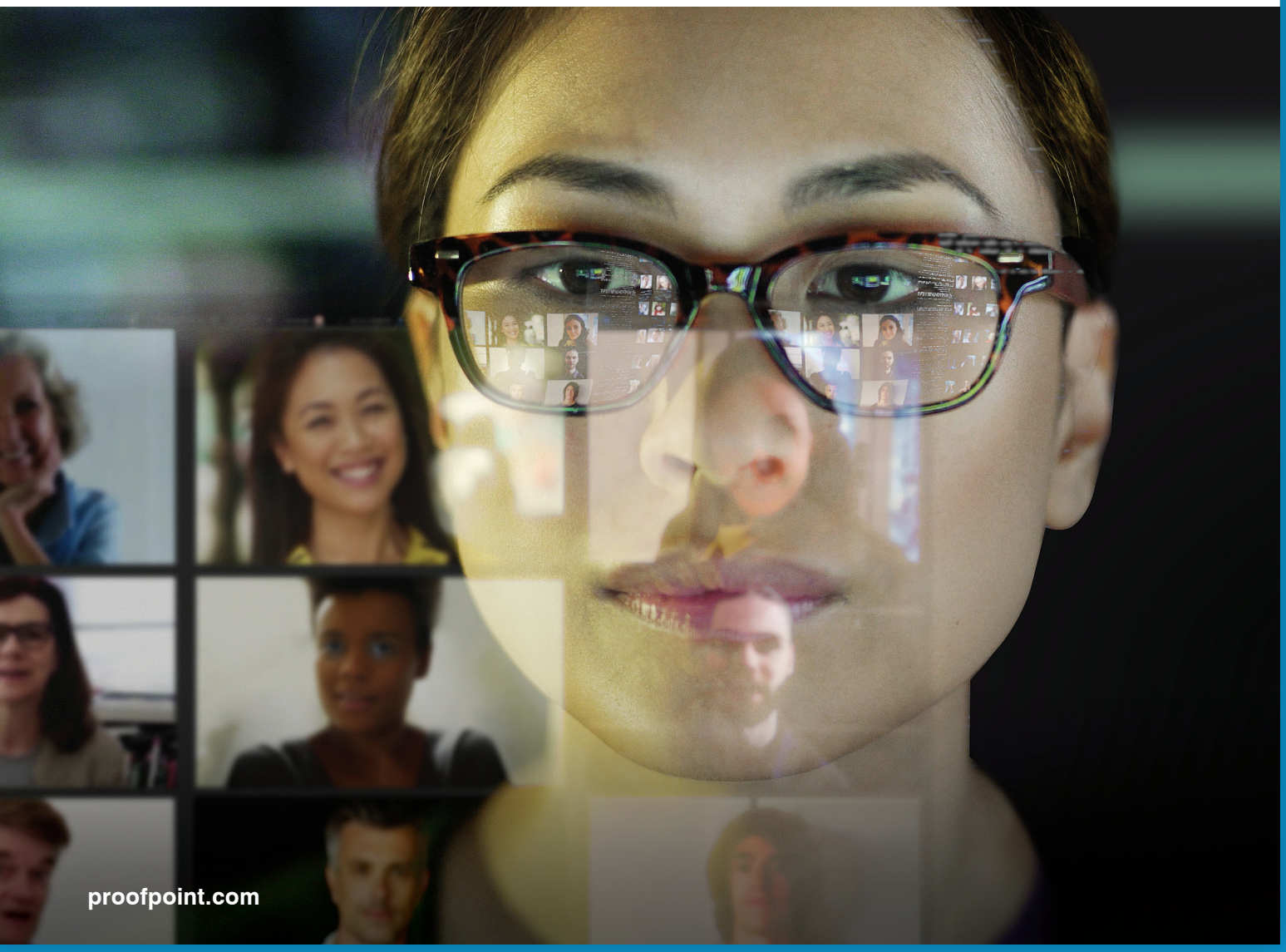
proofpoint.

REPORT

The Human Factor 2021

Cybersecurity, Ransomware and Email Fraud in a Year that Changed the World



proofpoint.com

Introduction

The tragedy, upheaval and historic changes of 2020 have been documented countless times over. But as organisations around the world take their first cautious steps to normal, "the year that wasn't"[1] still holds valuable lessons worth exploring. That's especially true in the realm of cybersecurity.

As the global pandemic upended work and home routines, cyber attackers pounced. They exploited suddenly unfamiliar work settings and people's fear, uncertainty and doubt to trick users and compromise organisations. And now in 2021 we're seeing what happens when emboldened cyber criminals press their advantage, as a rash of ransomware attacks target high-profile businesses and infrastructure.

People are returning to offices, factories, shops and show floors. But some pandemic-era trends may be here to stay. Many workers will enter hybrid arrangements, splitting their time between their homes and communal workspaces. Distributed teams will collaborate across geographies and legal jurisdictions. Shifts in ecommerce, the cloud and other areas, well under way before the pandemic, have only accelerated.

No matter what the post-COVID world looks like, protecting people—wherever and however they work—will be an ongoing challenge.

About this report

From its inception in 2014, The Human Factor report was founded on the simple premise that people—not technology— are the most critical variable in today's cyber threats.

Since then, this once-contrarian notion has become a widely acknowledged reality. Cyber attackers target people. They exploit people. Ultimately, they *are* people.

To effectively prevent, detect and respond to today's threats and compliance risks, information security professionals must understand the people-centric dimensions of user risk: vulnerability, attack and privilege. In practical terms, this means knowing:

- Where users are most vulnerable
- How attackers are targeting them
- The potential harm when privileged access to data, systems and other resources is compromised

Addressing those elements—the *human factor* of cybersecurity—are the core pillars of a modern defence.

What this report covers

This report dives deep into each of three facets of user risk. It explores how the extraordinary events of 2020, and the historic shift they sparked, has transformed the threat landscape. It examines the shifting threat ecosystem and what it means for the rest of us. And it explains how a people-centric defence can make users more resilient, mitigate attacks and manage privilege.

This report covers threats detected, mitigated and resolved during 2020 among Proofpoint deployments around the world, one of the largest, most diverse data sets in cybersecurity.

We largely focus on threats that are part of a broader attack campaign, or series of actions taken by an attacker to accomplish a goal. Sometimes, we can link these campaigns to a specific threat actor, a process known as attribution. But for reasons explained in **"The art and science of attribution" on page 27**, this is not always possible.

Scope

The data in this report draws from the Proofpoint Nexus Threat Graph using data collected from Proofpoint deployments around the globe. Every day, we analyse more than 2.2 billion email messages, 35 billion URLs, 200 million attachments 35 million cloud accounts and more—trillions of data points in all across all the digital channels that matter.

This report covers Jan. 1–Dec. 31, 2020. Except where noted, it includes threats observed directly by our global network of threat researchers and tied to an attack campaign, which we define as series of actions taken by an attacker to accomplish a goal.

For Section 3: Privilege, 300 customers shared their Insider Threat Management alerts, which indicates what forms of privilege abuse they were most concerned about. We compared alerts set February 2020 through January 2021, the height of the pandemic, with those set October 2019 through January 2020.

[1] *The Economist*. "2020: The year that wasn't." November 2020.

Table of Contents

Key Findings **4**

1 **Vulnerabilities** **6**

Putting users to the test: phishing simulation failure rates 9

Industry Failure Rates 10

2 **Attacks.** **11**

Ransomware on the rise 11

Battleground states:
US election related attacks 13

COVID-19: How attackers piggybacked the pandemic 15

Attack types 21

Attack techniques 22

Attack tools 24

3 **Privilege** **30**

Conclusion And Recommendations **31**

Key Findings

Here are some of the major findings in this year's report.

More than **48M messages contained malware** capable of being **used as an entry point for ransomware attacks**.

With the world absorbed in COVID-19 news, attackers capitalised on the situation. **Pandemic-related lures appeared more than those tied to any other current event or news item.** Almost every threat actor we track used pandemic related content at some point in 2020.

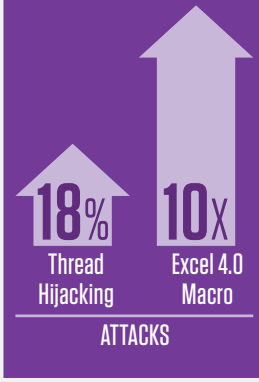
Nearly **10% of campaign-related malicious email** attempted to distribute Emotet malware. Before being shut down in a January 2021 law enforcement sweep, Emotet's infrastructure was offered for hire to other groups, which used it to distribute ransomware and other types of malware.

~10%

Nearly **25% of all attack campaigns** hid malware in compressed executable files, which run only after the recipient interacts with it.

25%

Credential phishing, both consumer and corporate, was by far the most common form of attack, accounting for nearly two-thirds of all malicious messages, outpacing all other attacks combined. Credential phishing leads to account compromise, which can be leveraged in other attacks, including data theft and business email compromise (BEC).



Techniques that require the recipient to interact with an attachment or directly with the attacks rosesubstantially. **Thread hijacking attacks increased 18%** from the year before. Those that used password-protected files jumped nearly fivefold. And the volume of **Excel 4.0 macro attacks swelled more than 10 times**.

More than 1 in 3 people targeted in attack campaigns that use steganography clicked the malicious email, the highest hit rate of any attack technique.

>50X Attacks that use CAPTCHA techniques captured **more than 50 times the number of clicks** as they did the year before.

Attack campaigns launched by threat actor TA542 (the threat actor linked to the Emotet botnet) persuaded the **highest number of users to click**. This total reflects their effectiveness and the sheer volume of emails they sent in each campaign.

With users suddenly shuttered to their homes and remote work the new normal, **organisations' views of privilege-based risks shifted**.

The number of organisations setting DLP alerts for these activities jumped significantly from pre-pandemic levels for these activities:

- Using USB devices
- Large file and folder copying (especially during odd hours)
- Assessing file-sharing services
- Activities that might circumvent user-monitoring tool

TOP 5 DLP and Insider Threat Controls set by customers, overall, were:

1. Connecting an unsanctioned USB device
2. Copying folders or large files
3. Uploading a sensitive file to the web
4. Opening a text file that may contain passwords
5. Downloading a file with a potentially harmful extension

How This Report Is Structured

In cybersecurity, risk is defined as: *threats* x *vulnerability* x *impact* +/- *security controls*

This report focuses on each of these facets through the lens of our people-centric model of user risk—vulnerability, attacks (threats) and privilege (impact)—with recommendations on ways you can mitigate each.

Just as people are unique, so is their value to cyber attackers– and risk to employers.

They have distinct **vulnerabilities**, digital habits and weak spots. They're **attacked** in diverse ways and with varying frequency. And they have different levels of access **privileges** to data, systems and resources.

These intertwined factors determine a user's overall risk.

Vulnerability

Users' vulnerability starts with their digital behaviour—how they work and what they click.

Many employees work remotely or access company email through their personal devices. They may use cloud-based file storage and install third-party add-ons to their cloud apps. Or they may be especially receptive to attackers' email phishing tactics.

Attacks

All cyber attacks are not created equal. While every one is potentially harmful, some are more dangerous, targeted or sophisticated than others.

Indiscriminate "commodity" threats might be more numerous than more advanced ones but they're usually well understood and more easily blocked. (Make no mistake, though. They can cause just as much damage.)

Other threats might appear in only a handful of attacks. But they can pose a more serious danger because of their sophistication or the people they target.

Privilege

Privilege measures all the potentially valuable things people have access to, such as data, financial authority, key relationships and more. Measuring this aspect of risk is crucial because it reflects the potential payoff for attackers—and harm to organisations if compromised.

The user's position in the org chart is naturally a factor in scoring privilege. But it's not the only factor—and often, not even the most important one. For attackers, a valuable target can be anyone who serves as a means to their end.

When risk factors collide

Elevated risk levels in any of these three categories is cause for concern and, in most cases, additional layers of security. When two or more are elevated, it's a signal of a more urgent security issue.

Here are four categories of users that highlight how combinations of vulnerability, attacks and privilege affect your overall risk:

- **Latent targets:** High-privilege users who are also more vulnerable to phishing lures are breaches waiting to happen. A high-privilege user doesn't always have a high-profile job. Even junior human resources, facilities and administrative employees can have a dangerous level of access in the wrong hands. They may not be on attackers' radar now, but they're ripe for the picking.
- **Soft targets:** Highly attacked users who are vulnerable to threats represent easy wins for the attacker. Fast response and remediation can contain the damage for low-privilege users. But a successful attack may give the threat actor a foothold to move on to users with access to more valuable data, systems and resources.
- **Major targets:** The risk posed by high-privilege, highly targeted users can be mitigated by reducing their vulnerability with security awareness training and good digital hygiene. People in this category will face countless attacks—and only one has to succeed to cause lasting harm to the organisation.
- **Imminent targets:** Users with high levels of all three risk factors are immediate and critical risks. They should be treated as an urgent security priority.

SECTION 1

Vulnerabilities

STEGANOGRAPHY
Attackers use this technique to hide the malicious payload into a seemingly innocuous file such as photos and audio. Typically, the payload is encoded into otherwise unused bits of data that users don't see and that are hard to detect with file- and sandbox-based tools. After landing on victims' machines, the hidden data is decoded and activated.

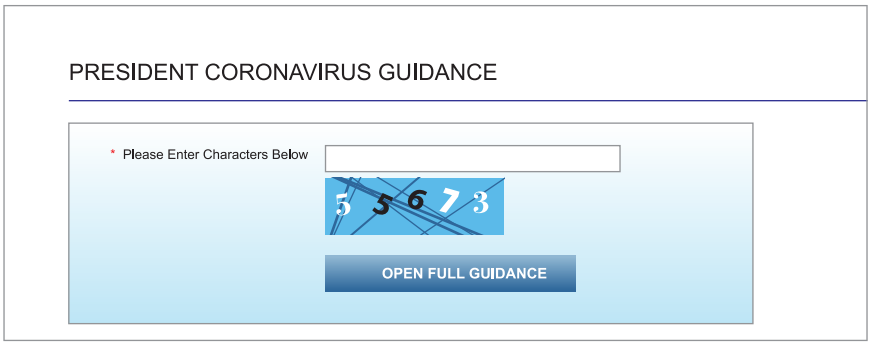
CAPTCHA
Most of the time, CAPTCHA techniques are used as an antifraud measure. By asking the user to perform a task that is easy for people but hard for machines, the technique helps ensure that an actual person—rather than an automated bot—is accessing a website. Cyber attackers use it in a similar, albeit more sinister way. By using a CAPTCHA challenge, they ensure that their malware is on the system of a real user—and not a security sandbox that could observe its malicious activity. The technique can also be used to determine where the user is from (based on the IP address) for attacks that target people in a given country or region.

Another way of thinking about vulnerabilities is asking "if my users are targeted in a cyber attack, how likely are they to become a victim?"

Some of the most successful attack techniques in 2020 were also the most targeted, used in campaigns that sometimes comprised only a handful of emails.

STEGANOGRAPHY, or hiding malicious code in pictures and other files types, appeared in just a few targeted campaigns. But the technique proved highly effective, getting three out of every eight recipients to click.* That's a response rate any attacker—let alone any email marketer—would envy.

CAPTCHA techniques, which use visual puzzles to tell human from machine, garnered more than 50 times the number of clicks vs. the year-ago period. While the overall response rate was a more modest 5%—which still would be deemed a resounding success in most email marketing campaigns—many more users succumbed to this technique than in 2019.



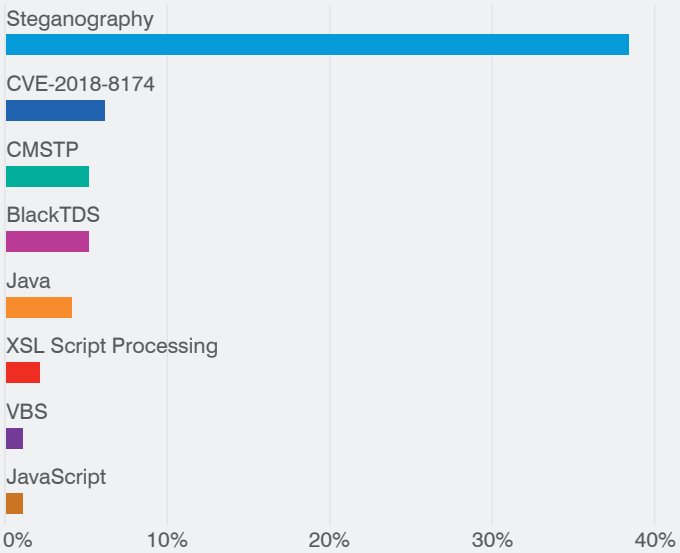
Screen capture of a CAPTCHA challenge from a COVID-themed attack in May.

It's not clear why users were more vulnerable to either technique. Remote workers may have been more distracted and cognitively taxed under the stresses of 2020. Perhaps some were even primed by new remote-work controls to see the CAPTCHA question as a normal security challenge.

* Within attributed campaigns.

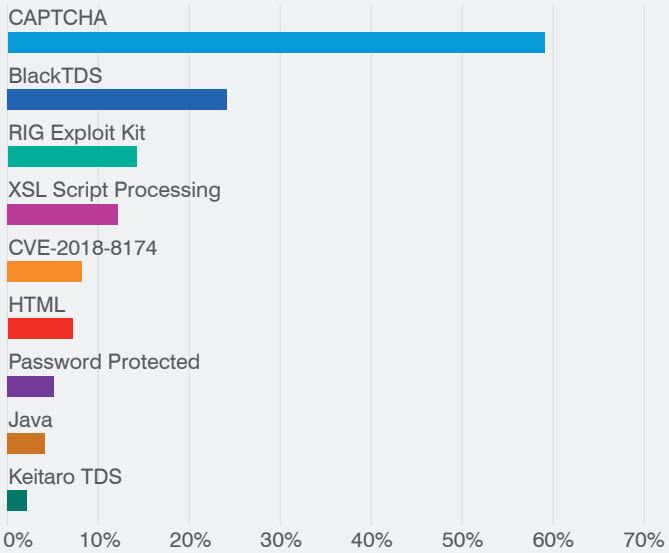
Techniques with Highest Clicks per Message*

Steganography proved highly effective in the few targeted campaigns that used the technique. Attacks that exploited Windows' CVE-2018-8174 vulnerability were also effective and used in larger, more frequent campaigns.



Year-to-year Change (Average Clicks 2020 vs. 2019)*

CAPTCHA techniques, which evade security tools by requiring human interaction, generated more than 50 times the number of clicks in 2020 vs the year before. It was used in several dozen large-scale campaigns.



TA542

Before its takedown in January 2021, TA542 had become one of the most prolific attackers in recent years due to massive campaigns that use a malware strain called Emotet. The group has targeted multiple industries around the world, sending hundreds of thousands—or even millions—of messages per day.

Emotet doesn't just compromise the systems they infected. It also uses these compromised machines to launch new attacks, absorbing them to a zombie-like network of more than a million similarly infected machines known as a botnet. Other cyber criminals used TA542's botnet infrastructure for all kinds of attacks.

TA576

This threat actor mostly sticks to tax-themed attacks. While it launched just two campaigns in 2020, both were massive.

TA407

Also known as Silent Librarian, Cobalt Dickens, and Mabna Institute, this threat actor operates within Iran. It has targeted universities throughout North America and Europe seeking intellectual property. In 2018, US authorities indicted nine alleged members of the group for stealing data valued at $3.4 billion USD.

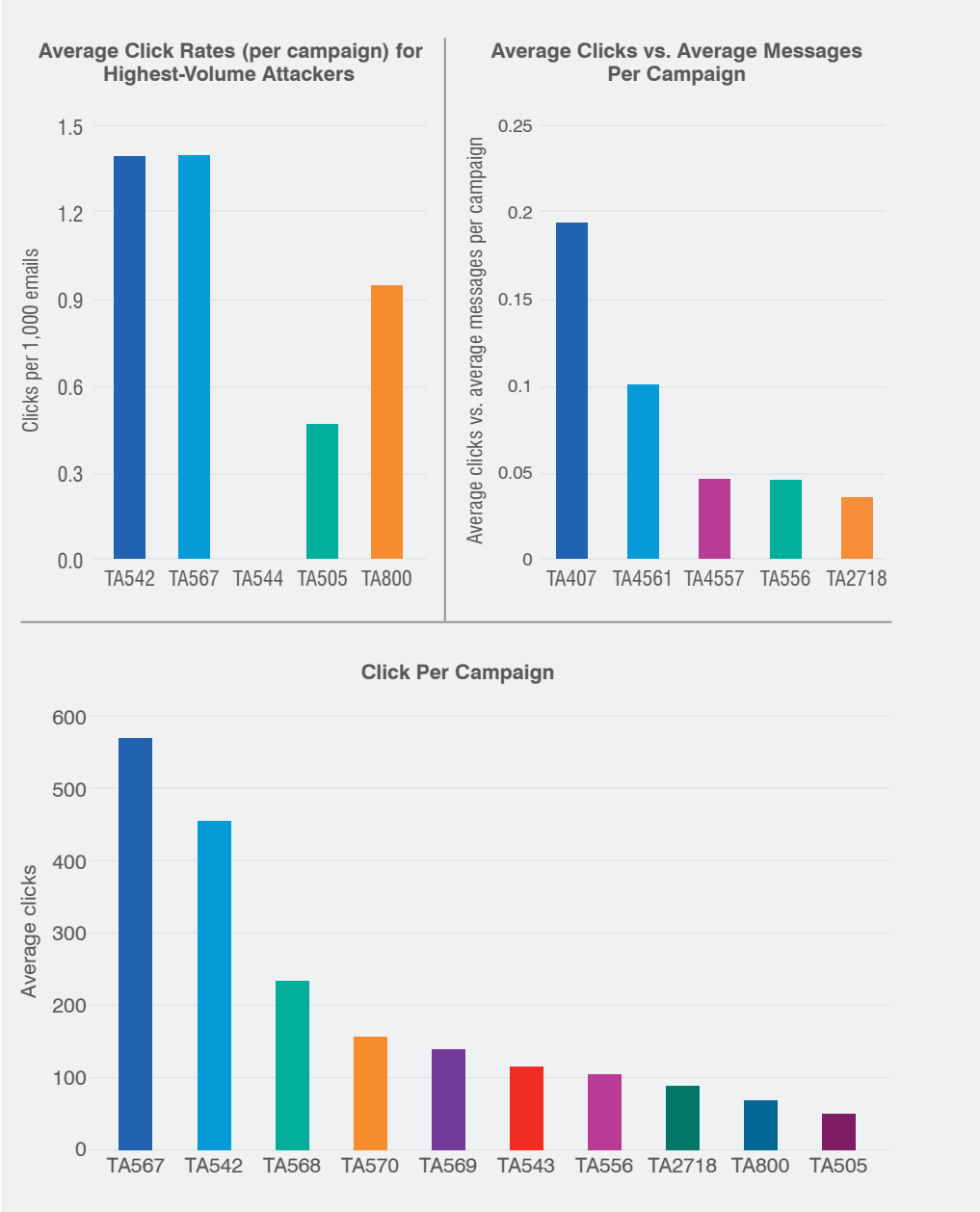
In any case, threat actors were quick to take advantage of vulnerable users.

An attacker we have dubbed **TA542**, 2020's highest-volume threat actor overall, yielded 454 clicks per attack campaign with a hit rate of about one-tenth of 1%. What it lacked in efficacy it made up in sheer volume. (More on this notorious threat actor in **Section 2: Attacks**.) **TA576**, another high-volume attacker, picked up 568 clicks per campaign with a similar hit rate.

Some of the most "effective" attackers—those with the highest hit rates—were among the smallest terms of message volume.

For example, an attacker we have tagged **TA407** averaged one click in about every five emails it sent in 2020, one of the highest success rates of any of those we monitor. The threat actor was highly selective, sending out just a few dozen emails in fewer than 100 campaigns in all of 2020.

The group is known for its advanced social engineering techniques. For example, its email campaigns use university branding, professional-looking websites and normal school activities (such as library renewals) to trick victims into providing account credentials.



Putting users to the test: phishing simulation failure rates

Another way of gauging vulnerability is simulated phishing exercises. These mock attacks can reveal what lures and tactics people are most likely to fall for in real-world settings and normal working conditions.

Our annual **State of the Phish report** analysed how users responded to more than 60 million simulated phishing emails over a 12-month period in 2020. By comparing the average failure rates—the percentage of users who took the bait—it shows how and where users might be more vulnerable.

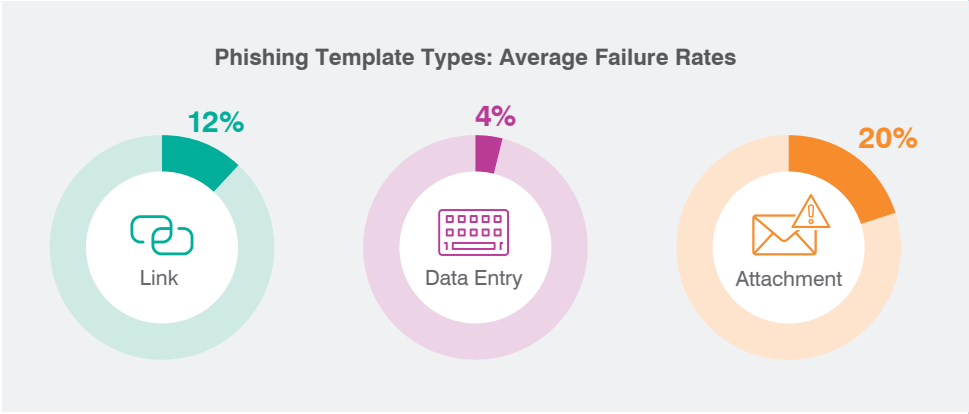
Here are a few highlights:

Failure rates by template type

Each "phishing" email is built on a template that lets the organisation mimic a wide range of attack styles, themes and lures. While the templates are as varied as real-world threats, they fall into three main categories:

- Link-based (those that include an unsafe URL that leads to malware and harmful websites)
- Data entry-based (those that take the user to a fake login page to steal credentials and other personal data)
- Attachment-based (those that include a malicious file)

An average[2] of 1 in 5 users clicked attachment-based emails. That's the highest of the three template types, a failure rate that exceeds the other two types combined.



2 To avoid weighing larger organisations too heavily, we averaged scores by customer rather than individual users.

Industry Failure Rates

Most vulnerable industries

Failure rates in simulated phishing attacks suggests that users in some sectors are more vulnerable than those in others.

Users in engineering, telecom, mining, education companies, for instance, were more likely to click. At the other end of the spectrum, those in hospitality/ leisure and entertainment/media were least likely.

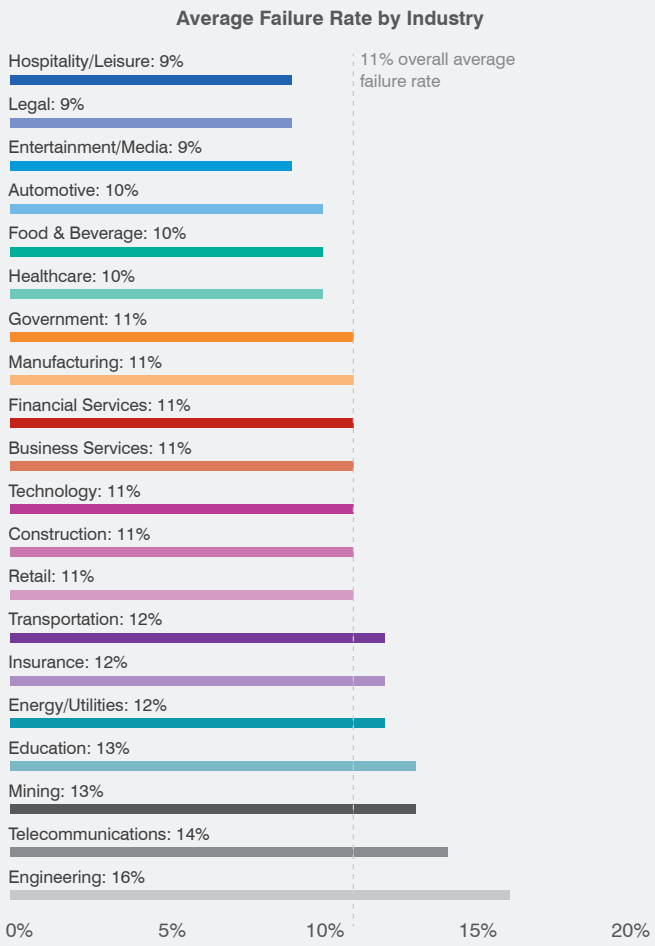
(Note: Industries in this chart include data from at least 15 organisations and at least 150,000 simulated attacks.)

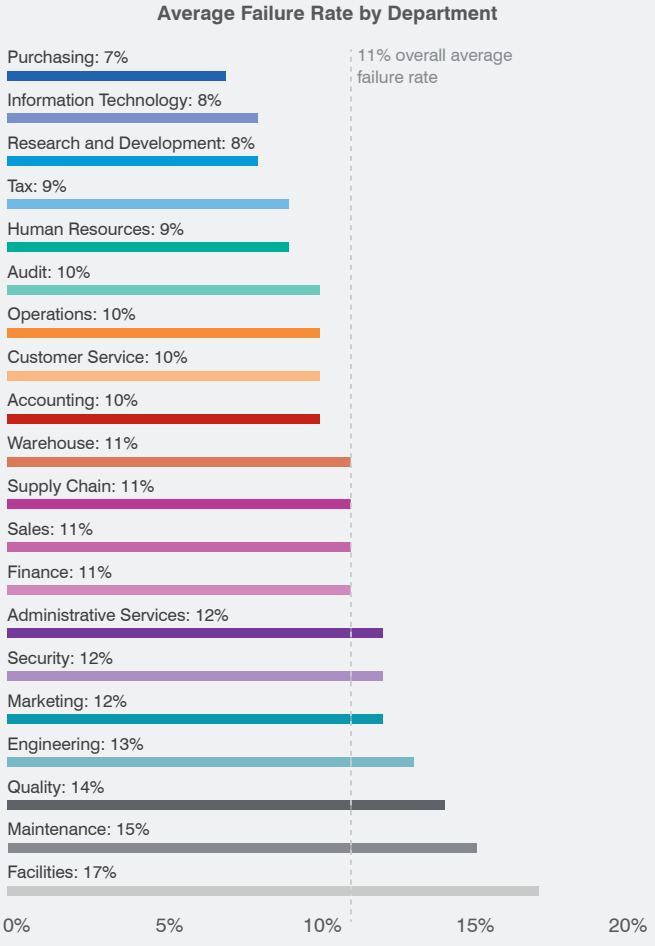
Most vulnerable departments

But industry-level failure rates alone will not show which roles and teams may be struggling. Attackers often target specific inboxes and email aliases. Department-level failure rates offer a finer-tuned view of potential weak spots.

Purchasing, IT, research and development, tax, HR and audit were among the least likely department to fall for simulated phishing emails. Facilities, maintenance, quality and engineering were among the most likely.

(Note: Industries in this chart include data from at least 15 organisations and at least 150,000 simulated attacks.)





SECTION 2

Attacks

Ransomware on the rise

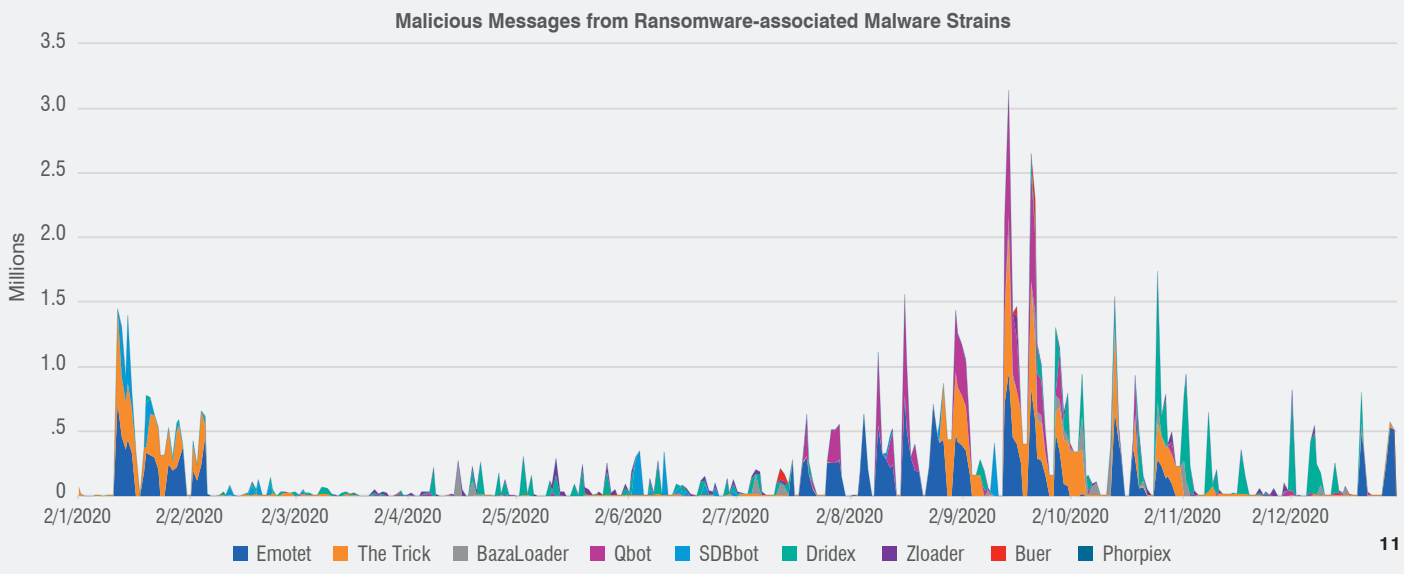
RANSOMWARE
This type of malware locks away victims' data by encrypting it, then demands a "ransom" to unlock it with a decryption key.

According to U.S. government figures[3], **RANSOMWARE** attacks increased by 300% last year. In the first half of 2021, the problem has reached even greater prominence with attacks on Colonial Pipeline, JBS Foods and Ireland's Health Service Executive showing that ransomware gangs can do real harm to critical infrastructure around the world.

Ransomware attackers still use email, but things have changed since 2016 when Locky appeared in millions of inboxes. Rather than being sent as a primary payload in malicious email campaigns, ransomware is now more likely to be downloaded by malware already present on a system or delivered through compromised remote desktop protocol (RDP) and virtual private network (VPN) access. However, email remains a crucial part of these attacks, as it is the route through which much of the first-stage malware used to download ransomware is distributed.

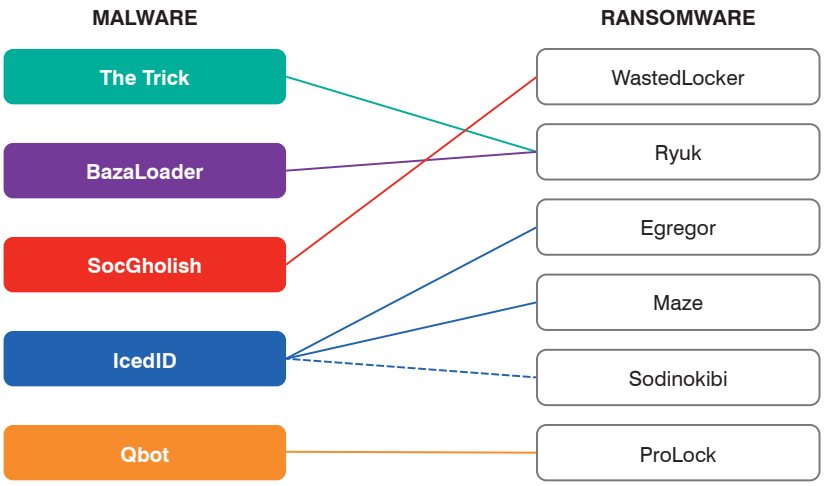
The cyber criminals in charge of these loaders and trojans then act as access brokers or facilitators, allowing ransomware groups to use backdoors into infected systems in return for a share of the profits. Rather than seeking wide distribution and small payouts, ransomware attackers now typically engage in "big game hunting"—targeting larger organisations with more to lose and more incentive to pay.

3 James Rundle and David Uberti (*Wall Street Journal*). "How Can Companies Cope with Ransomware?" May, 2021.



Because of this change in strategy, we don't see a lot of ransomware appearing in our email gateway, with a single strain called Avaddon accounting for 95% of all first stage ransomware payloads in 2020. However, several common first stage payloads, such as The Trick, Dridex and Qbot have been observed acting as entry points for later ransomware infection—and all three are among the highest volume threats seen in our data. In total, we saw more than 48 million messages containing malware capable of subsequently downloading ransomware or other secondary payloads in 2020.

There isn't a simple 1:1 relationship between the initial access malware and the eventual strain of ransomware. But our own observations and those of other researchers[4] suggest some prominent associations.



A sampling of initial access payloads threat actors delivered, and the associated ransomware deployed because of the initial access.

While the network of relationships between cyber criminal syndicates is complex, the sequence of events in a typical email-instigated ransomware attack is not: initial infection by a banking trojan or loader leaves you vulnerable to ransomware gangs prospecting for high-value targets. This means that for most businesses, the first line of defence against ransomware is ensuring protection from initial infection.

In other words, block the loader and you block the ransomware.

4 Clifford Krauss (*The New York Times*). "How the Colonial Pipeline Became a Vital Artery for Fuel." May 2021.

Although threat actors did not use election-themed lures until the election was in full swing in the fall of 2020, they attacked organisations linked to the elections throughout the year.

Battleground states: US election related attacks

Most security researchers anticipated that the 2020 US election would be an opportunity for cyber attackers. Some would seek to sow disinformation while others would use the election as social engineering fodder in email threats.

And that's exactly what happened. Although threat actors did not use election-themed lures until the election was in full swing in the fall of 2020, they attacked organisations linked to the elections throughout the year.

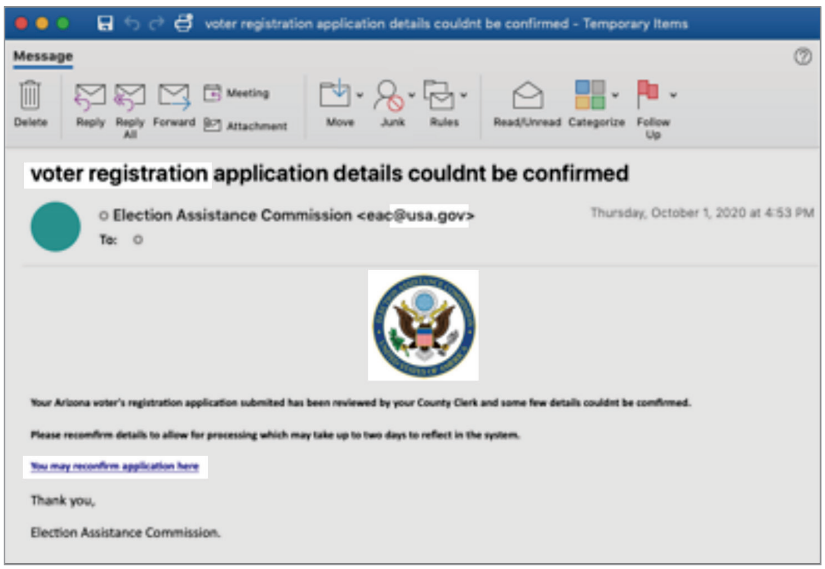
Financially motivated cyber criminals and state-sponsored threat actors targeted organisations both directly and peripherally linked to elections. That included every level of government and politics: from local, state and federal government entities to political action committees (PACs).

Political and election themed lures targeted numerous industries across the US Election-themed attacks spiked in October 2020 and dropped off after the election on November 3. Themes included:

- The health of then-president Donald Trump
- Democratic National Committee (DNC)
- The US Election Assistance Commission
- Voter registration

NOTABLE FEATURES:

- Piggybacks topic that often evokes strong feelings
- Spoofs Election Assistance Commission email domain
- Uses US Presidential Seal for a veneer of authority
- Includes malicious URL disguised as a registration website



Email lure impersonating the Election Assistance Commission.

THREAD HIJACKING
After taking over someone's email account, an attacker has free rein over the victim's inbox. With that control, the attacker can reply to past and ongoing email threads with a malicious email. Because the recipients know and trust the sender—and better yet, actively engaged with that person—this technique can be highly effective.

Some malware strains can now automate thread hijacking for social engineering at scale.

EMOTET
Prior to the 2021 takedown of its infrastructure, Emotet was the world's most frequently distributed malware. They were among the first groups to pivot from primarily stealing banking credentials to serving as an access broker for other criminal elements, including those distributing Dridex and Qbot.

URSNIF
Ursnif is a widely used banking Trojan that evolved from a malware strain called Gozi, whose source code leaked in 2015. Ursnif is the most popular of several Gozi-derived variants, which include Dreambot, ISFB and Papras.

Pulling on an email thread

One campaign targeted officials responsible for administering elections and planning election infrastructure. The attackers used a method called **THREAD HIJACKING**.

Some malware campaigns— such as **EMOTET** and some **URSNIF** attacks— automatically insert themselves into ongoing email threads. Here's how the technique works:

1. The malware scans emails in a compromised inbox.
2. When "re:" is identified in a subject, it creates a message to send to others in the email thread, appearing to be from the compromised user in the thread.
3. Because the email appears to be from someone the other participants trust— and indeed, and activity engaging with—recipients are more likely to fall for it.

Not-so-proud boys

One unusual election-focused email threat campaign posed as the violent, right-wing hate group the Proud Boys targeting Democratic-registered voters in Florida.

Messages with the subject line "Vote for Trump or else!" threatened violence if the recipient didn't comply. It contained a link to a Proud Boys-branded video of someone supposedly filling out voter registration and absentee ballots for Alaskan citizens. This campaign starkly contrasted typical election-related cyber threat activity with blatant threats and a call to take a physical action.

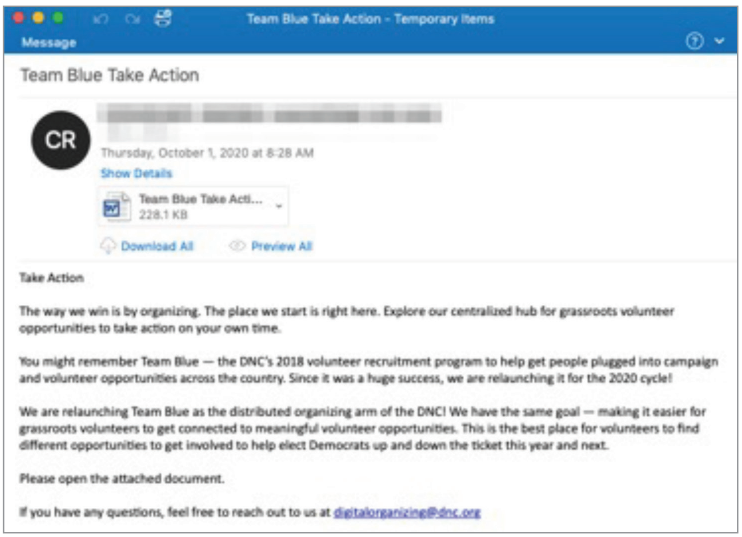
While Proud Boys members are known for violent attacks against the left, authorities and security firms say the emails were actually from state-sponsored attackers in Iran.

Emotet gets in on election fever

Emotet—the highest volume threat of the year—also used lures related to the election beginning in October 2020. TA542, the threat actor behind Emotet, launched election-related activities include:

- **Masquerading** as the DNC
- Encouraging recipients to volunteer
- Supporting political organising

(For more on Emotet, see **"Who's who in the threat landscape: top threat actors" on page 27**)



An Emotet attack piggybacking the election.

Emotet did not target specific people or organisations involved in the electoral process. Instead, it used interest in the elections and related events to create lures to appeal to broad audiences across multiple sectors.

COVID-19: How attackers piggybacked the pandemic

For most people, COVID-19 upended work and home routines. In this new and strange environment, knowing how users are being attacked—and if possible, who's behind the attack—are critical pieces of the cybersecurity puzzle.

Threat actors use current events in email lures all the time. But 2020 may be the first case of attackers all converging on the same themes at the same time. With the world's attention rapt in pandemic-related news, the entirety of the cyber threat ecosystem pivoted to the same thematic content in lockstep.

From spammers to **COMMODITY MALWARE** users to large-scale cyber criminals to **ADVANCED PERSISTENT THREATS** (APTs), just about everyone transitioned to COVID-19 as their social engineering content of choice. We saw nearly 250 million targeted messages associated with COVID-19—and billions more from wider attacks and spam.

COMMODITY MALWARE
Commodity malware refers to common, publicly available tools used by a wide range of attackers. While commodity malware should be known and easily blocked by security tools, attackers often use them in clever ways and high volumes—and they can be just as damaging as more advanced and targeted threats.

ADVANCED PERSISTENT THREATS
APT attackers typically engage in espionage on behalf of a government, though the category may also include advanced cyber criminals. Attacks may involve intellectual property theft, financial theft and attacks designed to disrupt or damage data and systems.

Co-Opting a Health Crisis

The COVID-19 pandemic was a good example of how cyber attackers adjust tactics in real time to cash in on victims' fear, uncertainty and doubt. Here's a timeline of major milestones in the global health crises and how threat actors responded.

Notable Attacks

January 19

Attacks targeting users in Japan use COVID-19 lures to trick recipients into opening infected Microsoft Word documents. The emails are part of a larger campaign distributing the Emotet malware strain.

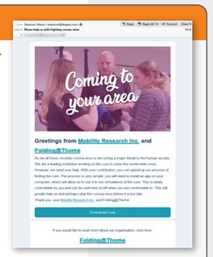
February 10

COVID-19-themed email lure sent to targets in Japan.

Emails sent to recipients in hard-hit Italy promise updates on the pandemic. The emails include a Microsoft Word attachment containing a URL that leads to a phishing page that steals credentials.

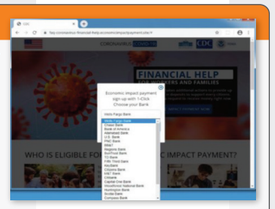
March 7

People in the US are targeted by emails purportedly from "Mobility Research Inc" that ask recipients to help find a coronavirus cure by participating in a Folding@Thome. The pitch mimics the legitimate Folding@home project, which uses spare computing cycles on user's computers for medical research. But instead of aiding COVID-19 research with the real Folding@Home app, recipients who click the URL get RedLine malware, which steals credentials and downloads other malware.



April

US residents are targeted with phishing emails, ostensibly from the "Federal Reserve System," linking to an official-looking website that asks recipients to enter their banking credentials receive their stimulus payments. The site was set up to steal credentials from most major US banks.



January 19, 2021

Emails targeting people in the US and Canada promise recipients doses of the Pfizer-BioNTech vaccine. When recipients click the URL, they are taken to a fake Microsoft 365 authentication page designed to steal their credentials.

Pandemic-related malicious email volume

Pandemic Milestones

JANUARY	FEBRUARY	MARCH	APRIL	MAY	JUNE	JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER	JANUARY
9 World Health Organization (WHO) announces mysterious coronavirus-related pneumonia in Wuhan, China.	**3** US declares public health emergency.	**6** 21 passengers on California cruise ship test positive.	**11** The first stimulus relief checks are deposited into US recipients' bank accounts.	**1** Remdesivir wins FDA approval for emergency use.	APPROVED • APPROVED • APPROVED • FDA	**22** US Health and Human Services (HHS), Department of Defense (DoD) announce vaccine distribution agreement with Pfizer and BioNTech to deliver 100 million doses of their COVID-19 vaccine candidates.	**7** Talks stall on second relief package.	**8** The University of Oxford and AstraZeneca halt Phase 3 trials of their vaccine because of a participant's suspected adverse reaction.	**2** President, First Lady test positive for COVID-19; Trump enters hospital.	**16** US Food and Drug Administration vows to move quickly on approving Pfizer, Moderna vaccines for emergency use.	**11** FDA approves Pfizer, BioNTech COVID-19 vaccine for emergency use.	
20 Three airports—JFK, San Francisco and Los Angeles—begin screening arriving travellers for coronavirus.	**25** CDC Says COVID-19 is heading toward pandemic status.	**11** WHO declares COVID-19 a pandemic.		**28** US COVID-19 deaths pass the 100,000 mark.				**21** Johnson & Johnson begins Phase 3 vaccine trial	**12** Johnson & Johnson halts Phase 3 vaccine trials after one participant's unexplained illness.		**14** Sandra Lindsay, an ICU nurse, is the first US citizen to be vaccinated.	
21 US Centers for Disease Control (CDC) confirms first US coronavirus case.		**13** US declares COVID-19 a national emergency, unlocking billions of dollars in federal aid. Travel ban on non-US citizens travelling from Europe takes effect.	**29** National Institutes of Health (NIH) trial shows early promise for Remdesivir.						**15** US cases spike again with 60,000 new reported COVID-19 cases, a number not reached since early August.		**18** FDA approves Moderna vaccine for emergency use.	
31 WHO issues global health emergency.		**19** California issues first statewide stay-at-home order.							**23** In separate decisions, AstraZeneca and Johnson & Johnson restart their respective vaccine trials.		**29** Second round of US stimulus checks begin reaching recipients.	
		26 Congress passes CARES Act, providing $2 trillion in aid to hospitals, small businesses and state and local governments. It is signed into law the next day.										

INFECTION VECTOR
An infection vector is the delivery channel or pathway of the attack. Email is the infection vector for most modern cyber attacks.

PAYLOAD
The payload is the malware the attacker ultimately intends to deliver to the victim's system. It's distinct from any malicious code used as the initial entry point into the system, delivery techniques or social engineering that tricks people into downloading and activating it.

The COVID-19 pandemic was the largest public health crisis in a century. The rapid spread of the virus across the globe forced organisations of all types to adapt. Businesses quickly adopted new policies and technologies as they walked a fine line between worker safety and business survival.

Threat actors quickly adapted, too. Fear and uncertainty about health and economic security, coupled with a hasty shift to remote work, created ideal conditions for more effective cyber attacks. By mid-March 2020, about 80% of all threats we scanned daily used COVID-19 themes.

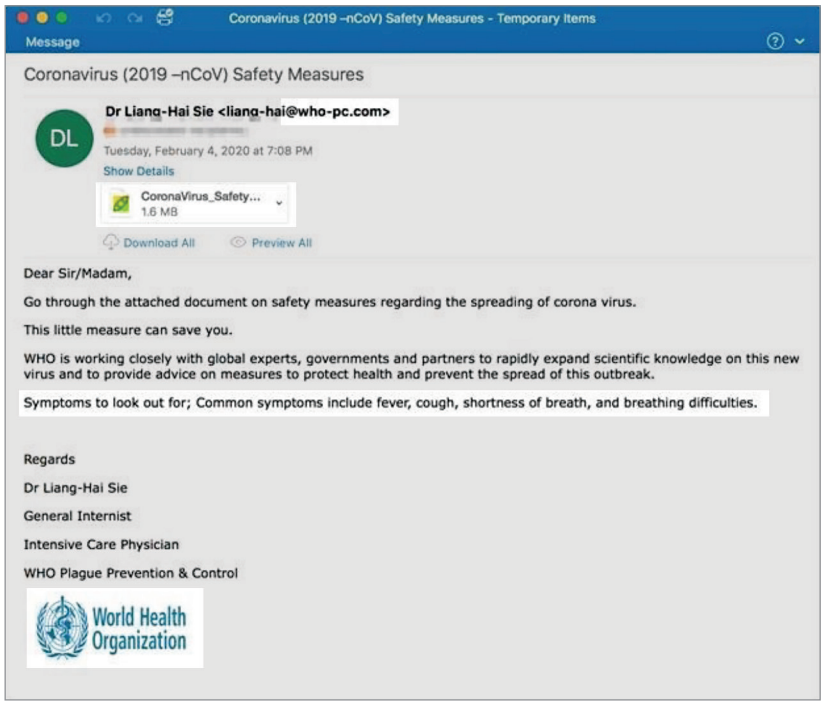
INFECTION VECTORS, **PAYLOADS**, and aggregate message volume of these threats remained largely unchanged. Threat actors continued to send the same malware and phishing campaigns at the usual intervals and quantities. What changed was a distressed workforce and disruption of regular business operations. The result was a larger attack surface and, in turn, higher infection rates.

Spring awakening

At the earlier stages of the pandemic, lures centered on stoking an emotional response. Many dangled updates about changes to organisational policy, government rules or how to stay safe. For example, threat actors masqueraded as the World Health Organisation, promising information about the virus.

NOTABLE FEATURES:

- Uses lookalike email domain to appear as a WHO announcement
- Malicious attachment uses filename that reinforces theme
- Offers basic COVID-19 information to help legitimise message
- Uses WHO logo to further masquerade



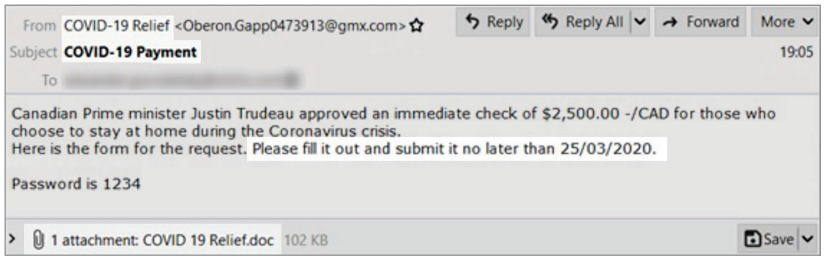
Phishing email impersonating WHO.

Following the money

As governments began discussing stimulus measures to avert economic collapse, attack lures began to capitalise on the idea of cash payments to people and businesses.

NOTABLE FEATURES:

- Uses display-name spoofing and subject line to catch recipients' attention with the promise of financial relief
- Provides a deadline to imply a sense of urgency
- Malicious attachment uses filename to reinforce theme of financial relief



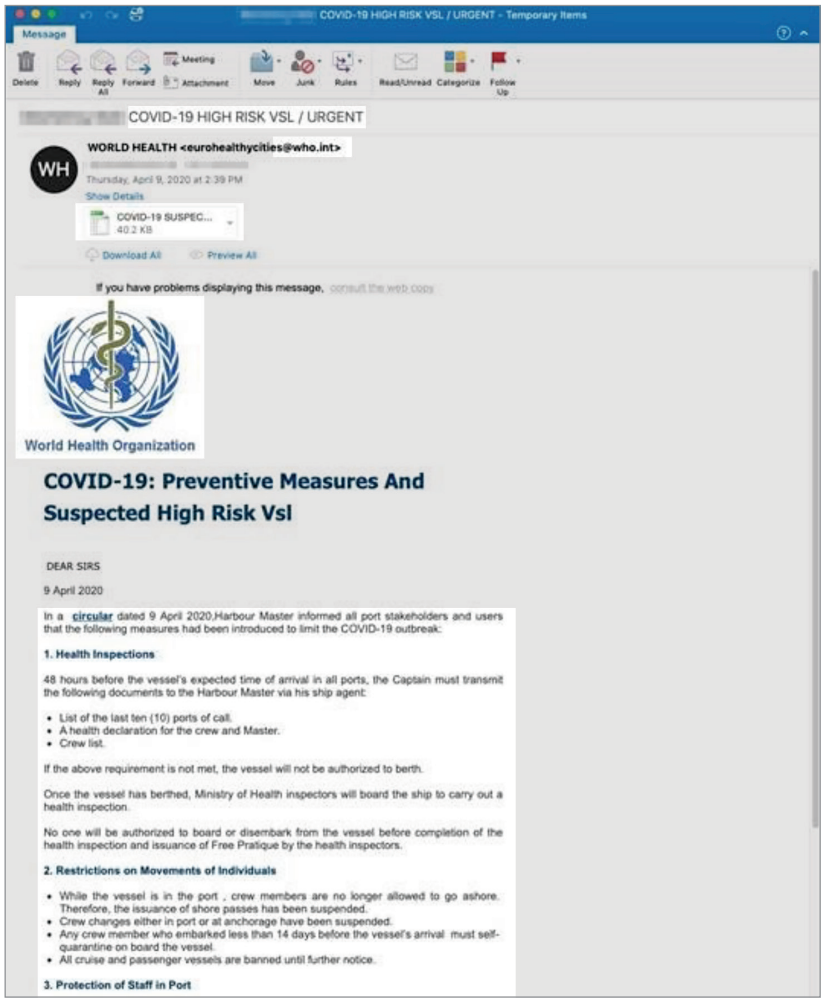
Phishing email purporting to be COVID-19 financial relief.

The golden rules

Then, as governments began issuing new policy and guidelines, lures began to adopt content about how to comply.

NOTABLE FEATURES:

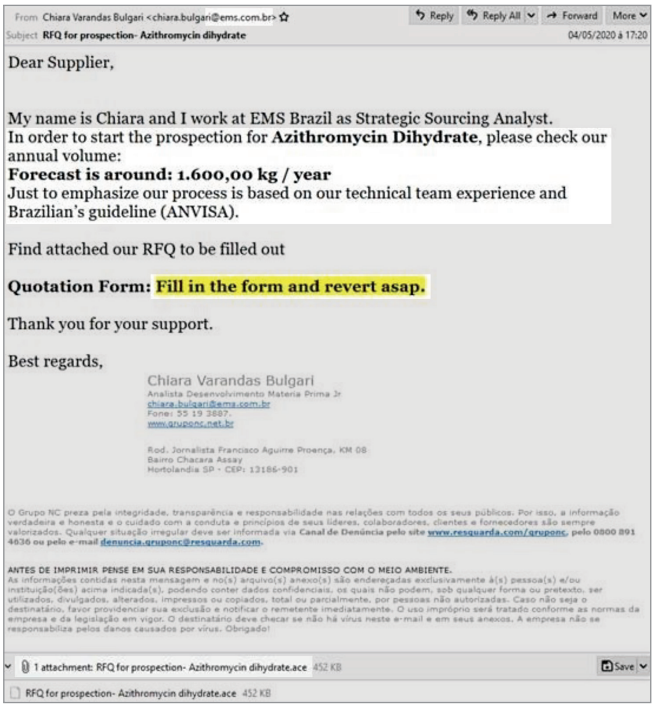
- Conveys a sense of urgency and risk to get readers to act instinctively
- Spoofs WHO email domain
- Malicious attachment uses filename to reinforces sense of fear and danger
- Uses WHO logo to appear official
- Provides actual COVID-19 information, reinforcing the email's apparent authority



Phishing email masquerading as WHO distributing COVID-19 details.

As the virus expands, so do tactics

As it spread further, the pandemic affected almost everyone and everything. Attackers' lures grew more varied and esoteric. Attacks tried to trick victims with fake grocery delivery notices, COVID-19 treatment forecasts and job cut news.


From: Chiara Varandas Bulgari <chiara.bulgari@ems.com.br>
Subject: RFQ for prospection- Azithromycin dihydrate
Reply | Reply All | Forward | More
04/05/2020 à 17:20

Dear Supplier,

My name is Chiara and I work at EMS Brazil as Strategic Sourcing Analyst.
In order to start the prospection for **Azithromycin Dihydrate**, please check our annual volume:
Forecast is around: 1.600,00 kg / year
Just to emphasize our process is based on our technical team experience and Brazilian's guideline (ANVISA).

Find attached our RFQ to be filled out

Quotation Form: Fill in the form and revert asap.

Thank you for your support.

Best regards,

Chiara Varandas Bulgari
Analista Desenvolvimento Materia Prima Jr
chiara.bulgari@ems.com.br
Fone: 55 19 3887.
www.grupoNC.net.br

Rod. Jornalista Francisco Aguirre Proença, KM 08
Bairro Chacara Assay
Hortolandia SP - CEP: 13186-901

O Grupo NC preza pela integridade, transparência e responsabilidade nas relações com todos os seus públicos. Por isso, a informação verdadeira e honesta e o cuidado com a conduta e princípios de seus líderes, colaboradores, clientes e fornecedores são sempre valorizados. Qualquer situação irregular deve ser informada via **Canal de Denúncia pelo site www.resguarda.com/gruponc**, pelo 0800 891 4636 ou pelo e-mail **denuncia.gruponc@resguarda.com**.

ANTES DE IMPRIMIR PENSE EM SUA RESPONSABILIDADE E COMPROMISSO COM O MEIO AMBIENTE.
As informações contidas nesta mensagem e no(s) arquivo(s) anexo(s) são endereçadas exclusivamente à(s) pessoa(s) e/ou instituição(ões) acima indicada(s), podendo conter dados confidenciais, os quais não podem, sob qualquer forma ou pretexto, ser utilizados, divulgados, alterados, impressos ou copiados, total ou parcialmente, por pessoas não autorizadas. Caso não seja o destinatário, favor providenciar sua exclusão e notificar o remetente imediatamente. O uso impróprio será tratado conforme as normas da empresa e da legislação em vigor. O destinatário deve checar se não há vírus neste e-mail e em seus anexos. A empresa não se responsabiliza pelos danos causados por vírus. Obrigado!

1 attachment: RFQ for prospection- Azithromycin dihydrate.ace 452 KB
Save
RFQ for prospection- Azithromycin dihydrate.ace 452 KB

Phishing email purporting to contain information about COVID-19 treatments.

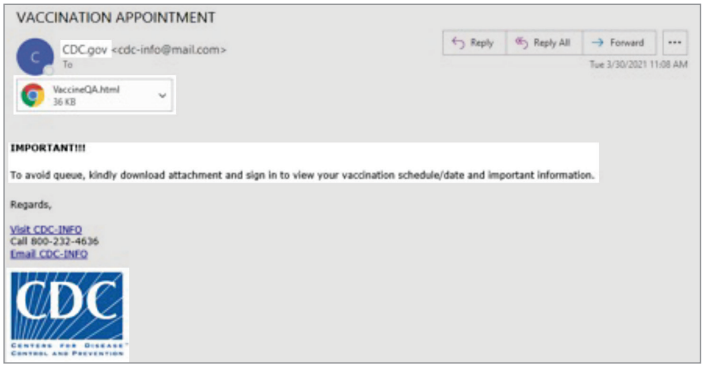
NOTABLE FEATURES:

- Spoofs email domain of EMS, Brazil's largest drugmaker
- Uses timely, emotion-laden topic to get the reader's attention
- Urges recipient to act quickly, short-circuiting the deliberative thought process
- Includes malicious attachment disguised as a normal business form

New year, similar themes

The pandemic and global response to it has improved in 2021. Still, threat actors continue to use COVID-19 related themes. Recent threats masqueraded as a vaccine scheduling confirmation.

No matter what 2021 holds in store, COVID-19 will likely continue to be a popular and effective theme in attacks.


VACCINATION APPOINTMENT
CDC.gov <cdc-info@mail.com>
To
Reply | Reply All | Forward
Tue 3/30/2021 11:08 AM
VaccineQA.html
36 KB

IMPORTANT!!!

To avoid queue, kindly download attachment and sign in to view your vaccination schedule/date and important information.

Regards,

Visit CDC-INFO
Call 800-232-4636
Email CDC-INFO

CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION

Credential theft phishing email masquerading as the CDC.

NOTABLE FEATURES:

- Uses display-name spoofing to appear as a CDC-sent email
- Attached HTML file is a credential-phishing site
- Promises quick access to a then-scarce resource (in this case, the COVID-19 vaccine)
- Uses CDC logo to reinforce the masquerade

CREDENTIAL PHISHING

Credential phishing involves tricking someone into providing their account login information, which gives attackers access to banking accounts, personal information, corporate accounts and more. While credential phishing can use any number of social engineering techniques, it typically plays out over email. Posing as a trusted brand or someone from the victims' organisation, the attacker sends an email that includes a link to a fake login page. When the user enters their username and password, the attacker uses the information to take over the person's account.

BUSINESS EMAIL COMPROMISE

Attacks in which the threat actor poses as a trusted colleague, executive or vendor using an assortment of impersonation techniques. The sender might ask the recipient to make a wire transfer, send a payment, divert payroll, change banking details or send sensitive information.

BEC attacks are difficult to detect because they don't use malware or malicious URLs that can be analysed with standard cyber defences. Instead, BEC attacks rely on identity deception and other social engineering techniques to trick people into taking action on the attacker's behalf.

Attack types

CREDENTIAL PHISHING, both consumer and corporate, was by far the most common form of attacks, outpacing all others combined. More than half of all email threats in 2020 were credential phishing attempts.

Stealing usernames and passwords can lead to everything from financial fraud to cyber espionage.

Other attack types included those that targeted financial systems, downloaded other malware, commandeered infected systems into botnets and stole sensitive information.

BEC

BUSINESS EMAIL COMPROMISE (BEC), a type of email fraud, is one of the most financially damaging threats to businesses of all sizes and industries. These schemes cost companies and individuals about $1.8 billion in 2020 alone, according to the FBI's Internet Crime Complaint Center. That represents 44% of all reported cyber crime losses, overshadowing most other types of cyber crime.[5]

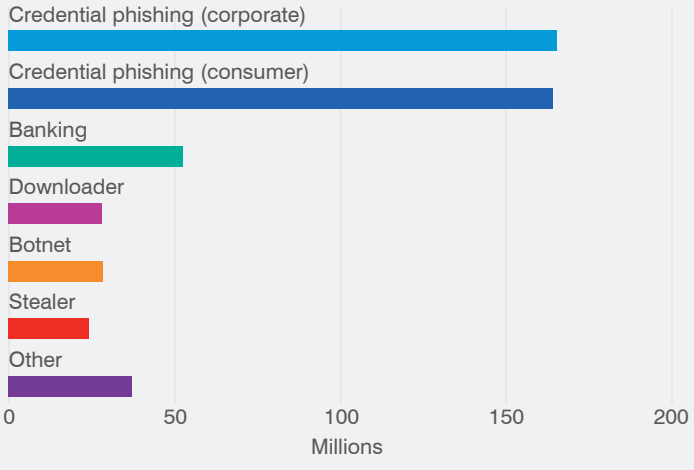
At Proofpoint, we take a people-centric approach to BEC, conceptualised through a **framework** made up of three tiers:

- Identity: who the threat actors are pretending to be
- Deception: the techniques they use
- Theme: the category of fraud they are attempting

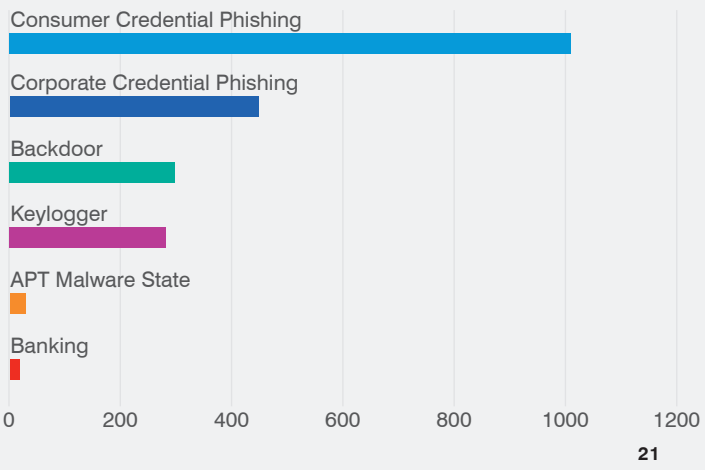
Deception typically falls into one of two categories— impersonation or compromise techniques. We define impersonation as an attack in which the threat actor alters one or more message headers to mask its origin. Compromise is an attack in which a threat actor gains access to a legitimate mailbox.

5 FBI. "2020 Internet Crime Report." March 2021.

Attack Types, by Message Volume (2020)
Corporate and consumer credential phishing were by far the most common attack types.



Change (2020 vs. 2019)



Our framework heavily emphasises themes because they produce actionable intelligence, including the various types of fraud involved, such as **invoice fraud**, payroll redirects and extortion.

Successful BEC schemes rely on social engineering. That may come in the form of the email's display name, tone or attachments used to make the message seem more credible.

In one of the more elaborate fraud attempts we observed during 2020, a threat actor we track as TA2520 used social engineering in several campaigns. Often impersonating a C-level executive through display-name spoofing, the threat actor instructed recipients to transfer money for what was falsely presented as a corporate acquisition deal.

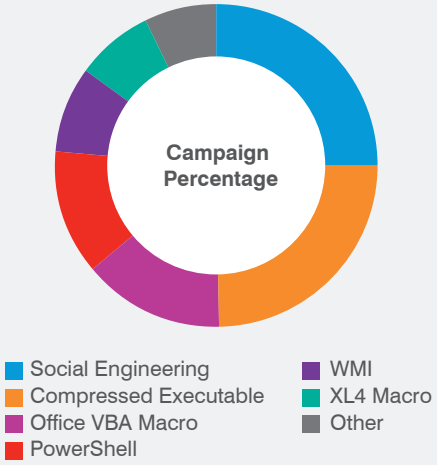
These attempts involved sums of more than $1 million USD, and often incorporated current events. Some mentioned COVID-19 restrictions, for instance, and a vaccine spurring an economic recovery.

Another threat actor of note that engaged in BEC in 2020 is TA2519, which launched multi-stage attacks. In the first stage of the attack, the threat actor focused on COVID-19 lures to deliver malware designed to steal victims' credentials. In the second stage, TA2519 then used the stolen credentials to take over the victim's account and use it to fraudulently bill a second victim, an attack known as supplier invoice fraud.

A fraudulent invoice can appear as though it came from anyone, such as a fellow employee or an unknown individual. The most successful appear to leverage supplier relationships, which include anyone or any business that sells products or services. Such attacks can end up costing companies anywhere from tens of thousands to multiple millions of dollars.

Share of Campaigns

A malicious email may contain multiple techniques, such as social engineering aimed at persuading the user to download and open a compromised attachment.



Attack techniques

Threat actors use a wide range of techniques to sidestep security controls, trick victims into activating the attack and infect targeted systems. But a common thread is the use of social engineering.

They use enticing subject lines, convincing appeals and the right degree of targeting to prompt the recipient to take action. As explained in **COVID-19: How attackers piggybacked the pandemic on page 15**, the pandemic was 2020's most popular theme.

Here are a few other notable trends.

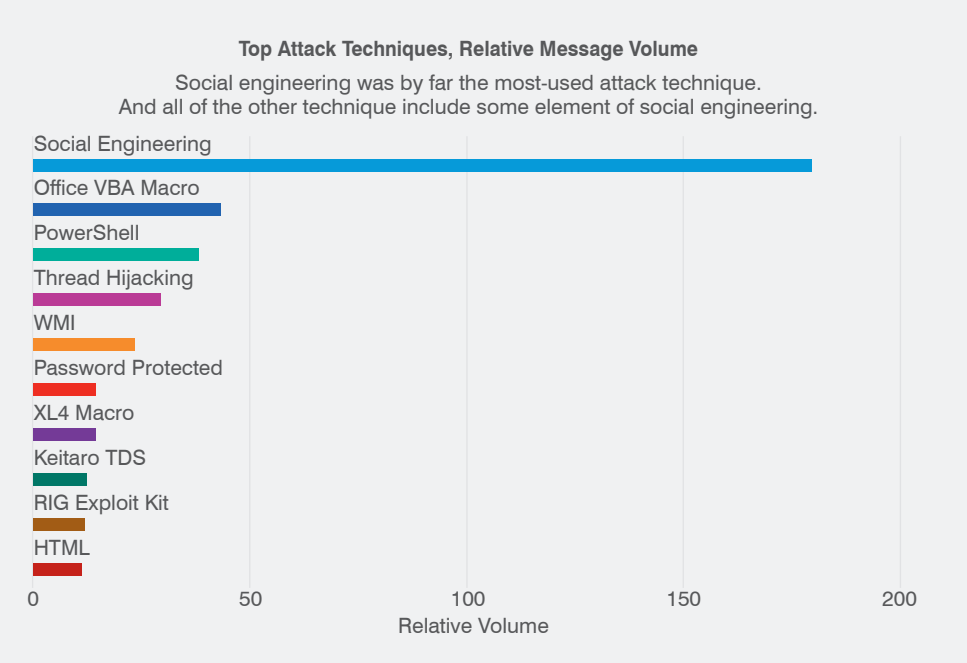
Compressed executables

Nearly 1 in 4 attack campaigns used compressed executable files to hide malware. This method relies on the victim to interact with a malicious attachment, such as a PowerPoint slide deck or Excel spreadsheet, to execute the payload. Because it runs only when a person unlocks the file, it's an effective way to evade automated malware detection.

Excel 4.0

Over the course of 2020, threat actors began **increasingly** using Excel 4.0 (XL4) macros to distribute malware. In the process, they shifted slightly away from Office Visual Basic for Applications macros. (Even so, the latter remains a much more widely used technique).

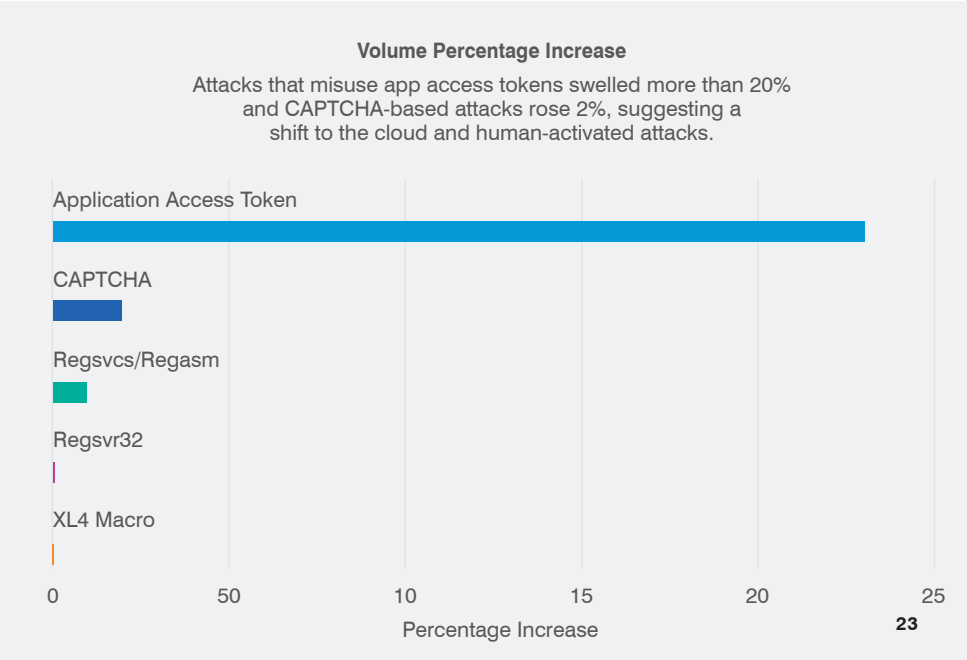
XL4-based attacks exploit an old Excel feature set, so it might seem puzzling to see a sudden spike in this technique. One possibility: limited detection coverage of XL4 in modern security systems. Although Microsoft still supports XL4 macros, the software giant has **urged** customers to migrate to the latest version of VBA.



CAPTCHA

Attacks that use CAPTCHA techniques spiked in 2020. (As noted in **Section 1: Vulnerabilities on page 6**, users were also more vulnerable to this technique than in 2019.)

The financially motivated threat actor TA564 often uses this method in malware campaigns targeting organisations in Canada. This attacker uses CAPTCHA to ensure a victim is located in the targeted region before acting. If not, the attack stops.



BANKING TROJANS
Historically, this type of malware focused on stealing bank login credentials, usually by redirecting to a fake version of a bank website or injecting fake login forms into the real site. Recently, many banking trojans have also served as a precursor to high-profile ransomware attacks.

LOADERS/DOWNLOADERS
Loader malware downloads additional malicious code hosted on the internet. Many different types of malware, such as banking and remote access trojans, now have this functionality. Droppers are similar to loaders, but instead of downloading additional code, they decrypt and run code that was included with the initial malware payload.

DRIDEX
Dridex, the modular banking trojan developed and controlled by the threat actors dubbed "Evil Corp", had a down year in 2019 before resurging in 2020. This malware is closely linked to subsequent deployment of Bitpaymer/Doppelpaymer ransomware.

QBOT
Qbot is a modular trojan that has seen its functionality extended since debuting in 2007. Like the other banking trojans listed here, Qbot is now predominantly an information stealer and loader for follow-on payloads such as Cobalt Strike.

ZLOADER
Zloader is an older banking trojan that surged with updated variants in 2020 and continues to be actively developed and widely adopted.

REMOTE ACCESS TROJANS
Remote access trojans provide attackers with administrative control of an infected system. Typically, they have a less sophisticated feature-set, but retain the ability to perform surveillance on compromised systems as well as download and execute additional malware.

Attack tools

BANKING TROJANS, which steals financial information and can act as a **LOADER** for other malware, were the most popular types of malware sent by threat actors. Top strains include **DRIDEX**, **QBOT**, and **ZLOADER**.

While activity from the Emotet botnet dropped sharply in 2020, it remained one of the most active groups. (For more on Emotet, see **Malware case study: Emotet in 2020 on page 28** and Malware metamorphosis: **Why labels don't always mean what they used to on page 26**.)

Winning the RAT race

REMOTE ACCESS TROJANS (RATs) represented almost a quarter of all campaigns that used malware. RATs can be used by threat actors to take control of a victim's machine and steal banking data, gather information and spread throughout the compromised environment. Examples of popular RATs include Ave Maria, NanoCore RAT and Remcos.

Although RAT campaigns were popular in 2020, they were less effective than campaigns that used other malware families. Users were more likely to click on or interact with emails with Emotet, malware backdoors and banking malware.

A lesson in ransomware: Attackers target schools in year of remote learning

Just as it did to business, the pandemic forced students, parents, teachers and schools to go remote. Classrooms spun up over video conferencing software. Students engaged with their peers and educators online, fully reliant on digital resources.

Threat actors proved quick studies. They capitalised on the change with using lures themed as classwork or other school resources to distribute malware—and in many cases, disrupted online learning.

An October 2020 campaign posed as a parent or guardian submitting an assignment on a student's behalf.[6] The email claimed that the child had run into technical issues. The malicious document attached to the email distributed Cryptme, a simple ransomware strain that encrypts files on a victim's computer.

6 **https://www.nbcnews.com/tech/security/parents-end-chain-ransomware-hit-kids-schools-rcna646**

Email posing as a parent.

Ransomware attacks on schools surged in 2020. With students all over the world learning from behind their screens, such attacks disrupt an already fraught learning environment.

Schools **continue to be a target** for cyber criminals, which we expect to be the case throughout 2021.

Cobalt spike

Often, threat actors co-opt RAT-like software tools that have legitimate uses for IT departments, security testers and advanced users. Some are even built into users' systems, allowing attackers to "live off the land" using resources already in the environment they're seeking to inhabit.

One example is Cobalt Strike, a commercial security tool designed to help organisations probe for system weaknesses through simulated attacks. (These are known as "red team" exercises, where someone at or working for the organisation plays the role of a cyber intruder.)

But more and more threat actors are using the tool for real attacks. The volume of threats delivering Cobalt Strike as the primary payload jumped 161% in 2020.

Other security researchers have observed the same trends as more threat actors adopt open-source hacking tools. For example, TA572 sent invoice-themed emails with malicious Excel and Word documents using Microsoft Excel 4.0 (XL4) macros to download Cobalt Strike.

Malware metamorphosis: Why labels don't always mean what they used to

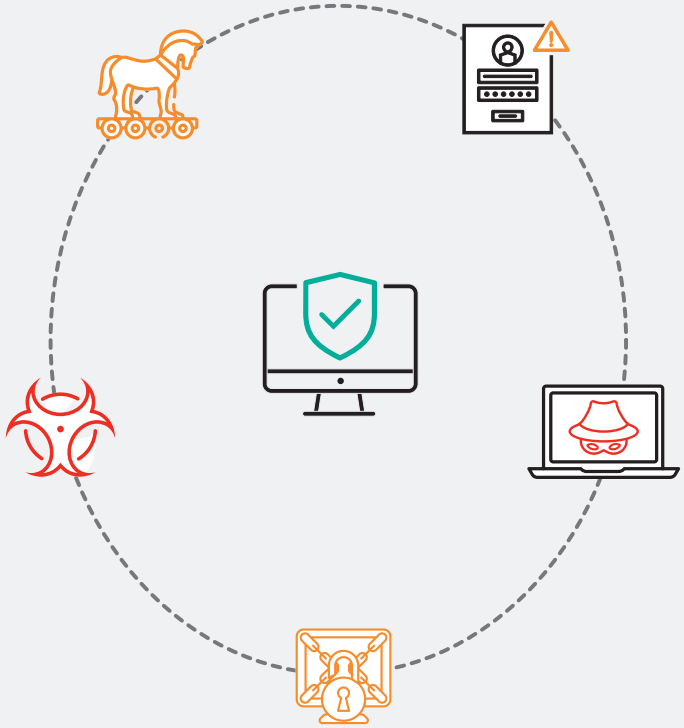
Classifying malware can be useful for understanding the scope and nature of the threats targeting your users. But these labels don't always tell the whole story. Malware strains are improved and enhanced. Attackers use them in unexpected ways. And like a versatile acting troupe who actors can fill in for one another when one falls ill, malware tools are often swapped out and used in different combinations as needed.

Using different strains of malware together is a longstanding practice that serves an important purpose for attackers. It provides the flexibility of having just the right tool for each stage of an attack. It provides redundancy and allows the attacker to persist in an environment, even when some of the malware is detected. And it extends the life of older malware that might be detected by security gateways—but not as a secondary download to already infected machines.

Take Emotet, the versatile and prolific malware service dubbed "the world's most dangerous malware" before a global law enforcement dragnet shut down its infrastructure in January. Emotet emerged in 2014 as a simple banking Trojan, stealing account credentials of a narrow set of targets in Germany and Austria.

It quickly gained downloader capabilities, making it a useful tool for downloading secondary malware. Over time, added features made it more useful to attackers, harder to detect, more able to spread and easier to extend.

It eventually grew into a versatile botnet, a network of infected machines that could be used like a zombie army to support a broad set of attacks around the world.



Who's who in the threat landscape: top threat actors

We identified 69 active threat actors in 2020. Here are those that were the most active, based on message volume. Like most high-volume attackers, all five are what researchers call financially motivated threat actors, meaning they focus on financial crimes.

The art and science of attribution

It's a question asked in the wake of any crime, cyber or physical: *whodunnit*? For security researchers, the answer isn't always clear cut.

Every attack leaves a trail of digital breadcrumbs—the malware used IP addresses of command-and-control servers, malware metadata, fonts and languages used in email lures, behaviour, configuration settings and other signs. By piecing these clues together and finding patterns between attacks, researchers get a picture of who's behind an attack. Threat researchers call this process attribution.

We group threat actors by their campaigns and behaviour rather than by nationality or organisation, although some are independently attributed by other research teams and law enforcement. But definitive attribution is not always possible.

That's because the cyber criminal ecosystem is vast and highly fragmented.

Some cyber criminal rings work like franchises. An advanced **THREAT ACTOR** creates the malware "product" and sets up the infrastructure as an easy-to-use package or service. Lower-level cyber criminals may rent the service for their attacks, paying to use it for a set period of time or getting a cut for each successful compromise. In other cases, they act as distributors, sending emails with the malware and earning a commission on each successful infection.

Because different cyber criminals may use the same tools and infrastructure, researchers can't always pin an attack on a specific threat actor. But analysing attacks that can be attributed to key threat actors—as we do throughout this report—remains a critical part of the security puzzle.

THREAT ACTOR

Threat actor is a term threat researchers use to describe an attacker or groups of attackers. They can include state-sponsored attackers, cyber criminal rings and, occasionally, hacktivists.

TA542

This is the cyber criminal group behind the notorious Emotet botnet. Despite the botnet's five-month **hiatus** in 2020, the group's activities still managed to account for nearly 10% of malicious email traffic worldwide. An international law enforcement sweep dismantled Emotet in January 2021 and arrested several alleged members of the group. Since then, the group's activities have all but disappeared.

Malware case study: Emotet in 2020

Emotet first emerged as a banking trojan in 2014 and evolved into one of the most notorious malware botnets by 2020.

In February 2020, Emotet activity stopped for five months before returning in July. Despite this downtime, Emotet remained the most prolific threat in 2020.

Emotet was known for its massive email volume and global distribution, using **multiple themed** lures that sometimes coincided with global news and events including COVID-19.

In **October 2020**, a month before the US presidential election, Emotet began using political themes in phishing lures. Emotet targeted organisations throughout North America, Europe, East Asia and Oceania. Second-stage payloads included Qbot and The Trick.

Once the group got into a victim's environment, it would sell access to other threat actors, leading to further compromise—including disruptive and costly ransomware attacks.

MALVERTISING
Malvertising embeds malicious code into online display ads. These ads often appear on legitimate, widely trusted websites, making them difficult to block at the gateway or endpoint.

TA567

This threat actor uses malicious advertising, also known as **MALVERTISING**, through Keitaro, a legitimate traffic distribution system (TDS) that helps advertisers target online ads by directing viewers to the right websites. Rather than sending out malicious email, TA567 uses the Keitaro TDS to distribute malicious content via legitimate advertising that ultimately results in a range of malware on unsuspecting websites. Benign emails may contain links to sites infected with these compromised ad units, giving Proofpoint a window on this attacker's activity. These threats often leverage geo-fencing techniques to tailor malicious ads to specific geographies.

TA544

This cyber criminal steals money through banking trojans and other malware. It accounts for just shy of 4% of total worldwide email volume. TA544 typically uses malicious Microsoft Office attachments containing malicious macros, tricking recipients into opening the attachment and enabling the macro to download the payload. The threat actor has targeted several industries across several regions, including Italy and Japan.

THE TRICK
Since emerging in 2016, this banking Trojan has grown into a versatile tool that can download other malware, spread itself throughout a network, update itself and more.

BAZALOADER
First discovered in April 2020, BazaLoader is used to download other malware. Though a relative newcomer, we have seen at least six variants of the malware, a signal that it is being actively developed.

TA505

This influential threat actor is known for conducting malicious email campaigns on an unprecedented scale. The group regularly changes its tactics, techniques, and procedures (TTPs) and are considered **trend setters** in the world of cyber crime. TA505 is an equal opportunity cyber criminal—targeting a wide range of industries and geographies. In 2020, TA505 primarily focused its efforts on the US, Canada, and German-speaking parts of Europe. Though sometimes linked to Evil Corp., a cybercrime groups based in Russia, we consider it a separate threat actor.

TA800

This threat actor distributes banking malware and malware loaders including **THE TRICK** (also known as TrickBot) and **BAZALOADER**. These loaders are closely tied to second-stage ransomware attacks using Conti and Ryuk, respectively. It was one of the first threat actors to begin using BazaLoader in April 2020, months before other groups. It targets a broad range of industries in North America, accounting for about 2% of total malicious email volume.

SECTION 3

Privilege

Assessing privilege is another way of determining how much damage a successful attack would cause. Compromising a high-privilege user gives the attack access to sensitive and valuable information.

Insider threats—whether they stem from malicious, negligent or compromised users—are another form of privilege abuse. For many organisations, an almost overnight shift to remote work complicated efforts to monitor and mitigate insider threats.

Organisations took a closer look at USB devices, large file and folder copying (especially during odd hours), assessing file-sharing services and activities that might circumvent user-monitoring tools. The number of organisations setting DLP alerts for these activities jumped significantly from pre-COVID-19 levels.

Top insider threat management alerts

ACTION	RANK	CHANGE FROM 2019
Connecting unlisted USB device	1	▲
Performing large file or folder copy	2	▲
Exfiltrating tracked file to the web by uploading	3	▼
Opening a clear text file that potentially stores passwords	4	▲
Downloading File with Potentially Malicious Extension	5	▼
Performing large file or folder copy during irregular hours	6	▲
Exfiltrating a file to an unlisted USB device	7	▼
Installing hacking or spoofing tools	8	▼
Accessing upload and sharing cloud services	9	▲
Opening ObserveIT Agent folder	10	▲

Conclusion And Recommendations

Today's threats require a people-centric approach to keeping them safe.

Attackers do not view the world in terms of a network diagram. They see org charts, connections, relationships and access.

Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

We recommend the following for a people-centric defence.

Vulnerability

Most cyber attacks can't succeed unless someone falls for them. Mitigating vulnerabilities starts with security awareness training and risk-based controls. We recommend the following:

- **Train users to spot and report malicious email.** Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.
- At the same time, **assume that users will eventually click some threats.** Attackers will always find new ways to exploit human nature. Find a solution that neutralises threats with by applying additional layers of security to your most vulnerable users.
- **Isolate risky websites and URLs.** Keep risky web content out of your environment. Web isolation can be a critical safeguard for shared email accounts, which are difficult to secure with multifactor authentication. The same technology can isolate users' personal web browsing and web-based email services.

Attacks

Cyber attacks are inevitable. But with the right mindset, tools and policies, they can be a manageable risk. Here's what we recommend for preventing, detecting and responding to attacks.

- **Build a robust email fraud defence.** Email fraud can be hard to detect. Invest in a solution that can manage email based on custom quarantine and blocking policies. Your solution should analyse both external and internal email—attackers may use compromised accounts to trick users within the same organisation.
- **Prevent ransomware by preventing the initial infection.** Ransomware distributors now prefer to prospect for high value targets already infected with a trojan or loader. Avoid becoming a ransomware victim by keeping out these more common strains of malware.
- **Protect cloud accounts from takeover and malicious apps.**
- **Partner with a threat intelligence vendor.** Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics, and targets—and then learns from them.

Privilege

The goal of every cyber attacker is access to data, systems and other resources. The more privileged the victim, the more access attackers have—and the more damage they can do. To manage privilege and help ensure that it's not misused, we recommend:

- **Deploy an insider threat management system** to prevent, detect and respond to malicious, negligent and compromised users—the most common scenarios for privilege misuse—in as close to real time as possible.
- **Respond quickly to potential privilege abuse** with tools that can help you determine what happened before, during and after the incident and determine the user's intent—without the usual false positives.
- **Enforce security policies** with user training, real-time reminders and blocking when necessary.

Learn how Proofpoint can help assess and mitigate vulnerability, attacks and privilege with a people-centric approach to today's biggest security and compliance challenges at **proofpoint.com**.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0400-005-01-01 07/21