28 - 30 September, 2022 / Prague, Czech Republic

EXPLOITING COVID-19: HOW THREAT ACTORS HIJACKED A PANDEMIC

Daniel Blackford & Selena Larson

Proofpoint, USA

dblackford@proofpoint.com
slarson@proofpoint.com

ABSTRACT

The global relevance of the COVID-19 pandemic created an environment primed for exploitation like none witnessed in the age of the cybercriminal. Adversaries of every sophistication level – advanced state-aligned groups, large- and small-scale crime-motivated actors, fraudsters and spammers of every variety – all pivoted to make use of COVID-19-related content for their respective nefarious ends.

Proofpoint researchers had not observed the entire landscape pivot to using the same social engineering theme prior to COVID-19. Over 30 known threat actors and many more unattributed threat clusters tracked by researchers used COVID-19 themes in campaigns. But why was the pandemic such a compelling choice for threat actors?

Fundamentally, the fear, uncertainty and doubt around COVID among people all over the world created conditions in which training and diligence broke down. This presented an opening for threat actors to exploit people.

Now in our third year living with COVID-19, we can look back and identify some key phases global societies moved through. Initial periods required a great deal of dissemination of policy changes across a broad spectrum of organizations including both country- and local-level mandates, as well as business-related guidelines. Lockdown, economic stimulus, vaccine development and eventual deployment, the rise of variants creating new surges of illness – all these stages provided threat actors with the content needed to exploit the human condition and produce engagement with malicious content.

In this paper, we will present the following:

- How cybercrime and advanced persistent threat (APT) actors leveraged the COVID-19 pandemic in social engineering activity.
- How activity changed throughout the lifecycle of the global pandemic.
- What social engineering tactics were most effective.
- What we can learn from threat actor behaviours to defend ourselves moving forward.

This paper examines the wide array of COVID-19-related content threat actors have leveraged, how that use evolved alongside real-world conditions, and how it fits into the overall picture of the threat landscape since the beginning of 2020.

METHODOLOGY

Proofpoint analysts conducted this research based on threat campaign data, or activity that has been manually analysed and contextualized from January 2020 through to April 2022. Then, researchers broke down campaign data by multiple variables including: threat type such as credential harvesting or malware; brands or organizations impersonated in email lures; and lure theme such as safety, company operations, economic, vaccines, related to COVID-19.

For the purpose of this report, a campaign is defined as a time-bound set of related threat activity. This implies, even in cases where no attribution is made, that the threats from a given campaign result from attacks perpetrated by the same threat actor. Threats may be related by a variety of factors including distribution or hosting infrastructure, overlap in message forensics such as header components, a common payload, or other facets.

It should be noted that while this analysis covers tens of thousands of campaigns and hundreds of millions of threats overall, it is still only representative of a portion of the threat landscape. To that end, there is some inherent bias present in the choice of what activity is campaigned.

Where click rates are denoted, be advised this does imply delivery of some number of threats. *Proofpoint*'s *URL Defense* rewrites URLs in the message bodies of delivered emails allowing both for data gathering around clicks and post-delivery mitigation actions. A single user's click triggers additional detection processes which may lead to additional remediations for the global customer base.

Proofpoint observed hundreds of millions of COVID-19-themed messages associated with business email compromise (BEC) threats. However, due to how the campaign data is identified and reported, BEC threats are not included in this dataset. It focuses exclusively on credential capture and malware threats.

This paper is organized to be a year-by-year analysis of threats to demonstrate how activity changed throughout the lifecycle of the global pandemic. It also includes a section detailing the effectiveness of the variety of COVID-19 themes observed during this period.

DEFINING SOCIAL ENGINEERING

Social engineering is used as an umbrella term that covers any attempt to manipulate an intended victim into taking some action. Social engineering is the most important component of all cyber attacks originating via email. Whether the goal of a threat actor is to directly perpetrate fraud, harvest credentials, or install malware, at some point a human being must be coerced into taking an action on the actors' behalf.

Effective email-based social engineering is about generating feelings within a user that drive them into engaging with content. Something is urgent, someone is trustworthy, someone can help. The most effective methods prey on natural

human tendencies and undermine instincts which raise an alarm that 'something isn't right'. Often, this means presenting the intended victim with content they may already be familiar with or regularly interact with in their day-to-day jobs: invoices, receipts, documents and spreadsheets. The content appears routine and therefore raises no alarm. A threat actor might impersonate a trusted partner, or an authority figure such as a company's executive.

Social interest is also frequently leveraged, no more so than throughout the COVID-19 pandemic. At the beginning of the pandemic there was a collective desire for information around updated health guidelines, company policies, regional mandates and safety measures. As we moved through 2020, people became more interested in what it meant for travel, and information relating to vaccines. From 2021 and into 2022, as multiple variants emerged, people were very concerned about spread in their communities. Email threat lures leveraged all of these concerns. Because of the universal relevance, threat actors of every skill level pivoted to make use of COVID-19-related content.

Campaigns that featured COVID-19-related content were labelled based on the social engineering theme presented to intended victims. In some cases, there was overlap between themes or multiple themes present. The themes are:

- **Safety**: content indicating that in order for the victim or victim's loved ones to remain safe they need to take some action. This extends to topics of personal protective equipment, sanitation, and governmental regulations around maintaining safe spaces.
- **Cure/vaccine**: content at first highlighting the development of vaccines, and later the deployment of them. This includes lures about vaccine appointments.
- **Travel**: content focusing on the impact of COVID-19 on travel, especially internationally. This includes governmental regulations on border closings.
- **Economic**: content centred around economic relief, to include personal stimulus payments and government relief for businesses. This extends to topics around disruption of global markets.
- **Shipping/logistics**: content insinuating disruption to supply chain, manufacturing, or the transportation of goods.
- **Conspiracies**: content pushing misinformation around the virus or the development and distribution of vaccines.
- **Spread**: content focusing on infection rates, positive tests, and the overall spread of the virus.
- **Company operations**: content masquerading as business communications from employer to employee, to include changes to company policy around travel, customer interactions, work from home, and potentially termination of employment.
- **Pass**: content centred around proof of vaccination status by way of card or 'passport'. Note this content was almost exclusively themed around non-US countries.
- **General**: content which was vague, generic, and/or did not fit into one of the above themes.

2020

COVID-19 first emerged in December 2019 in Wuhan, Hubei Province, China. The virus quickly began to appear in multiple East and Southeast Asian countries, including Thailand and Japan, before spreading globally. As the virus

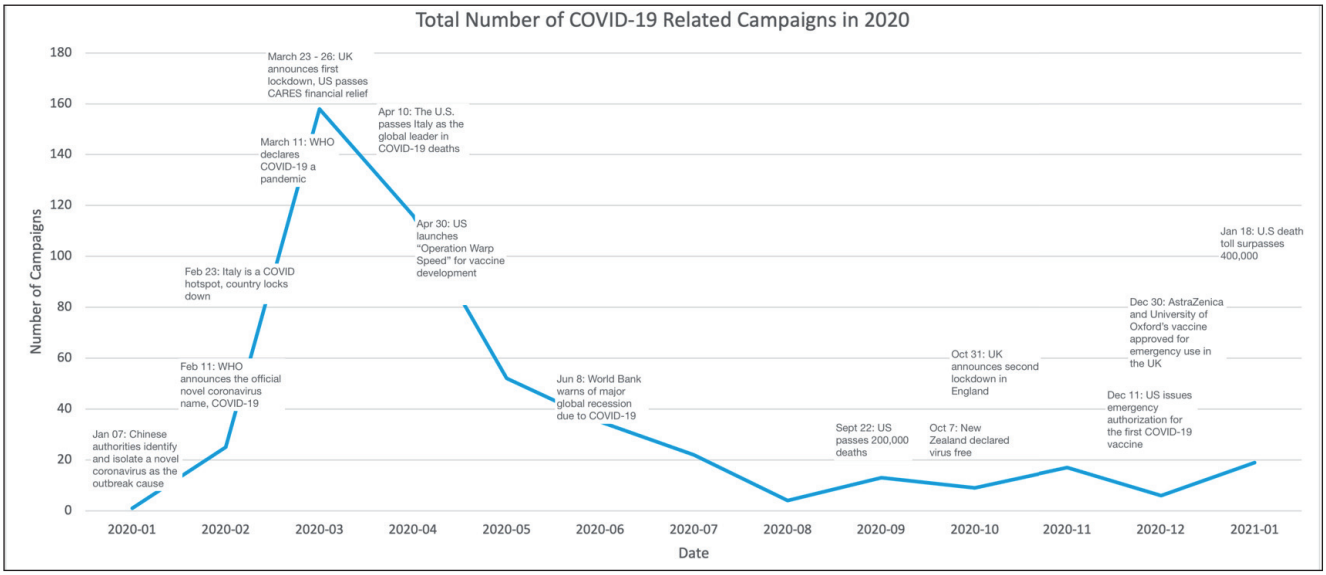


Figure 1: Number of COVID-19 related campaigns and notable moments during the COVID-19 pandemic in 2020. COVID-19 timeline data pulled from the US Center for Disease Control and Prevention [2] and the United Kingdom think tank Institute for Government [3].

propagated and countries began lockdowns to prevent spread, restricting visitors and international travel, threat actors began leveraging COVID-19 as a theme at an accelerated rate. According to *Proofpoint* data, the number of COVID-19-themed campaigns peaked in March 2020, shortly after the World Health Organization (WHO) officially declared COVID-19 a global pandemic [1]. At its peak, one in four malicious messages was COVID-19 themed.

Cybercriminal actors

TA542, the threat actor *Proofpoint* associates with Emotet, was the first threat actor observed by *Proofpoint* making use of COVID-19 themes, in late January 2020. Emotet is a prolific botnet and trojan that targets *Windows* platforms to distribute follow-on malware. TA542 masqueraded as a Japanese government entity and leveraged COVID-19 safety measures in emails to Japanese recipients. Notably, the threat actor used typical invoice-themed lures for English language targeting, but COVID-19 was enough of a mainstream concern in Asia that it customized Japanese language lures for this audience.

Figure 2: First Emotet COVID-19 lure used on 29 January 2020.

In this campaign, the messages contained macro-enabled *Word* documents which, if enabled by the users, downloaded and installed Emotet. Emotet routinely downloads additional malware including the Trick. Often the subsequent payloads can lead to ransomware.

During the initial months of the COVID-19 pandemic, *Proofpoint* researchers observed more threat actors leveraging themes related to safety measures and company operations than other theme types. Safety-themed emails included information on how to sanitize, use masks and other personal protective equipment (PPE), and safety measures announced by government entities. Company operations themes often referred to disruptions to business due to COVID-19, business continuity plans, and work from home policies.

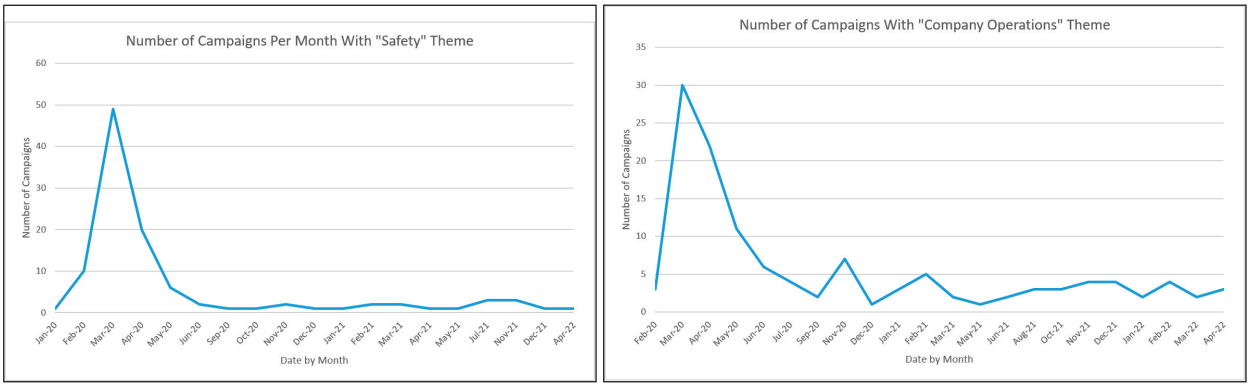


Figure 3: Number of campaigns associated with safety and company operations themes from 2020 to 2022.

For example, in a March 2020 credential phishing threat targeting healthcare entities (see Figure 4), the threat actor used emails with subjects such as 'Clinical Update On Covid19' that contained a *Word* document with an embedded URL that leads to a phishing page designed to steal credentials.

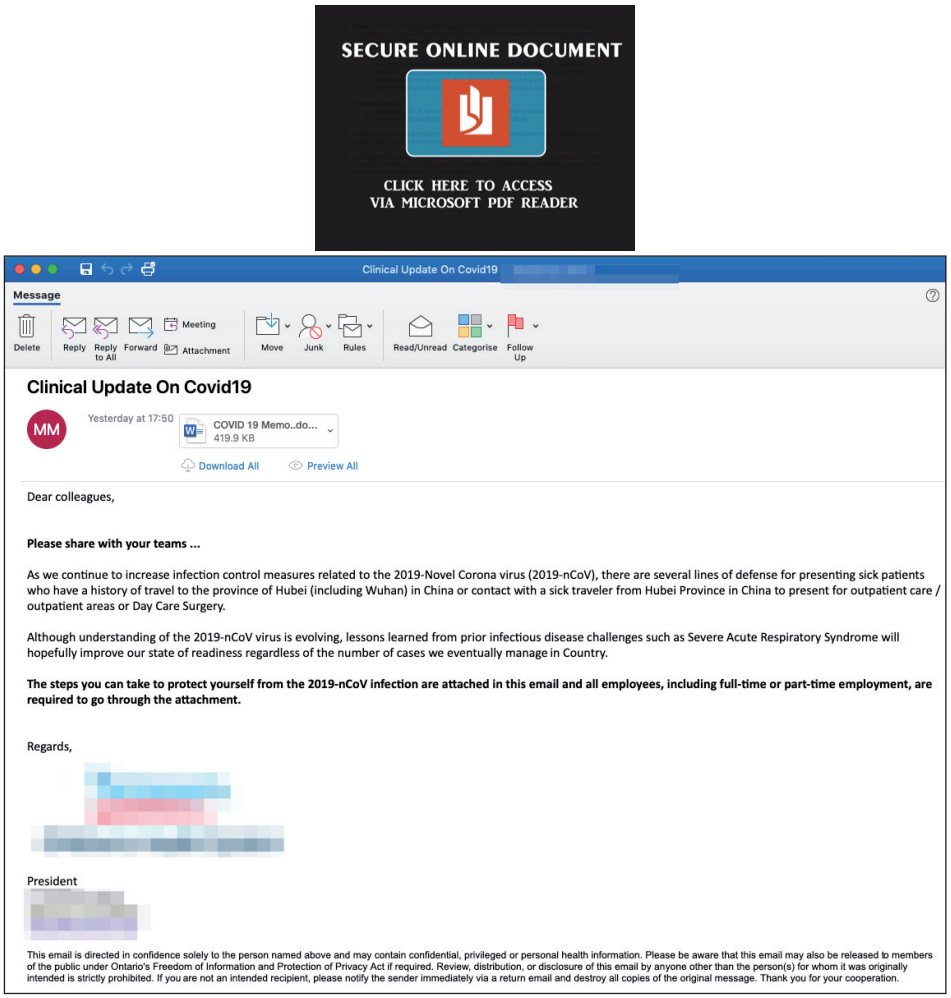


Figure 4: COVID-19 safety-themed lure.

Also in March 2020, *Proofpoint* researchers observed the cybercriminal actor TA564 spoofing the Public Health Agency of Canada to distribute Ursnif malware. These emails contained URLs linking to a twice compressed macro-enabled *Microsoft Word* document (e.g. Coronavirus_disease_COVID-19__461657952561561.doc), accessible only after passing a CAPTCHA verification. If enabled, the macros downloaded and installed Ursnif.

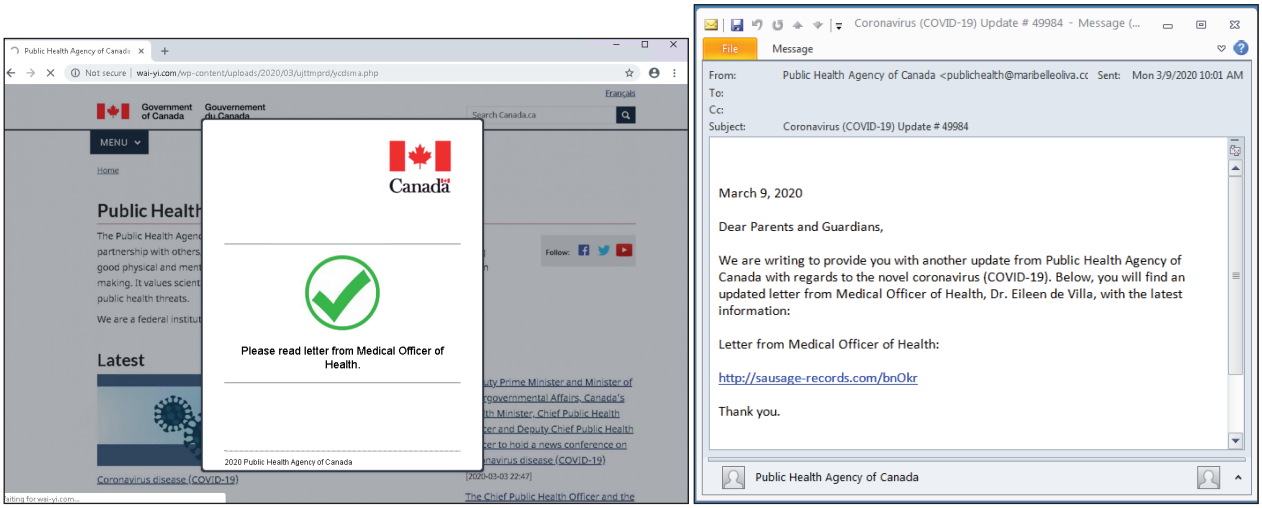


Figure 5: Email lure and spoofed Public Health Agency of Canada website.

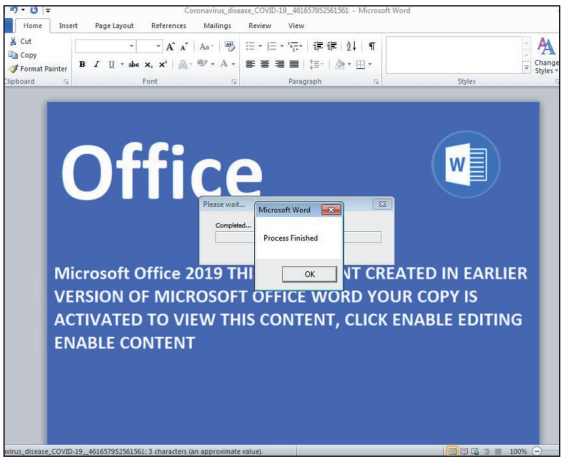


Figure 6: Macro-laden Microsoft Word document that downloaded and executed Ursnif.

In addition to the Canadian government, *Proofpoint* observed threat actors spoofing government entities in the United States, United Kingdom, Japan, Italy, Philippines, Brazil, Spain and Turkey.

In April 2020, *Proofpoint* identified a German language credential theft campaign targeting German entities. The emails contained the subject 'FORRS COVID-19 Business Continuity', with a German-language message about a business continuity plan for the German firm *FORRS*. The emails contained URLs linking to an *Outlook*-branded page attempting to steal login credentials.

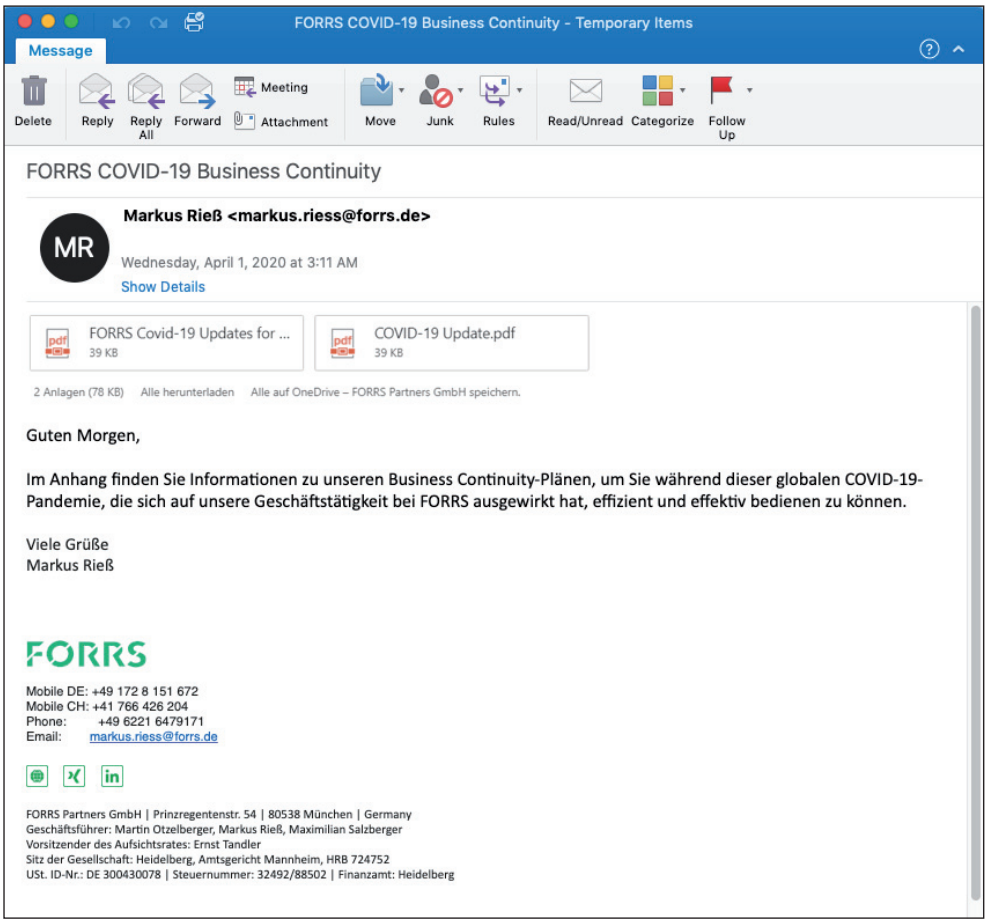


Figure 7: German language credential theft threat.

Threat actors also often preyed on people's concern for their employment during the COVID-19 pandemic, especially in the United States. In April 2020, the US Department of Labor announced that the unemployment rate had jumped to 14.7%, the highest since the Great Depression [4]. Throughout 2020, threat actors used those fears to create lures related to job loss and unemployment.

For example, in June, *Proofpoint* identified TA800 masquerading as human resources representatives for targeted companies distributing 'termination' emails. The messages contained URLs such as Sendgrid and Constant Contact that redirected the recipient to a landing page hosted on *Google Docs*. The landing page linked to a download of a BazaLoader executable, which downloaded BazaBackdoor, which in turn downloaded Cobalt Strike.

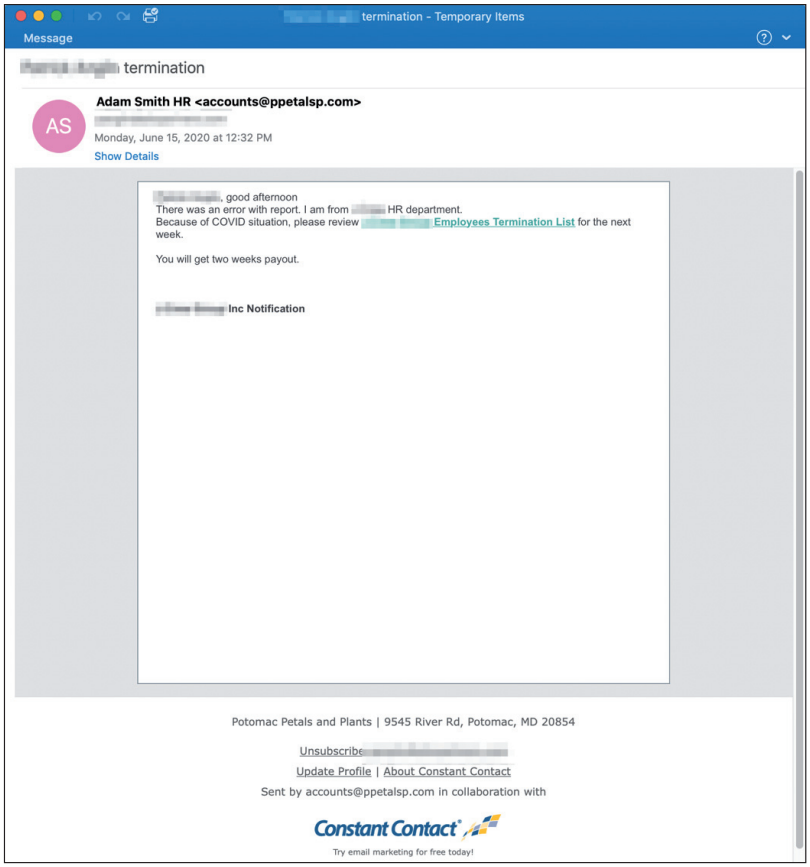


Figure 8: TA800 termination-themed lure.

While nearly all threat actors pivoted to COVID-19 themes at some point during the pandemic, some threat actors incorporated COVID-19 into already existing and consistent social engineering themes. For example, in the spring of 2020, TA2541 briefly pivoted to adopting COVID-related lure themes consistent with their overall theme of cargo and flight details [5]. This is a cybercriminal threat actor that largely targets aviation and aerospace entities, among others.

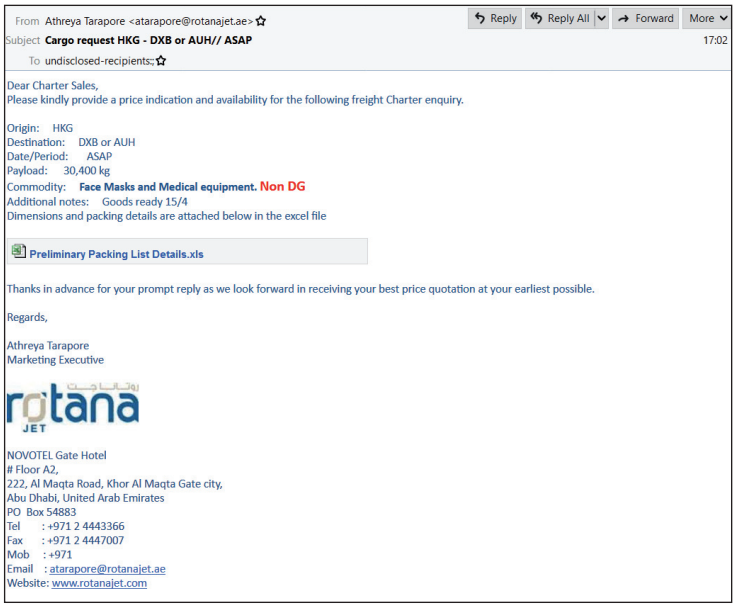


Figure 9: TA2541 cargo flight lure including COVID-19 equipment themes.

With the adoption of COVID-19 themes, TA2541 distributed lures associated with cargo shipments of PPE or COVID-19 testing kits and included information on coronavirus in emails related to travel and transportation.

As commercial travel remained restricted due to COVID-19, threat actors leveraged concern for the tourism industry using travel-themed lures. In a campaign from November 2020 (see Figure 10), the threat actor masqueraded as the United Nations World Tourism Organization, purporting to be hiring travel agents.

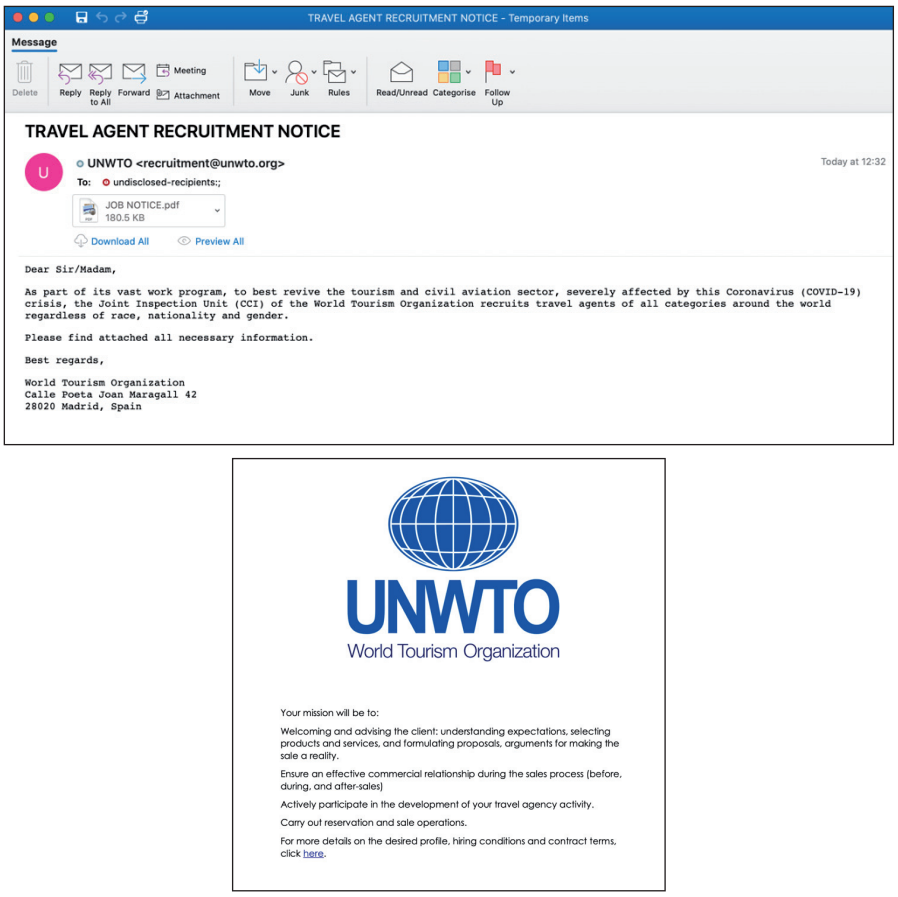


Figure 10: UNWTO travel-themed lure.

These messages contained a PDF with an embedded link to download a number of scripts, ultimately leading to the installation of Koadic malware. The threat largely targeted the hospitality and travel, business services, and transportation industries.

Unique in 2020 was the emergence and use of themes related to COVID-19 conspiracies, including that the virus was a hoax, or that it originated outside of Wuhan.

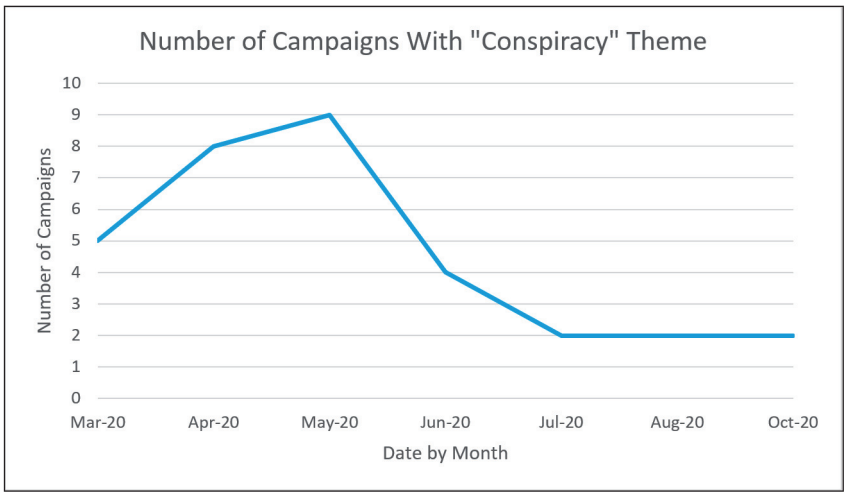


Figure 11: Number of campaigns using COVID-19 conspiracy lures.

In one example, a credential theft threat actor claimed COVID-19 was either a secret government world order weapon, or a hoax. The email contained a link to a credential-harvesting website to steal email addresses and passwords. Another recurring example featured an email claiming to know the 'truth about COVID' and its origination in the US. The message contained *Word* documents that exploited CVE-2017-8570 in conjunction with OLE objects, to drop a PowerShell script known as 'Lemon Tree' or 'Lemon_Duck'.

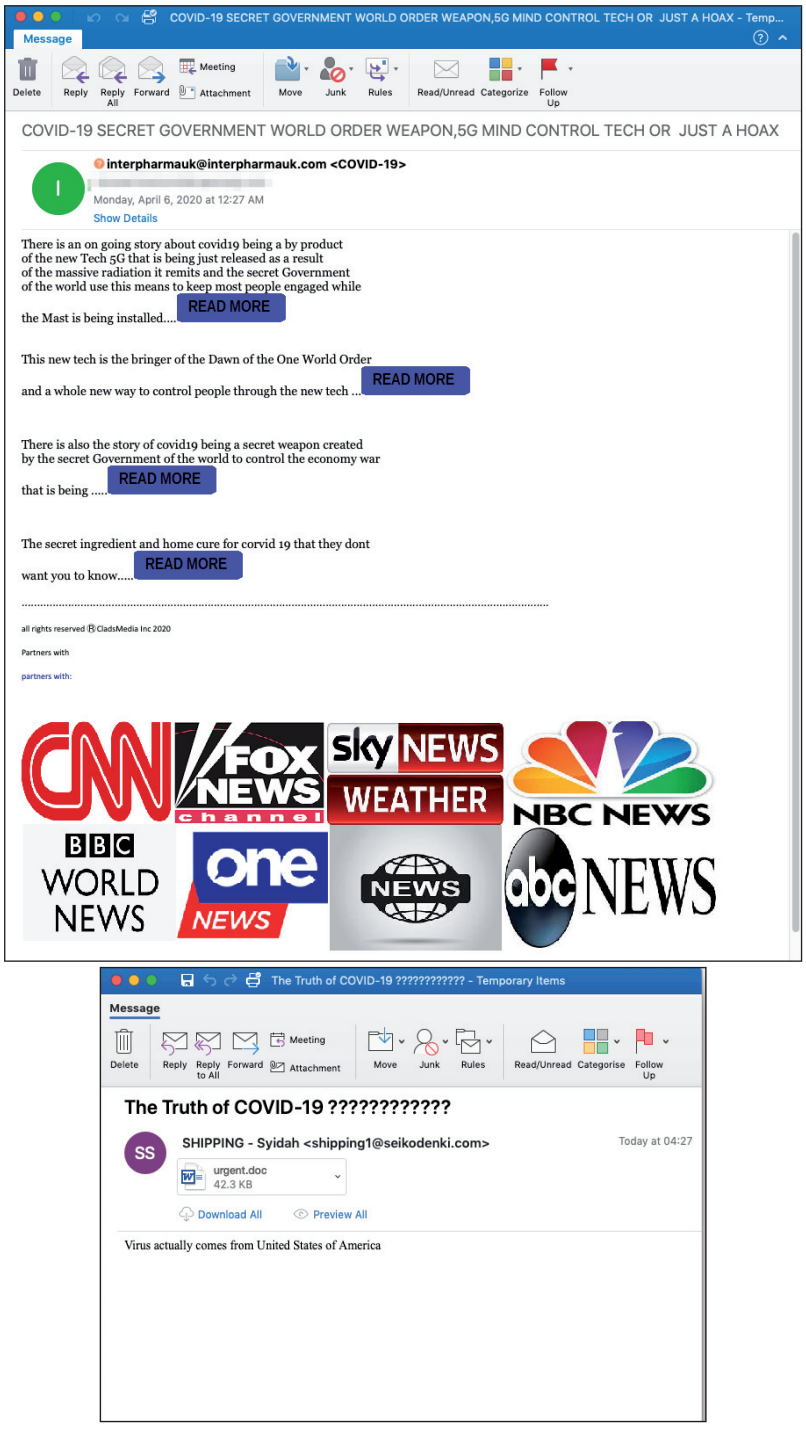


Figure 12: Conspiracy-themed credential theft (above) and malware (below) campaigns.

The number of credential harvesting or malware campaigns associated with conspiracy theories was lower than any other theme identified by researchers, and conspiracy themes were not used for long periods of time. This suggests the conspiracy themes were not effective lures and did not prompt consistent engagement from the victims. This is likely because it was easier to leverage the conspiracy theme early, due to a lot of uncertainty and misinformation distributed in the public sphere, but as people began to get a handle on the implications of the COVID-19 virus, conspiracy theories as email lures became less convincing.

APT actors

TA406, an actor aligned with the Democratic People's Republic of North Korea (DPRK) [6], was the first advanced persistent threat (APT) actor in *Proofpoint* data to use coronavirus themes, appearing before nearly every other criminal or APT in February 2020.

Figure 13: TA406 government-themed website purporting to distribute COVID-19 information impacting the Korean peninsula.

Soon after, TA413, a Chinese APT, began using COVID-19 themes as well. In March 2020, *Proofpoint* observed multiple emails with malicious RTF attachments sent to European diplomatic and economic entities. The messages impersonated WHO and contained purported information about state preparedness and response to the COVID-19 pandemic.

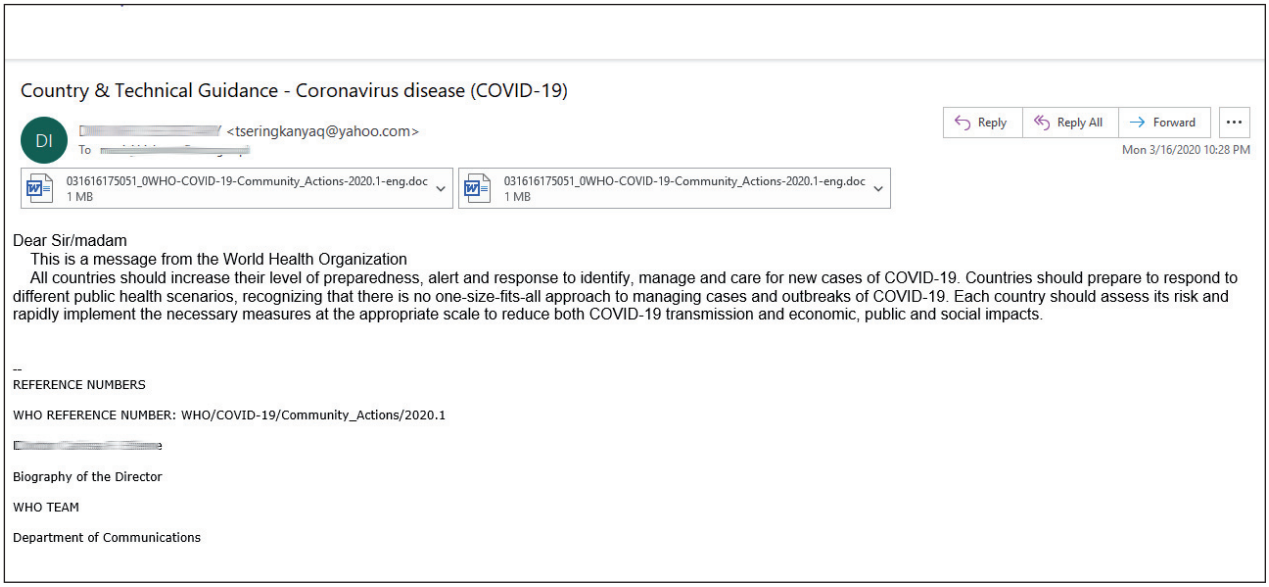


Figure 14: TA413 phishing email.

Proofpoint previously published details on this threat [7].

Proofpoint researchers also observed TA407, also known as Silent Librarian [8], leveraging COVID-19 themes in 2020. In May, *Proofpoint* identified a TA407 campaign targeting universities. The actor distributed emails with subjects such as 'Protecting Yourself from COVID-19 Related Scams' with a claim there was a problem with a database. The message urged the recipient to click on the link to reactivate their account. The email further claimed failure to do so would result in account access being permanently lost.

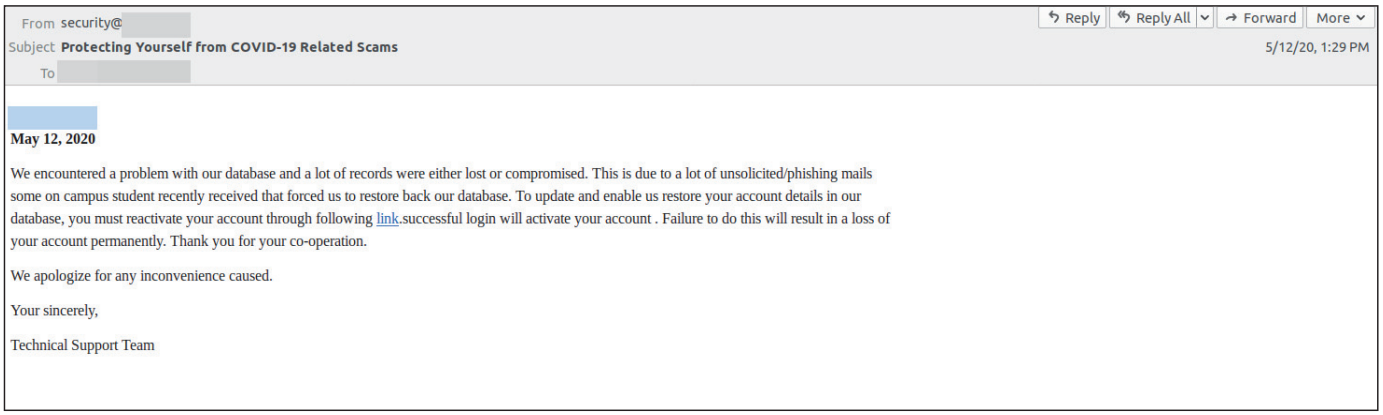


Figure 15: TA407 COVID-19 themed lure.

TA407 conducted multiple similar campaigns in the summer of 2020.

2021

2021 saw the second full year of the global pandemic, and although it remained at the forefront of most people's minds, threat actors used pandemic themes considerably less compared to 2020. The total number of COVID-19 campaigns in 2021 was approximately 40% of the number of pandemic-related campaigns the year prior. Threat actor use of COVID-19 themes in 2021 appeared mainly driven by mainstream narratives around vaccines, corporate responses to vaccines and masks, and the Delta and Omicron variants.

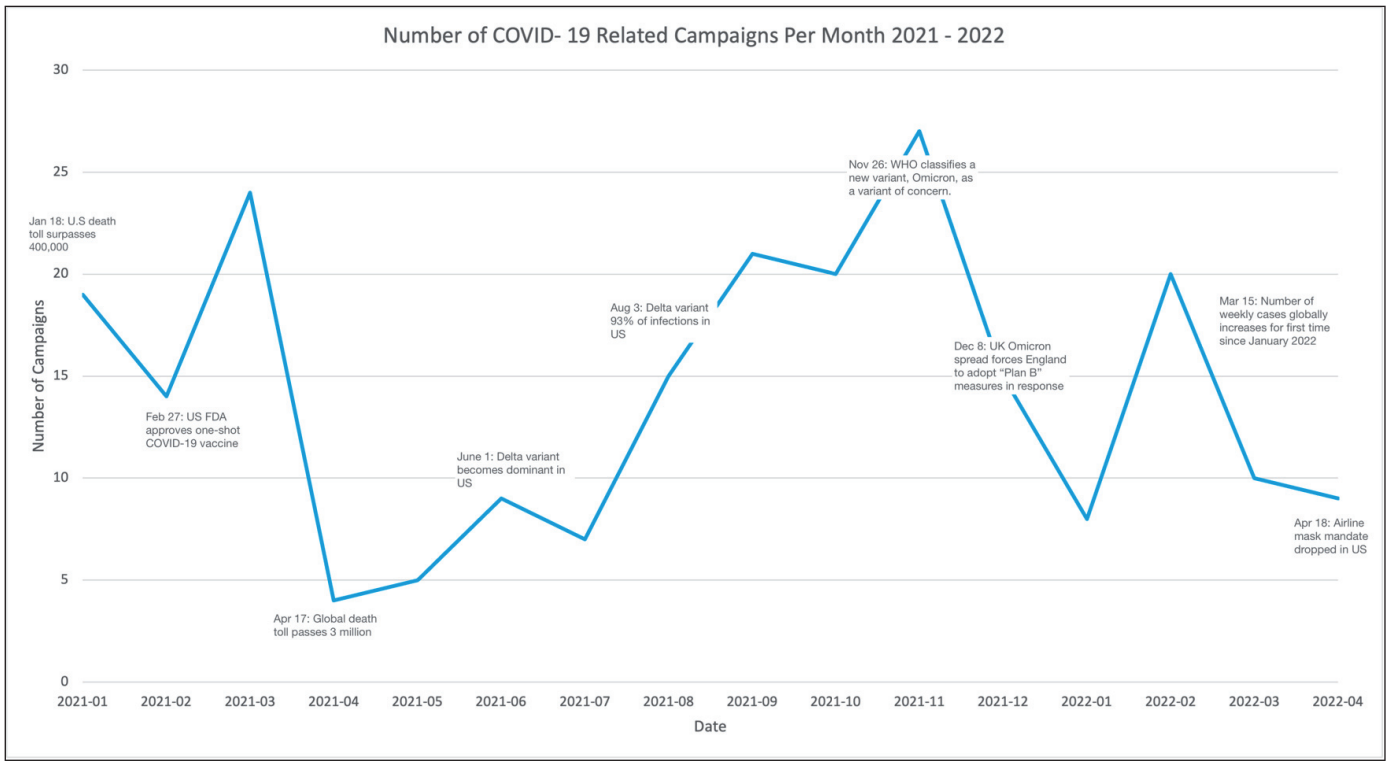


Figure 16: COVID-19 campaign data from 2021 to April 2022. COVID-19 timeline data pulled from the US Center for Disease Control and Prevention [2], the United Kingdom think tank Institute for Government [3], the World Health Organization [9], and the New York Times [10].

The drop in the number of COVID-19-related campaigns from 2020 to 2021 is likely due to public reporting and user education. People became more aware of threat actors using COVID-19 themes for malicious activities, and thus they became less effective.

On average, *Proofpoint* observed over six million COVID-19-related threats per day through 2021. Spikes in COVID-19 themes occurred when new variants were announced, specifically Delta and Omicron in the summer and autumn, respectively.

Cybercriminal actors

January 2021 kicked off with a high-volume campaign spoofing the WHO, an organization commonly used by threat actors associated with COVID-19 themes. The messages contained a URL which led to a fake WHO authentication page designed to harvest user credentials. After POST action the user was redirected to a login page on careers[.]who[.]int.

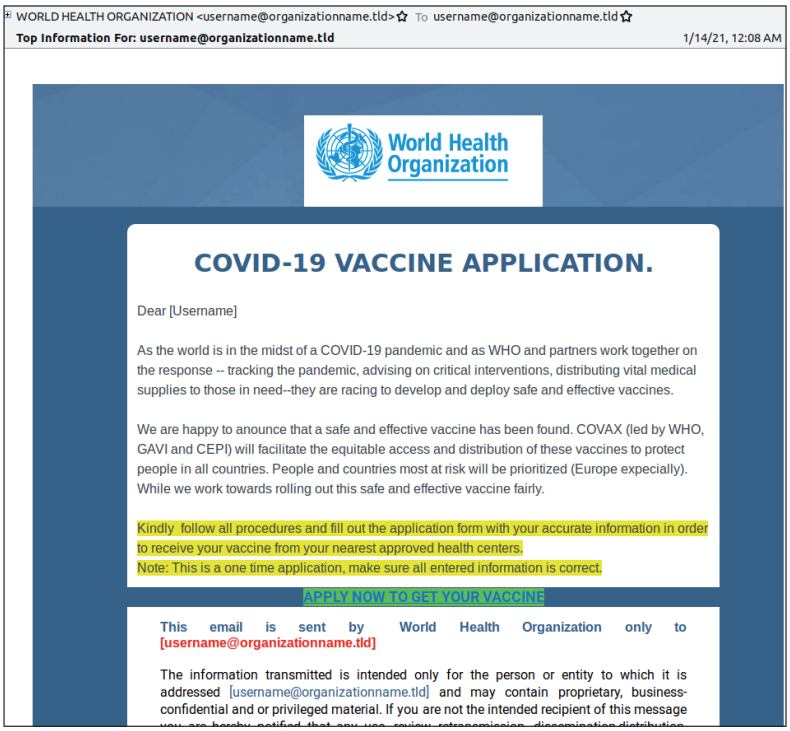


Figure 17: WHO-themed lure.

Throughout the pandemic, threat actors used legitimate health and safety organizations to add authenticity to their lures. From January 2020 to April 2022 approximately 12% of campaigned threats using COVID-19 themes spoofed the US Center for Disease Control and Prevention (CDC) or the WHO.

In many cases, threat actors would include the names or addresses of legitimate organization employees or resources to further convince a recipient the email was legitimate. For example, in October 2021, researchers identified an email threat masquerading as the CDC with the organization's legitimate Atlanta, Georgia address in the email body. The attachments were *Excel* documents containing macros which, if enabled, downloaded Cobalt Strike.

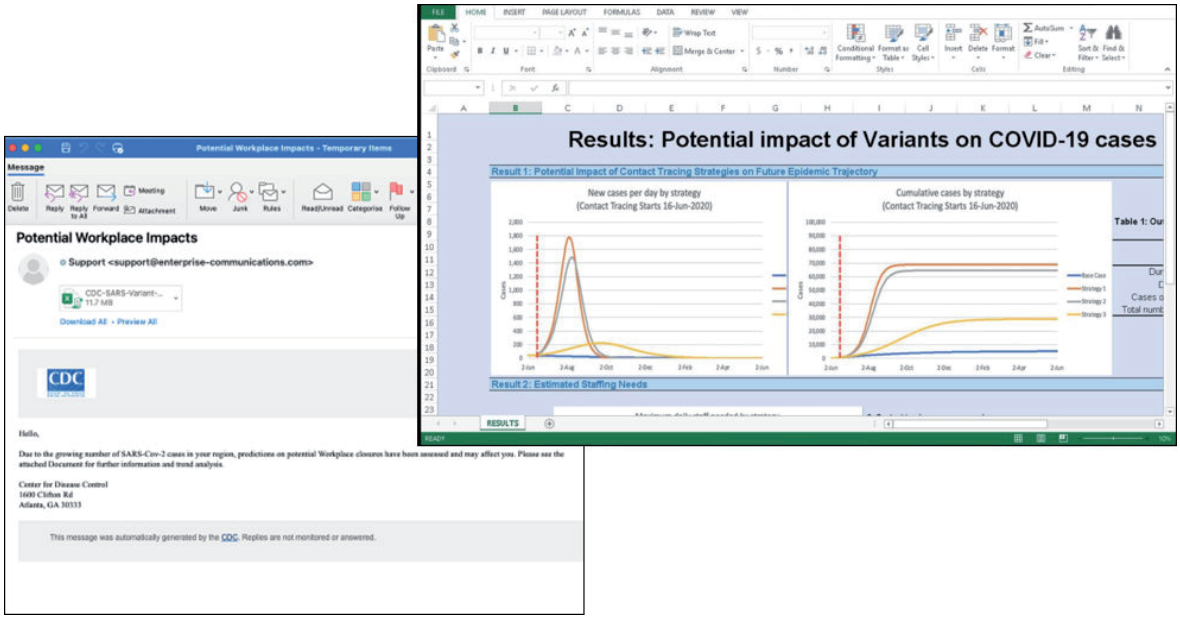


Figure 18: Email threat masquerading as the CDC with an Atlanta mailing address.

Notably, themes related to the spread of COVID-19, while popular at the beginning of the pandemic, fell between May 2020 and May 2021. However, with the appearance of the Delta variant and its rise to become the dominant variant in the US in June 2021, threat actors pivoted once more to using COVID-19 emails purporting to contain information about the spread of the virus, including potential infection rates.

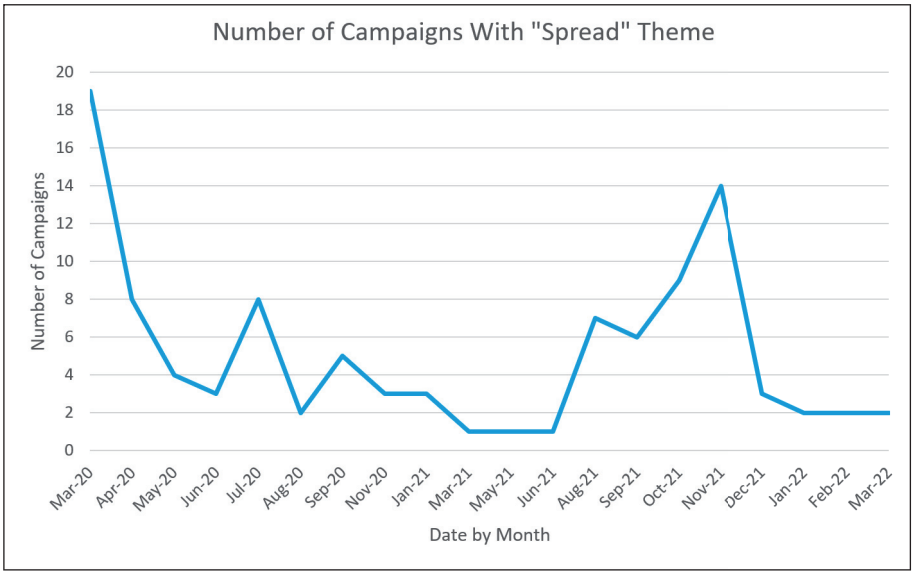


Figure 19: Number of COVID-19 campaigns using a theme related to virus spread.

For example, *Proofpoint* researchers identified a campaign in late May 2021 with messages that claimed a friend or relative had recently tested positive for COVID-19 and was using an application to notify their contacts. These messages contained a *Dropbox* URL which led to the BitRAT malware.

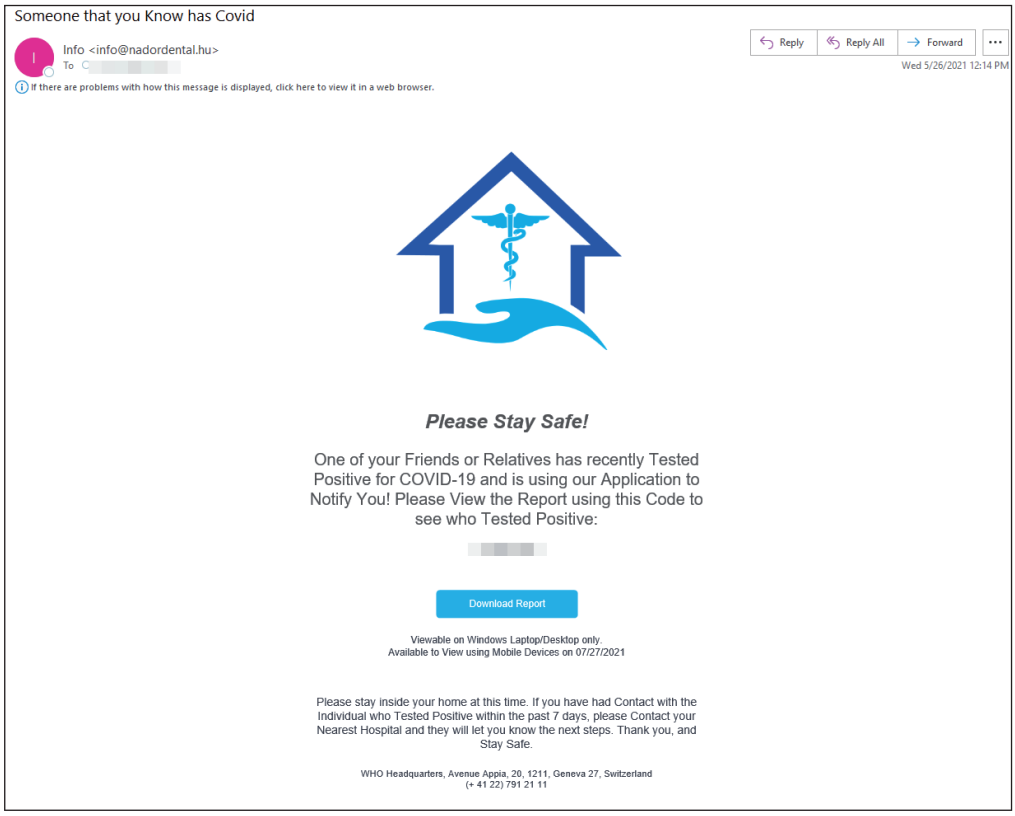


Figure 20: Email lure distributing BitRAT malware.

In September 2021, *Proofpoint* identified TA3546, also known as FIN7, leveraging COVID-19 themes to distribute the GRIFFON malware.

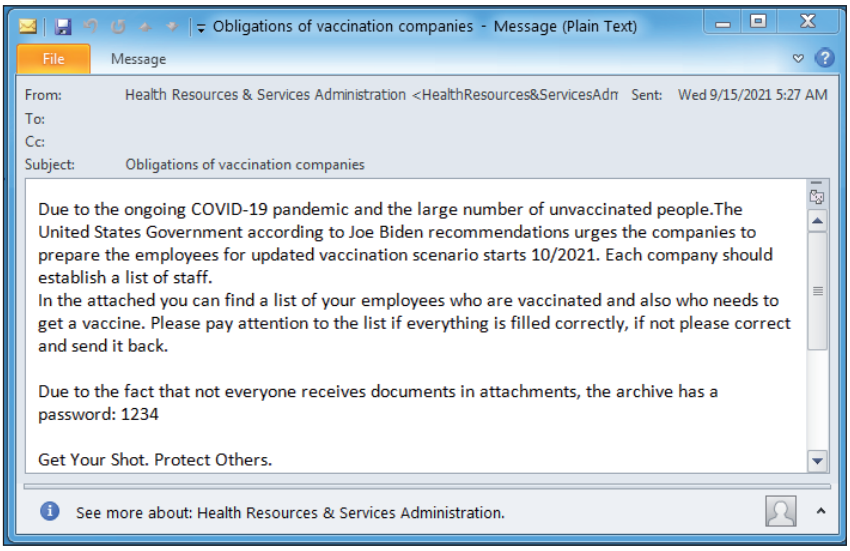


Figure 21: TA3546 lure.

The messages purported to be from a Health Resources & Services Administration. The messages contained zipped JavaScript attachments that installed the GRIFFON backdoor, which downloads additional code for system profiling.

From autumn to late 2021, *Proofpoint* researchers identified an increase in email threats targeting mostly North American universities attempting to steal university login credentials. The threats typically leveraged COVID-19 themes including testing information and the new Omicron variant.

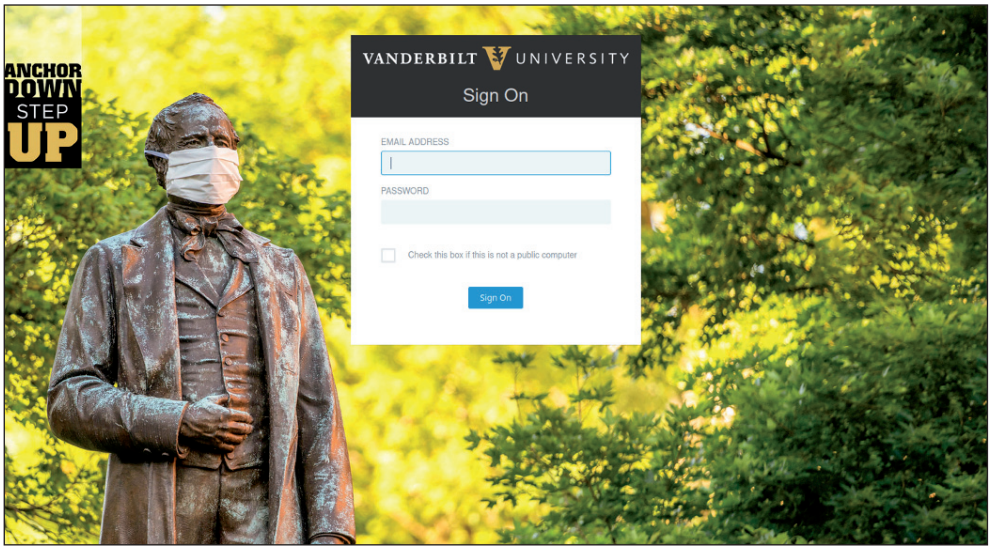


Figure 22: Credential capture portal spoofing a university web page.

The phishing emails contained attachments or URLs for pages intended to harvest credentials for university accounts. The landing pages typically imitated the university's official login portal, although some campaigns featured generic *Office 365* login portals [11].

APT actors

Proofpoint observed more APT actors leveraging COVID-19 themes in 2021 than 2020.

Early in 2021, *Proofpoint* researchers observed the Iran-aligned APT actor TA451 (APT33) using COVID-themed lures in a phishing campaign against a US defence contractor. Masquerading as the WHO, the actor delivered malicious emails with a link to a COVID19tracker[.]exe file. The executable reached out to download a batch script (iehchecker[.]bat) that downloaded a PowerShell script (Update-KB4524147[.]ps1) with reverse shell capabilities.

By late 2021, *Proofpoint* researchers had observed several more APT actors using COVID lures in their campaigns. The Russia state-sponsored TA421, publicly known as APT29, targeted various government entities worldwide with COVID lures that delivered an HTML which constructed an ISO file that ultimately led to the delivery of Cobalt Strike.

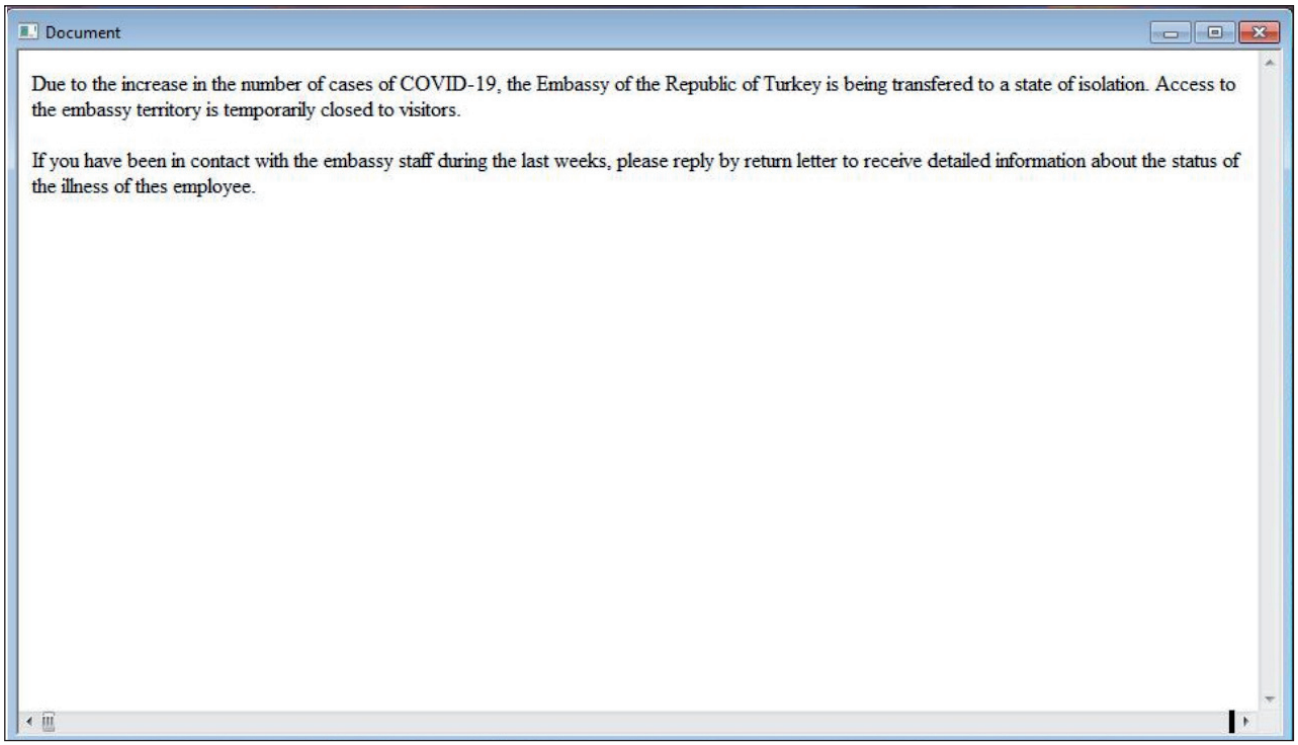


Figure 23: TA421 lure document.

Meanwhile, the Iran-aligned TA456, also known as Tortoiseshell, used Omicron COVID-19-themed emails in reconnaissance and profiling campaigns targeting academics. And, in yet another campaign, an Indian APT actor, tracked by *Proofpoint* as TA425, distributed emails with a COVID-19 booster shot lure targeting users in Pakistan. The landing page in this campaign impersonated the Pakistani National Immunization Management System and hosted a password-protected macro-laden *Excel* file which dropped *xRAT* – a legitimate remote administration tool.

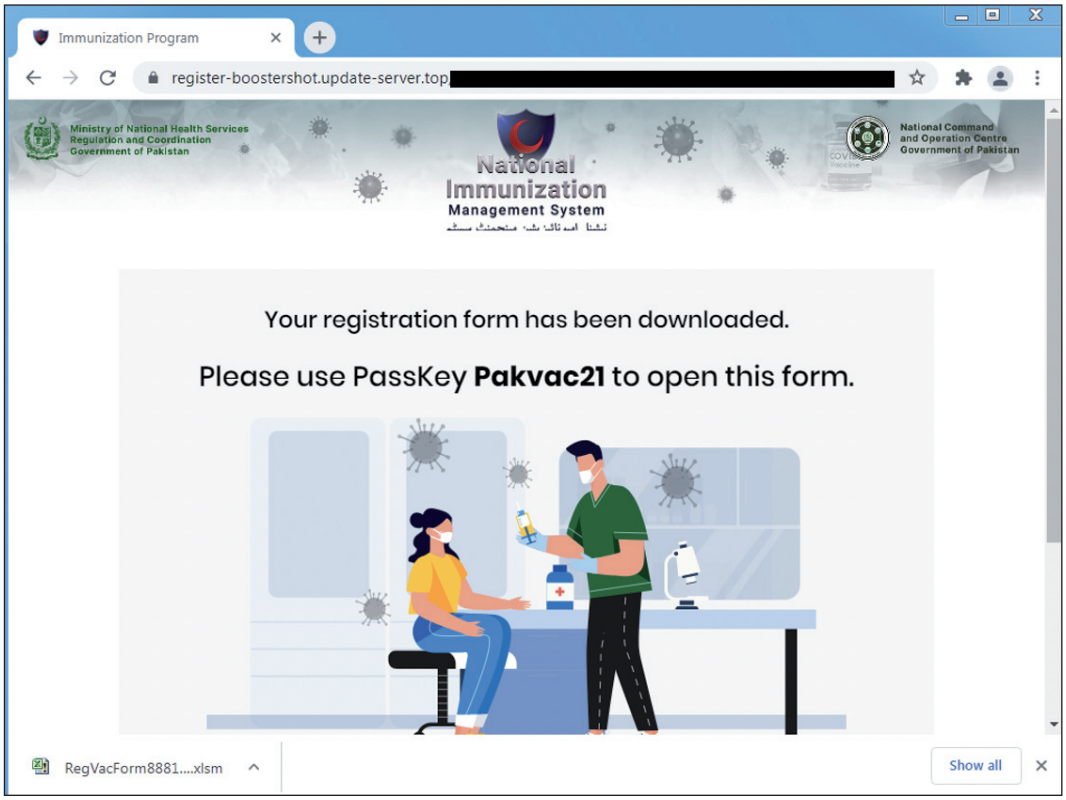


Figure 24: Landing page spoofing Pakistani National Immunization Management System.

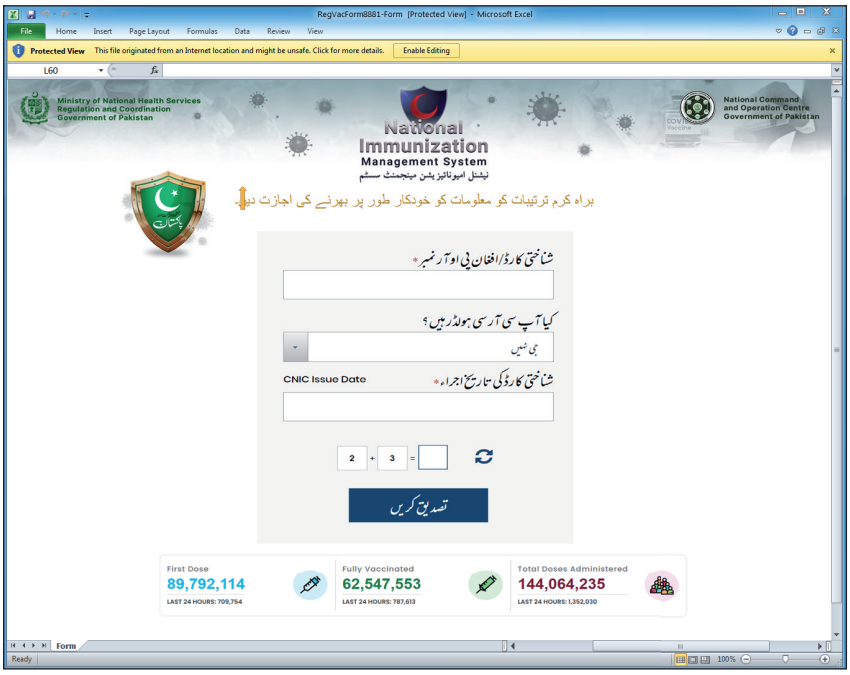


Figure 25: Macro-laden Excel document used to download and execute xRAT.

In November 2021, TA406 revisited COVID-19 themes, with messages containing the subject 'Article on DPRK during COVID-19'. The messages contained links to an attacker-controlled domain likely used for credential harvesting.

2022

As the world entered the third year of the pandemic, threat actors continued to use it in social engineering. The total number of campaigns in the first quarter of 2022 equalled the average number of campaigns per quarter in 2021.

Cybercriminal actors

The most commonly used themes were company operations and generic themes, meaning the threat actor did not include specific references to things like vaccines, spread, or other specific information. Threat actors may just use the terms 'COVID-19' or 'coronavirus' in the email subject with either blank email bodies, or language unrelated to the subject line.

For example, in one credential phishing campaign researchers identified the following message examples:

```
Sender: "Covid-I3S10256246_[RECIPIENT]" <no-reply@castodia[.]awsapps[.]com>
Subject: Early Covid22 Updated Request Processed on Tuesday, January 25, 2022
```

The emails with COVID-themed lures contained attachments designed to harvest credentials for *Adobe Cloud* accounts. After harvesting the credentials, victims were redirected to the Johns Hopkins Coronavirus resource centre.

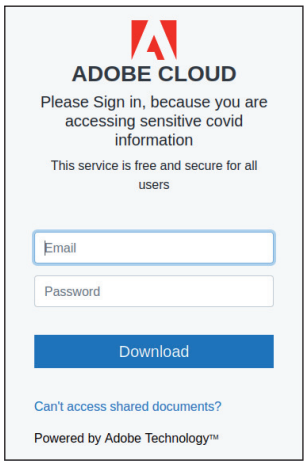


Figure 26: Adobe credential capture portal with generic COVID-19 theme.

The most notable actor leveraging COVID-19 themes so far in 2022 has been TA542, Emotet. After the first Emotet campaign back in January 2020 using COVID-19 themes, Emotet did not return to the pandemic lure themes until February 2022.

In early February, *Proofpoint* researchers identified an Emotet campaign leveraging *Excel* attachments or password-protected zipped attachments containing *Excel* documents. The *Microsoft Office* files contained macros which, if enabled, would download and install Emotet. The messages were replies to existing threads and contained 'Covid results' as attachment themes.

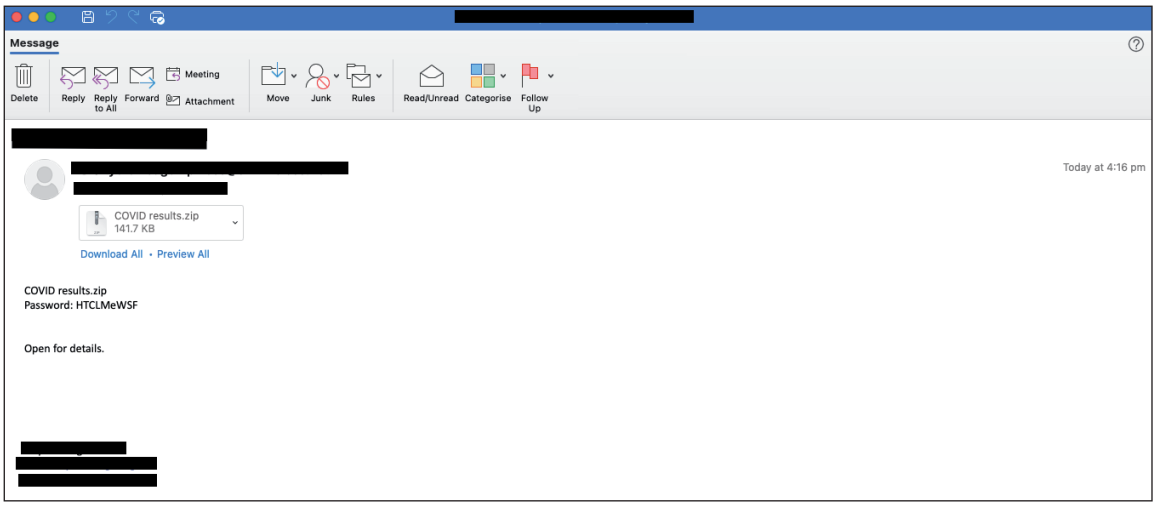


Figure 27: Sample Emotet COVID-19 theme lure.

Between January and April 2022, 13% of Emotet campaigns used COVID-19-themed lures. All these campaigns occurred between February and March 2022, making up nearly a quarter of all Emotet campaigns in this time.

Although not as prominent as 2020, threat actors did use travel themes more in 2022 than 2021, in addition to pass themes. For example, in February 2022, *Proofpoint* researchers identified credential theft campaigns using 'Covid Passport' lures containing HTML attachments that redirect to a *Microsoft* credential harvesting page protected by a *Google* CAPTCHA.

In March 2022, *Proofpoint* also observed the threat actor TA558 – which typically uses travel reservation theme lures to target travel and hospitality organizations – leveraging a COVID-19 theme. This actor used virus-related messages inconsistently in 2020 to 2021.

The Spanish language messages purported to relate to a hotel reservation that had been cancelled due to a positive COVID-19 test. These messages contained URLs which downloaded a macro-enabled *Microsoft Publisher* file (requiring *Publisher 2016* or higher), which led ultimately to the installation of AsyncRAT.

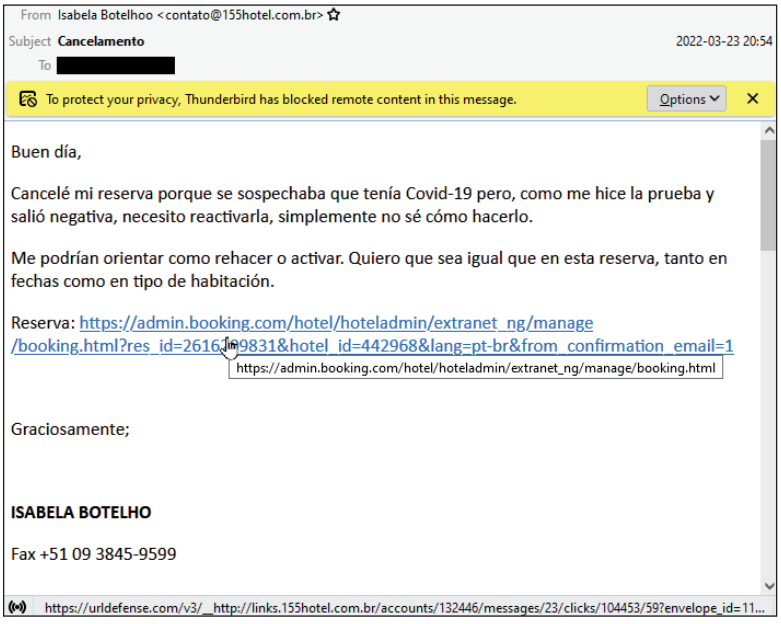


Figure 28: TA558 lure using a COVID-19 travel theme.

The global relevance of COVID-19 continued to show itself in lure themes. In April, *Proofpoint* identified emails with Spanish language COVID-19 vaccine lures, masquerading as the Spanish Ministry of Health, distributing the Bizarro Banker via links to a zipped MSI file. The emails were geofenced to Spain.

Figure 29: COVID-19 vaccine theme distributing the Bizarro Banker.

APT actors

The number of APT actors leveraging COVID-19 themes dropped significantly in the first quarter of 2022. *Proofpoint* identified TA416 [12] distributing COVID-19 digital certificate themes. The messages were sent to European diplomatic organizations.

CREDENTIAL PHISHING VS MALWARE

Proofpoint identified more than twice as many COVID-19-themed threats distributing malware compared to credential theft campaigns. Overall, 29% of threats were credential phishing, while 71% were malware.

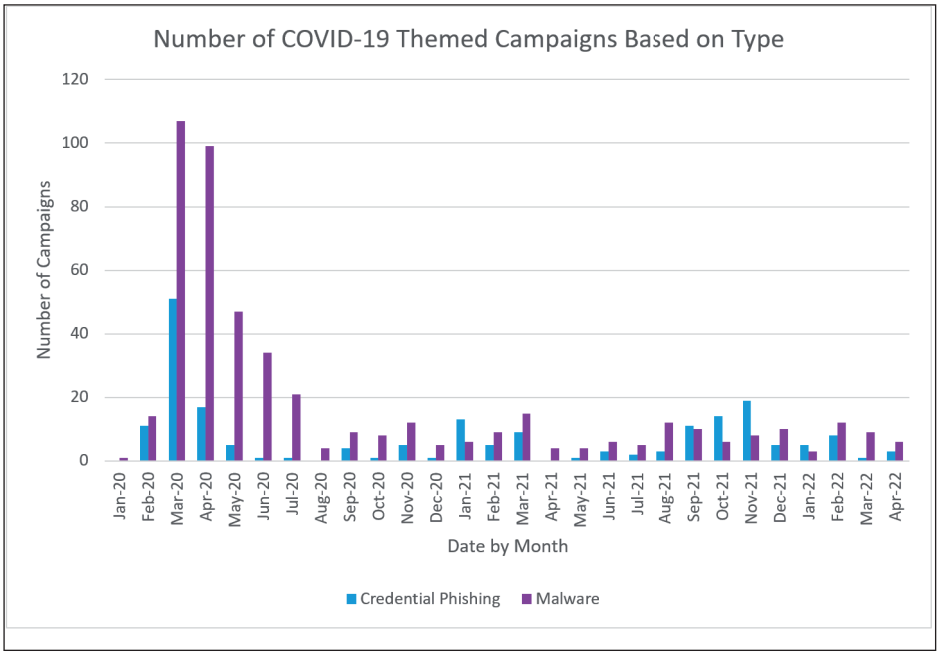


Figure 30: Total number of COVID-19-themed campaigns based on threat type.

However, in two theme categories – company operations and economic impacts – the total number of credential theft campaigns reached near parity to malware. The economic themes included messages pertaining to governmental financial aid and other economic support incentives.

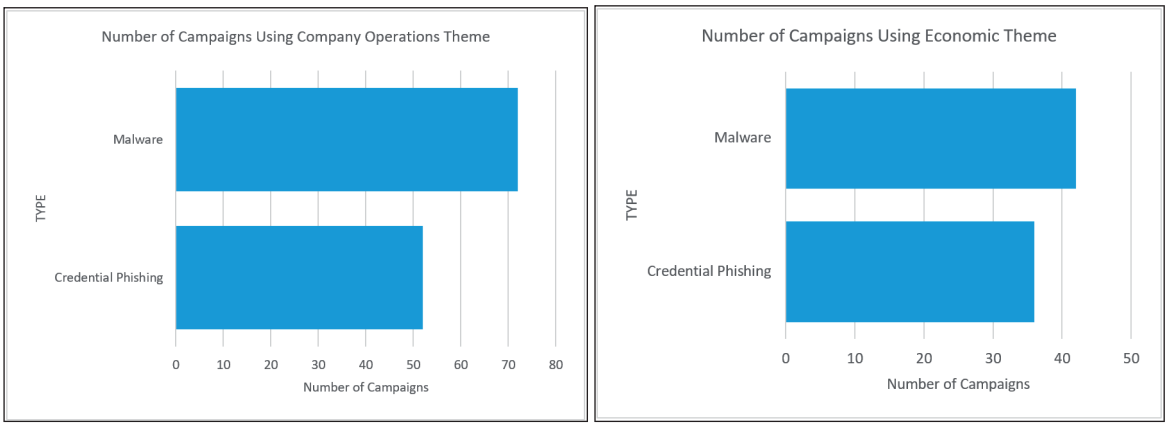


Figure 31: Number of credential phishing and malware campaigns for company operations and economic themes.

These results are not surprising. Most of the credential phishing threats associated with these themes attempted to steal credentials for corporate accounts including *O365* or personal or corporate banking credential information. Leveraging government programmes as lure themes related to business continuity and financial support are likely compelling and effective lures for credential theft as information typically must be shared in order to benefit from these types of programmes.

In one example, *Proofpoint* identified a credential phishing campaign purporting to be the US Small Business Administration (SBA) COVID-19 relief program. The messages contained a URL which led to a fake *DocuSign*-themed authentication page designed to harvest user credentials.

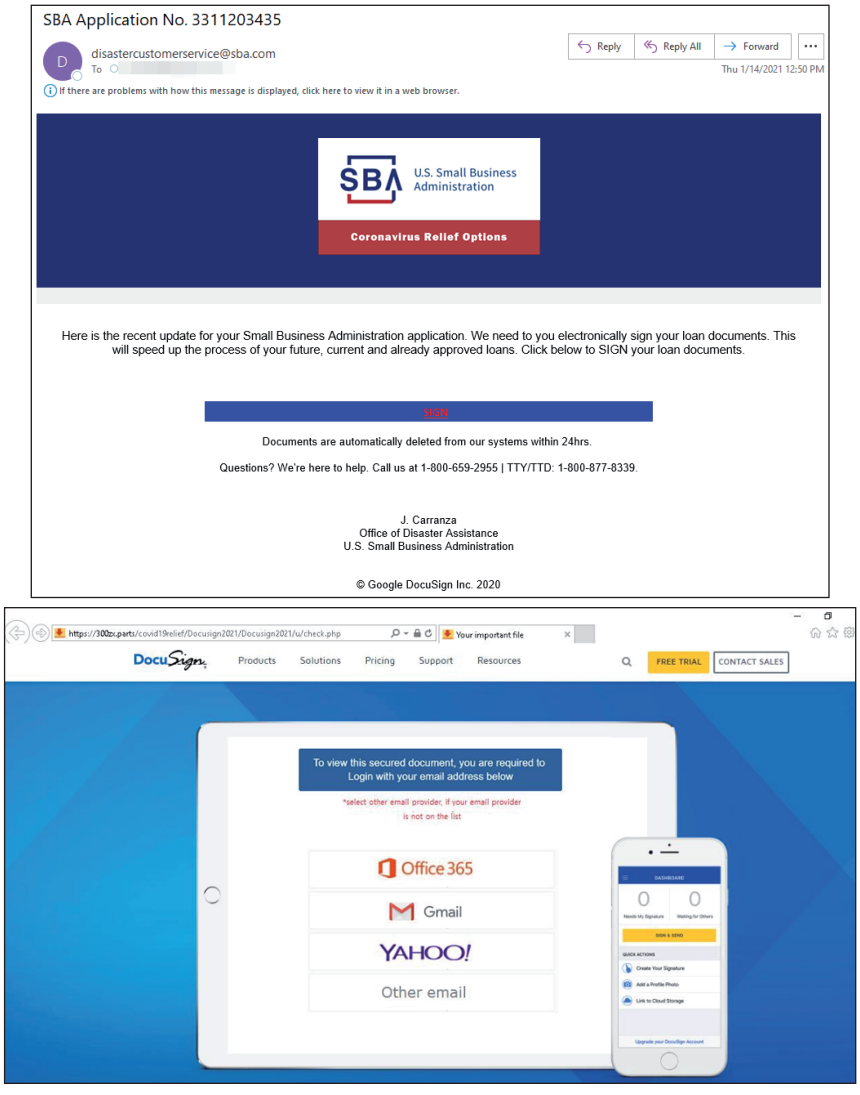


Figure 32: SBA theme lure and credential capture portal.

LURE EFFICACY

Proofpoint assessed the most effective lure types – or which themes generated the most engagement with recipients – based on click rate. That is, at least one recipient engaging in some way with the identified threat.

Based on available data, company operations themes had the highest click rate. These threats made up nearly 18% of the total themes overall, but nearly 30% of the average click rate. The generic theme (non-specific references to the virus) and economic theme (threats related to finances, aid, or bonuses) had higher click rates than threats related to safety and spread of the virus, despite comparatively making up a lower percentage of the overall COVID-19 threat landscape.

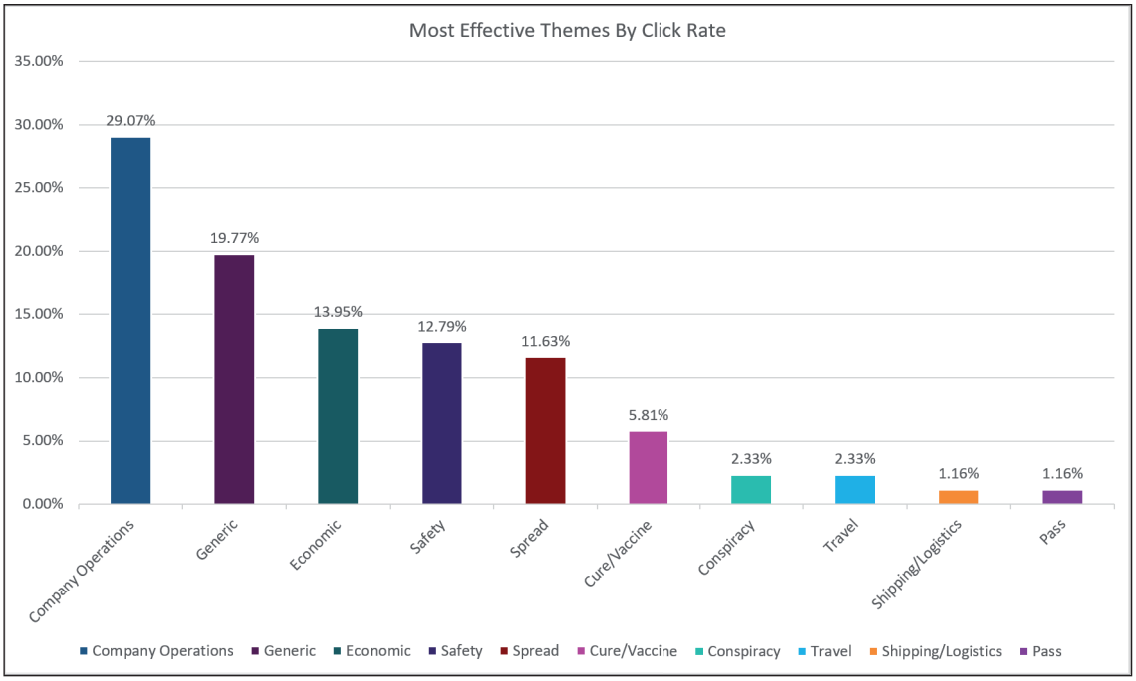
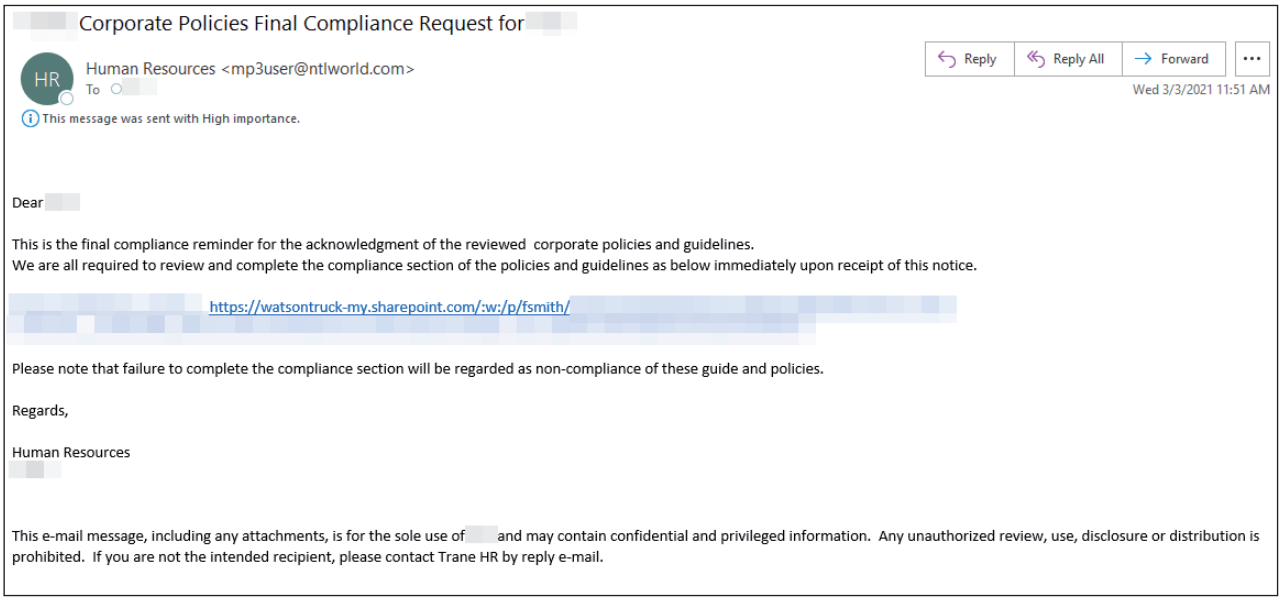


Figure 33: Most effective lures by click rate.

Of the total number of threats that included click rate data, 42% of them were credential phishing campaigns while 58% were malware. As noted above, a greater disparity existed between threat types overall. This suggests credential phishing campaigns were more likely to convince a recipient to engage with them than malware campaigns.

A good example of effective company operations themed credential phishing is the following March 2021 campaign. The messages contained a *SharePoint* URL purporting to host a document related to corporate policy and guidelines on COVID-19.


Corporate Policies Final Compliance Request for

HR Human Resources <mp3user@ntlworld.com>
To

Reply | Reply All | Forward | ...
Wed 3/3/2021 11:51 AM

This message was sent with High importance.

Dear

This is the final compliance reminder for the acknowledgment of the reviewed corporate policies and guidelines.
We are all required to review and complete the compliance section of the policies and guidelines as below immediately upon receipt of this notice.

https://watsontruck-my.sharepoint.com/:w:/p/fsmith/

Please note that failure to complete the compliance section will be regarded as non-compliance of these guide and policies.

Regards,

Human Resources

This e-mail message, including any attachments, is for the sole use of and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Trane HR by reply e-mail.

Figure 34: Company operations themed COVID-19 credential phishing email.

The document contained a link which led to a fake *Microsoft* authentication page designed to harvest user credentials. This campaign had a 56% click rate.

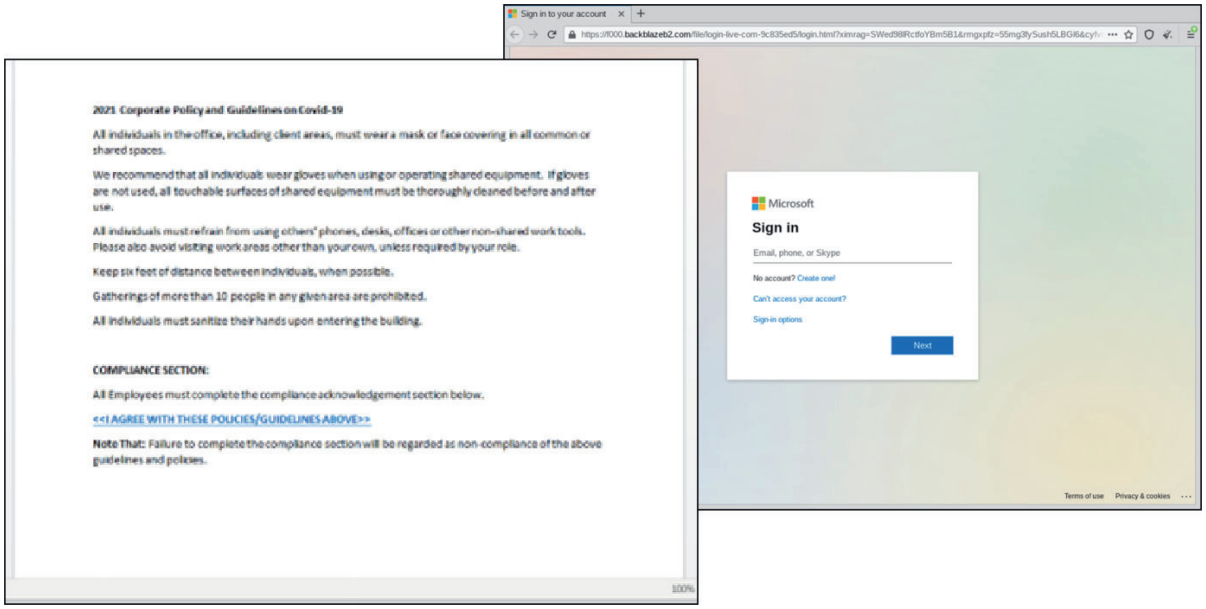


Figure 35: COVID-19 themed Word document and spoofed Microsoft credential capture web page.

Of the tracked threat actors that consistently used COVID-19 themes over time and demonstrated consistent click rates, TA2722 frequently demonstrated effective message lures that enticed recipients to engage with the content of the email.

The threat actor TA2722 [13], which *Proofpoint* identified in 2021, used COVID-19 themes throughout 2021 and 2022 in both credential theft and malware campaigns. Toward the end of 2021 and in early 2022, the actor focused on credential theft campaigns using COVID-19-themes referring to the spread of the virus, using URLs in the email body leading to credential capture web pages spoofing the Philippines government. In March 2022, the actor returned to distributing the Remcos and Nanocore remote access trojans (RATs) via URLs using multiple themes including COVID-19 vaccine certificates purporting to be from the Philippines Department of Health.

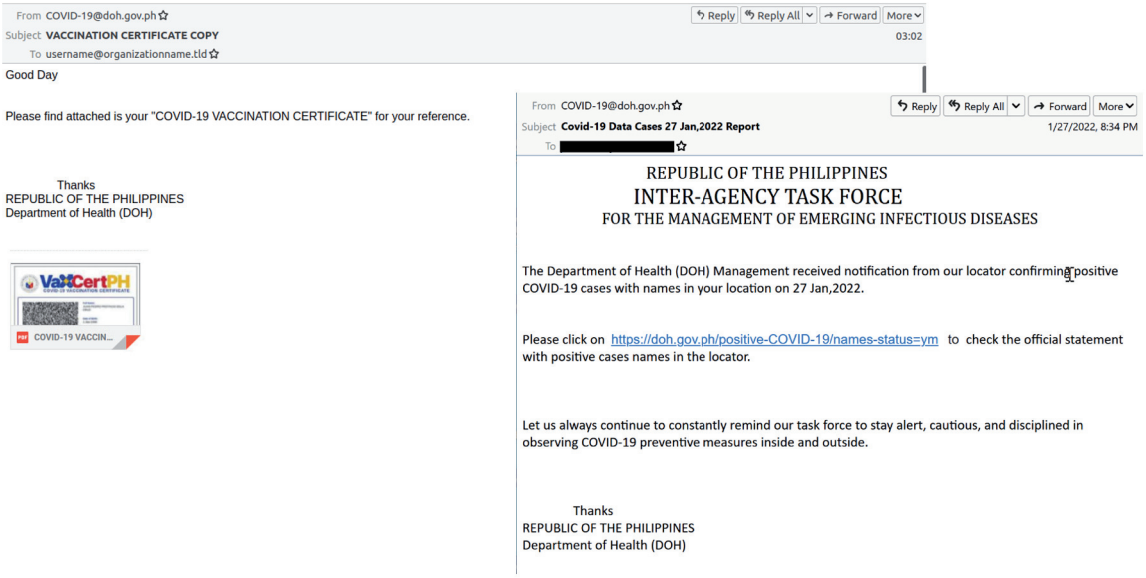


Figure 36: TA2722 lures including vaccine certificate to distribute malware (left) and credential harvesting (right).

On average, TA2722 demonstrates a 21% click rate while using COVID-19 themes and masquerading as an official government entity. When this group uses themes other than COVID-19, the click rate is 13%.

Of APT actors with the most clickable lures, TA407, also known as Silent Librarian, demonstrated the highest click rate. In the following 2020 credential phishing example, the threat actor used subjects such as 'Notice on Overdue Items' or 'Important notice', which contained a URL leading to a credential harvesting attempt. It appeared to be coming from a

spoofed or compromised university account. The message noted the university library had changed its loan policies in response to COVID-19.

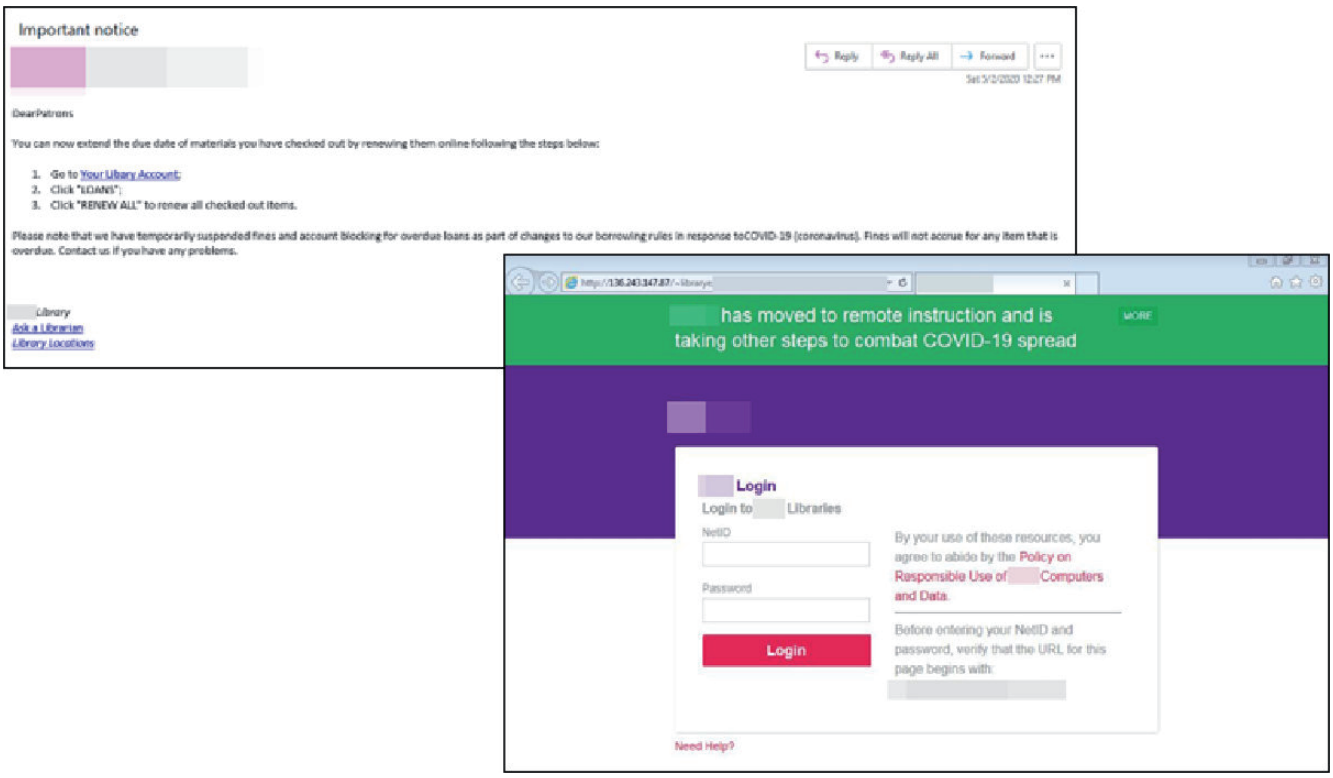


Figure 37: TA407 lure and credential capture portal.

This campaign had a 76% click rate.

CONCLUSION

In conclusion, the evidence provided demonstrates multiple key takeaways for defenders and decision-makers:

- Threat actors are inherently opportunistic and will pivot to make use of what is perceived to be effective. The more relevant a topic is to a certain victim population, the greater the likelihood an actor targeting that population will attempt to exploit it. In the case of COVID-19, this was the entire world.
- Regardless of whether an actor's objective was to perpetrate small- or large-scale crime, espionage, or support other nation-state goals, COVID-19 provided a favourable backdrop by which to initiate operations.
- COVID-19 impacted many spheres of personal and business relevance and threat actors were extremely versatile in their attempts to deliver social engineering content speaking to disruptions in essentially all of these spaces.
- People are more likely to interact with content that is related to their company operations, including business continuity, human resources policies, or remote work programmes.
- Threat actors responded to major events in the COVID-19 pandemic including announcements of economic incentive programmes and new variants with high infection rates, and incorporated these themes into message lures.
- Credential capture threats that mirror legitimate login portals from *Microsoft* and other organizations are effective at garnering engagement.
- Based on click rate data, content using COVID-19 themes was more compelling than other lure types.

Finally, we cannot properly call this paper a post-mortem as we are, globally, still dealing with new waves of COVID-19 and a variety of after effects. Threat actors continue to leverage COVID-19-related themes regularly in the delivery stage of their campaigns. It should be assumed that threat actors will continue attempting to capitalize on the topic for as long as it stays socially relevant.

In the larger picture, defenders must recognize the diversity and creativity displayed by an entire ecosystem of cybercriminals and state-aligned actors and use that to understand the current social engineering paradigm serving as the initial vector for the vast majority of cyber attacks every day.

REFERENCES

[1] World Health Organization. WHO Director-General's opening remarks at the media briefing on COVID-19. 11 March 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.

[2] U.S. Centers For Disease Control and Prevention. CDC Museum COVID-19 Timeline. https://www.cdc.gov/museum/timeline/covid19.html.

[3] Institute for Government. Timeline of UK Government Coronavirus Lockdowns and Restrictions. https://www.instituteforgovernment.org.uk/charts/uk-government-coronavirus-lockdowns.

[4] Long, H.; Van Dam, A. U.S. unemployment rate soars to 14.7 percent, the worst since the Depression era. The Washington Post. May 2020. https://www.washingtonpost.com/business/2020/05/08/april-2020-jobs-report/.

[5] Larson, S.; Wise, J. Charting TA2541's Flight. Proofpoint. February 2022. https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight.

[6] Huss, D.; Larson, S. Triple Threat: North Korea-Aligned TA406 Steals, Scams and Spies. Proofpoint. November 2021. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-threat-insight-paper-triple-threat-N-Korea-aligned-TA406-steals-scams-spies.pdf.

[7] Raggi, M.; Proofpoint Threat Research Team. Chinese APT TA413 Resumes Targeting of Tibet Following COVID-19 Themed Economic Espionage Campaign Delivering Sepulcher Malware Targeting Europe. Proofpoint. September 2020. https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic.

[8] The Proofpoint Threat Insight Team. Threat Actor Profile: TA407, the Silent Librarian. Proofpoint. October 2019. https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian.

[9] World Health Organization. Weekly epidemiological update on COVID-19. 15 March 2022. https://www.who.int/publications/m/item/weekly-epidemiological-update-on-covid-19---15-march-2022.

[10] Chokshi, N.; Murphy, H. For Airlines, the Mask Mandate Couldn't End Soon Enough. New York Times. April 2022. https://www.nytimes.com/2022/04/19/business/mask-mandate-travel-transit.html.

[11] Larson, S.; G, J. University Targeted Credential Phishing Campaigns Use COVID-19, Omicron Themes. Proofpoint. December 2021. https://www.proofpoint.com/us/blog/threat-insight/university-targeted-credential-phishing-campaigns-use-covid-19-omicron-themes.

[12] Raggi, M.; Myrtus. The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates. Proofpoint. March 2022. https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european.

[13] Larson, S.; Wise, J. New Threat Actor Spoofs Philippine Government, COVID-19 Health Data in Widespread RAT Campaigns. Proofpoint. October 2021. https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread.