Trustwave®

2021 Email Threat Report

Table of Contents:

Introduction

Some of the most significant threats organizations face come in through email. Email has a few advantages as an effective attack vector for hackers. End-users receive email messages whether they want them or not, and email can be easily spoofed to appear legitimate. It's no wonder that cybercriminals continue to rely on email to distribute malware, phishing scams, and spam.

This report looks at some of the significant email security trends and issues of 2020.

The COVID-19 pandemic left its mark on email security, with many criminals turning to COVID-themed malware and phishing lures to fool recipients into becoming victims. Attackers also got creative with their use of uncommon file types and techniques to defeat email scanners and avoid suspicion. Additionally, Business Email Compromise (BEC) scams grew more sophisticated with their efforts to swindle more money out of large companies, while phishers made ever greater use of popular cloud services to host landing pages and distribute spam.

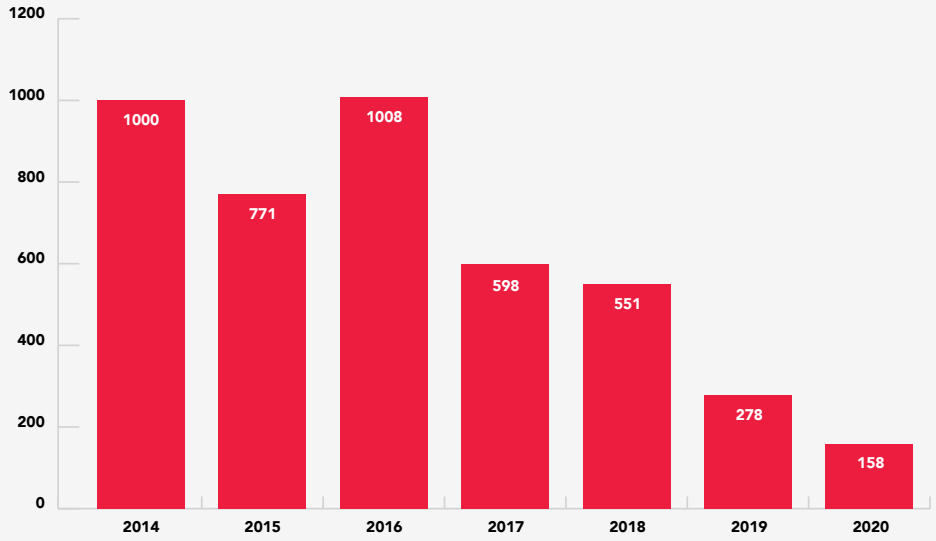
Executive Summary

- Spam volume continued its **long-term decline** in 2020, decreasing by 43 percent compared to 2019. Spam volume in 2020 represented just 15 percent of the levels seen seven years earlier in 2014.
- The proportion of **malicious attachments** in spam increased in 2020 but remains **relatively low** in a historical context.
- **Microsoft documents**, namely Word and Excel, are the most common way attackers delivered **malware through email**.
- Microsoft Excel file attachments were the single biggest attachment type utilized by attackers in 2020, representing 39 percent of malicious attachments, up from 7 percent in 2019. Forty-three percent of malicious Excel attachments made use of Excel 4.0 macros.
- The **Emotet botnet** was active in the second half of 2020, distributing malicious Word documents encased in password-protected archives before it was disrupted in early 2021.
- Fake **extortion scams** continued to be spammed out in volume, representing 10 percent of total spam.
- BEC scams continued to have a significant impact on organizations. Trustwave intercepted around **40 BEC messages per day** on average for its MailMarshal Cloud customers.
- Over **50 percent of BEC emails come from Gmail** accounts.
- **Phishers increasingly used free cloud infrastructure** to host phishing pages and files for sending emails, hosting phishing pages, storing files, and more. The services are free to use, and cybercriminals enjoy the benefits of piggybacking on the services' brand reputation.

Email Spam

Overall, spam volumes continued a multi-year decline in 2020. The Spam Volume Index chart illustrates the relative volume changes of spam seen by Trustwave MailMarshal Cloud each year since 2014 by a basket of domains we monitor.

Trustwave Spam Volume Index

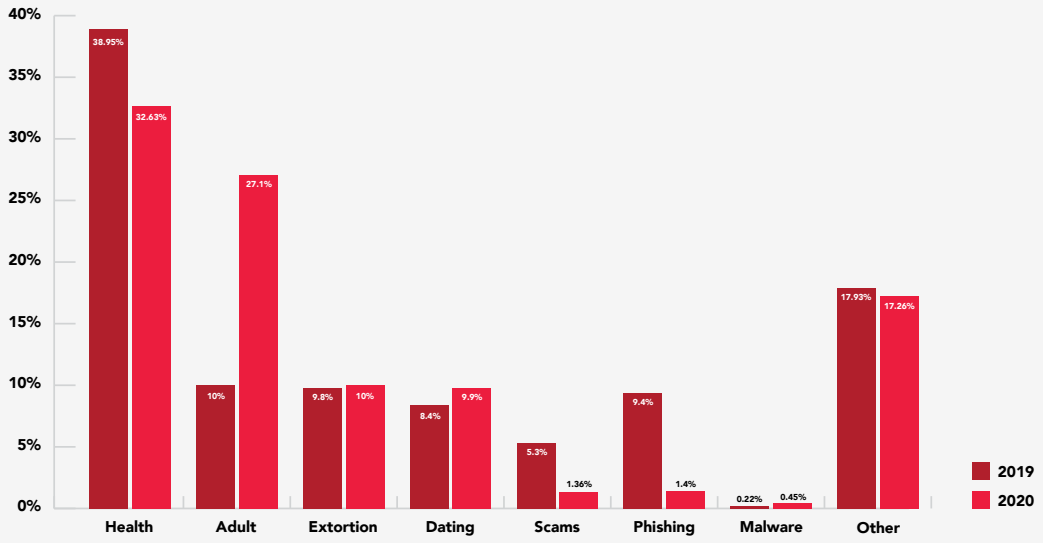


The spam received in 2020 measured 158 on the index, or 16 percent of the spam volume received in 2014—a 43 percent decline from 2019. With a number of large botnets having gone dark or ceased spamming in recent years, there is simply less spam circulating on the Internet now than there used to be. This is undoubtedly a welcome development from a spam-management perspective, but the spam that's left remains a significant threat as we'll explore later on.

Spam Subject Matter

The composition of spam changes from year to year, owing to underlying differences in cybercriminal behavior. The chart below highlights significant categories of spam in 2020 compared to 2019.

Spam Categories 2019-2020

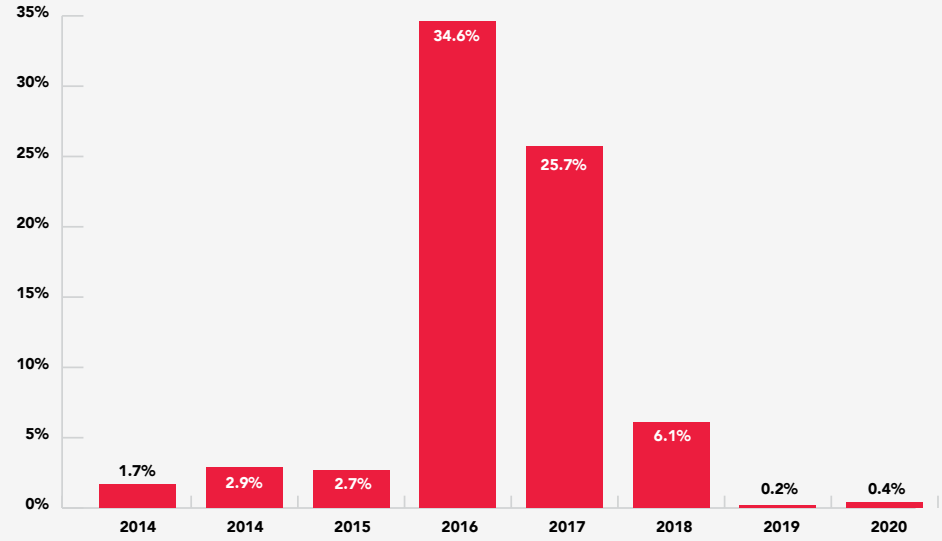


- Spam promoting **pharmaceuticals and health cures** is a perennial favorite for spammers, and not unusually, remained the top spam category in 2020 at around 33 percent of total spam.
- By contrast, **adult-themed spam**, which primarily advertises adult content sites, shot up from a relatively low 5 percent of total spam in 2019 to 27 percent in 2020.
- **Extortion scams** were consistent with last year, making up around 10 percent of total spam. These scams typically try to extort money from the recipient with fake claims of stolen data. Extortion scams evolved during the COVID-19 pandemic to use virus- and videoconferencing-related themes.
- **Dating spam**, mostly advertising online dating services, was up slightly to around 10 percent of all spam.
- **Email scam** volumes fell significantly to 1.36 percent of total spam in 2020. These messages mostly consisted of advance-fee scams in which the recipient is prompted to send the scammer a sum of money with the promise of profit or some other desirable outcome in the future. These include so-called 419 (or "Nigerian prince") scams, inheritance scams, investment scams, dying widow scams, romance scams, and compensation scams. In 2020 scams also started to use COVID-19 themes.
- **Phishing** messages dropped significantly in 2020 to around 1.4 percent of all spam. The phishing messages we did encounter in 2020 tended to be more targeted than in the past and included COVID-19 themed phishing messages targeting Microsoft Outlook and Microsoft 365 corporate logins. Another noticeable shift was an increase in common mass emailing services and cloud services to send phishing messages and host phishing landing pages.
- **Malware** represented about 0.44 percent of total spam, an increase from 0.22 percent in 2019.

Malware in Email

Email containing malware attachments accounted for 0.44 percent of total spam in 2020. This represents an increase over 2019 but remains far below the figures observed a few years ago when large botnets like Necurs routinely sent billions of malicious emails a day, at times representing more than one-quarter of all spam.

Email Malware as a Percentage of Total Spam 2013-2020

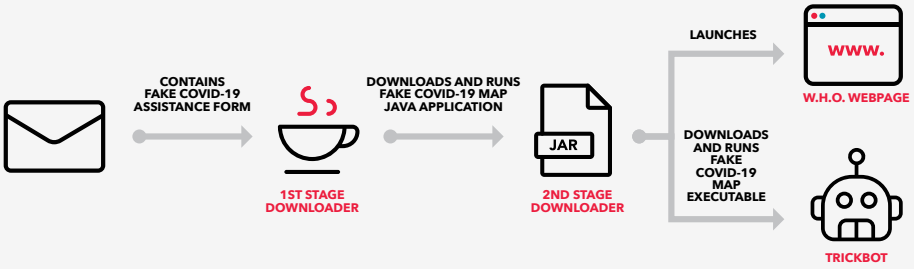


Malicious Email Trends and Developments

Some of the more interesting stories we tracked in 2020:

Covid-19–Themed Malware

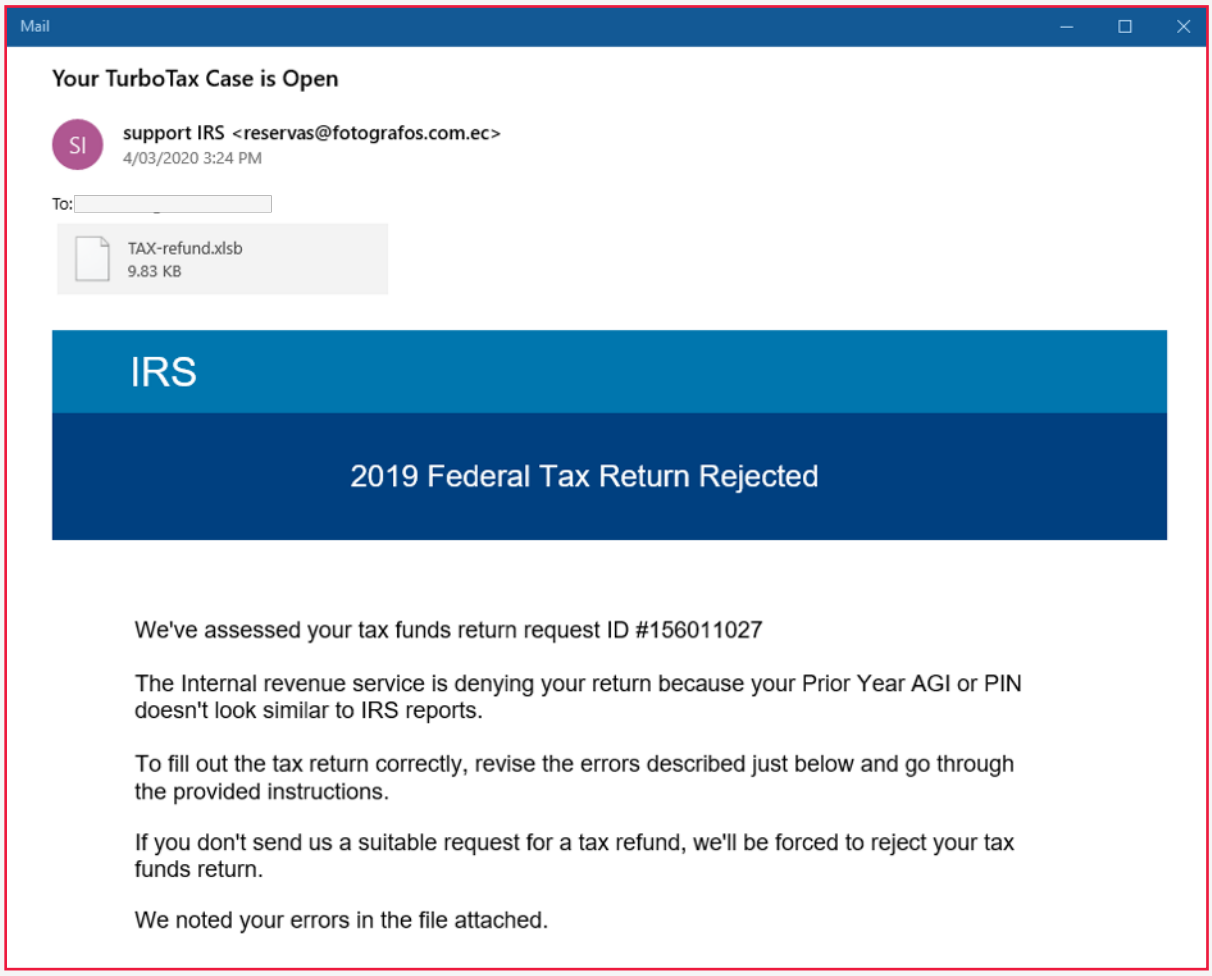
Unsurprisingly, attackers were quick to take advantage of the COVID-19 global pandemic in malicious email in 2020. The COVID-19 theme showed up in phishing emails, business email compromise (BEC) scams, and in emails containing links or attachments leading to malware. One interesting trick we saw involved sending a Java Network Launching Protocol (JNLP) file that downloaded malware disguised as a COVID-19 mapping program. See the associated Trustwave SpiderLabs blog post for more information.



A spam campaign distributed the TrickBot banking trojan disguised as a COVID-19 map

Malicious Excel 4.0 Macros

The Microsoft Excel 4.0 macro language was first introduced in 1992. Most Excel automation—and malware—today makes use of the more powerful Visual Basic for Applications (VBA) scripting language introduced in Excel 5.0, but even the latest versions of the spreadsheet product still support the old Excel 4.0 macros. Lately, cybercriminals have been taking advantage of this by embedding 4.0 macros in modern Excel workbook files with the .xlsm and .xlsb formats. The malicious macros use various obfuscation techniques to deliver malware payloads such as Gozi and Trickbot, among others.



A spam message containing a file with malicious Excel 4.0 macros

For more information about this phenomenon, see the following entries on the Trustwave SpiderLabs blog:

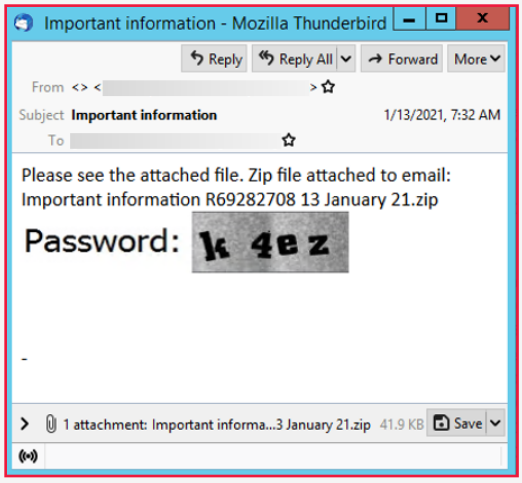
- Monster Lurking in Hidden Excel Worksheet
- More Excel 4.0 Macro MalSpam Campaigns

Working in a VelvetSweatshop

Another Excel 4.0 macro campaign we encountered in 2020 used a curious old feature to evade detection. Excel files can be encrypted using a password. Ordinarily, when such a file is opened, the program prompts the user to enter the password before the file can be decrypted. If the password is "VelvetSweatshop", though, Excel does not prompt for the password and simply opens the file in read-only mode. Attackers use this old default password, a part of Excel for more than a decade, to evade detection by malware scanners, which may not be able to identify the encrypted malware. When opened, the file launches malicious macros, which usually download additional malware from a remote server. See the Trustwave SpiderLabs blog for more information about this technique.

Emotet Evolves

The Emotet botnet operation continued to be a major source of malicious email attachments in 2020. After going silent for a time as the botnet operators reconfigured their systems, Emotet reemerged in the latter half of the year with new tricks and techniques, including eavesdropping on email conversations and including original text and attachments in the message alongside the payload attachment to make the message appear more realistic. One new technique the Emotet gang adopted involved putting their malicious document payloads into encrypted archive files, with the password contained in the message body, filename, or image.



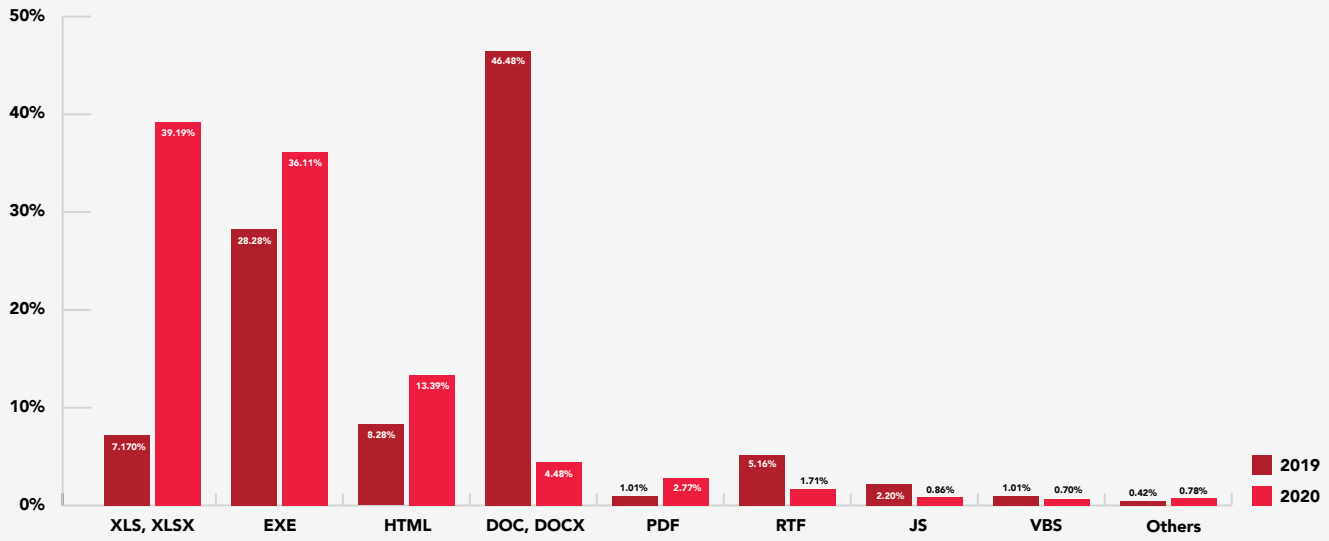
Emotet spam with an encrypted archive attachment with the password in an image

The Emotet botnet was disrupted in early 2021 via a coordinated effort between authorities and security firms. While Emotet is gone, for now, cybercriminals often restart their operations after such setbacks, under different names and configurations, so we would not be surprised to see a similar spamming botnet arise in the near future.

Malicious Email Attachment Types

The types of files used by spammers to distribute malware also change from year to year, with botnets such as Cutwail and Emotet driving some of the trends. This chart shows the file types of malicious attachments sent through email in 2020:

Email Malware Attachment Types 2019-2020

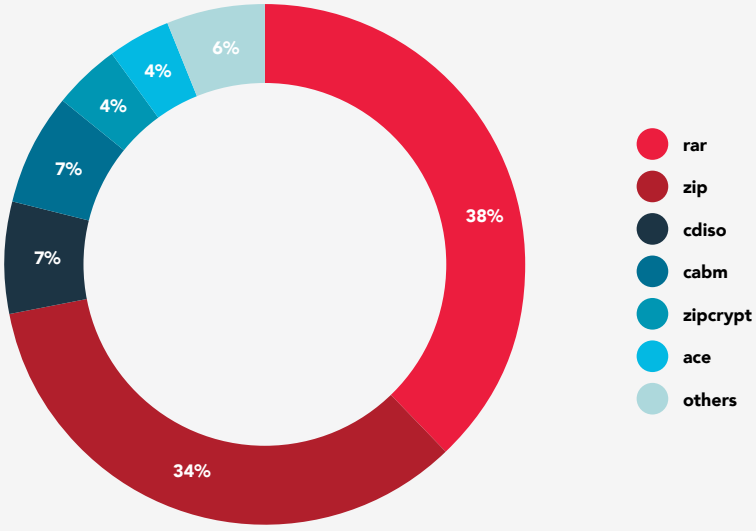


- **Microsoft** document files remain the largest category of malicious attachments, with embedded macros and other malicious code acting as downloaders for second-stage malware.
- Notably, there was a significant **shift from Word Document files to Excel files** in 2020. Excel file attachments were the single biggest attachment type in 2020, representing 39 percent of malicious attachments, up from 7 percent in 2019. Meanwhile, Word files dropped from 48 percent in 2019 to 4 percent in 2020. The Emotet botnet, which shifts its delivery mechanisms over time to achieve greater distribution, was partly responsible for this trend.
    - More than half (55 percent) of the malicious Excel files encountered were in the older Microsoft Office 97-2003 Binary file format (.xls, BIFF8), which is rarely used today due to being supplanted by more secure XML-based file formats. And 43 percent of malicious Excel attachments made use of Excel 4.0 macros. (See "Malicious Excel 4.0 Macros" above for more information.)
- Malicious **executable files** remained significant, at 36 percent of the total. About 60 percent of these were compiled for .NET, reflecting the predominance of RAT downloaders such as Agent Tesla and Nanocore.
- **HTML** attachments increased slightly from 8 percent to 13 percent. Most of these are either redirectors to websites or self-contained credential phishing attachments.
- **RTF** (Rich Text Format) files accounted for nearly 2 percent of the total. Of these, close to a third were exploits for CVE-2017-11882, a vulnerability in certain older versions of Microsoft Office.

2020 also saw an increase in malicious password-protected documents, which accounted for 8 percent of malicious attachments, up from 4 percent the previous year. Most such attachments were password -protected Microsoft document files with the passwords contained in the email body, including those protected with Microsoft Information Rights Management (IRM). Password-protected Microsoft documents are encrypted, which can make it more difficult for email scanners to detect malware.

Malware attachments often come packaged in archive files. This figure shows the most common archive file types used for malicious attachments in 2020:

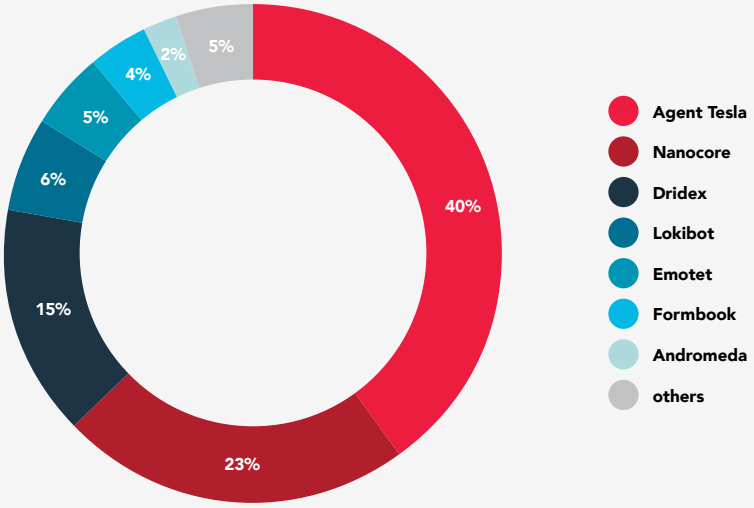
Archives Distribution in 2020



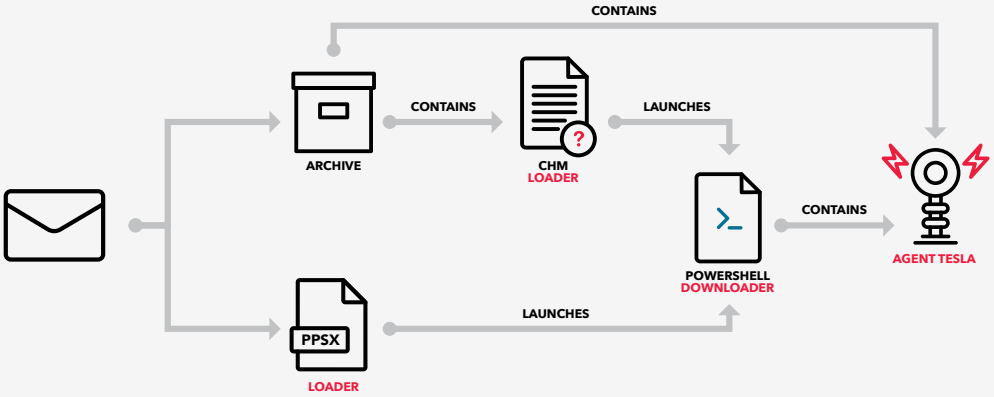
RAR, ZIP, and ISO, the top three malicious archive file types in 2020, were also the most common archive file types in 2019. Password-protected ZIP archives, the fifth most common type of malicious archive files in 2020, was commonly used by the Emotet botnet, as noted earlier.

Though attackers use a wide range of downloaders and techniques—often strung together in long attack chains—to deliver malware through email, the list of final-stage payloads they use is often quite small. More than three-fourths of the ultimate payloads we observed in email in 2020 came from just three malware families: Agent Tesla and Nanocore, both remote access trojans (RATs), and the banking trojan Dridex.

Top Spam Malware Payloads 2020



Agent Tesla, a common discovery in 2014, is capable of keylogging, screen capture, form-grabbing, and stealing credentials from a wide range of FTP, VPN, browser, and email clients. We observed it being spread through several widely disparate campaigns in 2020, including one that used a PowerPoint loader (.ppsx) file. See the Trustwave SpiderLabs blog for more information about this and other Agent Tesla campaigns.



The process flow of a spam campaign delivering Agent Tesla

Most emailed malware consists of simple trojans accompanied by social engineering intended to trick recipients into running them. Still, a significant minority seeks to exploit a vulnerability on the recipient's computer. In 2020, the most commonly encountered exploits in email attachments included the following, in order of prevalence:

Exploit	% of exploit encounters	Description
CVE-2018-0802	59.74%	Equation Editor - Microsoft Office Memory Corruption Vulnerability
CVE-2017-11882	35.56%	Equation Editor - Microsoft Office Memory Corruption Vulnerability
CVE-2014-6352	3.02%	Specially crafted Object Linking & Embedding (OLE) object allow remote code execution. Common attack in the wild were crafted Powerpoint document.
CVE-2010-3333	0.59%	Rich Test Format (RFT) Stack Buffer Overflow Vulnerability
CVE-2015-1641	0.41%	Microsoft Office Memory Corruption Vulnerability
CVE-2017-019	0.36%	Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API.
CVE-2014-4114	0.15%	Windows OLE Remote Code Execution Vulnerability
CVE-2015-5119	0.08%	Adobe ActionScript Remote Code Execution
CVE-2020-0674	0.03%	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1214	0.03%	VBScript Remote Code Execution Vulnerability
Others	0.06%	

Notably, most of these exploits are several years old, reinforcing that installing security patches promptly is one of the best ways to defend against attack. A computer that was up to date on Microsoft and Adobe security updates in 2020 would not have been vulnerable to most of these exploits.

Phishing

In 2020, phishing messages accounted for 1.4 percent of all spam. Though the specific approaches change and develop, phishing is always basically the same: Users are presented with a realistic-looking email that mimics real emails from organizations. In some cases, the attackers base their templates on real messages, just changing a few words and underlying links.

Phishing has evolved significantly since it first emerged as a criminal tactic many years ago. Whereas "traditional" phishing attempts usually targeted account credentials for financial institutions, phishers today often try to harvest credentials for cloud services such as Microsoft 365, from which other attacks can be launched. (See "Microsoft 365 Account Phishing" below for more information).

Some of the themes we encountered during 2020 included:

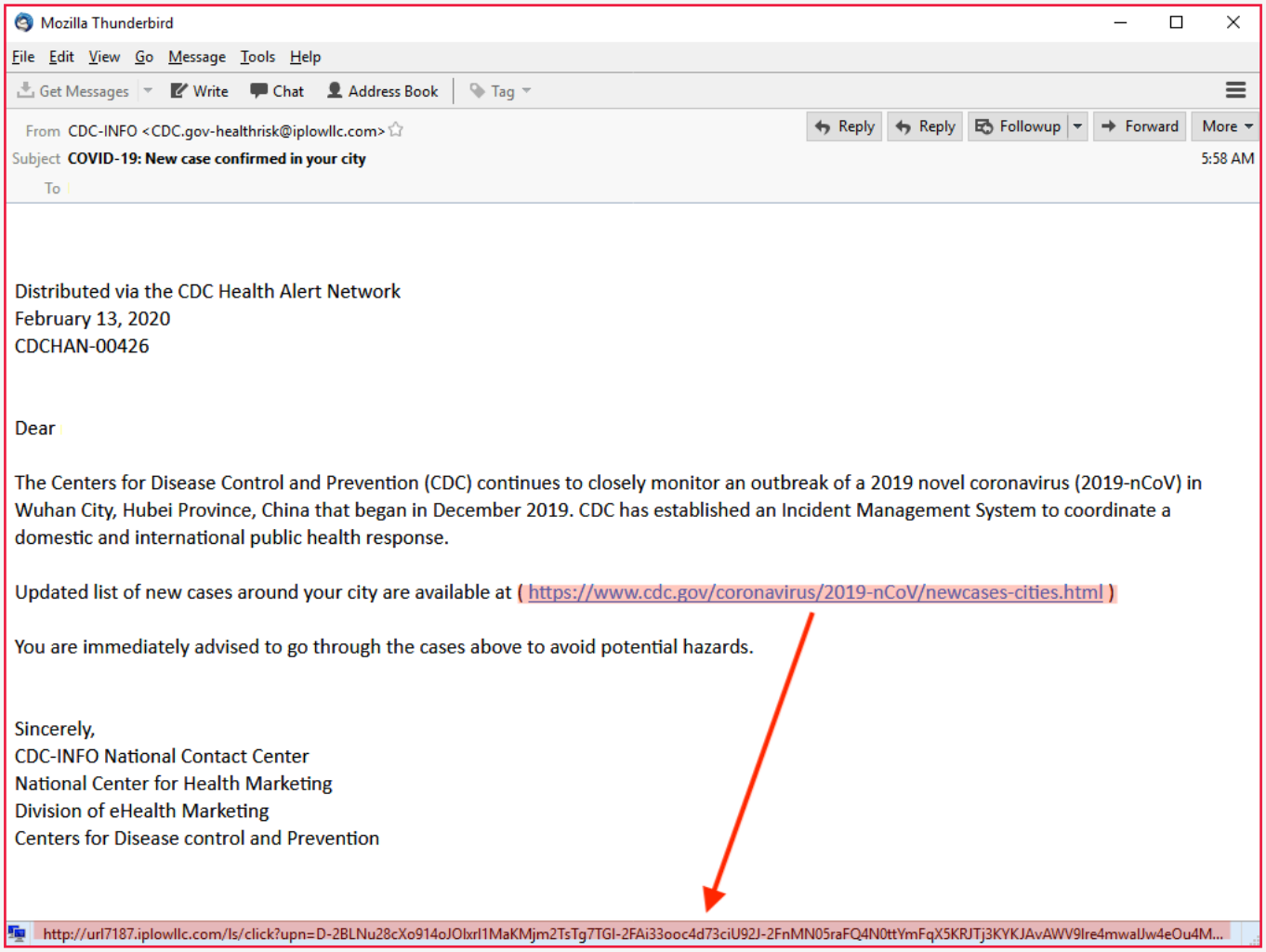
- Corporate email credential phishing campaigns around **Outlook and Microsoft 365**, with common themes such as requests to verify an account or email address, change a password, upgrade mailbox quota and storage, or listen to a missed voicemail message.
- Phishing sites hosted on **compromised websites**, to which the attacker has gained access through credential guessing or brute forcing, or by exploiting vulnerabilities in software such as WordPress.
- Phishers continued to use **free hosting** sites, such as 000webhost, Weebly and Blogspot, to host their landing pages.
- Phishers also use cloud-based **free disk space services** like Google Drive, OneDrive, Dropbox, Box, WeTransfer, and SharePoint URLs for hosting both phishing pages and malware. See "Phishing in the Cloud" below for more information.
- **Phishers abused legitimate mass-email marketing services like SendGrid** in 2020 to send out messages containing embedded SendGrid links that eventually redirect to phishing pages.
- Similarly, scammers also abused cloud services like **Microsoft SharePoint** and **Microsoft OneNote** to send out phishing messages that contained embedded Microsoft links pointing to a shared document, PDF, or note, which served as intermediaries for the final phishing page.
- Phishers used **URL shortener** services like bit.ly, bit.do, t.co (Twitter's internal link shortener) and tinyurl.com for links in their messages, presumably to conceal the true nature of the links. Clicking on these links redirects the victim to the final phishing page.
- Phishing emails containing **HTML attachments** disguised as invoices were prevalent in 2020. The attached HTML often contains obfuscated JavaScript that, on loading in a web browser, serves as a redirector leading the browser to the final phishing page.
- **PDF phishing documents** are still relatively common. Phishing URLs are hidden in PDFs instead of the email body. These PDFs incorporated blurred images with underlying URI (uniform resource identifier) actions. Clicking the image opens a browser and loads a URL of the attacker's choosing, leading to either a credential-stealing page or a malware download.

Phishing Trends and Developments

Some of the notable phishing campaigns and other developments we observed in 2020:

Phishing for COVID-19

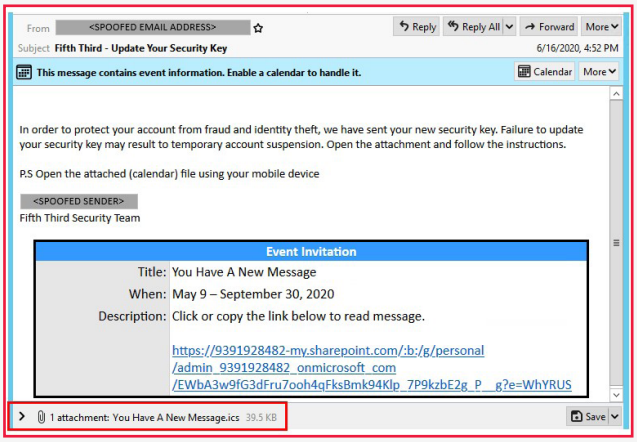
The COVID-19 pandemic has affected cybercrime along with the rest of the world. We observed multiple phishing campaigns that sought to exploit the pandemic with a variety of lures, using subject lines such as "Covid-19 employee relief fund," "Important Covid-19 guidelines for employees," "WHO Coronavirus Safety and Prevention guideline," and "Covid-19 Cure," and links and attachments purporting to be from health authorities such as the World Health Organization (WHO) or Centers for Disease Control and Prevention (CDC), but which actually led to phishing landing pages.



A phishing message masquerading as an official communication from the Centers for Disease Control and Prevention

Malicious Calendar Files

We also observed phishing campaigns using **ICS iCalendar** attachments in 2020. Attackers used these files, which contain calendar and scheduling information, to circulate Microsoft SharePoint phishing links as meeting invites.



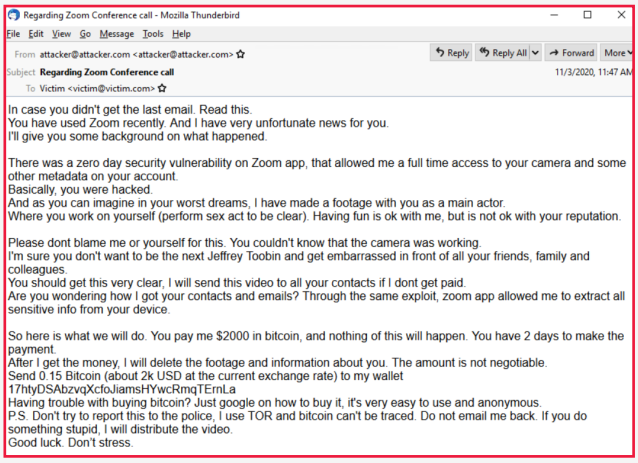
A phishing message with an iCalendar attachment containing a link to files hosted on Microsoft SharePoint

Extortion Spam

We observed a significant rise in extortion scams beginning towards the end of 2018 and continuing through 2019 and 2020. In these scams, the attacker sends messages to prospective victims falsely claiming that they have been hacked or infected with malware and that the criminal has obtained recordings of the victim performing sexual acts or evidence of illegal files or sexual content on the victim's computer. The scammers then threaten to expose the victim unless a ransom demand is paid in cryptocurrency within a given time to a provided crypto wallet address. Sometimes the criminal provides "proof" of the supposed hack by including passwords the victim has used, which are usually taken from publicly available password dumps obtained through unrelated data breaches.

The claims of hacking are false, of course, but some victims are persuaded to send money anyway. Analysis of some of the Bitcoin wallet addresses used in the scams confirms that enough people pay up to provide a regular stream of income for the scammers. Multiple botnet operators got into the extortion game in 2019 and 2020, including Pitou, Phorpiex, and others, at times pumping out huge volumes of these scams.

Several variants of the extortion scam have emerged over the last couple of years. In 2020 the scammers quickly adapted to the COVID-19 pandemic by claiming the victim was hacked during a recent Zoom videoconferencing session. We have observed variations of these messages written not only in English but in French, German, Italian, and other languages.



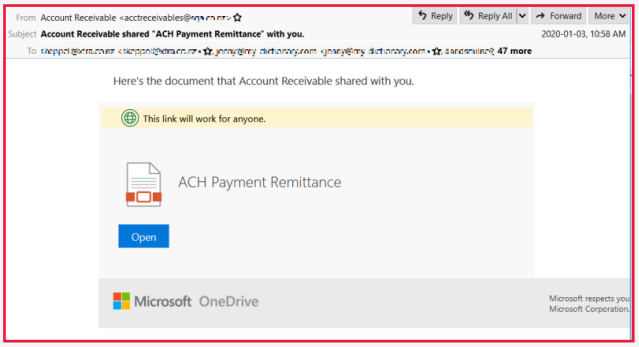
A typical Zoom-themed extortion scam email, with a Bitcoin wallet address provided for payment

Microsoft 365 Account Phishing

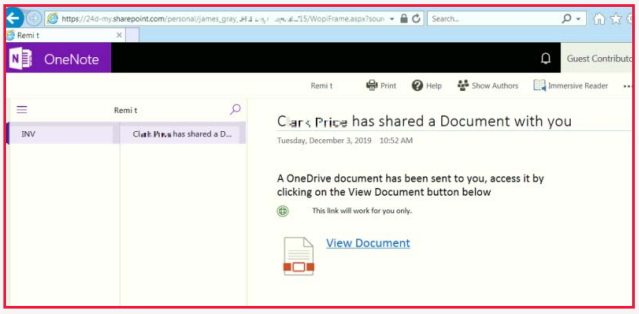
Credentials for Microsoft 365 email accounts are like gold for attackers, who use such compromised accounts differently. Email messages sent to the victim can be monitored for suitable content such as invoices about to be paid. The attacker can then insert themselves into the conversation and launch a BEC attack against the victim, who is particularly at risk in this scenario because they are already expecting such a message. Attackers can also use compromised accounts' good reputations to send further phishing or spam emails to the victim's contacts.

Phishing in the Cloud

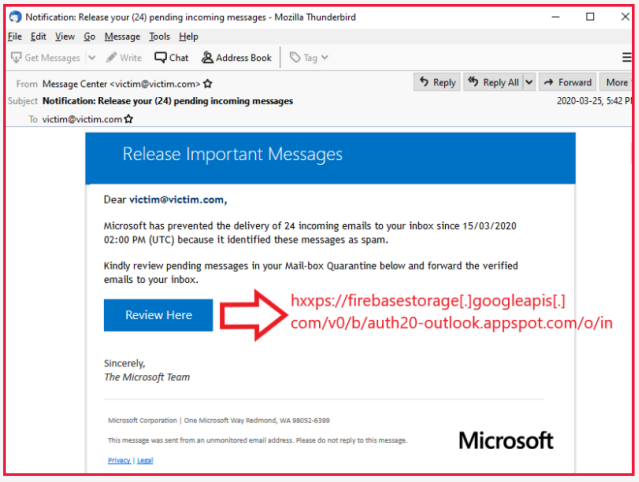
Phishers often abused cloud-based disk storage and office productivity services in 2020, including Google Firebase Storage, Google Drive, Microsoft OneDrive, Microsoft OneNote, Microsoft Sway, and Microsoft SharePoint. In some cases, the phishers used a cloud service to send the phishing message and host the phishing pages directly; in others, the cloud service was used as an intermediate stage in a multi-stage phishing chain. In the latter scenario, the intermediate stage hosts an innocuous-looking page with a link that redirects to another page located elsewhere, usually a compromised website. The phishers rely on the good URL reputation of the cloud services for the first stage of their attack.



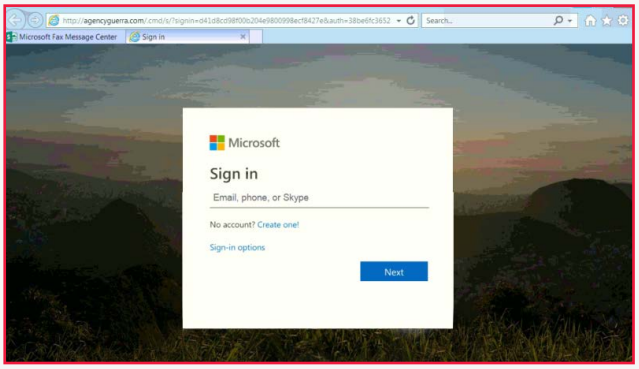
A phishing message sent through the Microsoft OneDrive cloud service



A first-stage phishing message hosted by Microsoft OneNote. The document can be clicked directly or downloaded



A phishing message claiming to originate from Microsoft. Clicking on the link takes the victim to a phishing page hosted at a Google Firebase Storage bucket



A forged Microsoft 365 credential phishing page serving as the second and final stage of a multi-staged phishing attack to harvest employee account credentials

To learn more about how phishers use cloud services in their attacks, see the following entries at the Trustwave SpiderLabs blog:

- Phishing in the Cloud
- Phishing in a Bucket: Utilizing Google Firebase Storage

Business Email Compromise

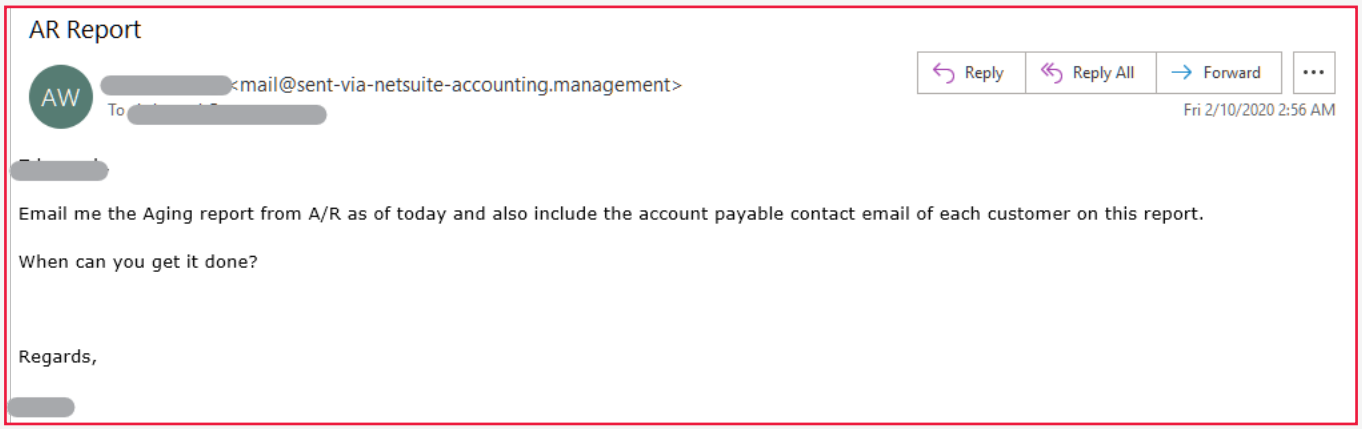
Business email compromise (BEC) is a targeted form of phishing that criminals use to steal large sums of money from companies. In a typical BEC scam, the target is a mid-level executive or financial officer with the authority to send money on behalf of a company. The scammer sends the target an email message purporting to be from the company's CEO or another important person, asking them to send a payment to a vendor or other party. In order to appear legitimate, the messages often forge the sender's address on the To: line and direct replies to a separate Reply-To: address. In 2020, Trustwave MailMarshal Cloud service intercepted around 40 BEC messages per day intended for customers.

According to the FBI, BEC is the most damaging type of cybercrime in terms of victim losses by a considerable margin, amounting to more than US $1 billion per year with an average of $75,000 per incident.

Learn more **here**.

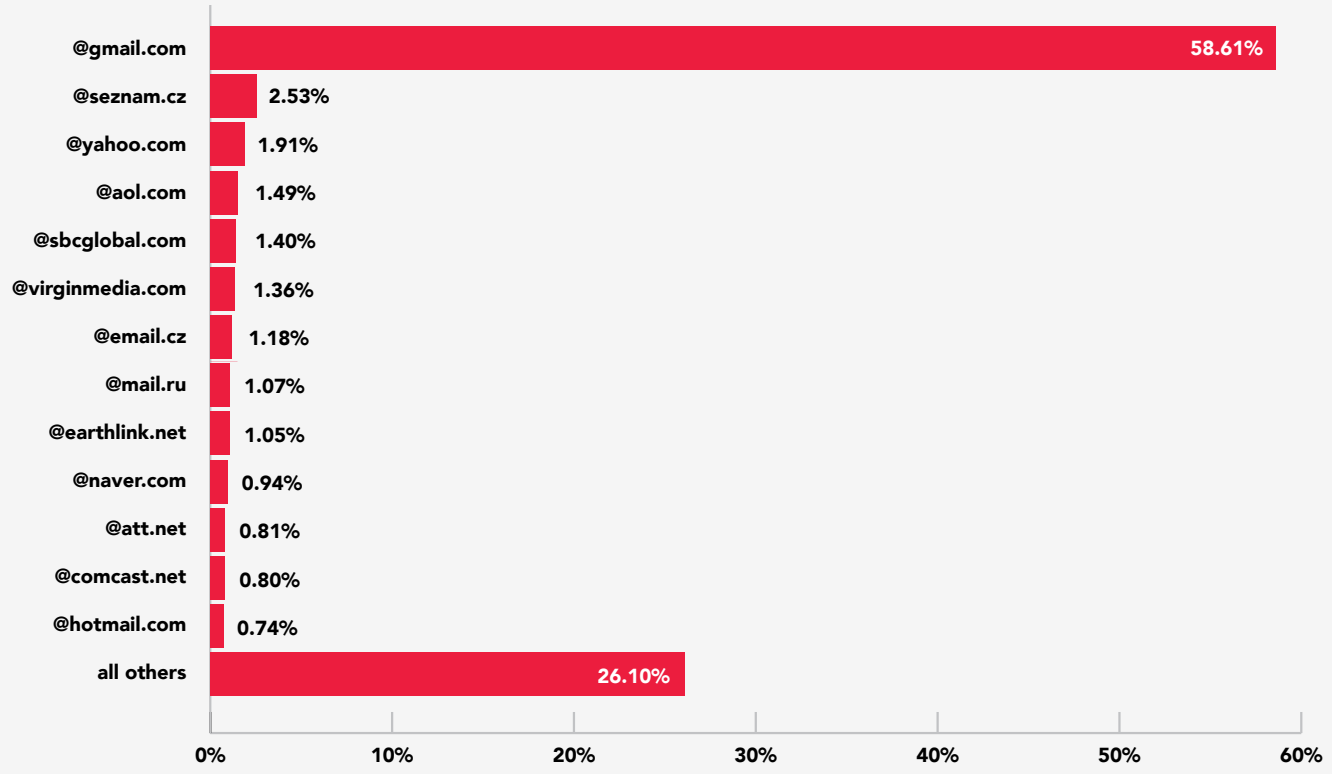
Some of the more common BEC approaches we see include the following:

BEC Type	Typical Subject Lines	Description
Vendor Payment or Invoice	• Urgent • Assistance needed • Are you at your desk? • Request • Available? • Invoice payment	Scammer impersonates the CEO or CFO and asks someone in Finance to urgently send a payment to a vendor or other party.
Gift Cards	• Need your help • Quick Task • Favor	Scammer impersonates the CEO, CFO or other manager and asks employee to purchase gift cards (iTunes for example), scratch them, take a photo and send back. Scammer then redeems the cards.
Payroll Change	• Payroll Update • DD Update • Direct Deposit Change • Change Bank Info	Scammer impersonates an employee and asks HR staff to change the bank account for salary deposits.
Phone Number	• Hello [person] • Quick Request	Scammer impersonates the CEO, CFO or other manager and asks employee for cell phone number, from where a text message conversation occurs.
Altered Invoice	• Varies according to actual email correspondence.	Scammer obtains access to real email accounts through credential phishing and monitors email looking for suitable invoices or transactions about to happen. Scammer then injects themselves in the middle of the email conversation and supplies an altered invoice, closely resembling the original, except for the bank account details.
Aging Report	• Aging report • A/R	Scammer asks for an aging report, which contains lists of customers with outstanding debts, and then targets those customers with new emails.
COVID-19	• Covid-19 • Covid-19 Support • Payment (Covid-19)	Scammer impersonates an executive and asks for funds relating to COVID-19 support. We detail examples in the Trustwave SpiderLabs blog.



Example aging report and COVID-19 BEC messages

This chart illustrates the most common domains used to send BEC messages in 2020:

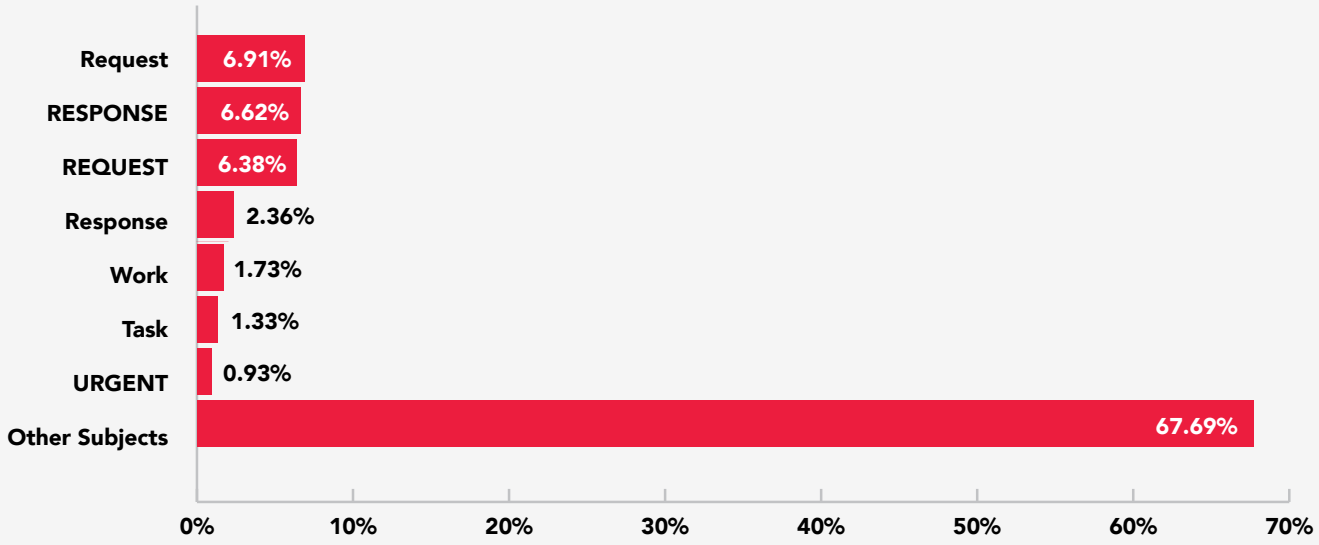


Most Common BEC From Address Domains

Gmail is a massively popular platform for sending BEC messages. More than 58 percent of BEC messages were sent with a gmail.com address in the From: field, with all others far behind.

BEC messages often share certain characteristics. Many are sent with single-word subject lines, such as the following (case sensitive):

Most Common Subjects in BEC Emails



Other characteristics we observed in BEC messages intercepted in 2020 include the following:

Characteristic	Percentage of messages
"I need you" in message	43%
"Sent by IPhone" in message	26%
Has Reply-To: address	25%
Upper case subject line	22%
"Are you available" in message	21%
Reply-To: address different than From: address	12%
Asks for favor	9%
Gift cards theme	8%

Defending the Email Attack Surface

To protect against the impact of email attacks, organizations should consider:

- **Deploying an email security gateway** - on-premises or in the cloud with multiple layers of technology, including anti-spam, anti-malware, and flexible policy-based content filtering capabilities.
- **Locking down inbound email traffic content as much as possible.** Carefully consider employing a strict inbound email policy:
  - Quarantine or flag all executable files, including Java, scripts such as **.js** and **.vbs**, and all unusual file attachments. Create exceptions or alternative mechanisms for handling legitimate inbound sources of these files.
  - **Blocking or flagging macros** in Microsoft documents.
  - Blocking or flagging **password-protected archive** files and blocking odd or unusual archive types, such as .ace, .img, .iso
- **Keeping client software** such as Microsoft 365 and Adobe Reader **fully patched** and promptly up to date. Many email attacks succeed because of unpatched client software.
- Ensuring potentially **malicious or phishing links in emails can be checked**, either with the email gateway or a web gateway, or both.
- Deploying **anti-spoofing** technologies on your domains at the email gateway and deploy techniques to detect **domain misspellings** to detect phishing and BEC attacks. Also, ensure there are robust processes in place for approving financial payments via email.
- **Educating users** – inform the rank and file up to the C-suite on the nature of today's email attacks. Conducting mock phishing exercises against your staff shows employees that phishing attacks are a real threat that they need to be wary of.

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries.
For more information about Trustwave, visit *www.trustwave.com.*

Trustwave®