proofpoint.

Exploiting COVID-19: how threat actors hijacked a pandemic

Daniel Blackford & Selena Larson

Proofpoint

September 29, 2022

Daniel Blackford

Manager, Threat Research, Proofpoint

@dansomware

Selena Larson

Senior Threat Intelligence Analyst, Proofpoint

Focus: Targeted cybercrime

@selenalarson

proofpoint.

COVID-19 Threats: So What?

The COVID-19 pandemic created an environment primed for exploitation **like none witnessed** before

In analyzing **social engineering** during the COVID-19 pandemic, we can learn about how human behaviors can be **preyed upon by threat actors** during major global events, and **what methods were the most effective**

Report Methodology

- Based on 700 campaigns manually analyzed and contextualized by threat researchers
- Categorized by multiple variables such as threat type, impersonation, and themes
- Representative of a portion of the overall threat landscape

Themes

Safety: includes topics of personal protective equipment, sanitation, and governmental regulations around maintaining safe spaces

Cure/Vaccine: highlighting the development of vaccines, vaccine appointments, possible cures, etc

Spread: relating to the spread of the virus

Travel: focusing on the implications of COVID-19 on travel

Economic: centered around economic relief

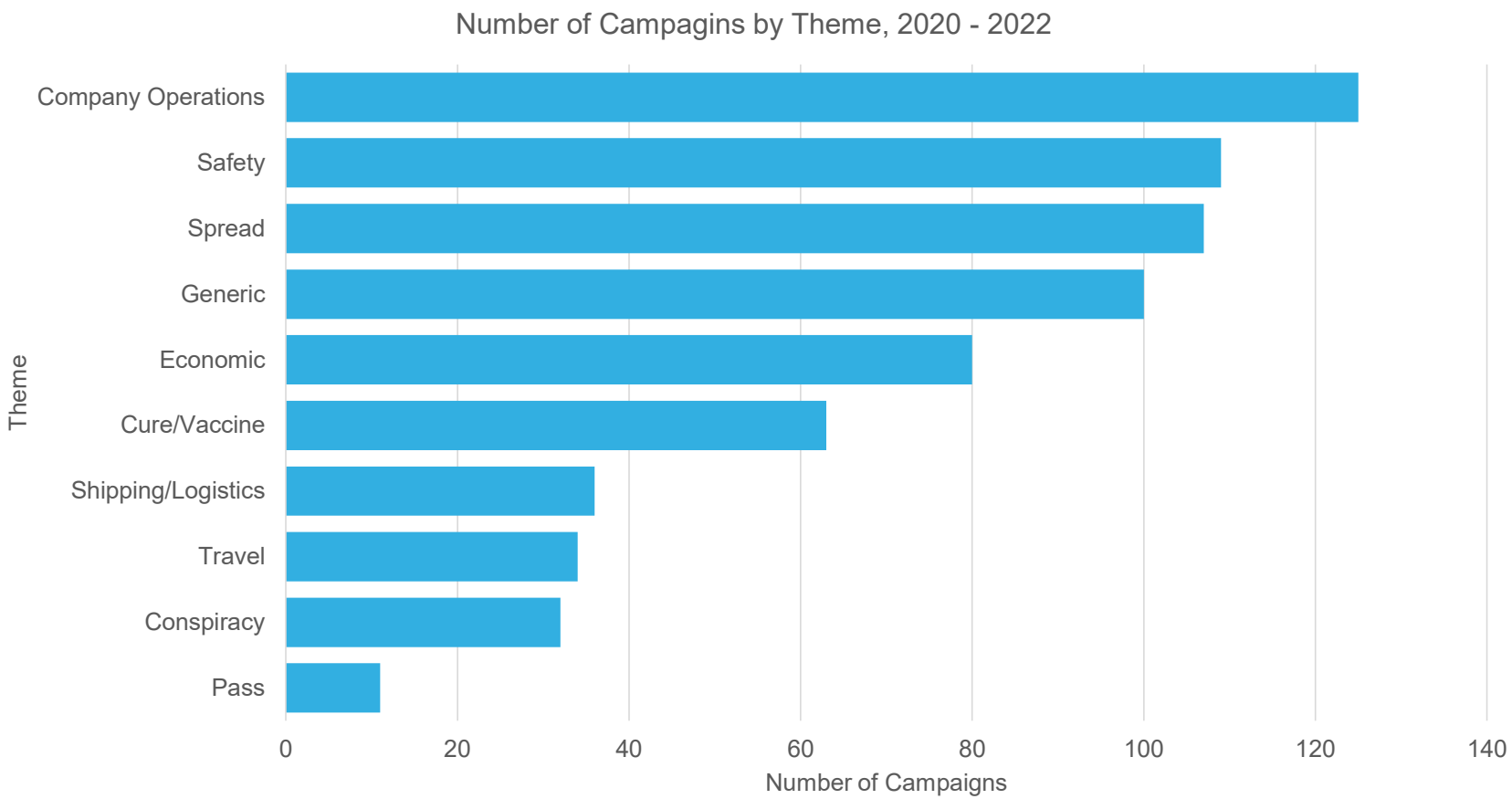
Shipping/Logistics: insinuating disruption to supply chain, manufacturing, or the transportation of goods

Conspiracies: pushing misinformation around the virus or development and distribution of vaccines

Pass: centered around proof of vaccination status by way of card or "passport."

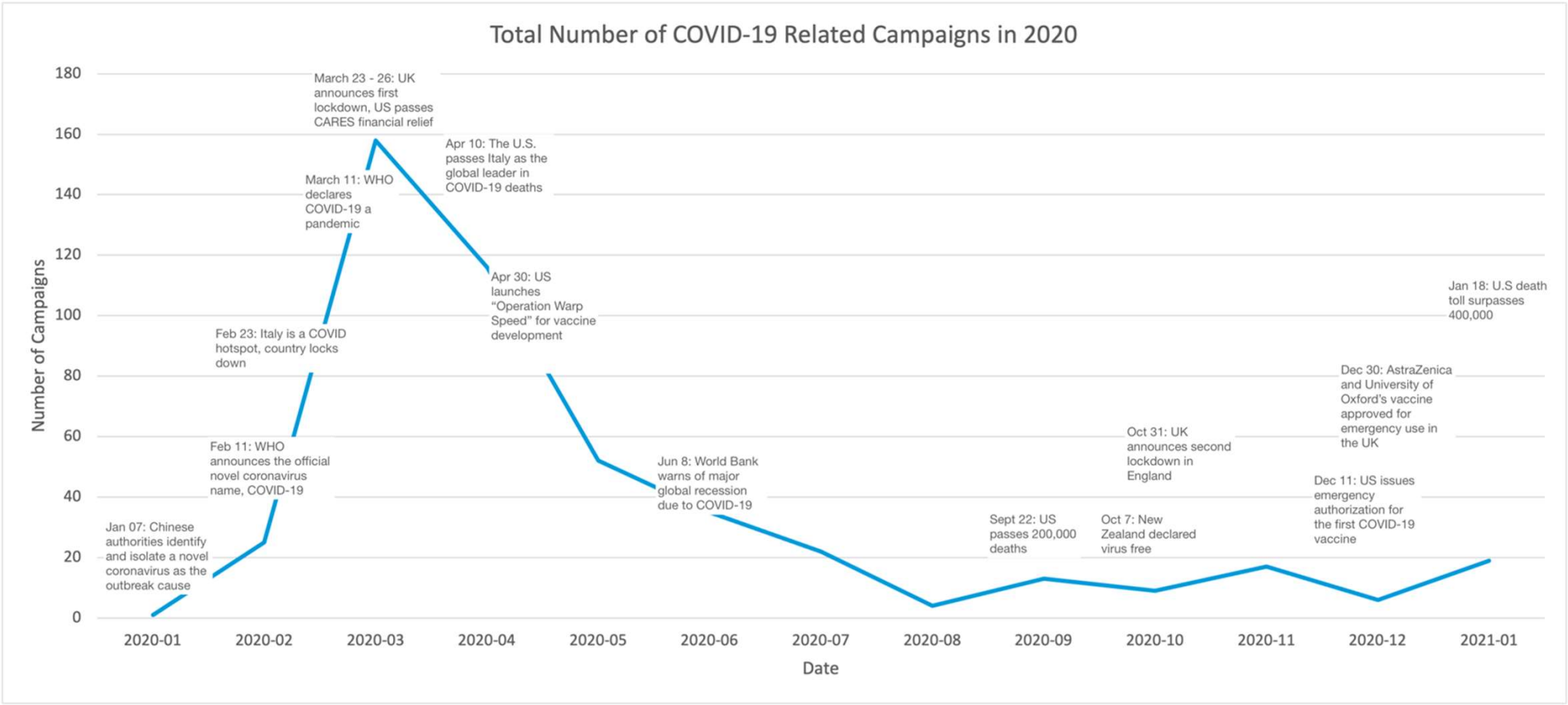
General: vague, generic, and/or did not fit into one of the above themes

Themes



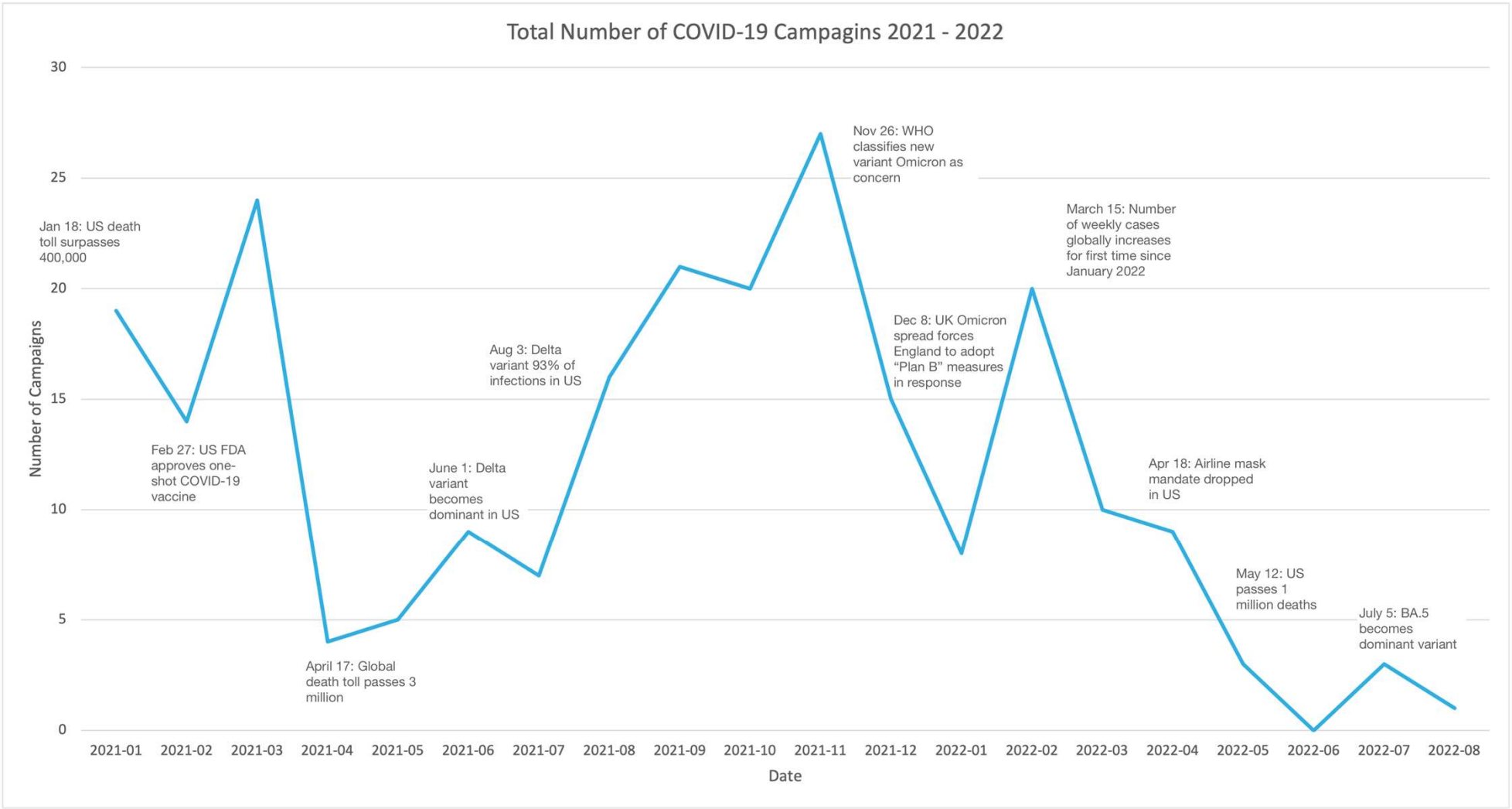
proofpoint.

Timeline



proofpoint.

Timeline


Total Number of COVID-19 Campagins 2021 - 2022
Number of Campaigns
Date
30
25
20
15
10
5
0
2021-01
2021-02
2021-03
2021-04
2021-05
2021-06
2021-07
2021-08
2021-09
2021-10
2021-11
2021-12
2022-01
2022-02
2022-03
2022-04
2022-05
2022-06
2022-07
2022-08
Jan 18: US death toll surpasses 400,000
Feb 27: US FDA approves one-shot COVID-19 vaccine
April 17: Global death toll passes 3 million
June 1: Delta variant becomes dominant in US
Aug 3: Delta variant 93% of infections in US
Nov 26: WHO classifies new variant Omicron as concern
Dec 8: UK Omicron spread forces England to adopt "Plan B" measures in response
March 15: Number of weekly cases globally increases for first time since January 2022
Apr 18: Airline mask mandate dropped in US
May 12: US passes 1 million deaths
July 5: BA.5 becomes dominant variant

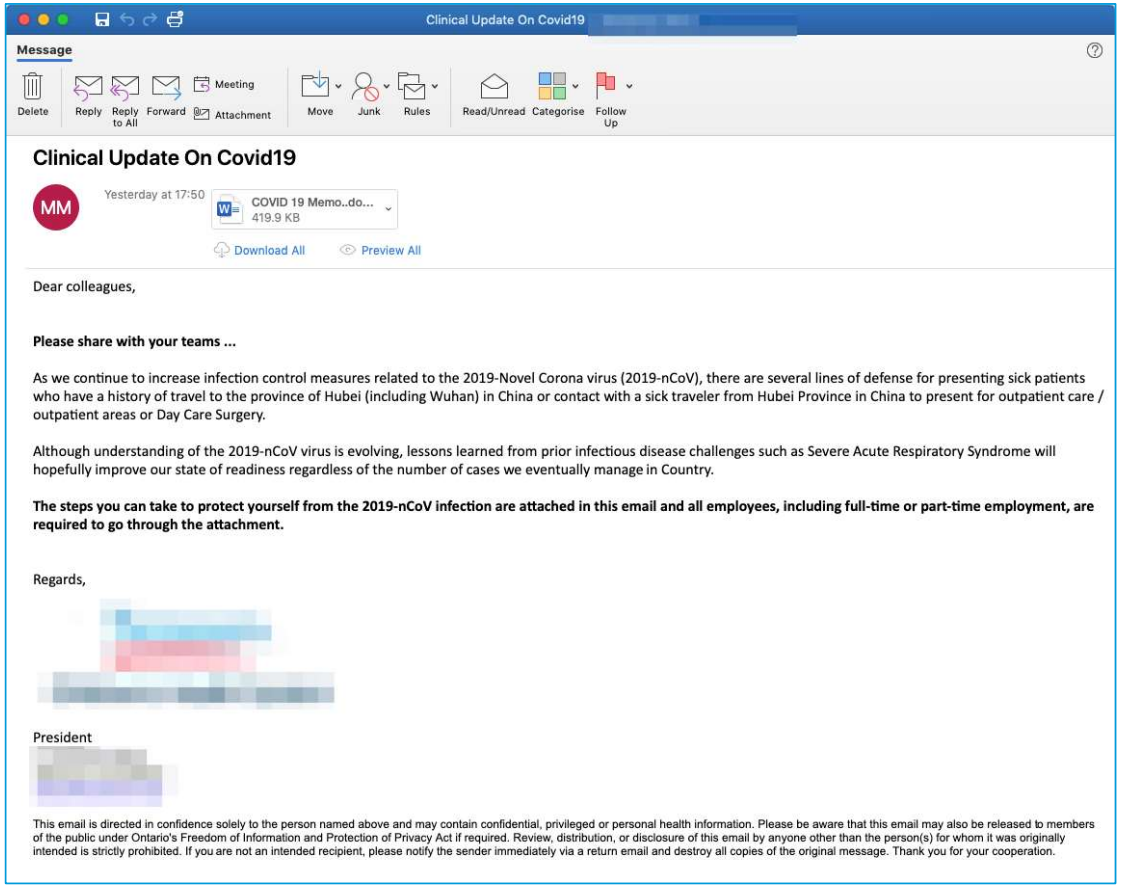
Emotet First Used COVID-19

- First observed threat actor using COVID-19 themes in January 2020 was TA542/Emotet
- They pretended to be a Japanese government entity and leveraged COVID-19 safety measures in emails to Japanese recipients
- TA542 used typical invoice-themed lures for English language targeting in this campaign

proofpoint.

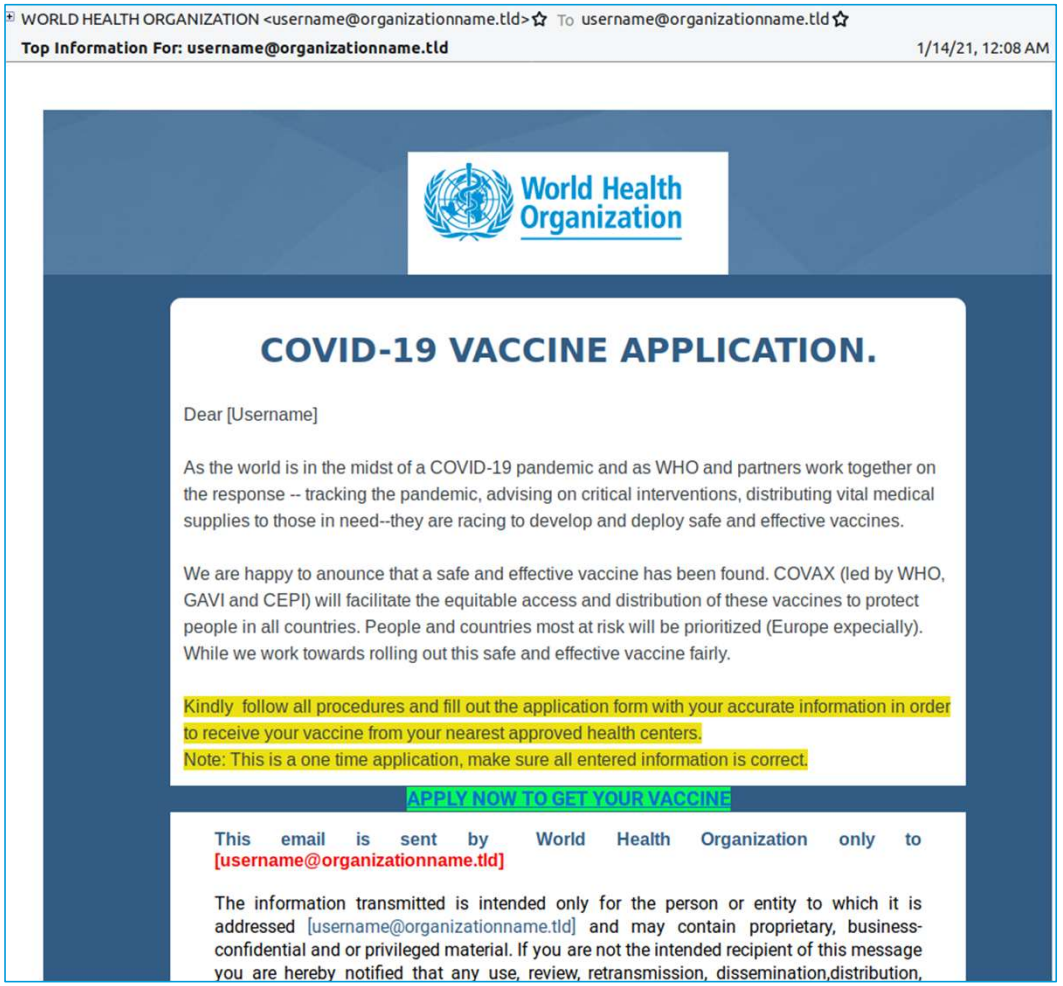
Threat Actors Prey on Health Fears and Uncertainty

During the initial months of the COVID-19 pandemic, more threat actors used themes related to **safety measures** and **company operations** than other theme types



Spoofing Health Entities

12% of campaigned threats using COVID-19 themes spoofed the US Center for Disease Control and Prevention (**CDC**) or the World Health Organization (**WHO**) from January 2020 through April 2022

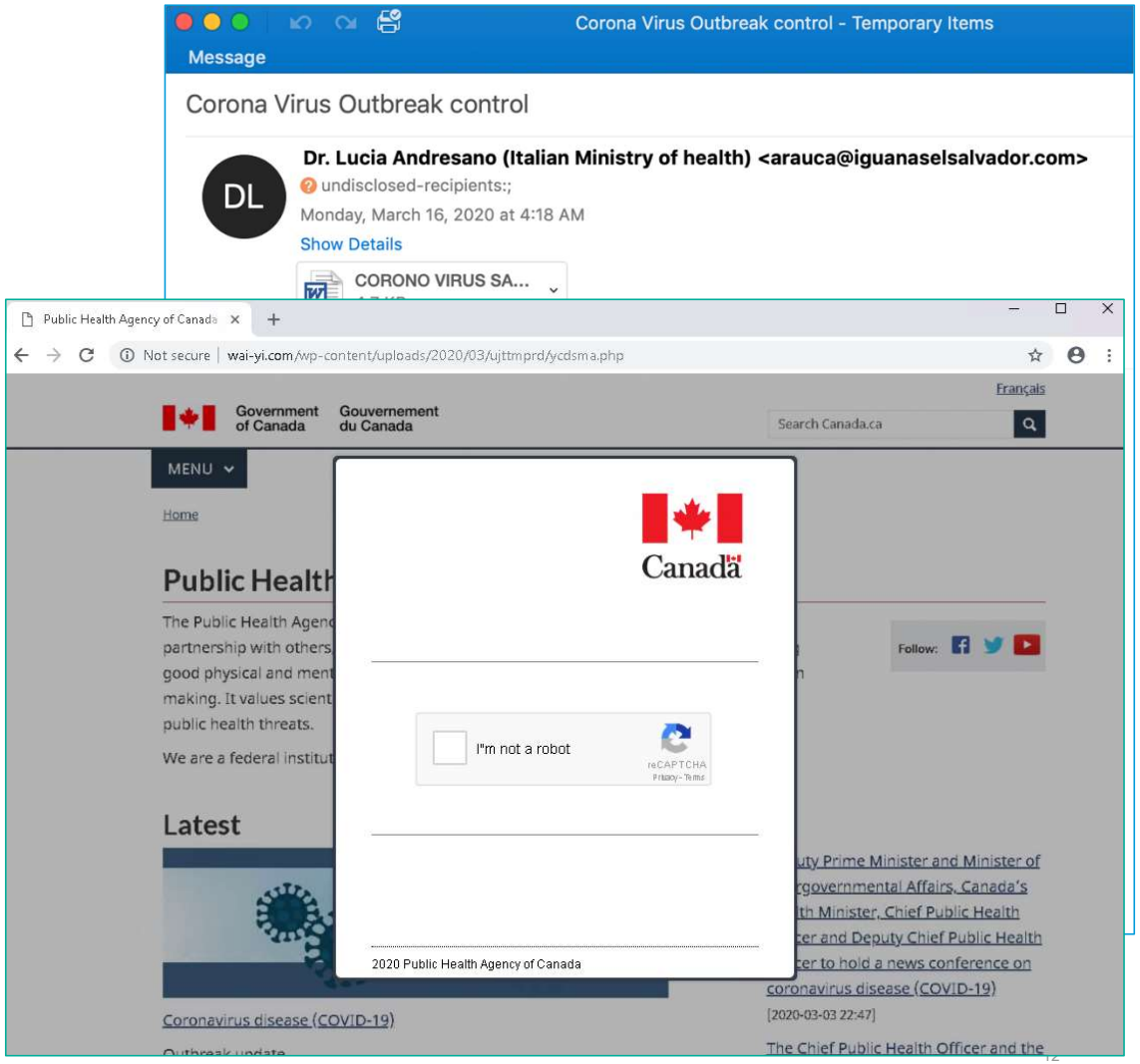


proofpoint.

International Concerns

The global relevance of COVID-19 meant actors sent threats in many languages to organizations globally

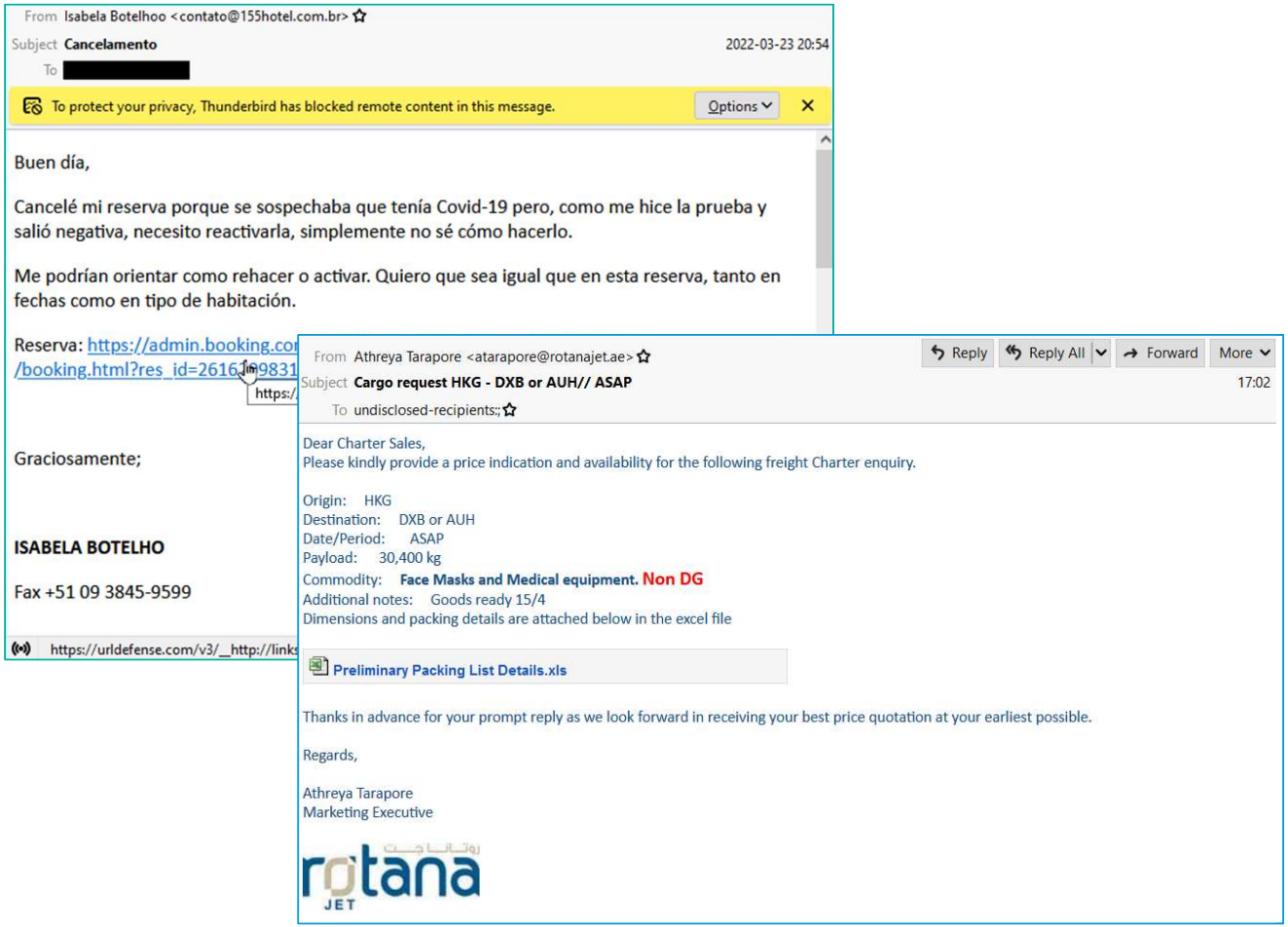
Proofpoint observed threat actors spoofing government entities in the United States, United Kingdom, Canada, Japan, Italy, Philippines, Brazil, Spain, and Turkey



proofpoint.

Incorporating COVID-19

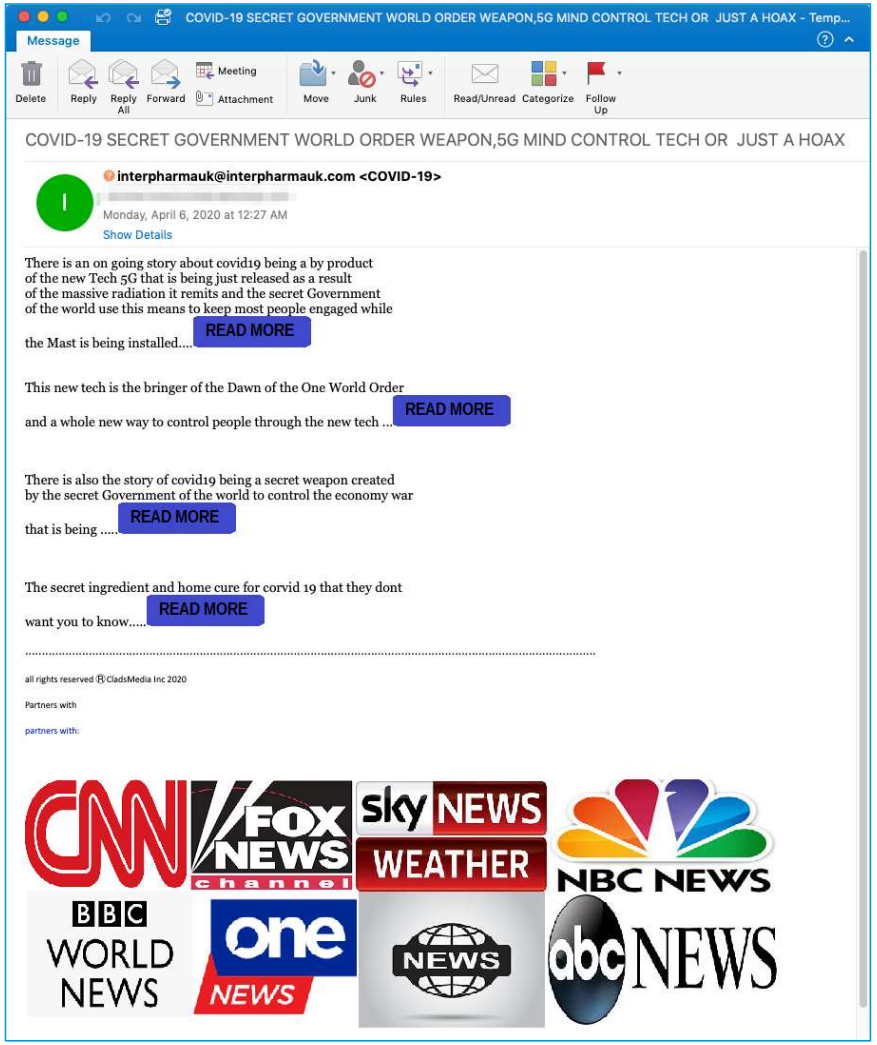
While nearly **all threat actors pivoted** to COVID-19 themes at some point during the pandemic, some threat actors incorporated COVID-19 into already existing and consistent social engineering themes



Conspiracies Don’t Work

The number of 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

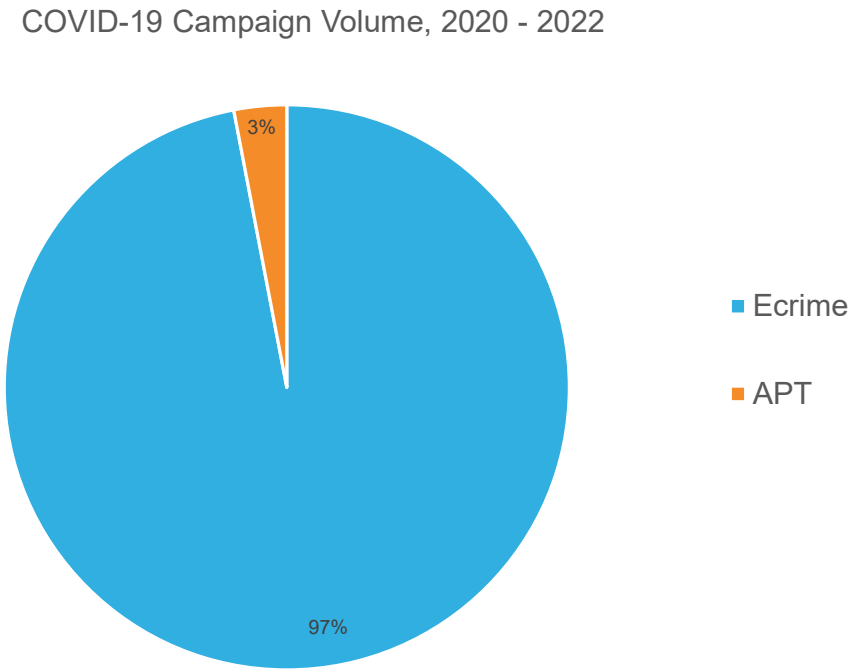
This suggests the conspiracy themes were not effective lures and did not prompt consistent engagement from the victims



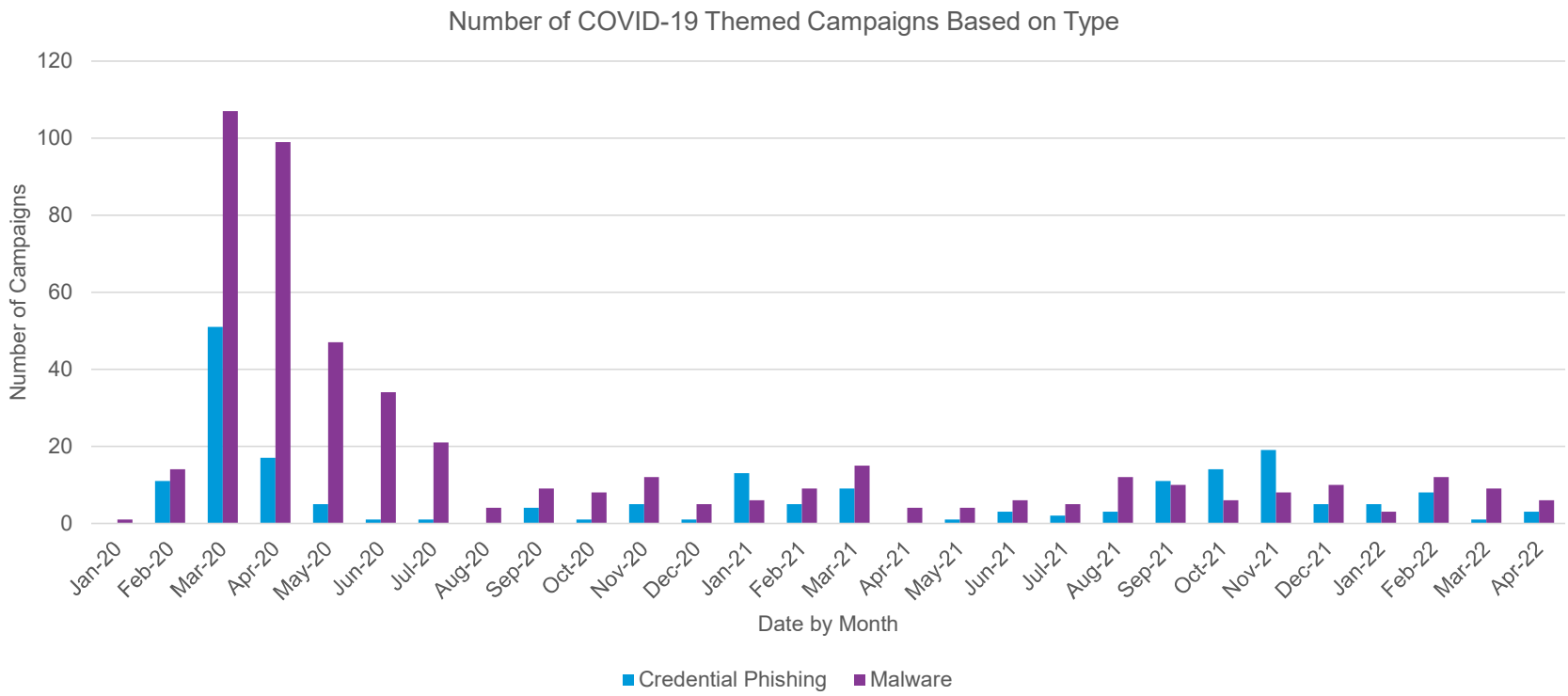
APT vs. Cybercrime

Most COVID-19 themed emails were associated with cybercriminal activity

Multiple APT threat actors leveraged COVID-19 themes, with most COVID-19 themes used by APT occurring in 2021

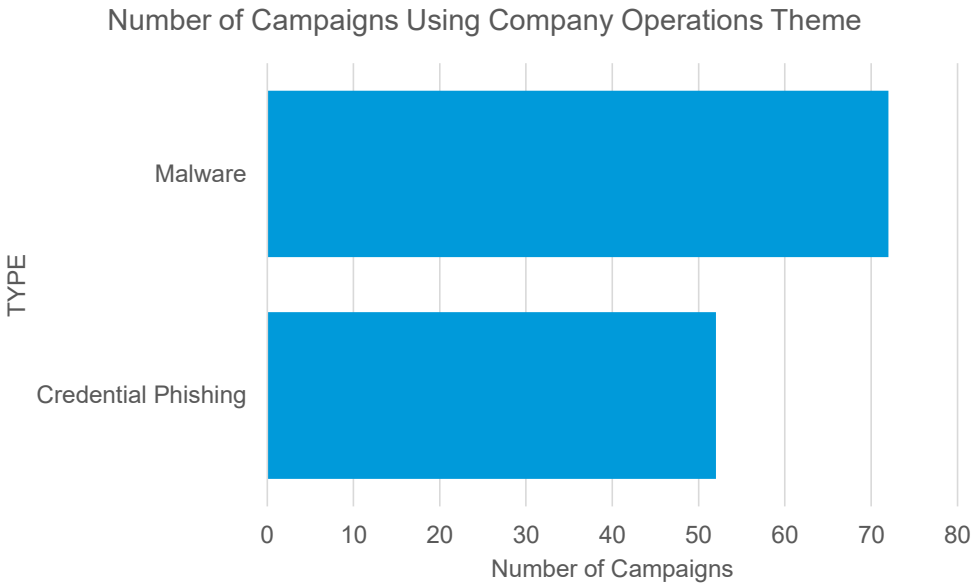


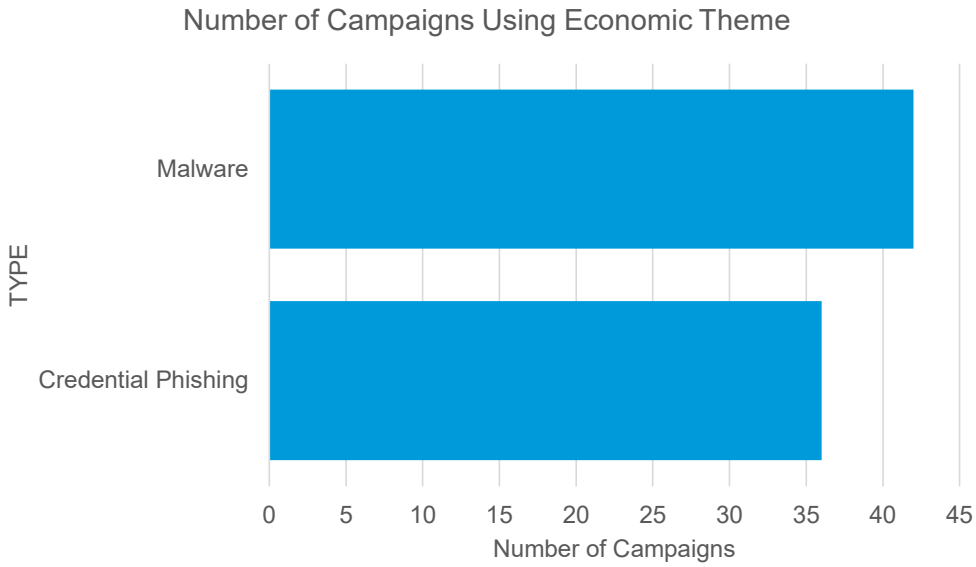
Credential Theft vs Malware



Overall, 29% of threats were credential phishing, while 71% were malware

Credential Theft vs Malware



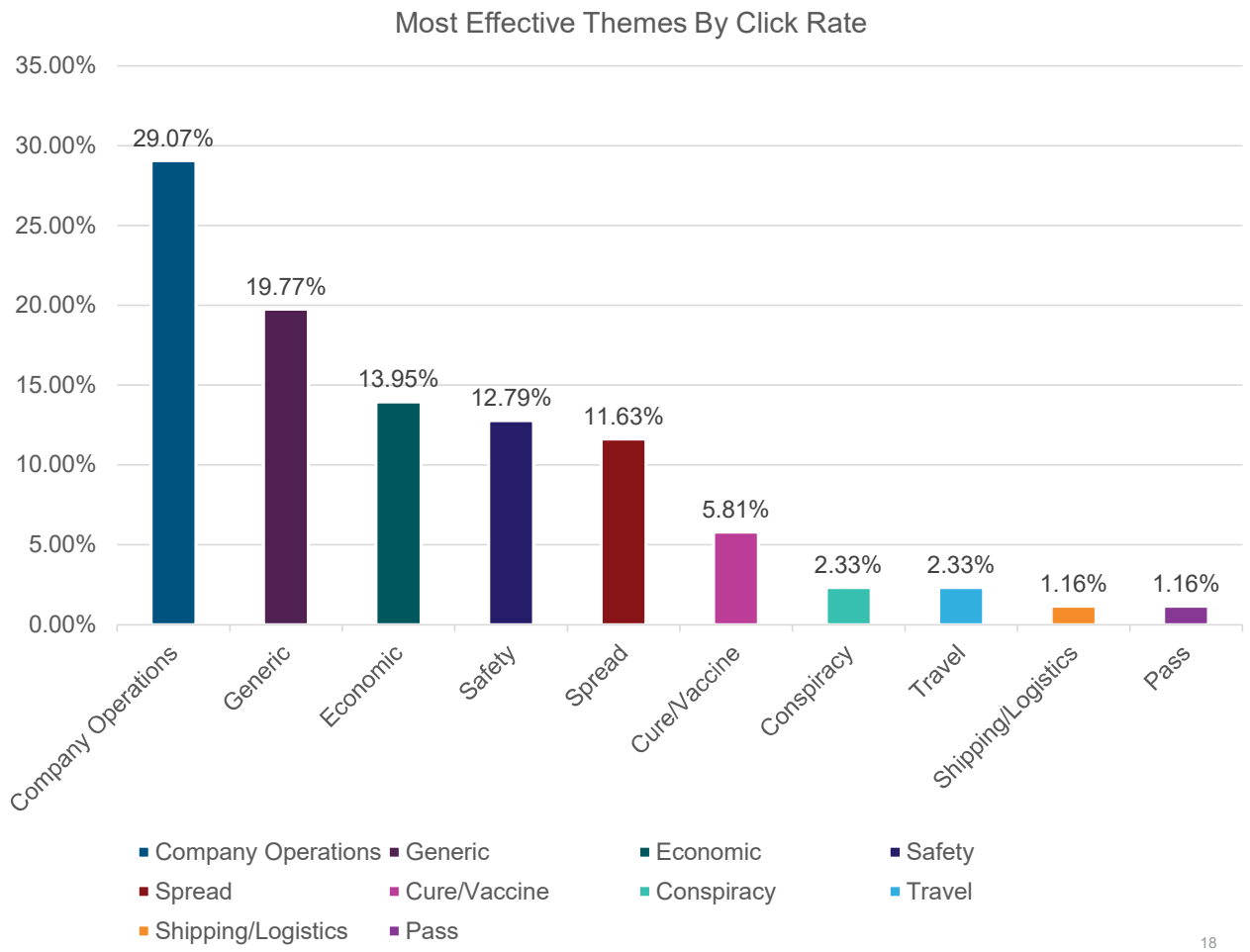


The total number of credential theft campaigns reached near parity to malware in two theme categories: **Company Operations** and **Economic** impacts

proofpoint.

What Worked?

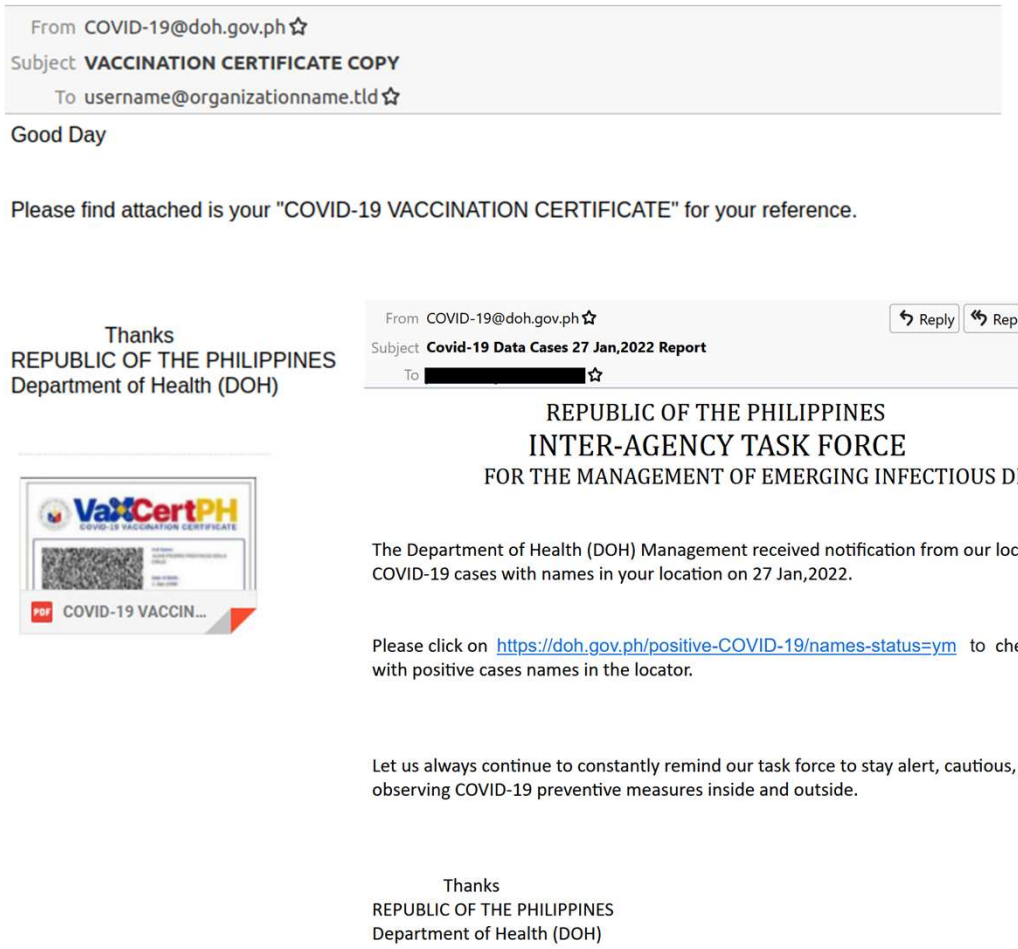
Company Operations threats made up nearly **18%** of the total themes overall, but nearly **30%** of the average click rate



Effective Lures: TA2722

TA2722 has 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%



From COVID-19@doh.gov.ph
Subject **VACCINATION CERTIFICATE COPY**
To username@organizationname.tld

Good Day

Please find attached is your "COVID-19 VACCINATION CERTIFICATE" for your reference.

Thanks
REPUBLIC OF THE PHILIPPINES
Department of Health (DOH)

VaxCertPH
COVID-19 VACCIN...

From COVID-19@doh.gov.ph
Subject **Covid-19 Data Cases 27 Jan,2022 Report**
To [redacted]

Reply | Reply All | Forward | More
1/27/2022, 8:34 PM

REPUBLIC OF THE PHILIPPINES
INTER-AGENCY TASK FORCE
FOR THE MANAGEMENT OF EMERGING INFECTIOUS DISEASES

The Department of Health (DOH) Management received notification from our locator confirming positive COVID-19 cases with names in your location on 27 Jan,2022.

Please click on https://doh.gov.ph/positive-COVID-19/names-status=ym to check the official statement with positive cases names in the locator.

Let us always continue to constantly remind our task force to stay alert, cautious, and disciplined in observing COVID-19 preventive measures inside and outside.

Thanks
REPUBLIC OF THE PHILIPPINES
Department of Health (DOH)

proofpoint.

Key Learnings

- People are more likely to interact with content that is related to their **Company Operations**, including business continuity, human resources policies, or remote work programs.
- Threat actors **responded to major events** in the COVID-19 pandemic including announcements of economic incentive programs and new variant strains 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.

Key Learnings

- 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 favorable backdrop** by which to initiate operations.

- 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.

- 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.

Questions?

@selenalarson

@dansomware