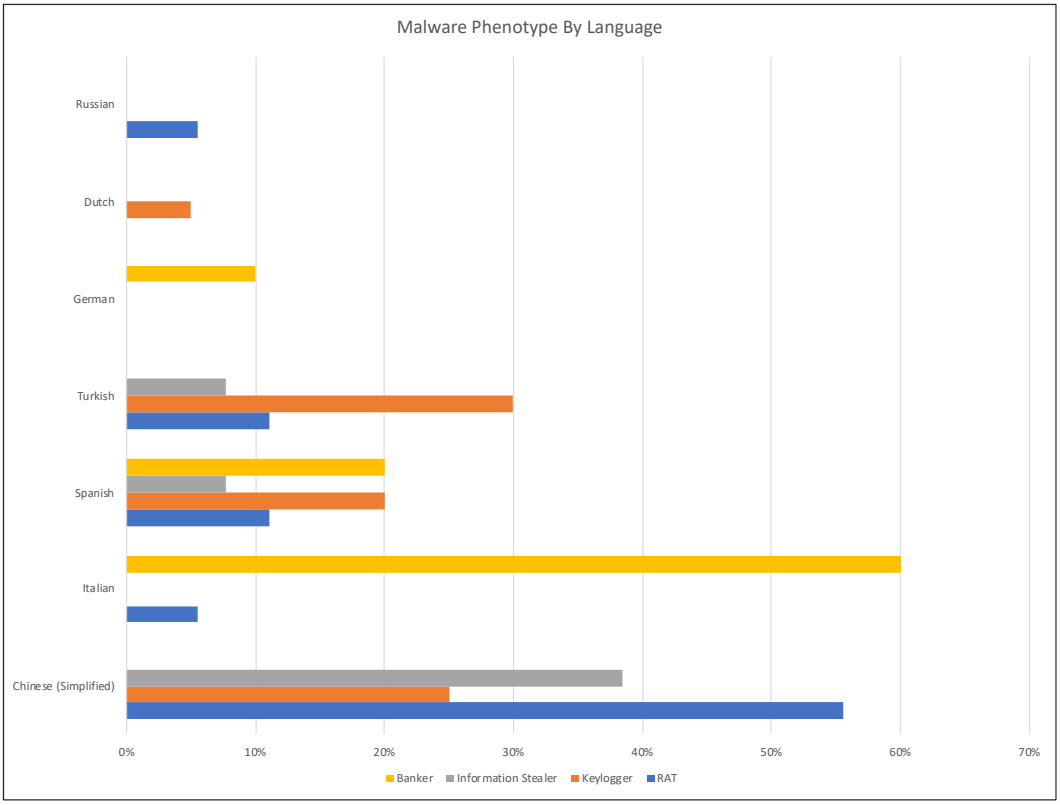


*Figure 6: Phenotype of delivered malware based on the language of the email for the top seven non-English languages*

## COVID-19 Threat Landscape

COVID-19-related campaigns peaked in April, as the pandemic continued to dominate daily life and several countries had just passed financial aid measures. As new cases stabilized in many regions and we adjusted more to the "new normal," COVID-themed campaign volume dropped by nearly 40% in May and again by over 50% in June. The majority of the emails were credential phishing attacks, with Agent Tesla payloads a distant second. The rest of the emails included a small assortment of other malware, mostly RATs.

Just as in Q1, many of the campaigns spoofed government and health organizations, along with key industries relevant to work-from-home shifts. The sophistication of the disseminated malware varied, ranging from simple executable attachments to creative new SEG-evading payloads. As the pandemic continues to disrupt normal life and business operations, threat actors can be expected to exploit users' desire for information, financial assistance, and support or guidance for remote working.

For more information and daily updates around the COVID-19 pandemic, visit the Coronavirus Infocenter, which is available to the public[6]. Cofense Intelligence customers are receiving IOCs daily as these campaigns are identified.

## Change in Ransomware Targeting

Some ransomware campaigns in Q2 2020 targeted a wider user base than typically seen in previous years. Overall, targeting has changed dramatically in the past few years based on available technology, law enforcement initiatives, economic factors, and target viability. Broad-targeted ransomware campaigns surged in 2017 as Ransomware-as-a-Service (RaaS) took hold and made sophisticated, widespread attacks easy. Ransomware campaigns faded overall during 2018. We assess that this was due to improved disruption and response from both victims and law enforcement, while fluctuating cryptocurrency prices made other types of attacks more comparatively lucrative.

In 2019, ransomware returned, but with a different target focus. This time, campaigns were narrowly targeted against high-value organizations—typically organizations offering essential services such as government, transportation and healthcare organizations that were unlikely to be able to withstand downtime, but likely to pay. Over the last year, ransomware campaigns again began to increase, with targeting remaining narrow and sophisticated. More recently, such ransomware campaigns expanded to include data exfiltration, delivering a ransomware/data breach two-for-one. This increases the pain for organizations prepared to recover their files or otherwise unlikely to pay, as adversaries release sensitive and confidential data over time as victims refuse to pay.

Starting in Q1 2020 and continuing in Q2, threat actors have shown signs of expanding their target bases, in campaigns that more closely resemble those widely disseminated ransomware campaigns of 2017. For example, the Trik botnet disseminated a widespread Nemty ransomware campaign in Q1, and more recently shifted to similar delivery of the newly discovered Avaddon ransomware in Q2[7]. These campaigns went to a broad, generic set of users rather than to any particular industry. Threat actors will likely continue to see these broader user sets as higher-value targets, as COVID-19 keeps users from all types of organizations working remotely, potentially increasing the organizations' attack surface.

[6] https://cofense.com/solutions/topic/coronavirus-infocenter/

[7] Cofense Intelligence customers can find more details in the following Strategic Analysis: "*Avaddon Ransomware Signals Possible Return to Broad-Targeting Ransomware Campaigns*" published June 11, 2020

# Predictions

## Delivery Mechanisms are Divided but Improving

Q2 2020 has seen more unusual delivery mechanisms being used than has been typical of the preceding four quarters. The newer GuLoader has become extremely popular, well exceeding the popularity of other comparable malware downloaders. We have also seen threat actors identify old features as new attack opportunities. Threat actors weaponized Microsoft Excel 4.0 macros and .jnlp file extensions as delivery mechanisms, making use of older, overlooked and oft-forgotten software features to deliver malware. Cofense Intelligence predicts that while more advanced threat actors may find additional old features to abuse, these delivery mechanisms will likely not see widespread popularity. Instead, low level threat actors who deliver most of the RATs and keyloggers seen on a daily basis will continue to use delivery mechanisms like CVE-2017-11882 or GuLoader, because these have builders and are simple and easy to use. Although the techniques developed by more experienced threat actors may not see widespread usage, they will still likely impact many organizations, and will be preferred by sophisticated threat actors due to their ability to evade SEGs. Following procedures like disabling macros by default can help. However, staying up to date with the latest patches, paying attention to newly identified CVEs, and understanding which CVEs are exploited in the wild helps defenders maintain a more proactive defense against the noisy phishing threat.

## Continued COVID-19 Disruption

COVID-19 remains a critical subject at the front and center of our minds and daily discourse, and it is certain to continue to contribute to a fertile threat landscape. Though these campaigns have tapered off from their peak, they do continue and may resurge if and when COVID-19 hot spots develop in the summer and fall. If a second wave of infections occurs in the winter, then a corresponding increase in pandemic-themed emails is likely as well. Our predictions from Q1 2020 were validated in Q2: simpler-to-use malware (GuLoader and Agent Tesla) spiked, and new malware (Mass Logger) emerged in COVID-19 campaigns. Cofense Intelligence predicts that these trends will continue during the rest of the year.

## US Elections Create More Phishing Opportunities

As the United States draws closer to its general election in November, cybercriminals and state-sponsored threat actors will almost certainly attempt to gain access to critical assets and information. Open-source reporting indicates that APT groups have already targeted the campaigns of both major political parties. Other election-related assets such as voting systems and accounts on email and social media services are likely to be targeted as well. The COVID-19 pandemic adds extra complexity to this election, as social distancing requirements may interfere with in-person voting or force the use of new voting methods. Phishing remains one of the most effective intrusion vectors in general, with a history of major impact in the 2016 election. Cofense Intelligence expects to see phishing campaigns that target elections or use election themes to spread malware.