zix | appriver

Global Security Report

End Year 2020

Executive Summary

The Zix | AppRiver Global Security Report for 2020 highlights the threats and trends Zix | AppRiver Security analysts saw throughout the year.

In 2020, analysts saw attackers shift their tactics to take advantage of the unprecedented situation the world faced due to the Covid-19 pandemic. These attacks:

- Aimed to take advantage of uncertainty surrounding the pandemic and the shift to "work from home" throughout much of the year.
- Leveraged other world events, like the contentious US election, to distribute their attacks.
- Multiplied "living off the land" attacks across many new and otherwise legitimate services.
- Continued shift from high volume email blasts to a much more focused and customized attack style.
- Posed impersonation attacks as internal executive communications and were persistent throughout 2020.

In this report, we will take a deep dive into many of the threats and trends we saw in email security as well as discuss examples of prevalent attacks and explore potential impacts.

Introduction

Threat actors have always leveraged both local and world events to help spread their attacks. Never more so than in 2020. Early in the year, as the global pandemic came to fruition, attackers began launching spam, phishing and malware attacks utilizing interest in the pandemic. It wasn't long before they had begun crafting attacks centered around the surge in remote work. Later in the year they took advantage of the contentious US Election cycle to distribute attacks.

In 2020, Attackers continued to embrace the use of more targeted attacks versus the large volume email blasts we have seen in the past. Attackers continued to evolve and improve their distribution methods especially with "living of the land" style phishing attacks. They did this by ramping up their abuse of many legitimate service providers as well as adding new services to their toolbox on a regular basis throughout the year.

BEC attacks continued to turn up the heat in 2020 by using thousands of stolen email credentials to launch attacks from familiar and trusted sources. Impersonation attacks persisted with new theme variations.

Malware threats continued their evolution toward more chained attack techniques. We saw the use of Remote Access Trojans increase which often led to the subsequent download of a banking trojan and/or ransomware. We also observed malware as a service options become even more available on underground markets.

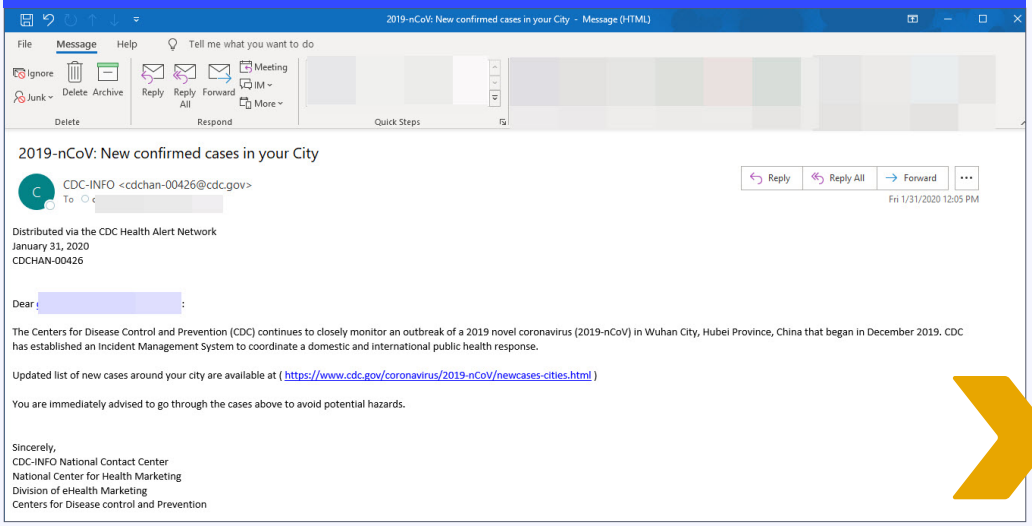
And finally, while most of us have had breach fatigue for many years now, breaches continued at a substantial rate. Credential stuffing and password spraying attacks are also still quite popular. The good news is there are some simple steps that can be taken to avoid these attacks.

Pandemic Prominent During First Half of the Year

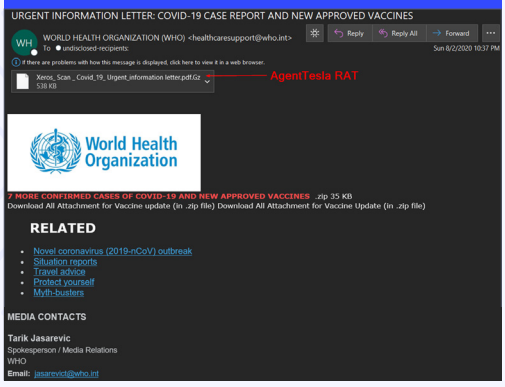
Keeping true to form, attackers were quick to take advantage of the global pandemic. The first attacks we observed in early 2020 were phony PPE distribution email scams. While these emails contained no malicious code, they were and continue to this day to be quite damaging to entities that need this equipment. With so many on a tightened budget they can hardly afford to lose funds to scammers at such a critical time.

Not long after though, we began seeing phishing attacks exploiting the pandemic to spread their attacks. Attackers were seen posing as organizations such as the CDC, WHO and SBA pushing out hundreds of thousands of phishing and malware attacks per day.

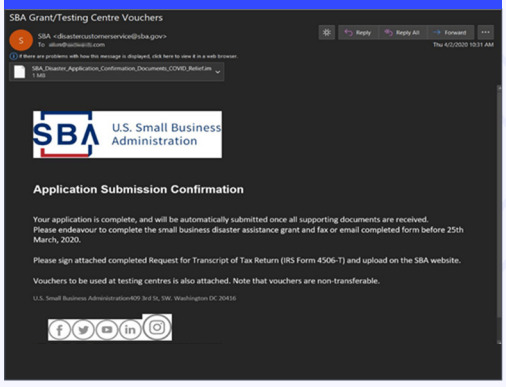
EXAMPLE 1: CDC



EXAMPLE 2: WHO



EXAMPLE 3: SBA

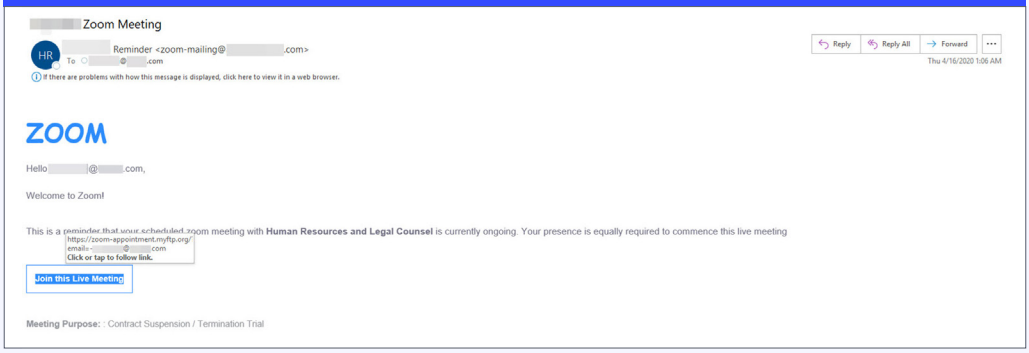


Pandemic themes continued to evolve throughout the year and were relied on by both phishing and malware distributors.

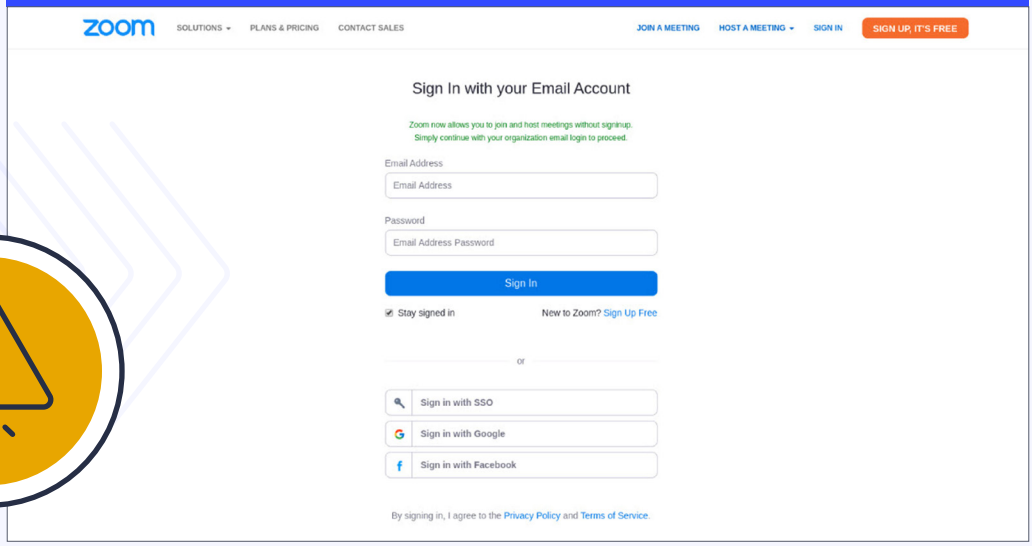
Work From Home Exploited

Through the first half of 2020 we also observed an uptick in attacks posing as collaboration and productivity solutions. Attack themes included Microsoft Teams, SharePoint, Dropbox, Slack, and many others. Perhaps the most prominent and relevant of those were attacks leveraging the Zoom brand. As Zoom saw usage skyrocket overnight, threat actors were eager to take advantage. Attackers jumped at the opportunity, knowing full well that so many users were new to the platform and unfamiliar with Zoom and therefore, naturally more susceptible to attacks posing as legitimate Zoom notifications. This example (pictured below) was one of the many attacks we captured attempting to pose as a Zoom notification.

EXAMPLE: ZOOM



The link in the message, in this case, led to another credential harvesting site...



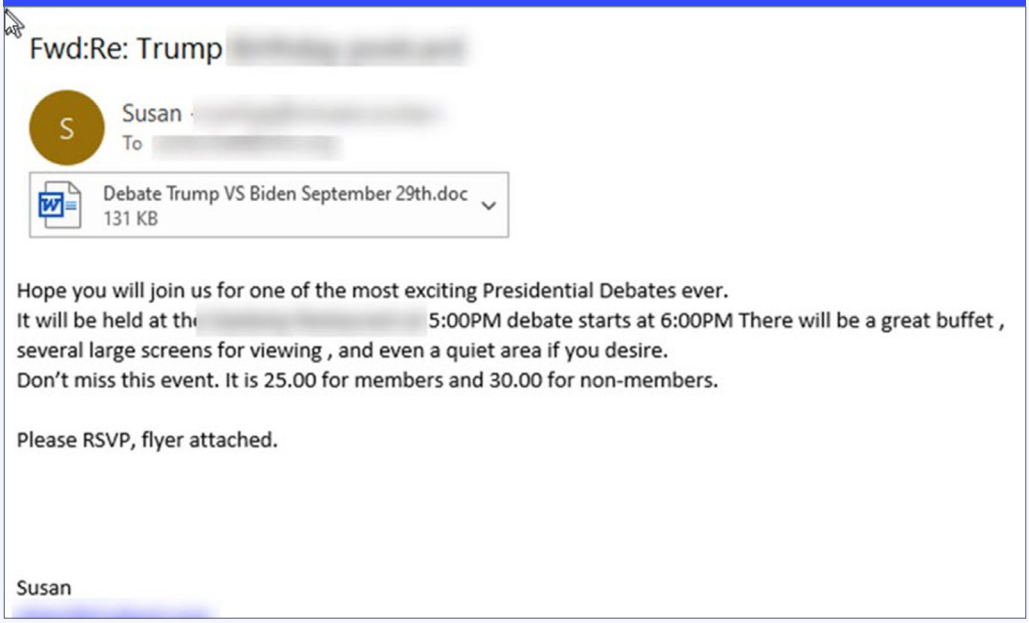
PREVENTIVE TIP: These attacks will continue to evolve while remote work remains prominent. Organizations should focus on reducing the risk associated with these attacks by educating employees through employee awareness training and other means such as acceptable use policies. These options may need to be revisited in the age of the current widespread work from home environment.

US Election Cycle in the Latter Half of 2020

In September with the US election in full swing we began seeing attackers taking advantage of the contentious topic to spread attacks.

One attack of note was launched the day of the first US Presidential debate and was using the debate to garner interest in the email. These were posing as a personal invitation to a local debate watch party, however, the attachment was a loader to pull down the Emotet banking trojan.

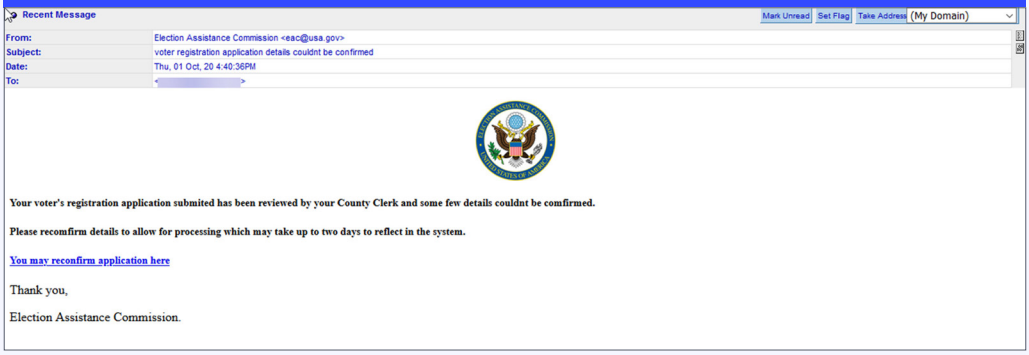
EXAMPLE 1: US PRESIDENTIAL DEBATE



This malware threat, known as Emotet, has been busy over the last several years. One of their primary means for infection has been to utilize compromised email account credentials to launch malware attacks by replying to existing conversations. Post infection, the Emotet malware family (and its follow up infections) have been observed conducting several many different criminal activities including data theft, direct financial theft, and ransomware deployment.

Only a few days later we captured another election themed attack. These messages were posing as emails from the "Election Assistance Commission" and were purporting that there is an issue with the recipient's voter registration.

EXAMPLE 2: US ELECTION



Recent Message

Mark Unread | Set Flag | Take Address (My Domain)

From: Election Assistance Commission <eac@usa.gov>
Subject: voter registration application details couldnt be confirmed
Date: Thu, 01 Oct, 20 4:40:36PM
To:

Your voter's registration application submited has been reviewed by your County Clerk and some few details couldnt be comfirmed.

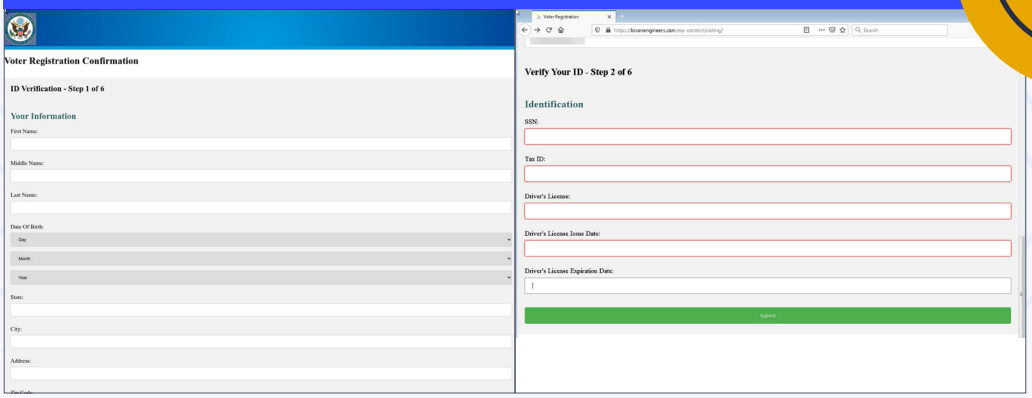
Please recomfirm details to allow for processing which may take up to two days to reflect in the system.

You may reconfirm application here

Thank you,

Election Assistance Commission.

These links redirect to one of several compromised WordPress sites. There the attackers are looking to gather personal data from the target. The page below is one of six pages designed to gather personal details...



Voter Registration Confirmation

ID Verification - Step 1 of 6

Your Information

First Name:

Middle Name:

Last Name:

Date Of Birth:

Day / Month / Year

State:

City:

Address:

Verify Your ID - Step 2 of 6

Identification

SSN:

Tax ID:

Driver's License:

Driver's License Issue Date:

Driver's License Expiration Date:

Submit

We later saw many other attacks using the election as a lure and afterward, the election results.

Malware Attacks

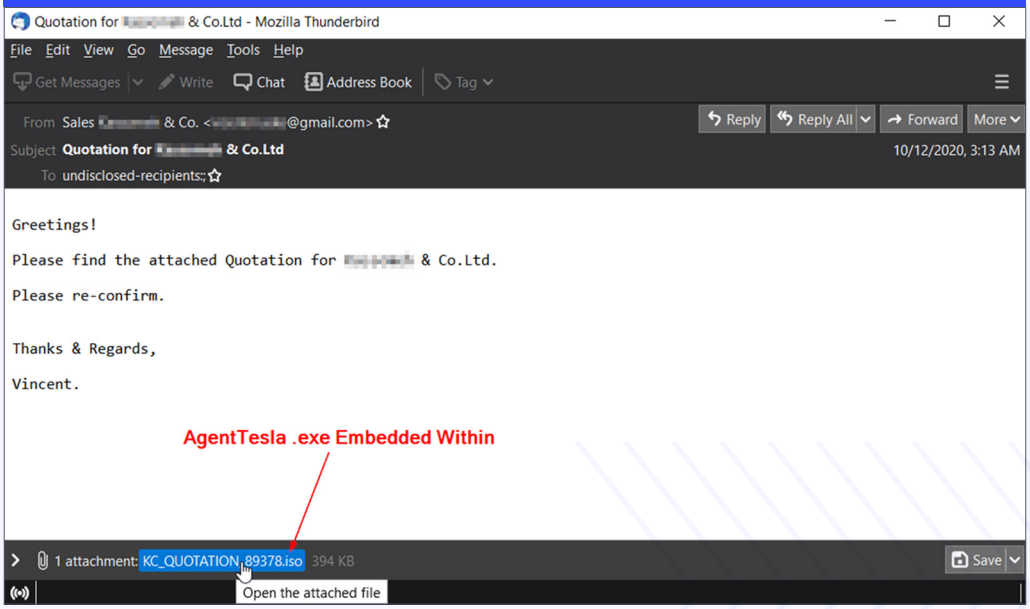
There has been a popular trend by threat actors to 'chain' malware attacks. We have increasingly observed attacks that begin as a remote access trojan to gain a foothold into systems. Once that backdoor is established, a banking trojan can be deployed to steal as much credential and financial data as possible from the victims. If the attackers decide the environment is suitable or they have compromised a high-value target, then additional data exfiltration and an end-stage ransomware deployment may be the final payload delivery.

Remote Access Trojans

Remote access tools are commonly used by system administrators to aid employees, however, some of these tools are used for nefarious purposes and are termed Remote Access Trojans. There are a wide variety of RAT's with different capabilities that threat actors may choose from. Some of the more most common capabilities include deploying other payloads onto a system, log keystrokes, monitor webcams and microphones, capture screenshots, edit the registry, restart the system, scrape passwords, and use the system as a proxy to pass their connection through.

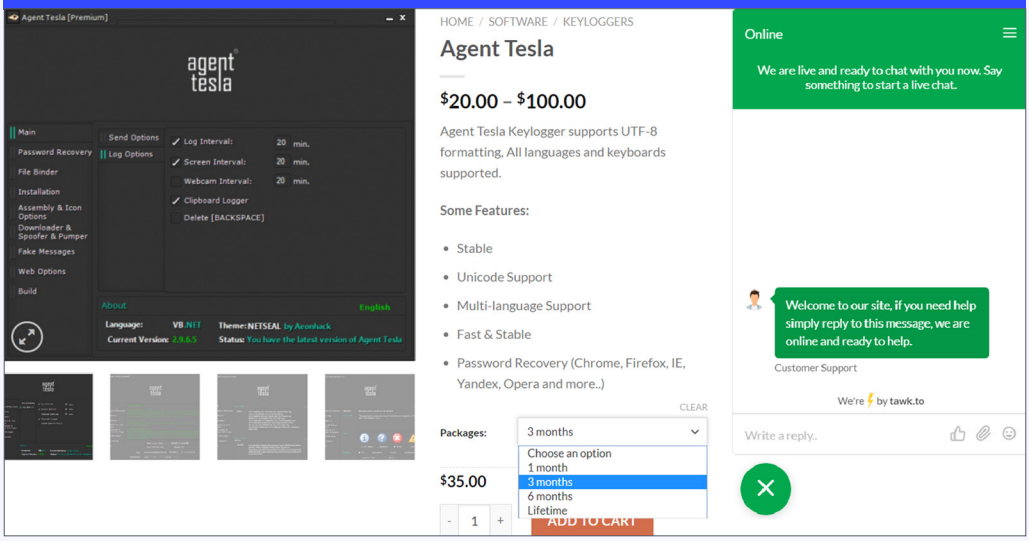
The most prolific remote access trojan our email threat protection filters captured this year was AgentTesla. It has been used for targeting customers via many different attachment filetypes and links.

EXAMPLE 1: AGENT TESLA



AgentTesla is extremely popular for threat actors due to its continuous development improvements and extremely low cost of entry. Due to the commoditization of malware as a service, virtually anyone can buy and deploy it with minimal effort. We found an advertisement that offered a one-month license for $20, 3 months for $35, 6 months for $65 or a lifetime for $100. The seller also offered some basic technical support and there was a chatbot to help potential purchasers with any questions.

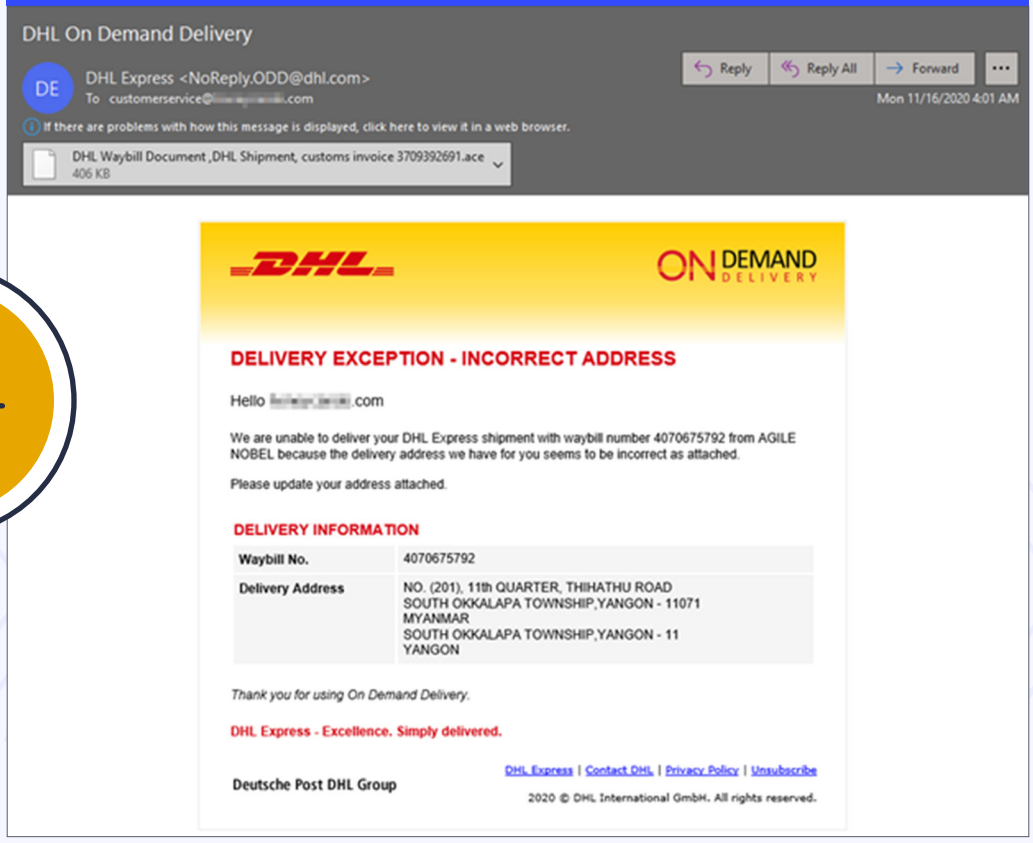
EXAMPLE 2: AGENT TESLA



FormBook has been trying to keep up pace with AgentTesla and was also distributed heavily throughout the year using a myriad of different tactics. Formbook is a remote access and information-stealing trojan that first appeared on the scene in January 2016. In addition to other capabilities, it can steal the contents of the Windows clipboard, log keystrokes, and browser data.

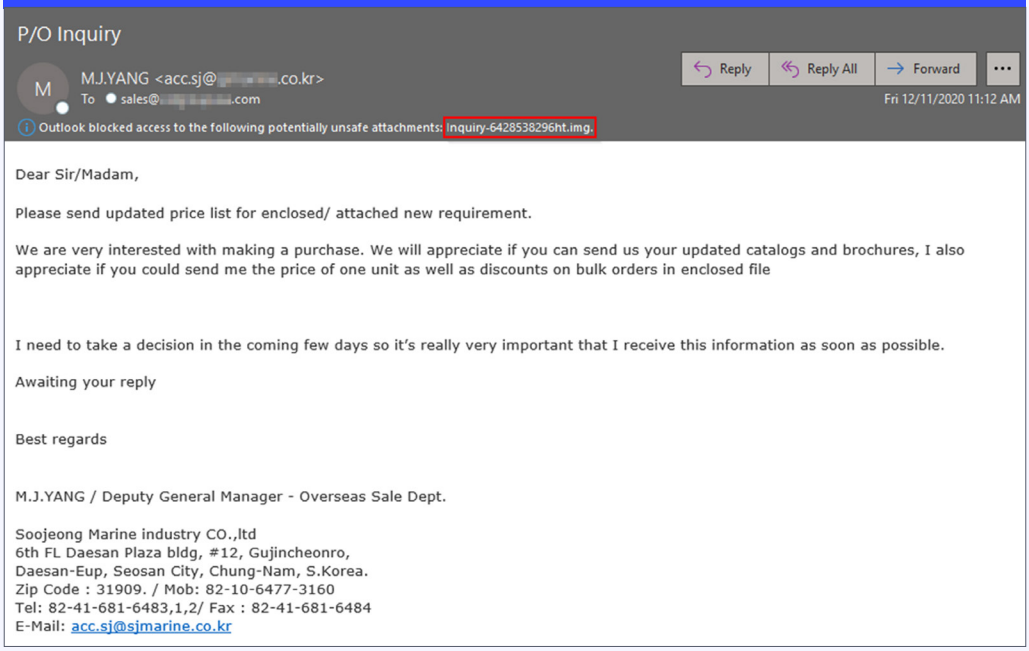
In the example below, the threat actor is spoofing DHL, which has been a favorite tactic by malicious actors this year. The attached ace archive holds an executable file that kicks off the infection chain. Banning obscure and less commonly used file extensions (such as ace) in your organization is recommended, if possible, to help minimize the avenues of delivery threat actors can use.

EXAMPLE 1: FORM BOOK



In this next Formbook example, the threat actor is using img files (disc image file) with a malicious exe file embedded within. Outlook automatically blocks this extension but other mail clients, such as Thunderbird, don't so blocking the img file extension in your organization is suggested, if possible.

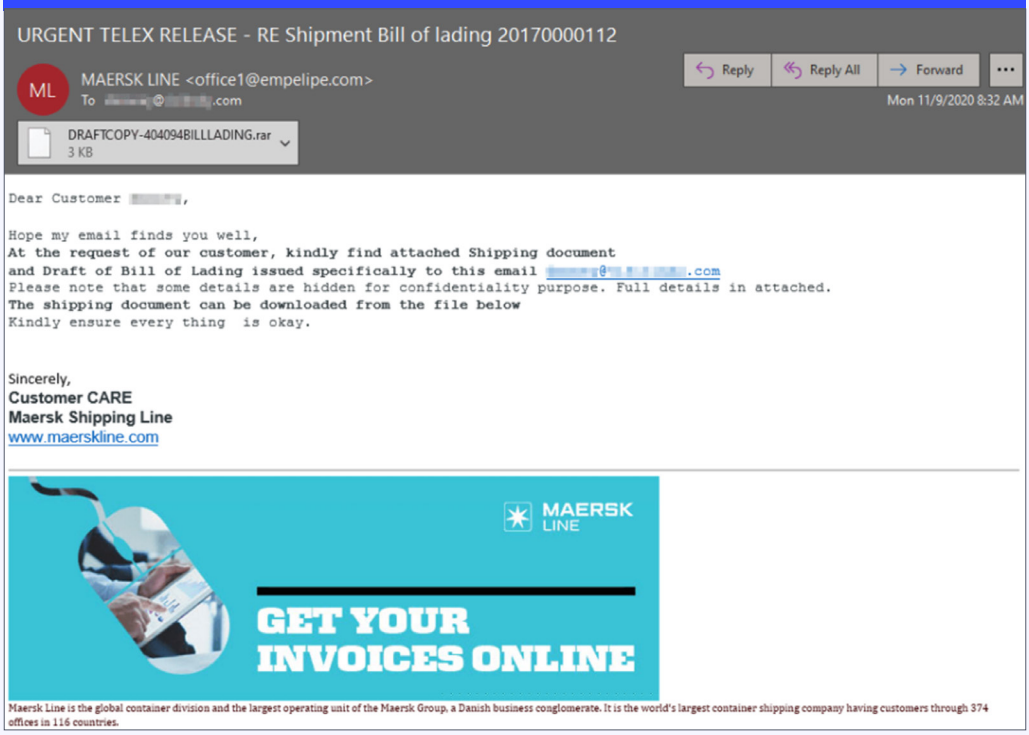
EXAMPLE 2: FORM BOOK



Vengeance Justice Worm (Vjw0rm) first appeared in November 2016 but we saw an uptick in attacks utilizing it in Q4 this year. It is a hybrid worm/RAT that is publicly available and has modular functionality for various payload delivery methods.

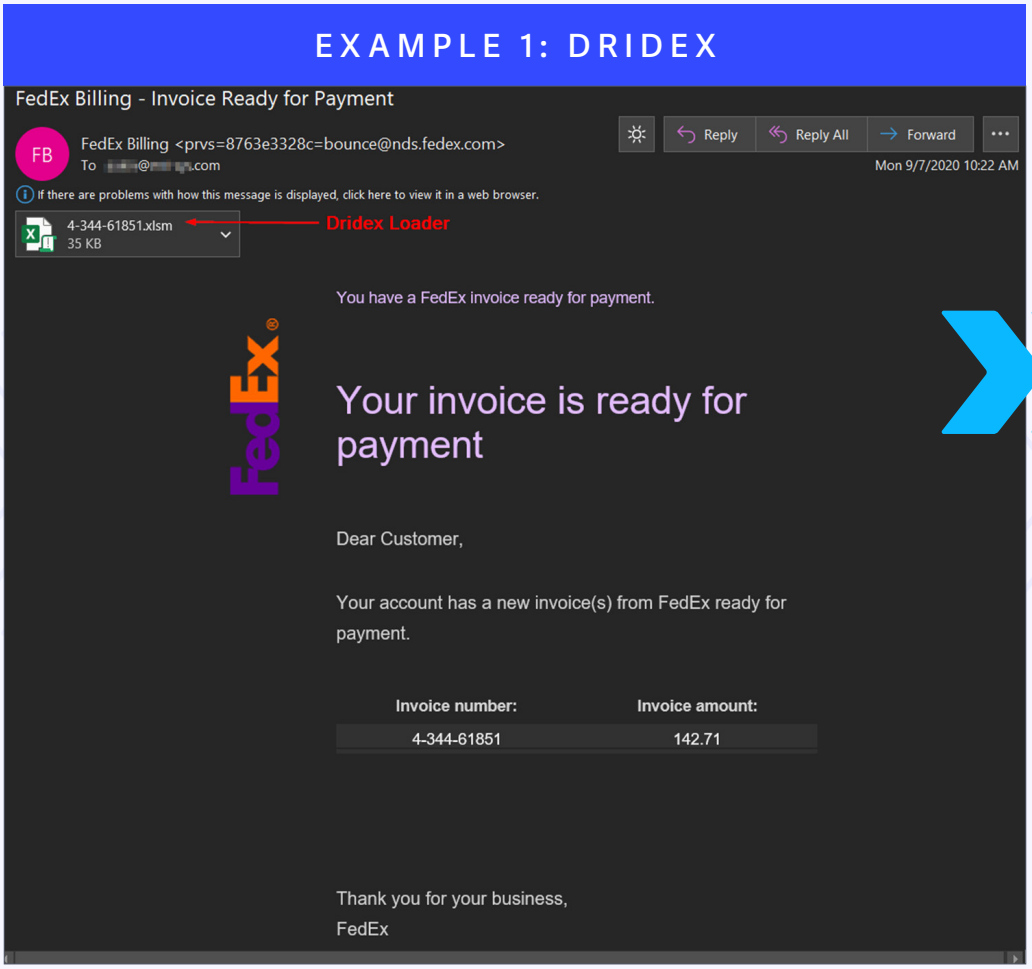
In this example the threat actor is spoofing Maersk Line with a rar archive containing a malicious js (java script) file that begins the infection chain.

EXAMPLE 3: VENGEANCE JUSTIC WORM



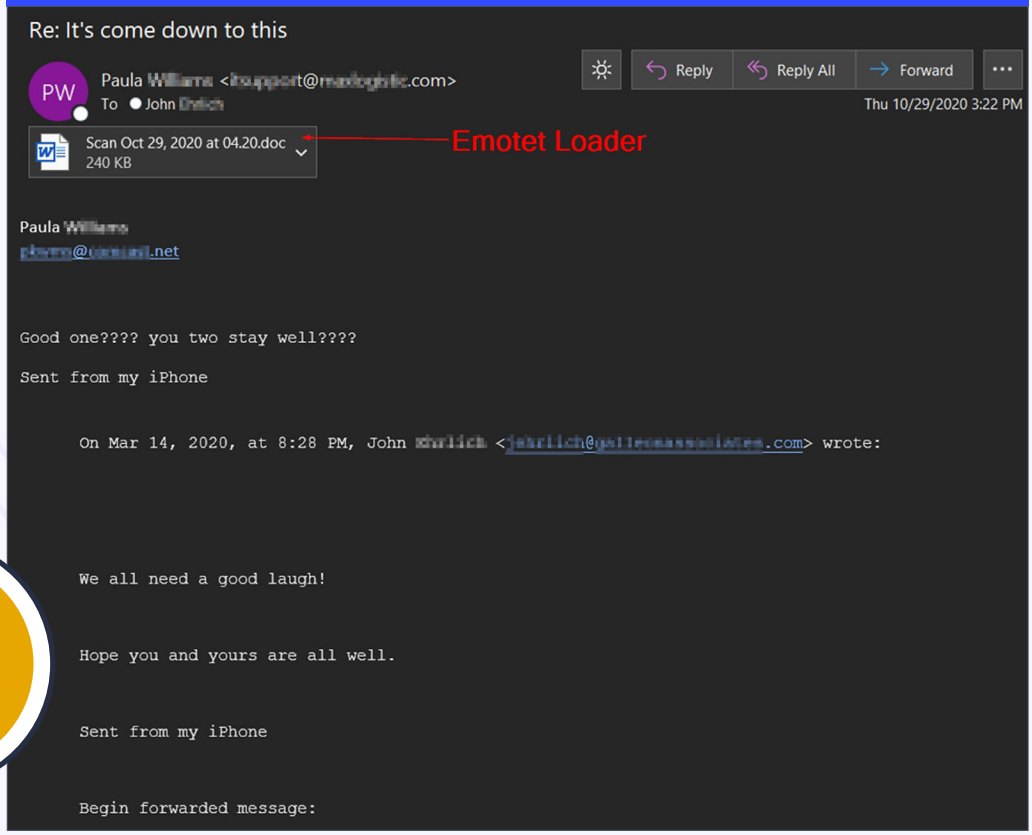
Banking Trojans

Banking trojans dominated the malware landscape this year with the largest volume originating from Dridex threat actors. The Dridex banking trojan was first seen back in 2012 but has undergone significant updates since the first versions. It is a highly versatile and evasive banking trojan that is capable of form-grabbing, click shot taking, and site injections. This gives it the ability to capture credentials from sites the user logs into. In addition, it can also download and execute more modules to load other payloads such as Bitpaymer, Doppelpaymer, or WastedLocker ransomware.



It was no surprise that the Emotet banking trojan was following up last year as another prolific threat which organizations faced during 2020. The threat actors behind Emotet operates its large botnet with three distinct clusters known as Epoch 1, 2, & 3. These separate clusters would commonly distribute simultaneous attacks via different vectors. One might be sending malicious attachments while another sends malicious links, and the third cluster could be used for testing different campaigns and measuring infection rates for future campaigns. Synonymous with Dridex, Emotet is also modular and follow-up payloads can deploy other trojans or ransomware.

EXAMPLE 2: EMOTET



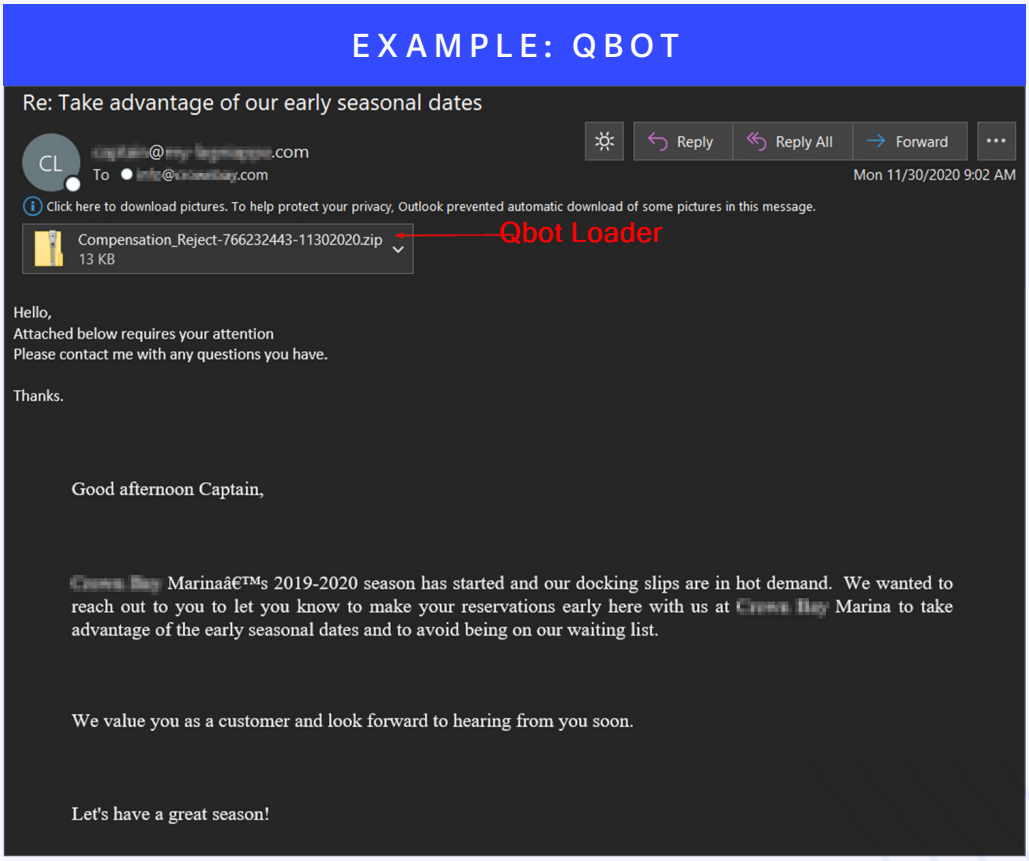
It was no surprise that the Emotet banking trojan was following up last year as another prolific threat that organizations faced during 2020. The threat actors behind Emotet operates* its large botnet with three distinct clusters known as Epoch 1, 2, & 3. These separate clusters would commonly distribute simultaneous attacks via different vectors. One might be sending malicious attachments while another sends malicious links, and the third cluster could be used for testing different campaigns and measuring infection rates for future campaigns. Synonymous with Dridex, Emotet is also modular and follow-up payloads can deploy other trojans or ransomware.

**Update January 2021: Europol has announced a global collaborative law enforcement effort has successfully disrupted Emotet's command and control infrastructure, disabling known Emotet payloads and programing the malware to erase itself. Unfortunately, the criminals behind Emotet have not been apprehended. We expect similar attacks to surface, either by the Emotet threat actors or by others inspired to leverage their techniques.*

Conversation Hijack Attacks

Conversation hijack attacks continue to persist from both Emotet and Qbot banking trojans. These two have email scraping modules designed to steal earlier legitimate email conversations. After doing so, they reply to messages with malware either attached or within a link using one of these previously hijacked messages. This is a very convincing tactic used to add a sense of legitimacy to the message. This increases attack efficacy for duping unsuspecting recipients. Any time an unsolicited message arrives, even from a trusted contact, which has an attachment or link - the recipient should be wary as the trusted contact's account may be compromised.

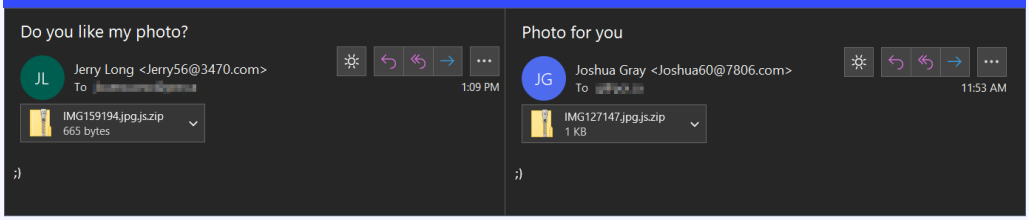
Both Qbot and Emotet banking trojan are extremely serious threats to organizations. For some of their victims, these are just first stage infections before follow-up payloads. Many times, the attackers will use Rclone to exfiltrate data before deploying ransomware such as ProLock or Egregor. These threat actors use the breached data as added leverage against the company and threaten to release it publicly if the ransom demand is not paid. Often, data breaches such as this can cost the company more over the long run from potential regulatory fines and loss of customer confidence.



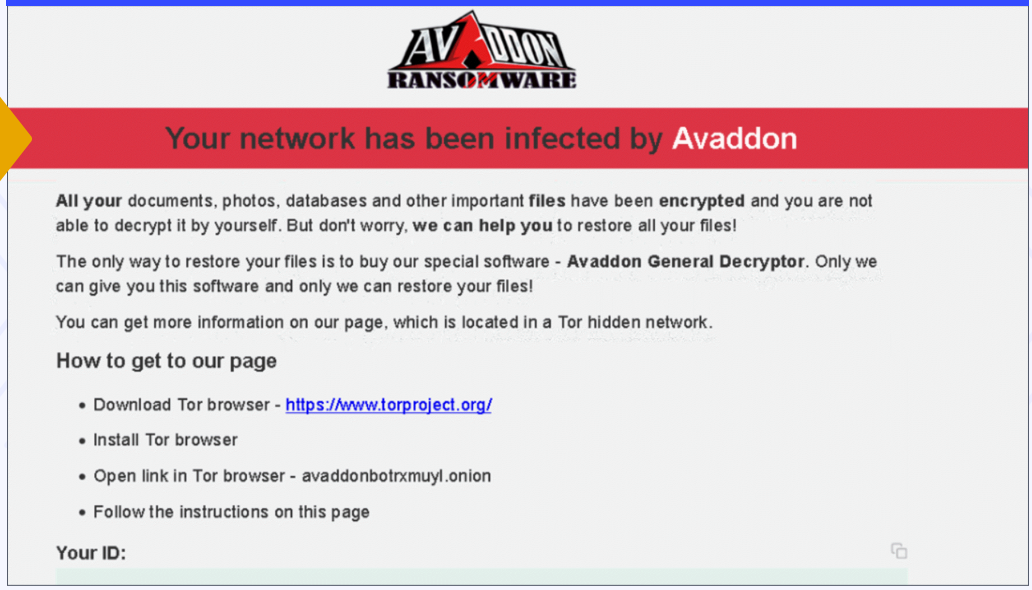
Ransomware

The largest ransomware as the first-stage payload campaign we captured this year was Abaddon, meaning doom or destruction, distributed by the Phorphiex/Trik botnet. The theme for these messages was quite simple as they all had various subject lines trying to entice the recipient to open a "photo" along with a wink emoji in the body of the email. The display names for the campaign appear to be all male sender names, unlike the female names seen in a similar Phorphiex/Trik campaign sent last year. However, synonymous with last year, the attackers used four numbers as a friendly from domain for this campaign.

EXAMPLE 1: ABADDON

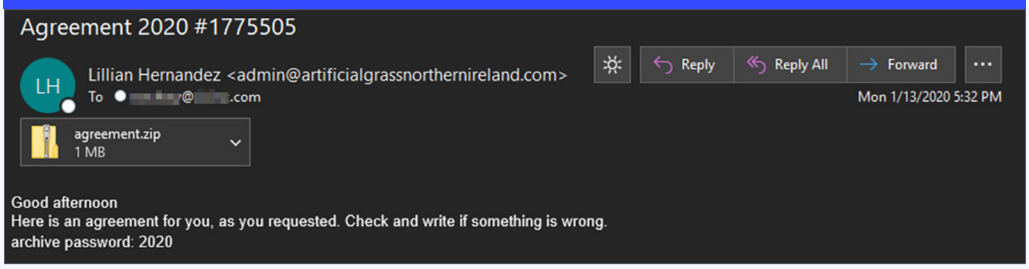


Inside the zip there was a small java script file that upon execution launches PowerShell to retrieve and run the Abaddon executable. Once the ransomware had completed the encryption process, a readme file was left on the victims' desktop with a ransom message directing to a darknet onion address for further decryption information. The ransom demands we saw ranged anywherefrom $500-$800 dollars but appeared to vary...

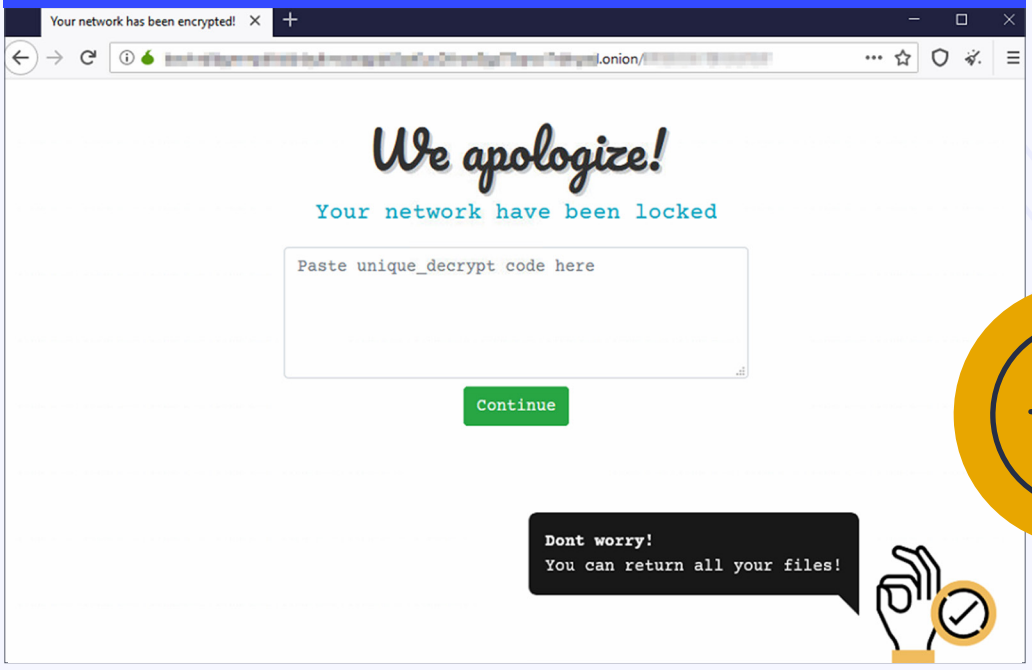


Another ransomware attack that began with encryption as the first-stage payload was AKO ransomware. The messages had a ruse purporting to be "an agreement, as you requested." Attached was an encrypted zip file with a password in the body of the email. The zip file attachment held a file that was named agreement.scr (screensaver file extension), but this file was the ransomware payload.

EXAMPLE 2: AKO



AKO ransomware was particularly troublesome for network admins due to its lateral movement capability to pivot across network environments. It encrypted not only Windows 10 desktops, but also Windows SBS 2011 servers using the typical ransomware modus operandi by first deleting, disabling, or encrypting native shadow files and backup recovery options. The ransom demand examples we saw ranged between $3000-$3800 in Bitcoin with the amount doubling after 2 days...



Phishing Threats via Living Off the Land

Malicious "living off the land" (LOtL) attacks attempt to fly under the radar by utilizing native tools that already exist in the target environment. Malicious actors leverage these existing tools and processes to commit their malicious activities while hiding among the white noise. LOtL phishing attacks are increasingly relying on the same methodology. These attacks attempt to blend in by leveraging well known services that are already seen in daily legitimate traffic. They do this to mask the true nature of their attacks and to evade capture.

We have been seeing this sort of activity for years, but in 2020 LOtL phishing saw a marked escalation of these tactics. We saw many otherwise very reputable services abused on a scale we had not yet seen. New services cropped up weekly as they were leveraged by attackers to help distribute and host their attacks. We even saw some product 'spammers' beginning to utilize the tactic while trying to avoid detection.

Some of the attacks involve sending messages directly from a legitimate platform while other LOtL attacks abuse the legitimate platform to either redirect to or host the payload — credential harvesting/phishing sites or malware delivery. Some of these attackers will even use all the above techniques in their attack by spoofing the brand they are sending from and using the platform itself for intended payloads. The top threat groups commonly rotate the platforms they abuse for these attacks to increase the efficacy of their campaigns.

Commonly Abused Services

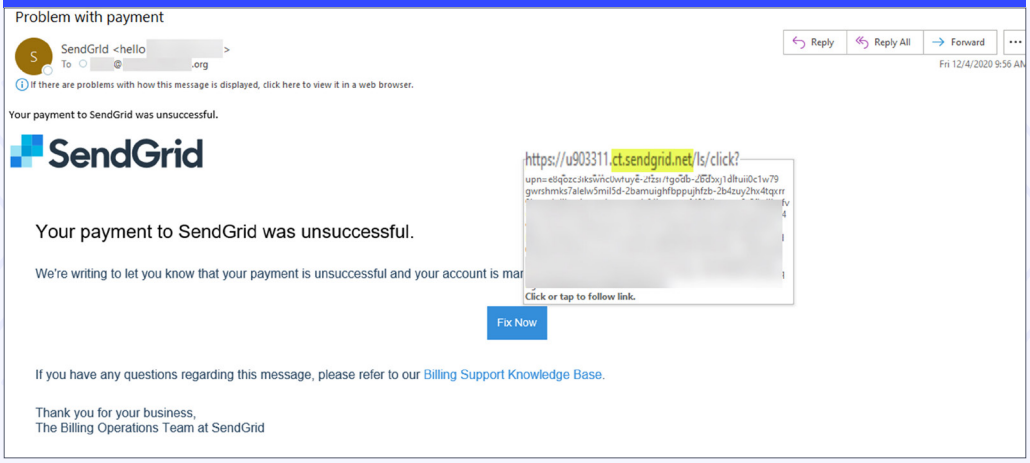
Most Common Abused Services of 2020	
page. link	PageLink is a Full-Service Digital and Marketing Agency
storage.googleapis.com	Google's cloud storage service
appspot.com	Google's cloud computing platform for developing and hosting web applications
docs.google.com	Google's word processor within its Google Drive service
amazonaws.com	Amazon's content delivery network (CDN)
sendgrid.net	Sendgrid is a cloud-based SMTP provider
web.app	Mobile platform used for building mobile apps hosted by Firebase — Google's mobile and web app platform
sharepoint.com	Microsoft's web-based collaborative platform
blob.core.windows.net	Microsoft's azure blob storage
rebrand.ly	Rebrandly is a link management platform
firebaseapp.com	Google's cloud-based app-development platform
onedive.live.com / 1drv.ms	Microsoft's file hosting and synchronization service
wetransfer.com	WeTransfer is an internet-based file transfer service
forms.gle	Shorthand URL for Google's forms service
sites.google.com	Google's structured wiki and page-creation tool
list-manage.com	MailChimp's shared click tracking domain
app.box	Box is a file hosting and synchronization service
blogspot.com	Blogger is an American blog-publishing service
surveygizmo.com / alchemer.com	Alchemer (formerly SurveyGizmo) is a survey software company
gitbook.io	GitBook is a modern documentation company
genial.ly	Genially is a media creation company
filedn.com	pCloud is a secure cloud storage company
hsforms.com	HubSpot's forms processing engine
azurewebsites.net / azureedge.net	Microsoft's cloud computing platform

Business Email Compromise

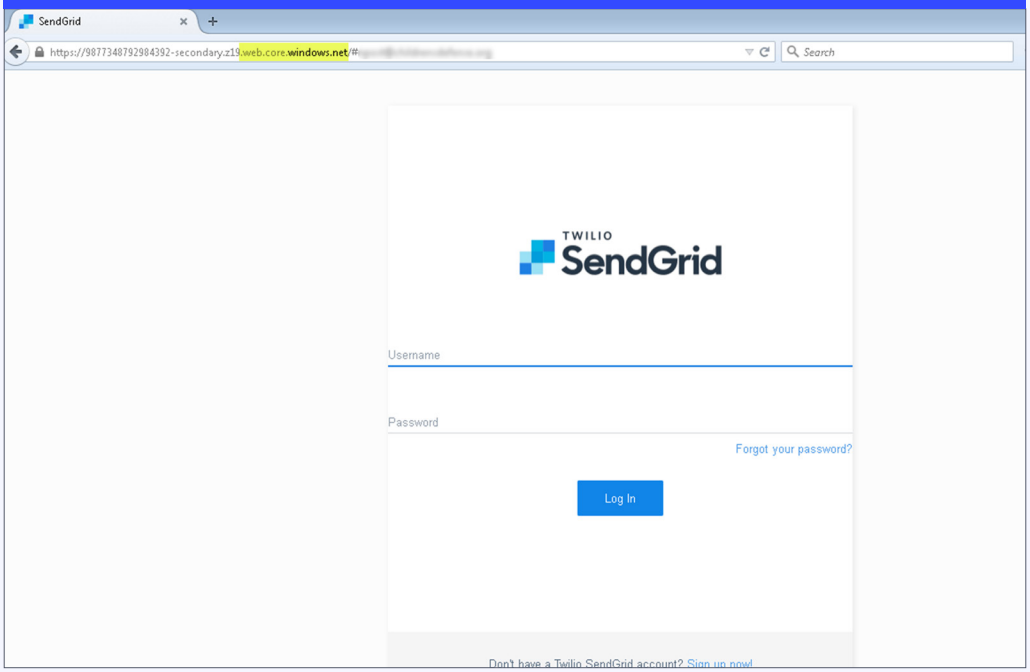
The following is an Amazon themed Business Email compromise (BEC) phishing attack we captured in late October. For this message, attackers are posing as Amazon and hosting their phishing link in the body of the message on Amazon AWS. This tactic adds a great layer of perceived validity in the eyes of the recipient.

However, Amazon was not the only brand to fall victim to having their own service abused in attacks posing as their own brand. In December we saw attackers sending messages posing as SendGrid while also utilizing SendGrid hosted URL's in the message body.

EXAMPLE 2: SENDGRID

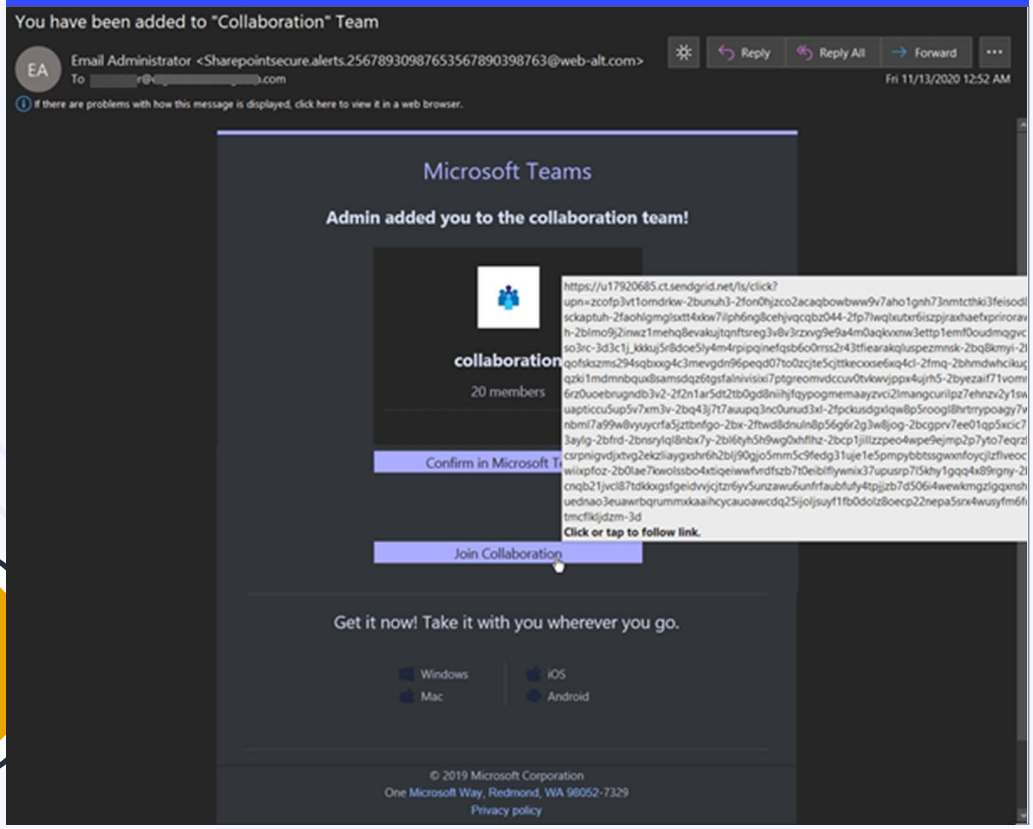


These URL's serve as a redirect to the phishing page which was being hosted on Azure/windows.net. So, this attack is in fact using two legitimate services to reach their target. While many of these types of phishing attacks target email passwords, these were aimed at gathering SendGrid account credentials. This allows attackers further infrastructure to circulate more phishing attacks using these freshly breached accounts...



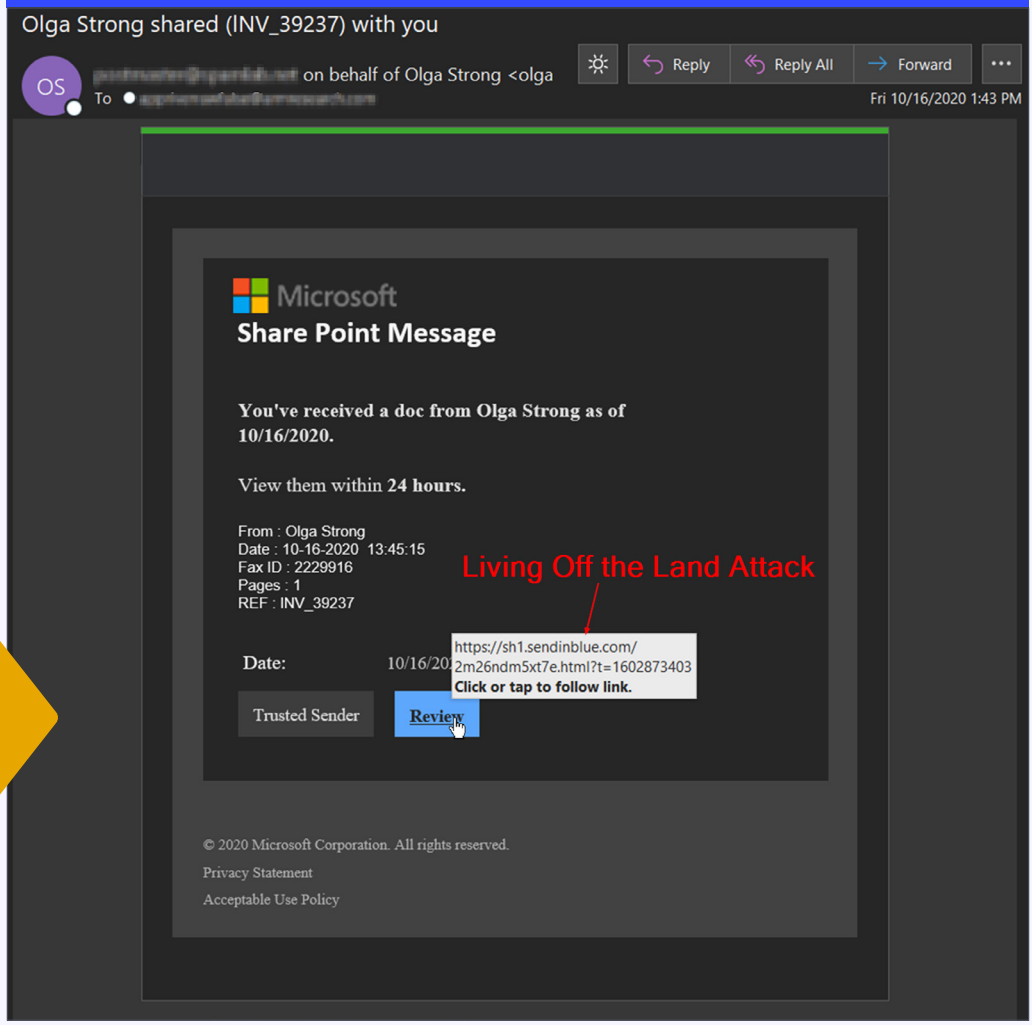
Attackers abused SendGrid to launch phishing attacks quite extensively in the latter half of 2020. Of course, the message theme and the service used in the URL payload do not always match. One of these attacks, a Microsoft Teams themed campaign, stated that the recipient had been added to a "collaboration team". The SendGrid link redirected to a credential harvesting page using the Google Firebase App storage. The performance metrics that Firebase offers to attackers has proven beneficial to their campaign tracking and targeting efforts. These attacks could prove especially problematic for those users that are new to Teams and are thus more likely to click on the URL.

EXAMPLE 3: SENDGRID



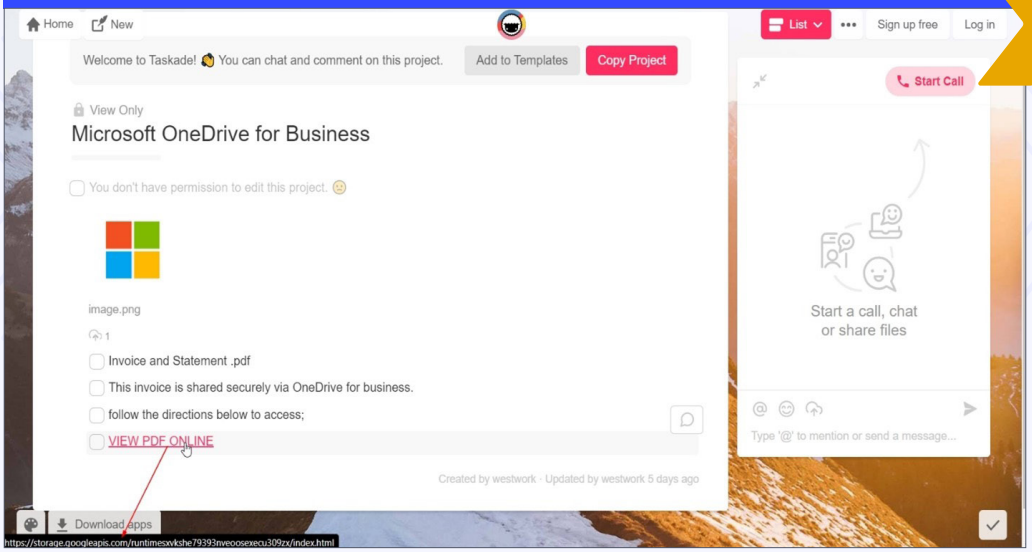
Another LOtL attack utilized the all too familiar theme, "You've received an invoice document via fax from SharePoint." The payload link leads to the SendinBlue marketing platform. Attackers had been abusing SendGrid so much we began seeing SendGrid IP's being blocked by third-party RBL's such as Spam Haus. SendinBlue was a natural failover platform for attackers which offers similar analytics abilities for tracking the efficacy of their malicious campaigns.

EXAMPLE 4: SHARE POINT



One BEC LOtL attack spoofed a shared OneDrive for Business attachment but the payload link led to the Taskade remote collaboration platform. Taskade was used to host the intermediary jump page which entices the user to "view the pdf" by clicking on to a Google page hosting the final credential harvesting portal.

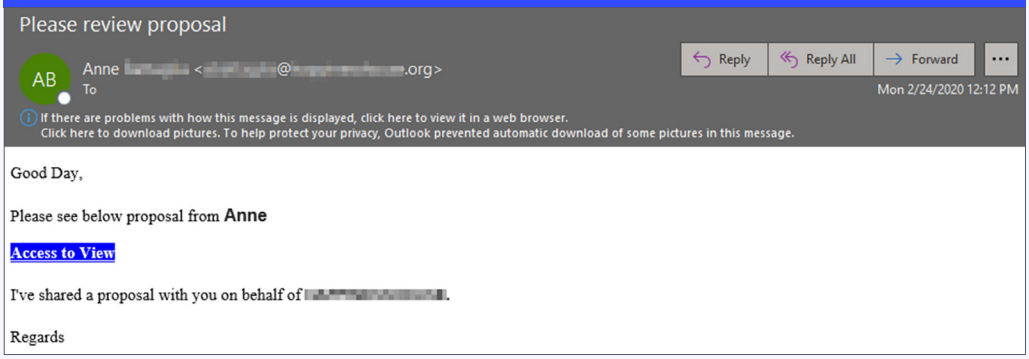
EXAMPLE 5: ONEDRIVE FOR BUSINESS



Google services have been abused at unprecedented levels this year by LOtL phishers. The sample below is from a legitimate mailbox that was compromised and used to propagate this attach to all their contacts. This is often the case with this kind of phishing, these campaigns can have a long and successful life cycle.

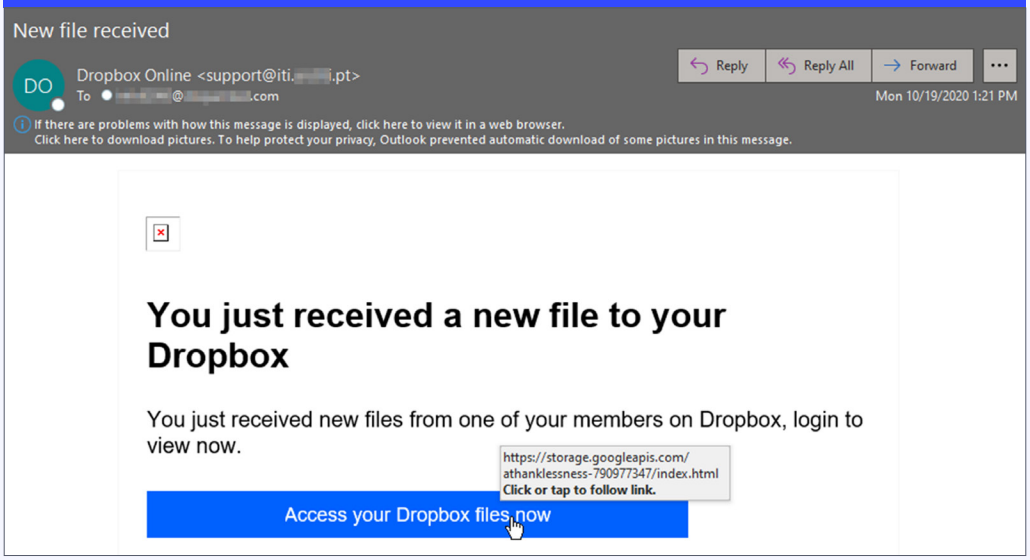
The phisher in the sample below is using the "Access to View" link to direct through sites.google.com which lands on a credential harvesting page.

EXAMPLE 6: GOOGLE



And here the phishers are spoofing Dropbox and using a storage.googleapis.com link to direct unsuspecting victims to a credential harvesting page.

EXAMPLE 7: DROPBOX



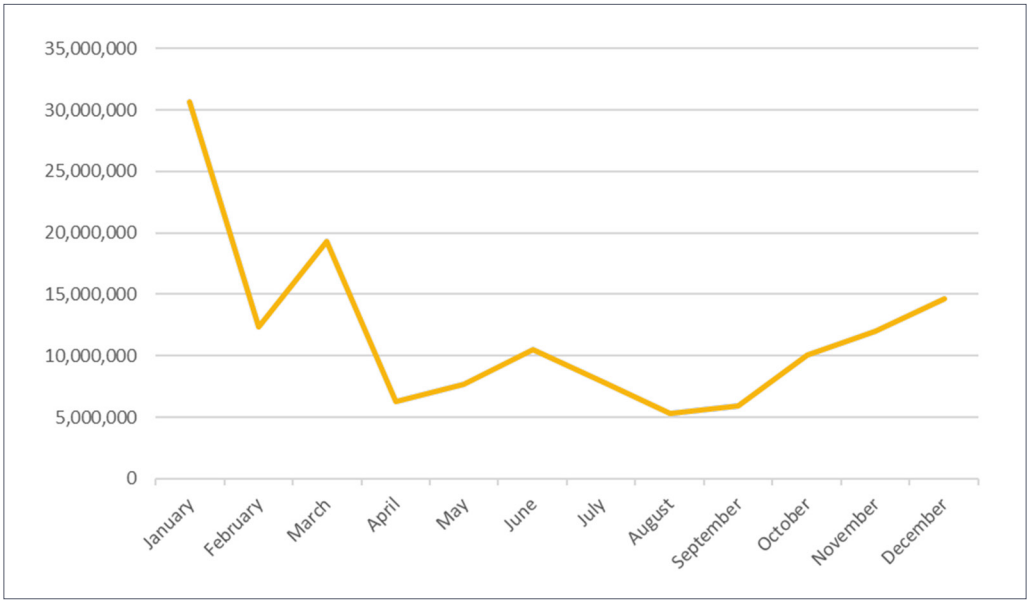
Channel Switching

A tactic that scammers have increasingly attempted, especially with impersonation attacks, is trying to gain the recipients cell phone number so they can text them for their attacks. This is most often done with gift card fraud purporting to come from an executive. By doing this, the attacker circumvents any edge gateways or email filtering defenses by obtaining a direct line of communication to the recipient.

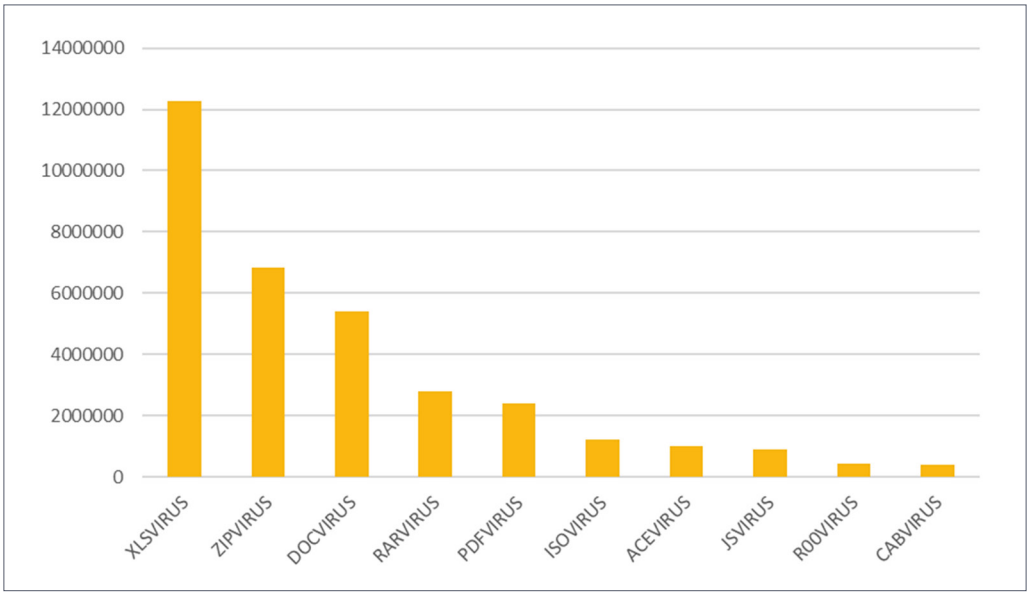
Metrics

Malware Traffic

The volume of malware being delivered via attachment was down overall from last year as malicious actors opted for more targeted attacks vs the scattergun tactic we have captured over the past. Throughout the year, our Advanced Email Threat Protection quarantined about 143 million emails containing malware in a message attachment. Malware (as an attachment) activity peaked in January and again in March before falling off prior to a return to larger volumes in the fall of 2020.

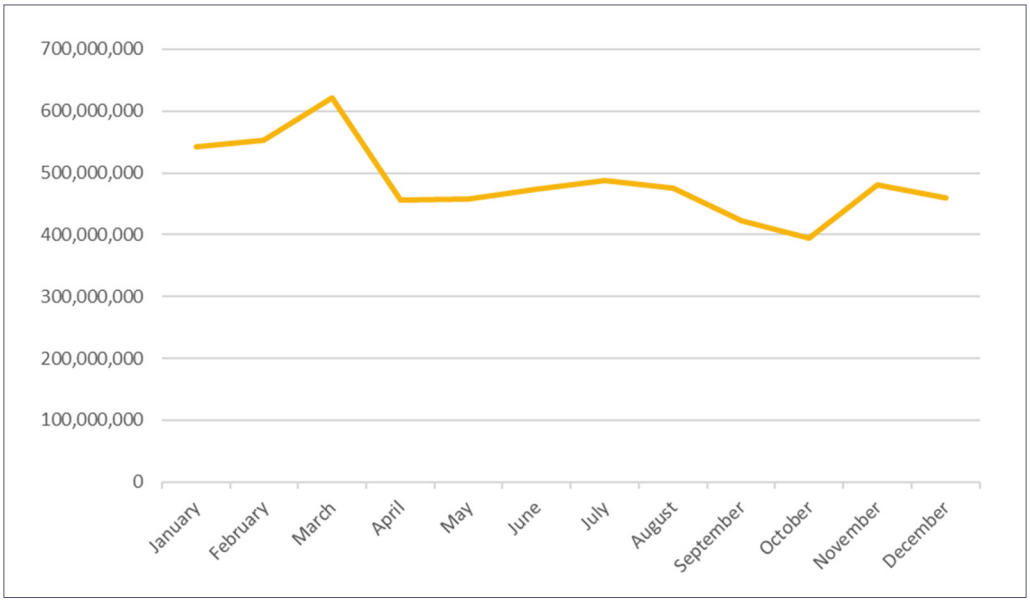


Below are the top 10 most prevalent attachment type for malware distribution. This year's malicious traffic was a departure from years past as Excel files (XLS, XLSM) were favored over Word files as the most used attack vector. However, word files were still heavily relied upon throughout 2020.



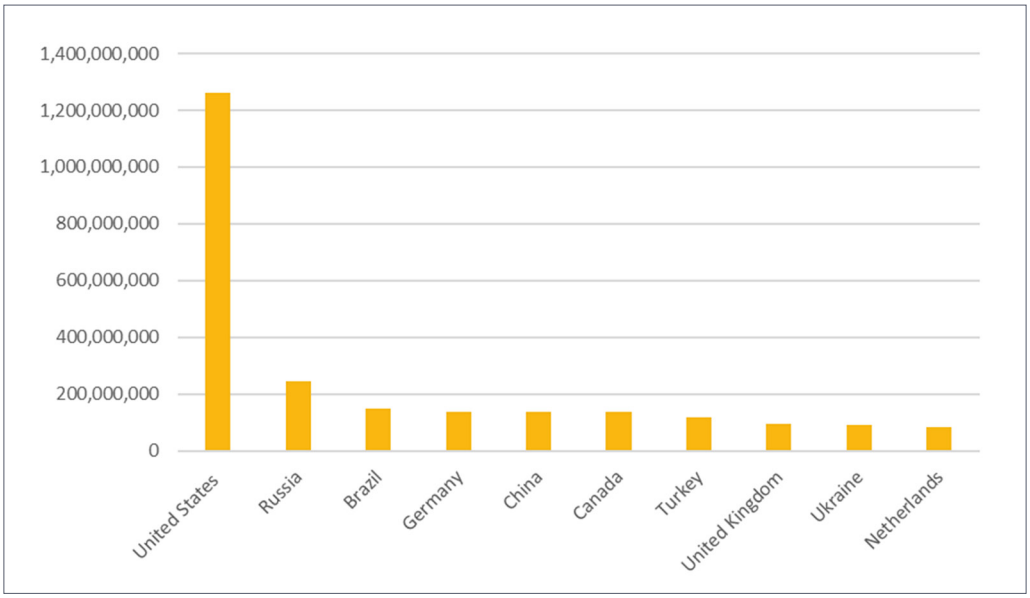
URL and Text-Based Attack Traffic

The following chart depicts the amount of all other quarantined email threat traffic caught by our email filters. The majority quarantined contained URL-based malware and were phishing attacks. We also saw a significant volume of text-based attacks, which rely solely on social engineering tactics. In all, we quarantined 5.8 billion of these type messages in 2020. The downward trend on volume-based attacks continues as attackers opt for more customized, leveraged and focused attacks.



Top Ten

Of the billions of bad email messages quarantined in 2020, the majority originated in one of these 10 countries. As the chart below depicts, the most common origination points for email-based attacks was once again the United States. However, we observed a much larger portion of email-based threats emanating from Russia in 2020.



Public Breaches

Fittingly, 2020 set new records with countless billions of company records breached. It is hard not to become desensitized to the constant flow of data breaches, but it is important to be aware of them as they may impact you eventually, if they haven't already.

Utilizing a password management app is necessary nowadays because credential stuffing is as prevalent as it has ever been. Credential stuffing is the act of inputting harvested credentials into a myriad of services to see where else that password is being used and compromising said accounts. This Wired article does an excellent job of breaking down the top-rated password management applications.

The list below details a select few of the major breaches from this year that most likely impacted you.

Microsoft

This breach happened in December 2019 but was not disclosed by Microsoft until January of this year. Microsoft's response to the breach can be found here.

Microsoft stated "Our investigation has determined that a change made to the database's network security group on December 5, 2019 contained misconfigured security rules that enabled exposure of the data. Upon notification of the issue, engineers remediated the configuration on December 31, 2019 to restrict the database and prevent unauthorized access. This issue was specific to an internal database used for support case analytics and does not represent an exposure of our commercial cloud services."

According to Microsoft they did not find any evidence of malicious use of the data, and most customers did not have personally identifiable information (PII) exposed. However, this demonstrates that all companies are unfortunately at risk of data exposure.

Walgreens

In March Walgreens announced a data breach that occurred on January 15, 2020. Walgreens official statement can be found here.

Walgreens stated "Our investigation determined that an internal application error allowed certain personal messages from Walgreens that are stored in a database to be viewable by other customers using the Walgreens mobile app."

According to their statement, their investigation determined the following information might have been viewed by another customer: first and last name, prescription number and drug name, store number, and shipping address where applicable.

No financial information such as Social Security numbers or bank account information was involved in this incident.

This breach was limited in scope to the Walgreens app, but the app has well over 10 million downloads.

T-Mobile

In March T-Mobile disclosed a data breach, their official statement can be found here. T-Mobile stated, "Our Cybersecurity team recently identified and shut down a malicious attack against our email vendor that led to unauthorized access to certain T-Mobile employee email accounts, some of which contained account information for T-Mobile customers and employees."

The statement also discloses "The personal information accessed could include names and addresses, Social Security numbers, financial account information, and government identification numbers, as well as phone numbers, billing and account information, and rate plans and features."

T-Mobile also said they did not find any evidence of this PII being used for nefarious purposes.

Keepnet Labs

In an incident summary the anti-phishing and cybersecurity awareness training company Keepnet Labs stated, "In March 2020, we started to work with a new service provider, and this service provider was performing scheduled maintenance and was migrating the ElasticSearch database. During this operation, regrettably, the engineer responsible later reported that he had to disable the firewall for approximately 10 minutes to speed up the process. During this window, the Internet indexing service, BinaryEdge indexed this data. A security researcher (Mr. Bob Diachenko), found this indexed data and could access the ElasticSearch database via an unprotected port."

Fortunately, the articles surrounding this breach were confirmed by Keepnet Labs to be misleading and primarily because it is impossible to extract 867 gigabytes (5+ billion records) inside of this 10-minute window. Additionally, this affected data was publicly known data-breach data that Keepnet Labs defined as "(1) source of the breach; (2) year the breach was made public; (3) breached email address; (4) breached password or hash; and (5) format of the breached password (e.g., plaintext, encrypted or hash)."

FireEye

In the month of December, the cybersecurity company FireEye was breached and in their disclosure they stated "During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers' security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the tools contain zero-day exploits."

Thankfully, none of these compromised tools contained zero-day exploits, but this is a genuinely concerning breach. Additionally, FireEye stated "We have seen no evidence to date that any attacker has used the stolen Red Team tools. We, as well as others in the security community, will continue to monitor for any such activity."

Red team penetration testing tools in the hands of a malicious state-sponsored actor is unsettling to say the least, as these are some of the very same tools organizations use to guard themselves against state-sponsored attacks.

SolarWinds

On December 14th, Microsoft and FireEye confirmed an ongoing supply chain attack of SolarWinds's Orion IT monitoring and management software beginning in March. This attack is reported by the press to have been carried out by APT29, also known as Cozy Bear, that is a state-sponsored group part of Russia's foreign intelligence service (SVR).

SolarWinds published a statement disclosing "our systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5 through 2020.2.1, released between March 2020 and June 2020. We have been advised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely targeted, and manually executed attack, as opposed to a broad, system-wide attack."

The DHS-CISA is issuing orders to all federal civilian agencies to "immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network." Meanwhile SolarWinds is recommending all customers upgrade to Orion Platform version 2020.2.1 HF 1.

It is currently being reported that 18,000 organizations downloaded the 'trojanized' SolarWinds® Orion® versions. Many of SolarWinds customers are large organizations and government entities. This makes this breach extremely concerning and the current fallout is still being investigated.

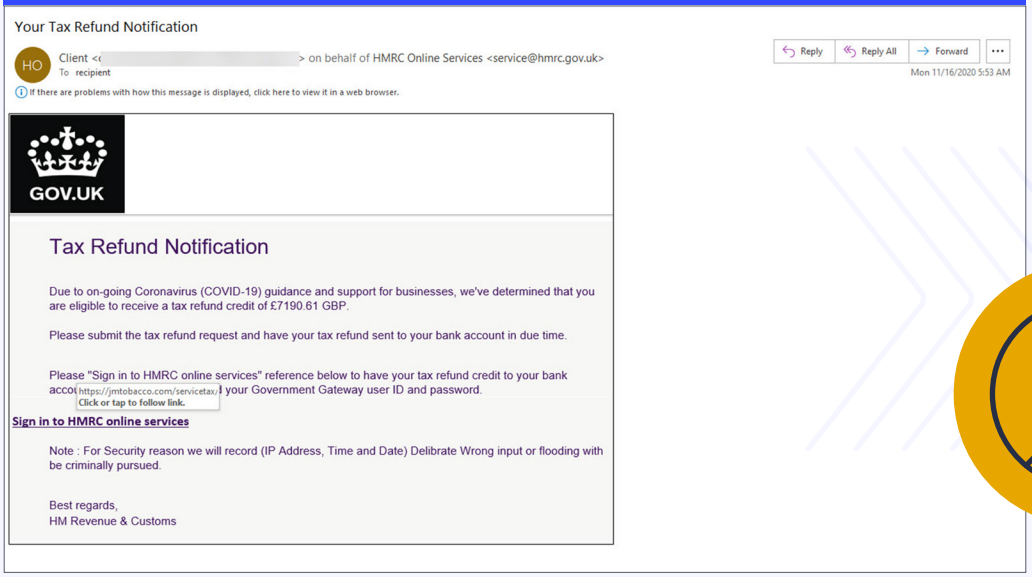
Other Noteworthy Breaches

- **CAM4** — The adult live-streaming website disclosed an exceptionally large database breach of 10.88 billion records in March.
- **Advanced Info Service (AIS)** — The major Thailand-based mobile network operator suffered a massive data breach of 8.3 billion records in May.
- **BlueKai** — The cloud-based big data startup coughed up billions of records in June.
- **Whisper** — The anonymous social media app disclosed that one of their databases was unprotected which led to 900 million breached records in March.
- **Sina Weibo** — The Chinese social network company had 538 million records exposed in mid-2019 but this was not exposed until March this year.
- **Estée Lauder** — The cosmetics titan had an exposed database which contained ~400 million records that were compromised in January.
- **Broadvoice** — The Voice over IP (VoIP) telecom vendor exposed ~350 million records due to an exposed cluster of databases.
- **Wattpad** — The service for writers to publish new user-generated stories suffered a large data breach that exposed ~268 million records in June.
- **Facebook** — In April some 267 million Facebook user identities were discovered on the dark web dating back to last year.
- **Instagram, TikTok, and Youtube** — In August a database breach exposed profile data for ~235 million users of these services.
- **Google** — In March an exposed database led to ~200 million records being compromised.
- **MGM** — In February it was discovered that 142 million personal details were on sale on the dark web after a data breach.
- **Barnes & Noble** — An unknown amount of data owned by the American bookseller was compromised in October.

Tax Scams Arrive Early

Even though tax season is still several months away, attackers did not waste any time attempting to exploit the event. In mid-November, we observed a phishing attack posing as an HMRC notification. Attackers were looking to capitalize on the uncertainty and need surrounding Covid-19 relief once again. This time utilizing the tax credit angle to gain access to their targets personal data. The massages claimed to be from the HMRC and contained a link to a phishing site.

EXAMPLE: HMRC



Predictions 2021

The Dirty Dozen

- Covid19 vaccine themed attacks have already been occurring. We expect to capture state-sponsored vaccine mis-information campaigns in addition to e-crime groups spoofing companies poised to deliver the vaccines.
- Supply chain attacks will become more common. We have only just begun to see the fallout from the Solar Winds compromise but it is a prime example of what is possible with this sort of breach. We expect both e-crime groups and state sponsored actors to further escalate these attacks.
- Living Off the Land attacks will continue to be one of the most popular tactics by threat actors. They will expand their scope of companies to abuse to help blend in with legitimate traffic and confuse recipients.
- BEC threat actors may begin to integrate Deep Fake technologies into their attacks. Given that identity is often exploited in these attacks, look for attackers to leverage this technology to lend added credibility to their attacks.
- Security professionals will have to account for the "new normal" work landscape. Defenses will continue to evolve for in-office, work from home, and hybrid-model work scenarios.
- Phishing attacks will become even more personalized, localized, and geographically targeted. Much in the same way tech companies have been so successful in building personal profiles of their users to provide pinpoint ad targeting, we expect attackers to follow suit by building personal profiles of their targets using public data, information gained from stolen data and historical interactions with prior attacks.
- Ransomware double-extortion via threatening to leak data and holding locked data hostage will increase. With the number of hacking groups exfiltrating sensitive data before encrypting files, ransomware attacks must be considered data breaches now until proven otherwise.
- Ransomware has also resulted in death of hospital patient this year. Attackers will increasingly target hospitals and the U.S. government has warned healthcare providers of this threat.
- Nation vs nation cyberwarfare will increase and carry into space for electronic dominance.
- As prices and adoption for virtual currencies such as Bitcoin increase, so will attacks trying to steal the currency.
- While the 5G rollout continues to gain steam, the associated cyber risks grow. This is due to the move toward decentralized hardware, increased reliance upon software, IoT device vulnerabilities, and dynamic spectrums for sharing bandwidth.
- Mobile devices attacks will only increase over time. Their attack surfaces and possible vectors targeting them are numerous. The devices connect to many different networks, use many different communication protocols, routinely conduct sensitive communications and transactions, and are considered "softer targets" for attackers due to the lack of traditional security solutions that protect against threats.

THIS REPORT POWERED BY ZIX CYBER INTELLIGENCE
AUTHOR: TROY GILL, SECURITY RESEARCH MANAGER