COFENSE™

Q1 2020 PHISHING REVIEW

Strategic Analysis provided by Cofense Intelligence | COFENSE.COM

Cofense Intelligence™ Quarterly Report

Q1 2020 Phishing Trends

Executive Summary

The first quarter of 2020 began with a continued seasonal lull in malware volume and ended with a drastic spike in the last six weeks, as the COVID-19 virus spread globally into a pandemic. The initial low volume in Q1 can almost certainly be attributed to the holidays at the end of 2019 and Orthodox Christmas in early January. As expected, soon thereafter threat actors resumed phishing activity, which we expect to continue into the summer. The short-lived resumption in Emotet resulted in a quieter-than-expected Q1 overall. The malware volume vacated by Emotet was quickly replaced with a high volume of malware phishing campaigns leveraging COVID-19/remote work themes in March 2020.

Threat actors across different skillset levels are using a myriad of delivery mechanisms and malware to compromise an endpoint, frequently leveraging the COVID-19 pandemic in phishing themes. Cofense Intelligence identified several campaigns where COVID-19 themed phishing emails evaded Secure Email Gateways (SEGs) to reach enterprise end users. Often, these TTPs involved the use of trusted sources to help evade SEGs and network content filtering. This new threat landscape has shown some innovative Tactics, Techniques, and Procedures (TTPs) rarely seen before in phishing. The usual cast of malware families were identified in abundance during this quarter, while some older malware families came out of retirement. Some of the older malware families were re-wrapped by threat actors for improved use in modern environments.

The top malware delivery mechanism in phishing campaigns remained consistent with Q4 2019, as Microsoft Office documents laden with malicious macros remained the most prevalent. However, the other top three delivery mechanisms overall have changed, with the Malicious Downloaders category bringing more complex delivery methods. With the threat landscape turning towards pandemic themes in the latter half of Q1, more benign attached documents with malicious links were on the rise. These campaigns delivered both credential phish and malware, with credential phish evading SEGs at a higher rate than malware attachments.

Finding the right Command and Control (C2) infrastructure for a hosted binary or credential phish has become easier for threat actors, as more organizations adopt cloud storage solutions, which adversaries in turn abuse to deliver malware. The United States continues to host the most C2 servers globally, which is no surprise given the amount of available infrastructure.

Cofense Intelligence continually provides phishing campaign updates throughout the year, which include these quarterly reports, Flash Alerts, Strategic Analyses (comprehensive threat reports), and Executive Phishing Summaries (bi-weekly trend synopses) communiqués. More details on the themes and campaigns referenced in this quarterly can be found in those reports.

Phenotype Overview

Phenotypes are distinguished by the observable characteristics that compose a malware's primary function—essentially the type of malware that a particular family is classified as. For example, malware that primarily performs keystroke capturing is labeled as a keylogger. Cofense Intelligence tracks a broad set of malware families, which produces a large data set. Each set is seen in phishing-borne vectors.

Malware volume started to increase from its Q4 lull around the middle of January, when Emotet resumed phishing operations. Emotet halted operations around the middle of February. This may be due to the pandemic, as the timing of Emotet's suspension coincides with COVID-19's global spread. The 404 Keylogger became increasingly well-known and more easily detected, and we assess that security measures have improved in defending against this keylogger, leading to its decline in dissemination via phishing. This has contributed to the decline of the keylogger phenotype overall, as compared to other phenotypes. Overall, information stealers were the top phenotype identified by Cofense Intelligence in phishing campaigns. These families have been prolific in COVID-19 themed campaigns, which could be attributed to an influx of novice threat actors using simple malware families that are cheap or open source and thus, typically well-known and more easily detected.

Generally, Cofense Intelligence has observed an increase in ransomware campaigns distributed via phishing. Ransomware operators are similarly leveraging this pandemic with COVID-19 themed emails. While most ransomware campaigns continue to be targeted, Cofense has assessed that more widely targeting ransomware campaigns may make a return due to the fact that the attitude toward ransom payment has shifted in the last year.

Older, complex, and even re-wrapped malware families have reemerged in phishing in the last quarter. In some instances, the payload never touches disk, while in other instances, a payload drops multiple additional payloads to disk. In all cases, it only takes one payload to be executed on the endpoint for it to be compromised. The chart below identifies our top 6 malware phenotypes delivered via phishing in Q1 2020.

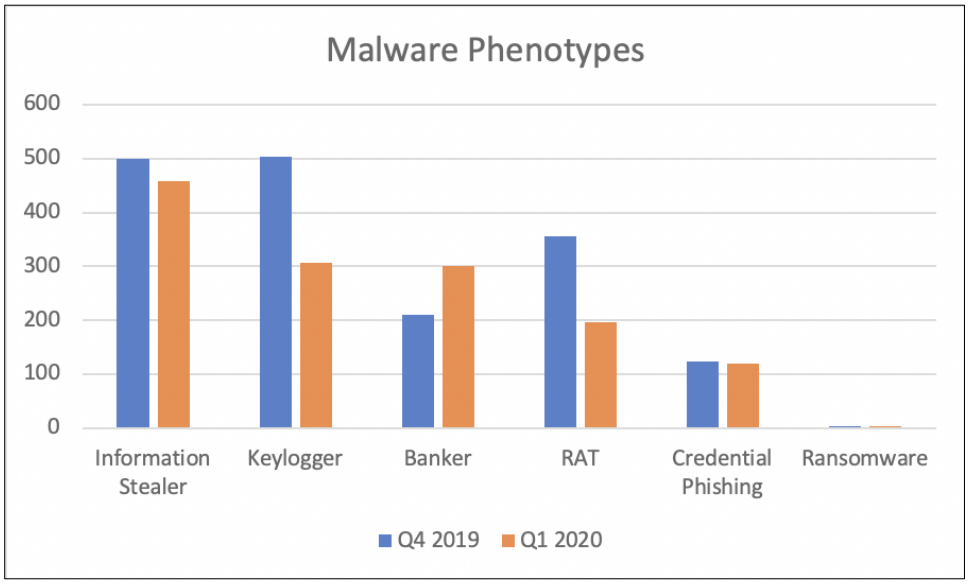

Figure 1: Q4 2019 (blue) phenotype trends compared with Q1 2020 (orange).

Note: These malware families are either directly delivered via unique phishing campaigns or as a secondary download. The delivery mechanisms noted below are responsible for some of these distributions. For credential phishing, these statistics only focus on emails that contain attachments; the amount of link-based credential phishing emails is far higher.

Delivery Mechanism Rundown

Office macro-enabled documents remain the number one malware delivery tactic via phishing. Emotet's month-long run boosted this statistic, as Emotet heavily favored malicious macros as its first stage loader. The prevalent use of Office macro-embedded documents to deliver malware almost certainly lies in the fact that it is easy to operationalize and still works within many organizations, as they rely on macros for everyday business tasks. CVE-2017-11882, also known as the Equation Editor vulnerability, ranks second among delivery mechanisms despite a patch being available since 2017. This highlights the difficulty organizations have in comprehensively patching and defending against longstanding attack vectors.

Malicious downloaders were common in phishing campaigns over Q1, though not nearly as common as malicious macros or CVE-2017-11882. Malicious downloaders include custom, often single-use, delivery mechanisms that are included within the infection chain of a phishing campaign. These delivery mechanisms include, but are not limited to, custom VBS, JS, and Powershell loaders that are each designed to be small in size and highly obfuscated to avoid analysis. HTML attachments also fit into this category. They are used to primarily hold a script that downloads and executes a payload upon opening or a link to manually download and execute the payload.

Newly identified on the phishing threat landscape, the GuLoader delivery mechanism is trending with recent global pandemic phishing campaigns. This is an executable that typically downloads DLL files from a trusted source. Once downloaded, the DLL file is then XOR'd with a hardcoded key by the GuLoader sample. The output of this function is then compiled into a malicious binary which is executed in memory and typically is not placed on disk. The use of GuLoader as a delivery mechanism is on the rise and adaptations of it will likely appear in other infection chains within the year.

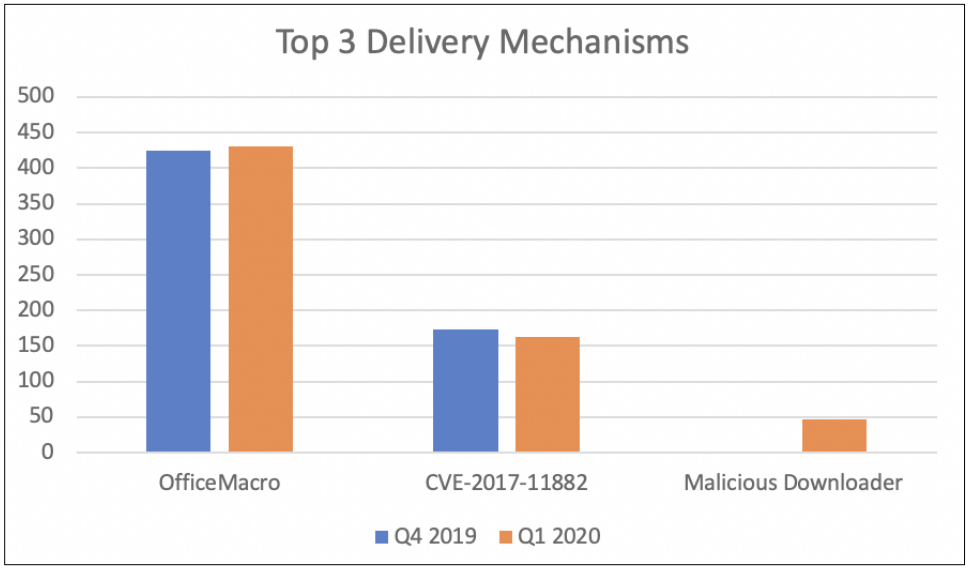

Figure 2: Q4 2019 (blue) delivery mechanisms compared with Q1 2020 (orange).

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. Keeping consistent with 2019, the United States accounts for the majority of C2 locations worldwide and has grown 10% in market share over the last nine months—increasing almost 4% since Q4. Germany is holding strong in the second spot with the Netherlands taking its spot in third, jumping there from sixth. Russia has been dropping in hosted C2 servers for the last two quarterly reports and it looks like that trend continues, dropping from 10% to 3% in the last 6 months. The decline in Russian hosted C2 servers could be attributed to the country-wide network implementations put in place by the Russian government, with the most recent rollout phase in late February. 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 emanating from. That said, security teams may see a C2 server (often as part of a server-hosting farm like AWS or Azure) originating from one of these top C2 hosting nations.

Country	Percentage	Country	Percentage
Q4 2019		Q1 2020	
United States	41.77%	United States	45.10%
Germany	6.33%	Germany	4.78%
Russia	3.10%	Netherlands	4.02%
France	2.99%	Russia	3.82%
Great Britain	2.82%	France	2.84%

Figure 3: Q4 and Q1 percentages for C2 sources by IP address geolocation.

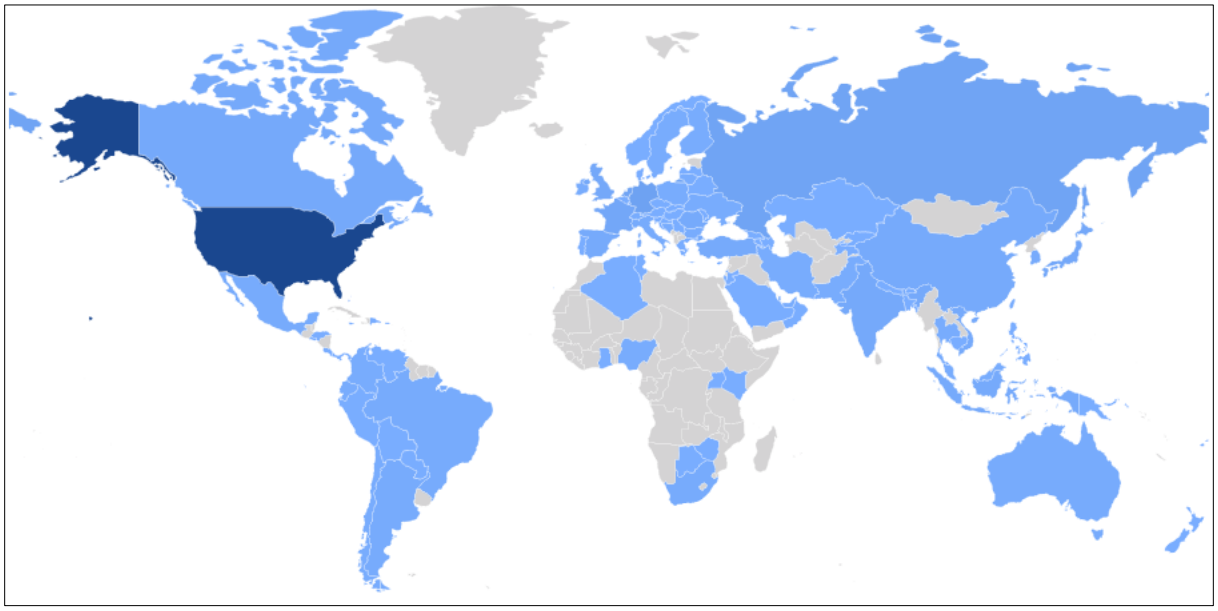

Figure 4: Global heatmap of C2 sources. Darker shades reflect more IP addresses.

STAYING CYBER-SAFE WHILE **WORKING FROM HOME.**

Phishing emails are bypassing perimeter controls, designed to target employees working remotely. Cofense is keeping you ahead of the threats.

REMOTE WORK INFOCENTER

COFENSE

UNITING HUMANITY
AGAINST PHISHING

COVID-19 Threat Landscape

Cofense Intelligence has seen a massive spike in phishing email campaigns centered around the COVID-19 pandemic, delivering credential phish and malware that range in complexity. Threat actors are spoofing global, state, and local healthcare, education, shipping, telework platforms and other organizations to appear timely and legitimate. Weaponizing the fear and curiosity of the pandemic makes for a provoking lure. Couple this tactic with the new security vulnerabilities that are being publicized as employees around the globe shift to Work From Home (WFH) status, and we have a scenario where many organizations may be more vulnerable to a security incident.

The complexity of malware and delivery mechanisms included in these campaigns range greatly. On the unsophisticated side, Cofense Intelligence has identified simple infection chains, such as a simple executable email attachments without obfuscation or compression. More complicated infection chains included many different loaders in sequence, leading to the download of a binary which, once unpacked, dropped five samples of different malware families onto the endpoint. Threat actors are aware of the current times and are gearing up for maximum impact and monetization, which includes the use of ransomware. We have uncovered two ransomware families delivered in COVID-19 themed campaigns: Nemty and Hakbit. For more information and daily updates around the COVID-19 pandemic visit the Cofense Information Center, which is available to the public. Cofense Intelligence customers are receiving IOC's within in each of these campaigns as they are identified.

Trusted Platforms

Organizations rely on trusted platforms and services to conduct efficient business operations, and they must constantly weigh efficiency against security risks. Once a platform is considered to be trusted and key to operations, typically it will be whitelisted or allowed for at least some users of that organization. Threat actors are eager to hide in plain sight, abusing these trusted services to compromise users. Cofense Intelligence has analyzed multiple campaigns that have used trusted sources as a part of the infection chain. These sources include, but are not limited to, cloud services, customer/employee engagement surveys, and third-party connections.

Organizations cannot simply block the connections to these sources, but they must implement restrictions and appropriate monitoring so that they do not become an open gateway for compromise. This threat vector is prevalent because organizations must allow connectivity to these trusted platforms and services for business operations, and because providers can be slow to respond to threats abusing their resources. The use of trusted sources should be well scoped and defined, and whitelists should be audited. Threat intelligence also helps organizations identify and defend against such abuses. Securing one's environment with safeguards like content-

filtering, network access control, network sandbox, and others can help mitigate the risk, but educated end users who can identify and report phish that indeed made it to their inboxes are critical for maximum risk mitigation.

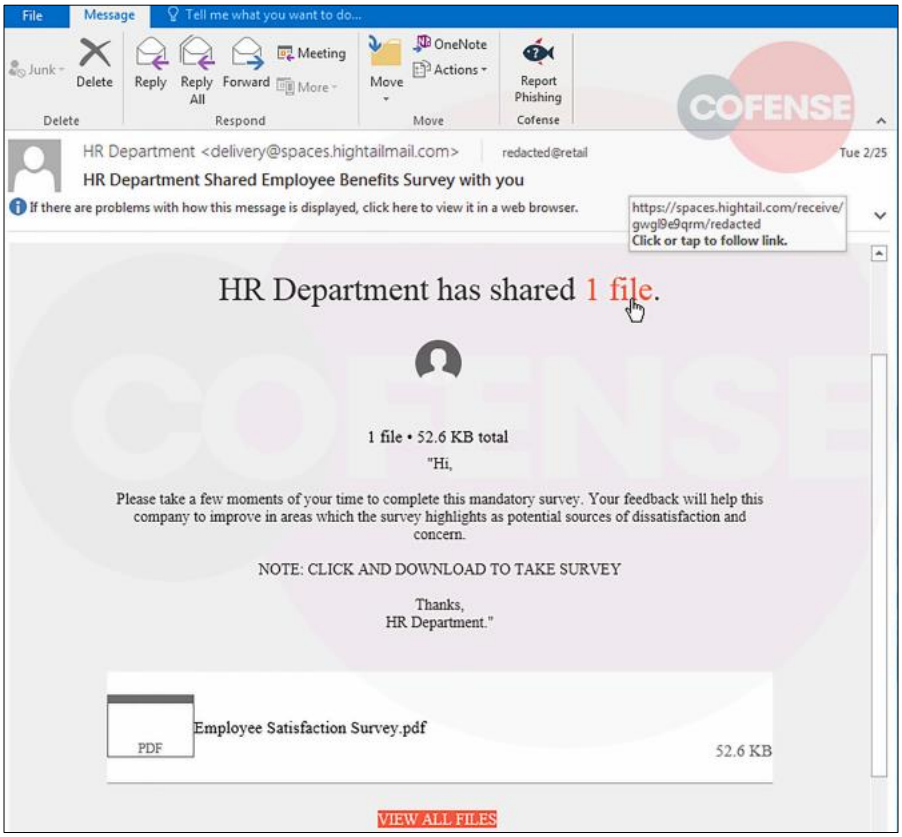

Figure 5: Example of cloud services being abused in a phishing campaign to deliver credential phishing.

Ransomware

While the widespread use of ransomware has not returned to its peak, Cofense Intelligence has analyzed targeted ransomware campaigns using themes playing on the global pandemic. Ransomware operators have also upped the ante on several campaigns- combining a ransomware infection with a data breach and releasing sensitive data if ransom is not paid. This further extorts organizations who are prepared to recover from ransomware campaigns without planning to pay.

Cofense Intelligence noted an increase in phishing campaigns delivering ransomware in Q1. Phishing campaigns delivering Hakbit and Nemty ransomware targeted the healthcare industry and purported to deliver a monthly meeting agenda using a URL shortener to a password protected download within the email body. These campaigns unconscionably leveraged pandemic email themes. Dharma ransomware campaigns were also uncovered targeting Italian users, leveraging finance themes more commonly associated with campaigns targeting a broad target population. We discovered that multiple SEGs allowed COVID-19 themed ransomware campaigns to reach the end user in enterprise organizations because of the tactics used, including URL shortening, URL redirects, and password protected files. Fortunately, these particular end users were trained to identify and report such campaigns. That said, we cannot be sure that the same holds true for all recipients of these phish.

Threat actors are almost certainly finding targeted ransomware attacks to be more lucrative, as public opinion toward paying ransom is changing and insurance companies encourage and directly contribute to payment. The shift toward targeted ransomware attacks has almost certainly reduced exposure and ensured longevity and effectiveness of many ransomware strains in the wild, giving ransomware operators more time for more targets with increased monetization over time. The overwhelming impact that a ransomware incident can have on any infrastructure could be damaging but targeting healthcare organizations during a global pandemic could be deadly.

Note: Cofense Intelligence does not encourage payment of ransom in cases of ransomware infections.

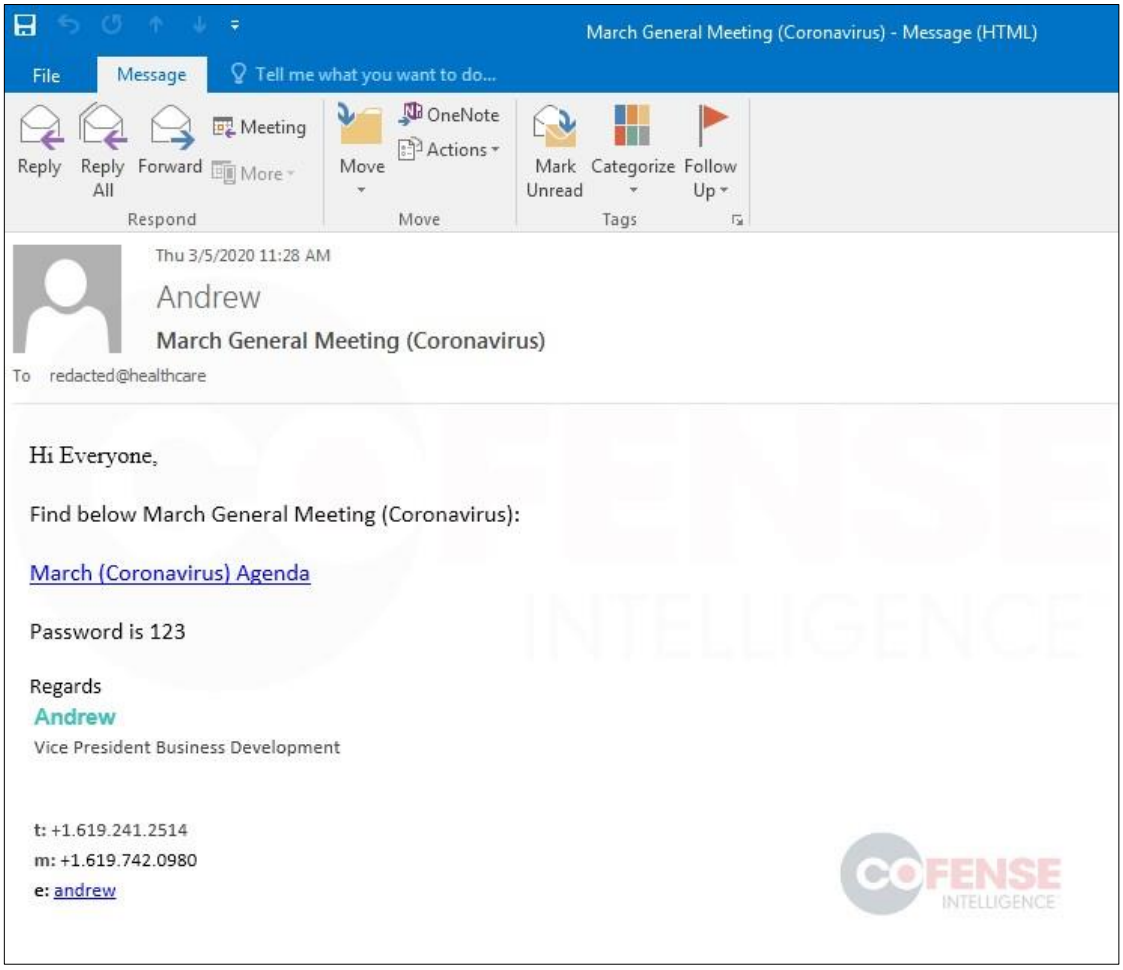

Figure 6: Example of an email targeting a healthcare industry with a COVID-19 lure delivering ransomware.

Phishing Predictions for Q2 and Q3

COVID-19 The Next Chapter

The COVID-19 global pandemic will have multiple chapters, and unfortunately, threat actors will almost certainly continue to take part in the story. The pandemic has already been used as a lure for a variety of phishing

campaigns types, and we anticipate that as fallout from the pandemic takes shape, phishing themes will follow. Themes that revolve around the "new normal" may emerge. Examples may include social gathering application invitations, notices of death, funding requests for an affected population, supply chain chaos notices, medical device/supply requests, and financial stimulus notices. As more countries are impacted in different ways, it is extremely likely that threat actors will customize their phishing themes to mirror the local headlines. With the global near-term economic downturn, more individuals may move into the illicit economy and join the ranks of today's phishers. We assess that more novice threat actors will take to cybercriminal activity, likely increasing the volume of less sophisticated malware families. It is also possible that new malware families will be created and likely used within phishing campaigns for the first time with a pandemic theme lure.

Ransomware in 2020

There are multiple transformations occurring across organizations in response to COVID-19 that can create reduced overall security. Meanwhile, ongoing changes are being made by organizations to upgrade their infrastructure for 5G network deployment. These changes are very likely going to bring about vulnerabilities that ransomware operators will seek to take advantage of.

Threat actors have already been observed leveraging the pandemic theme to deliver ransomware like Nemty and Hakbit. We have identified multiple campaigns targeting healthcare organizations for mass impact and quick monetization. Targeted attacks with ransomware will almost certainly continue. In addition, more novice threat actors will likely begin to deliver ransomware due to the broader current economic downturn, quarantine requirements, and the resurgence of reportedly available for-purchase ransomware on hacker forums. The targets of these ransomware campaigns will very likely continue to include healthcare, education, small business, and state and local governments, which are among the most vulnerable industries to these attacks. However, the types of organizations and users targeted may expand. As a result of recently publicized successful attacks, we will likely see an increase in ransomware paired with data exfiltration from organizations, to further extort victims to pay the ransom, lest their sensitive data be leaked. Cyber security insurance companies have shaped the playbook on ransomware attack response, often encouraging and directly contributing to ransom payments. With the proliferation of third-party negotiators coming into the foreground, this trend may unfortunately continue, encouraging more ransomware operations overall.

The US Election Season Will Almost Certainly Bring About More Phishing

This year's United States general election, especially in the time of social distancing, will likely become a battlefield of cyber activity. Since the 2016 presidential election, more countries that almost certainly seek to influence US elections have reportedly increased in sophistication in terms of their offensive cyber programs. It is likely that cybercriminals and state-sponsored threat actors will seek to gain entry into voting systems, email services, and social media accounts. Phishing has proven to be an effective intrusion vector into critical systems and servers, enabling attackers to reach sensitive data or essential functions for nefarious purposes. Malicious activity can also be employed to sway the opinions of voters, create disinformation, and disrupt systems to prevent voting entirely. Cofense Intelligence expects to see phishing campaigns that target elections or use election themes to spread malware.

As the COVID-19 pandemic continues, discussions around online/app-based voting abound. A quickly assembled online voting system would almost certainly pave the way for phishing campaigns and increased likelihood of voting interference. The Iowa Caucus highlighted issues around app-based voting technology earlier this year.

Though there is no evidence of malicious interference in that caucus, the limitations of such technology were highlighted, and the general election would very likely incite far more malicious activity.

Emotet is Quietly Waiting

Emotet returned from a typical lull on January 13th of this year, but stopped atypically early on February 7th. The brief nature of that spike in Emotet activity may be related to COVID-19, but we do not have evidence to directly support that hypothesis. Alternatively, Emotet's operators may have opted to recede in order to retool. The Emotet botnet today indicates its operators are actively keeping the infrastructure alive during this downtime.

Emotet was observed to be in initial testing phases of a new WiFi spreader during its most recent period of activity, and this spreader was observed to be deployed after they shut down phishing operations as well. This was a new addition to Emotet's arsenal and while rudimentary, it is an interesting addition to bolster the botnet's capabilities. Cofense Intelligence assesses that based on the status of its infrastructure, Emotet almost certainly will return, and we expect that its threat operators will continue to follow the same operating style of infection. This often includes the deployment of secondary payloads, such as TrickBot and Ryuk ransomware. Ryuk infections did continue post campaign shutdown, indicating threat operators of Emotet monetized what they had already deployed, or that Ryuk is being disseminated via other methods. Emotet is a highly advanced botnet that organizations need to be aware of and take steps to protect their assets from.

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