proofpoint.

HEALTHCARE REPORT

2020 Healthcare Threat Landscape

proofpoint.com

INTRODUCTION

The COVID-19 pandemic represents the largest public health crisis in a century. As cyber attackers seek to exploit the crisis, it has also become a major security issue for healthcare organizations.

The industry has quickly adapted to what is both a medical and business challenge. Organizations adopted new sanitation and safety protocols. They embraced remote care and shifted to remote work where possible. And in many cases, they adjusted to new patterns of healthcare demand, purchases and financing.

Unfortunately, the bad guys have also adapted. Spammers, cyber crime actors, nation states and other cyber attackers—collectively known as threat actors (TAs)—have integrated COVID-19 themes into phishing and social engineering campaigns.

To help healthcare leaders better understand the evolving threat landscape, we analyzed a year of data, focusing on the first half of 2020. Proofpoint Threat Research studied thousands of campaign threats across millions of messages. This report outlines our findings, providing data, real-world examples and insights to shed light on threats that target the healthcare industry.

Audience and objective

This report is intended for leadership and security executives in healthcare. It aims to help reduce risk healthcare organizations face to personally identifiable information (PII), intellectual property (IP), protected health information (PHI), financial data and third-party healthcare ecosystems. The report is also designed to help educate healthcare workers for better security awareness, digital health, safety and security.

Research methodology

This body of research analyzed a combination of Proofpoint data across threat actors, campaigns, business email compromise (BEC), and Very attacked People™ (VAPs) in the first half of 2020. In some cases, we use open source information to address security topics that we are researching but not directly observing in Proofpoint-sourced data.

This Proofpoint Premium Threat Report explores the threats, trends and transformations we see within our customer base and in the wider security landscape, especially those that affect healthcare and related industries.

Table of Contents

Healthcare Insights—by the Numbers

- We tied **35 actors** to campaigns against healthcare companies. Here's a breakdown: **22 were large-scale cyber crime** actors, **10 were** smaller cyber crime, one was an advanced persistent threat (or APT, typically a state-sponsored attacker), and two were unknown threat actors.
- In the first half of 2020, ransomware activity represented less than **1% of healthcare-focused** campaign activity directly delivered in email—about the same compared to industries throughout 2020. We observe and prevent botnets, such as Emotet, and later stage Trojans, such as Trickbot, that are often examples of threats preceding the ransomware attack chain.
- During the height of the pandemic in March 2020, healthcare organizations, compared to other industries, received about **16% more malicious messages** associated with campaigns. The lures representing this content pivoted to COVID-19 themes in healthcare and other sectors.
- In **77% of all threat campaigns** in the first half of 2020, at least one healthcare customer received a malicious message. Some 34% of these contained remote-access Trojans (RATs), 25% information stealers, 22% backdoors, 5% phishing and 0.8% ransomware.
- The Iranian actor Silent Librarian has targeted pharmaceutical business intelligence portals. Based on public information, we are moderately confident that Russia and China are pursuing access and intellectual property related to COVID-19 vaccines.
- In **90% of healthcare-focused business** email compromise (BEC) attacks we analyzed, the email had a blank subject line, which is a strong indicator for detection in security operations teams and awareness for users.

Threat Landscape

Commodity cyber crime is a broad concern for any industry. For the highly regulated industries such as healthcare, it may be even more worrisome. As security lags and data governance matures, healthcare organizations are required to report lost, stolen or exposed data. Threat actors (TAs) are well aware of this imbalance and eager to exploit it.

At the same time, the cyber crime landscape has evolved. Take well-known threat actors such as Emotet (TA542) and botnets such Trickbot and Dridex. Expanding beyond their roots as banking Trojans, these threats can now deploy many other malware strains. In essence, they have become large-scale distribution service for affiliated cyber crime actors. If we can stop these initial infections, then we reduce the risk of secondary threats, both planned and opportunistic.

For the first half of 2020, we attributed healthcare threat campaigns to 35 threat actors. (Attribution is the often complex process of identifying who is responsible for an attack.) Our attributions are based on evidence of at least one healthcare company identified in a campaign linked to an identified threat actor.

We found that about 93% of campaign data in the healthcare sector is a combination of large-scale and small-scale cyber crime. Figure 1 compares three different campaigns (called out in orange) with different campaign volumes, message volumes and infection vectors. Despite the different volumes, the following examples underscore the opportunistic nature of these campaigns and that this is not specific to healthcare but exemplary of commodity threats faced by all businesses and organizations.

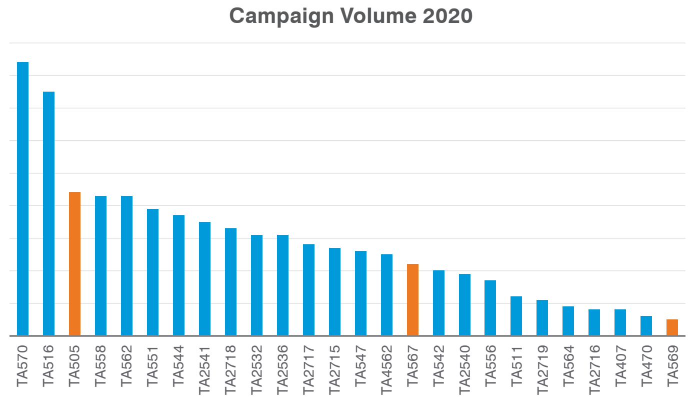


Figure 1. Campaigns volumes by threat actor in the first half of 2020

- Large scale actors have represented 64% of the threats received by the healthcare industry in 2020. TA570 is associated with Qakbot malware campaigns and represents the largest set of campaigns. TA567 (just past the mid-point) represents the largest volume of messages delivered to healthcare in the first two quarters and shows a spike in activity in May 2020.
- In 2020 29% of healthcare industry campaigns were attributed to small-scale threat actors. While the targeting by these types of threat actors may not be specific to the healthcare industry, their prevalence makes them very important because the smaller scale can often make it easier to assess intent or association across verticals.

Large-scale threat actors

Large-scale threat actors send high volumes of threats to many organizations, operating on economies of scale. They cast a wide net and draw on a diverse arsenal of techniques and features, such as unique URLs or macro features in attachments. They tend to be sector agnostic in who they target.

Still, attacks in the category can vary widely in message volumes and threat vectors. TA505 sends a high volume of malicious messages (over 200,000) directly to targets. In contrast, TA569 compromises legitimate websites and relies on indirect methods, such as automated mailers, to deliver messages in a lower volume of intended victims.

TA505

TA505 focuses on large-scale crimeware campaigns, using SDBot RAT and Get2 downloader as their primary malware.

After a short hiatus, TA505 campaign activity returned with a vengeance at the end of Q2. (See Figure 2.) The group launched one of the largest-scale campaigns of the year, with 200,000 messages directed at drugmakers. (We cover the pharmaceutical sector more fully in later sections.) TA505 has a reputation for large campaigns like these—it once sent about 50 million attachments in a single day.

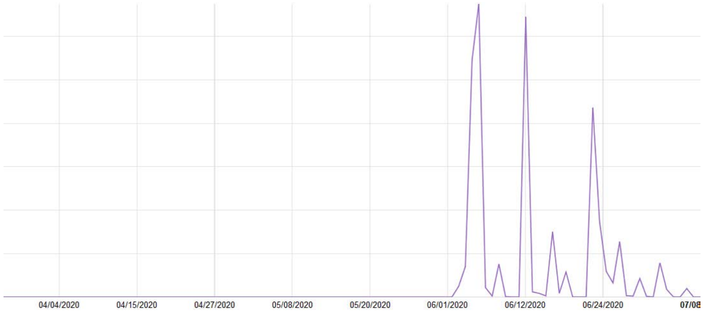
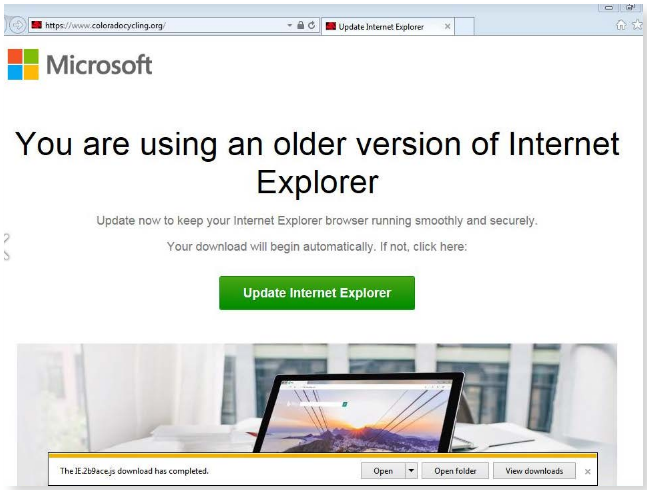


Figure 2. TA505 Message volume over time during Q2 2020

TA569

TA569 has been on our radar since 2018. It is reportedly loosely linked to the Russian cyber crime group known as Evil Corp.[1] Its business model relies on SocGholish, a malicious web framework, that assesses whether an infected system is part of a larger enterprise network or is just an individual user (who presumably doesn't have the same access to valuable corporate data).

In June 2020, links to compromised websites with SocGholish HTML injects were delivered through automated mailers. The group piggybacked otherwise legitimate outlets such as newsletters, marketing email, social media promotion and sharing links with friends. The injects were delivered to more than 1,000 customers, with a regional hospital system. (See Figure 3 for an example.)



You are using an older version of Internet Explorer

Update now to keep your Internet Explorer browser running smoothly and securely.

Your download will begin automatically. If not, click here:

The IE.2b9ace.js download has completed.

Figure 3. TA569 compromised website

The injects were selective. They assessed the user's operating system, browser and geolocation before downloading the malware payload. Users in the United States, France, Spain, Japan, Australia and the U.K. were the intended victims. TA569 has recently been associated with opportunistic ransomware campaigns delivering Wastedlocker.[2]

[1] https://home.treasury.gov/news/press-releases/sm845

[2] https://blog.fox-it.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

Small-scale threat actors

Small-scale threat actors usually focus on smaller subsegments or verticals rather than entire industries. Their campaigns tend to be less frequent and lower volume—in some cases consisting of a single message to just one organization. This smaller scale allows for a degree of customization and social engineering that greatly increases the likelihood that the recipient will take the bait.

TA2717

TA2717, first identified in December 2019, exploits vulnerabilities in the Equation Editor of Microsoft Office. By tricking email recipients into opening a malicious Office attachment, TA2717 installs various information stealers, keyloggers and RATs on the infected system. It also distributes several payloads, including Agent Tesla keylogger, Loki Bot credential stealer and Formbook credential stealer. Historically, the volume of campaigns from this actor have been on the scale of hundreds or a few thousand messages, typically posing a greater risk to PII and user data based on the fact that these tools are designed to steal data and resell it.

TA2536

TA2536, which has been active since at least 2015, is likely Nigerian based on its unique linguistic style, tactics and tools. It uses keyloggers such as HawkEye and distinctive stylometric features in typo-squatted domains that resemble legitimate names and the use of recurring names and substrings in email addresses.

One of TA2536's favorite tactics in 2020 was spoofed DHL shipping lures. It ramped up from smaller campaigns to larger offensives that peaked at more than 70,000 messages in late June. (See Figure 4.) TA2536 uses multiple payloads, including the NanoCore RAT, the Agent Tesla, Remcos RAT, Loki Bot and FormBook.

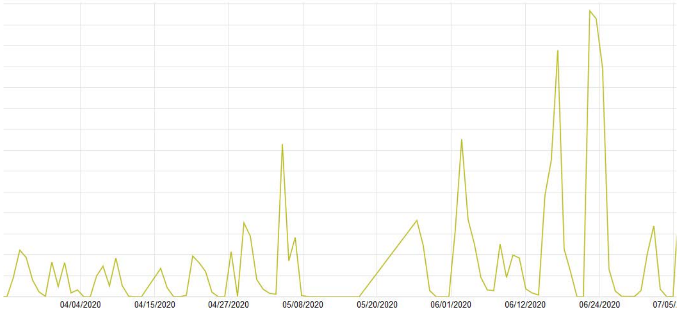


Figure 4. TA2536 campaign volumes over Q2 2020

Vertical and Threat Vector Insights

We identified key campaigns that demonstrated more specific variance in message volume, vector of delivery and potential risk to a specific vertical in the healthcare sector.

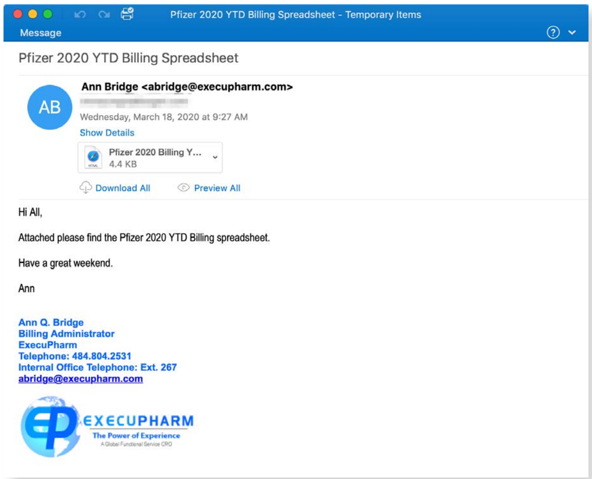
A vertical is a specific subset within the sector. Without an established threat actor intent, our researchers established assumed areas of risk, such as intellectual property (IP), PII, personal health information (PHI) and third-party organizations with digital connections, based on observed campaigns verticals, including pharmaceuticals, large healthcare systems, nonprofits, children's hospitals and insurers.

Below are a number of examples of specific attacks against healthcare entities.

Pharma: IP, financial data and PII risk

TA505 targeted pharmaceutical manufacturers as the pandemic raced toward its peak. In this campaign, 78% of over 250,000 malicious messages were intended for pharmaceutical and life science organizations.

Figure 5 shows this campaign spoofing employees from a business support service for clinical trials. The message subjects included billing information and, in one case, a clinical researchers name who is researching antibody therapy to prevent and treat COVID-19.


Pfizer 2020 YTD Billing Spreadsheet - Temporary Items
Message
AB
Show Details
Download All
Preview All
EXECUPHARM
The Power of Experience
A Global Functional Service CRO

Pfizer 2020 YTD Billing Spreadsheet

Ann Bridge <abridge@execupharm.com>
[redacted]
Wednesday, March 18, 2020 at 9:27 AM

Pfizer 2020 Billing Y...
4.4 KB

Hi All,

Attached please find the Pfizer 2020 YTD Billing spreadsheet.

Have a great weekend.

Ann

Ann Q. Bridge
Billing Administrator
ExecuPharm
Telephone: 484.804.2531
Internal Office Telephone: Ext. 267
abridge@execupharm.com

Figure 5. TA505 spoofing email

Hospitals: third-party risk

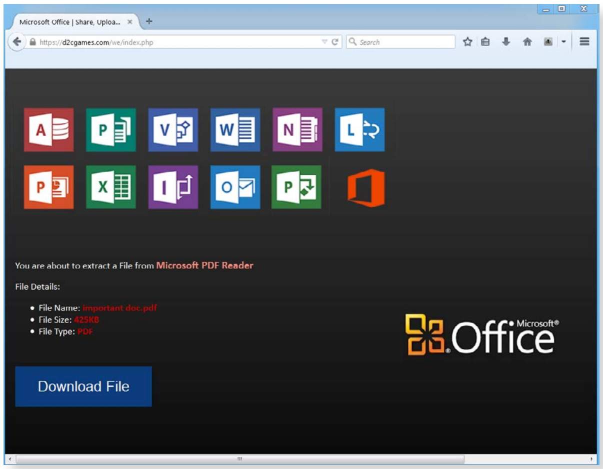
Hospital gift shops are often inside hospitals. If they are connected to the hospital's network, then they are likely weak, transitive access points that can expose hospitals to risks introduced by those third parties. Our analysts were able to identify a payment processing system uniquely serving hospital giftshops compromised by MageCart.

In this case, the web-based payment system of a gift shop supplier was compromised. Legitimate advertising and news emails from this supplier unwittingly directed customers to the compromised website. Out of more than 200 organizations receiving these legitimate emails directing recipients to this now-weaponized third-party website, 74% were healthcare institutions. More than 80% of those messages were delivered to large healthcare systems.

Australian nonprofit: targeted credential phishing

An unknown threat actor targeted a small number of individuals at an Australian healthcare nonprofit with the subject "Update On Novel Coronavirus (2019-nCoV)." The emails spoofed the target company's president, informing recipients that travel to China was suspended.

The email contained an attached Microsoft Word document with an embedded URL that led to a Microsoft-branded phishing page, as shown in Figure 6. Upon entering credentials, the victim was directed to a genuine World Health Organization web page with a situation report on the coronavirus, as shown in Figure 7.

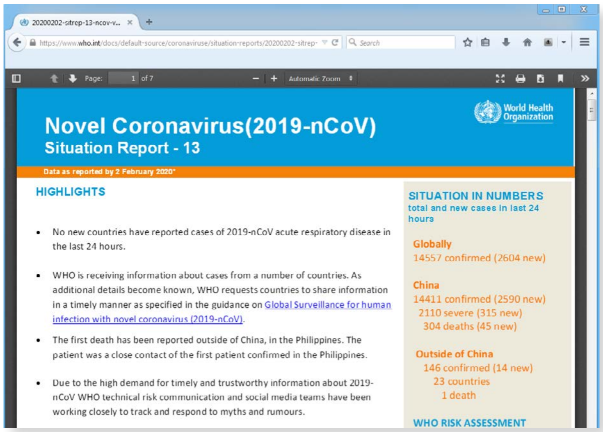

Microsoft Office | Share, Uploa...
https://d2cgames.com/we/index.php
Search
A
P
V
W
N
L
P
X
I
O
P
Microsoft® Office
Download File

You are about to extract a File from Microsoft PDF Reader

File Details:

- File Name: important doc.pdf
- File Size: 425KB
- File Type: PDF

Figure 6. TA569 compromised website


20200202-sitrep-13-ncov-v...
https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-
Search
Page: 1 of 7
Automatic Zoom
World Health Organization

Novel Coronavirus(2019-nCoV)
Situation Report - 13

Data as reported by 2 February 2020*

HIGHLIGHTS

- No new countries have reported cases of 2019-nCoV acute respiratory disease in the last 24 hours.
- WHO is receiving information about cases from a number of countries. As additional details become known, WHO requests countries to share information in a timely manner as specified in the guidance on Global Surveillance for human infection with novel coronavirus (2019-nCoV).
- The first death has been reported outside of China, in the Philippines. The patient was a close contact of the first patient confirmed in the Philippines.
- Due to the high demand for timely and trustworthy information about 2019-nCoV WHO technical risk communication and social media teams have been working closely to track and respond to myths and rumours.

SITUATION IN NUMBERS
total and new cases in last 24 hours

Globally
14557 confirmed (2604 new)

China
14411 confirmed (2590 new)
2110 severe (315 new)
304 deaths (45 new)

Outside of China
146 confirmed (14 new)
23 countries
1 death

WHO RISK ASSESSMENT

Figure 7. A legitimate benign COVID-19 WHO website

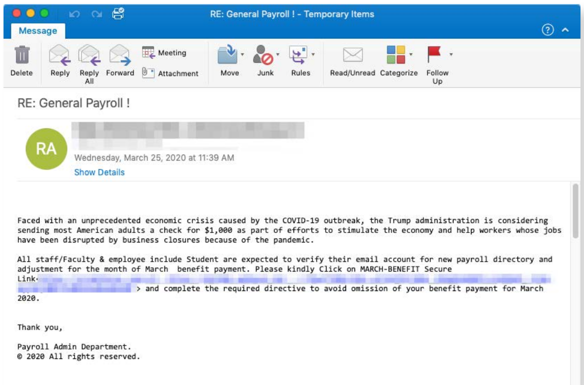
The redirection to a relevant, benign decoy site after credentials have been harvested is an uncommon tactic in credential phishing attacks.

In the weeks following, this threat actor reused this branded material to target other healthcare industry entities—always with low message quantities to individual companies.

Children's hospitals

In this example, a phishing attack leveraged the United States CARES Act in a lure related to economic stimulus payments associated with COVID-19 and was heavily directed at the healthcare industry. In contrast to the targeted nature of the last example, 88% of the message volume was sent to entities in the healthcare vertical.

This attack was sent to small, medium and large healthcare systems, but children's and academic hospitals were the top recipients of this threat. Given the sensitivity of children's identity data, any exposure of PII in this vertical can have long-term impacts to the integrity of an individual's identity.



RE: General Payroll !

[redacted]

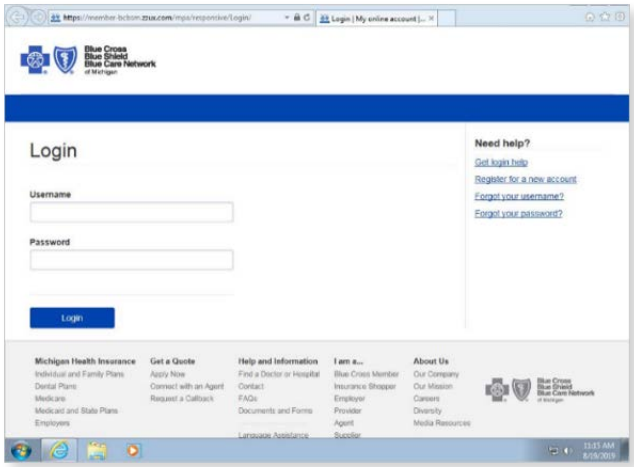
Wednesday, March 25, 2020 at 11:39 AM

```
Faced with an unprecedented economic crisis caused by the COVID-19 outbreak, the Trump administration is considering
sending most American adults a check for $1,000 as part of efforts to stimulate the economy and help workers whose jobs
have been disrupted by business closures because of the pandemic.

All staff/Faculty & employee include Student are expected to verify their email account for new payroll directory and
adjustment for the month of March  benefit payment. Please kindly Click on MARCH-BENEFIT Secure
Link<[redacted]
> and complete the required directive to avoid omission of your benefit payment for March
2020.


Thank you,

Payroll Admin Department.
© 2020 All rights reserved.
```

Figure 8. Cares Act payroll lure

Cloned insurance portals

In this example an unknown threat actor developed a cloned portal and used emails with subjects such as "updating our Privacy Notice" as lures to the portal. As shown in Figure 9, the malicious page was cloned using a web page from the legitimate authentication portal for Blue Cross Blue Shield in Michigan and would attempt to harvest credentials.



Login

Username

Password

Figure 9. A cloned portal meant to mimic an Insurer

The message sender in the lures was spoofed to appear as though the message originated from "Blue Cross Blue Shield Association". The emails also included a graphic image tag that loaded the BCBS logo from the attacker's page.

Get to know your Very Attacked People (VAPs)

The role of Very Attacked People (VAP) analysis is to establish a strategic signal of what roles and responsibilities receive significant pressure from cyber attacks. The use of this data can guide security awareness, policy updates, access control and risk-reduction initiatives.

This chart shows a high-level summary of VAPs in various segments of the healthcare sector. We assessed attacks and their targets using Proofpoint Targeted Attack Protection (TAP), which includes sandbox analysis. The profiles are based on an analysis of dozens of healthcare organizations.

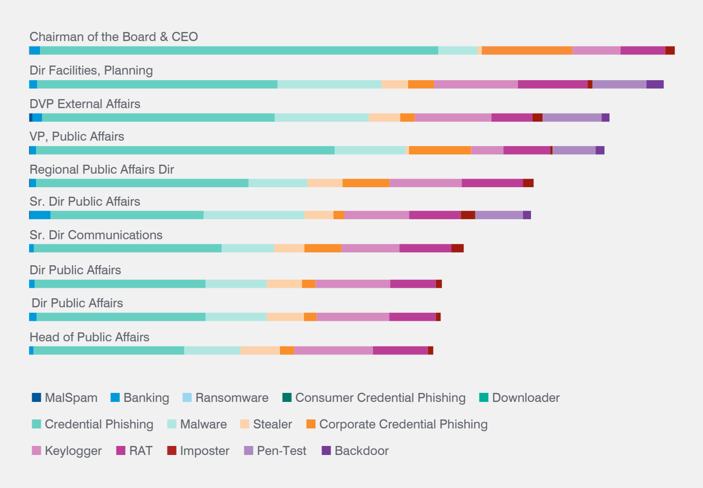
Pharmaceuticals	Executives	Public Affairs	Email Alias
Large Health Systems	Clinical Staff	Rehab Therapy	Executives
Insurers	Patient Support	Executives	Finance
Children's Hospitals	Research Teams	Clinical Staff	Accounts Payable
Teaching Hospitals	Professors	Alumni	Grants / Finance

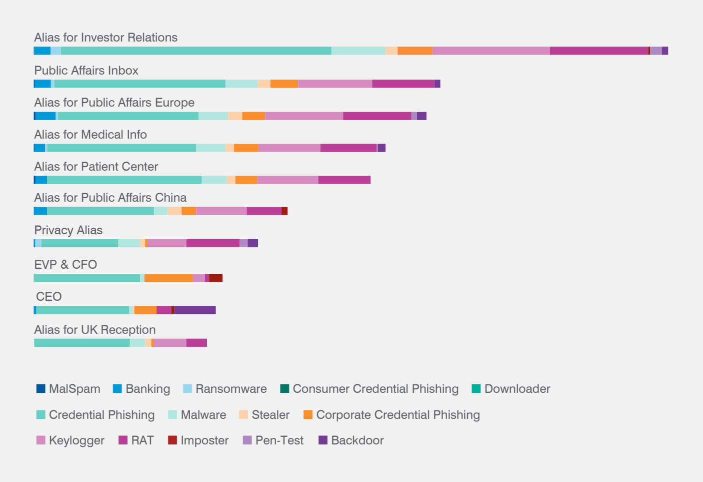
We compared real-world examples of VAPs within five categories of healthcare. We determined the most heavily targeted email addresses at each organization. Using social engineering research and the same public information an attacker might use, we matched each address to its owner. (We omitted some details to protect customers' privacy.)

Pharmaceuticals

We compared VAPs at two American multinational medical device and biotechnology companies, looking at public-facing email addresses and aliases and found public affairs (PA) titles and aliases received the highest volumes of email.

PA roles are highly visible, addressing policy issues related to funding, regulations and intellectual property, as well as positioning pharmaceutical companies to political leaders. These email addresses are often exposed and easy to obtain making them likely targets. We also noticed several addresses, such as those of CEOs and CFOs, that belong to positions that fit the standard definition of a VIP. Both organizations showed VIPs as VAPs.



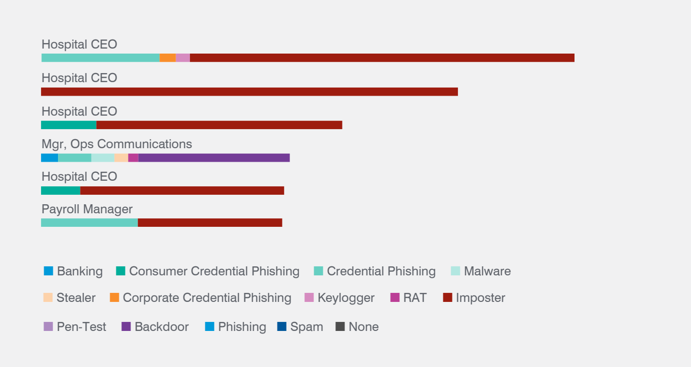


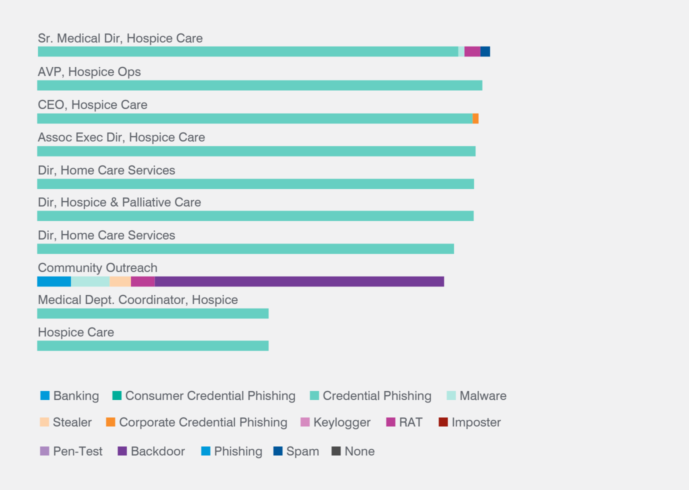
Large Healthcare Systems

The first example from a large U.S. healthcare system is from a Fortune 500 healthcare system with more than 20 hospitals. Here we found a significant volume of BEC attacks, particularly against various hospital officers but also a payroll manager.

In the second VAP example from a large nonprofit integrated health network, the most attacked departments were in hospice and home care. Given the news cycle coverage of COVID-19 effects on the elderly, hospice and palliative care may be exposed to increased cyber crime risks.

As the pandemic death toll rises, hospices are information rich but potentially less secure based on technology, training and security awareness. Additionally, individuals near end-of-life are at increased risk of cyber crime due to an increased portfolio of PHI, controlled substance access, insurance information and patient identifiers for identity theft.



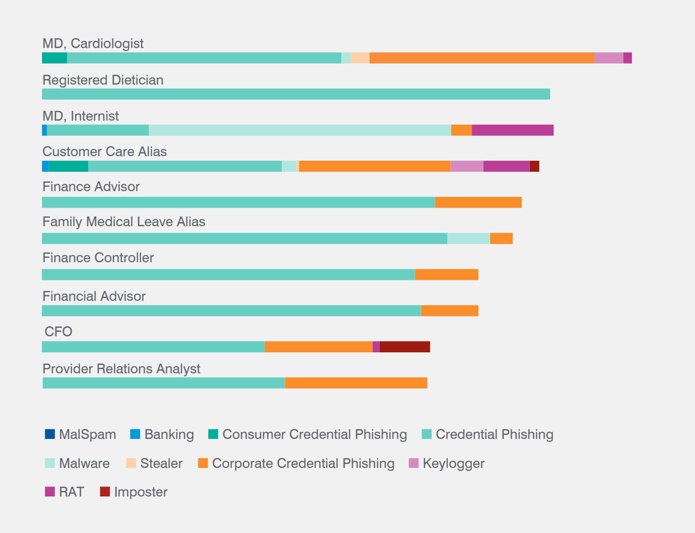


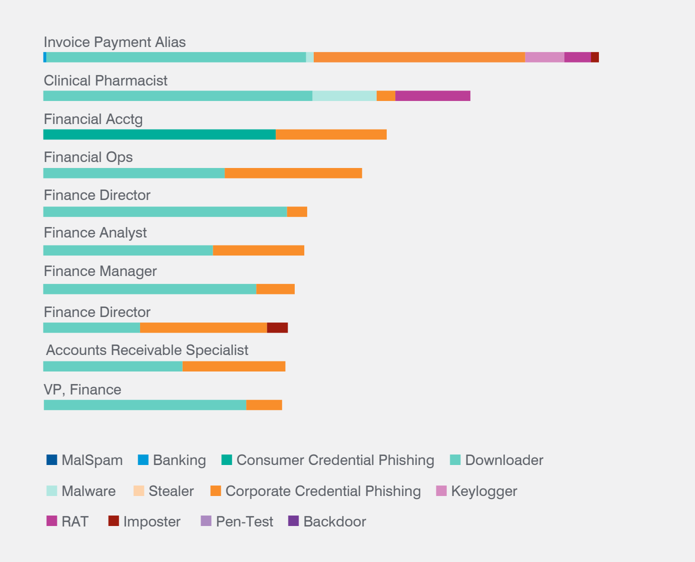
Insurers

We analyzed two large health insurance providers.

In the first VAP example, public-facing email addresses and aliases are among the most targeted. Three of top 10 VAPs were clinicians with strong online identities. Several patient support team aliases also occupied the top 10 list. Five of top 10 VAPs had a "finance" title. Given the nature of the organization's business this would be a natural target. One of the Top 10 VAPs, a CFO, is also considered a VIP and was the recipient of a high volume of BEC attacks.

In the second VAP example, nine out of 10 top VAPs were finance related, the outlier being a clinical pharmacist. Pharmacy staff are attractive targets because they have access to controlled substances with high value on the dark web or underground economy.



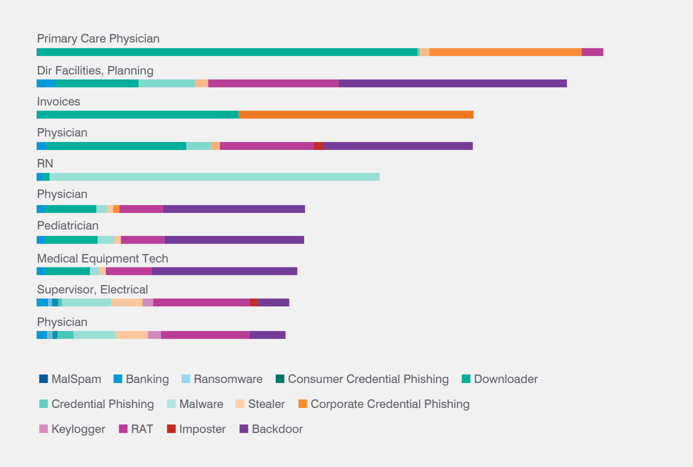


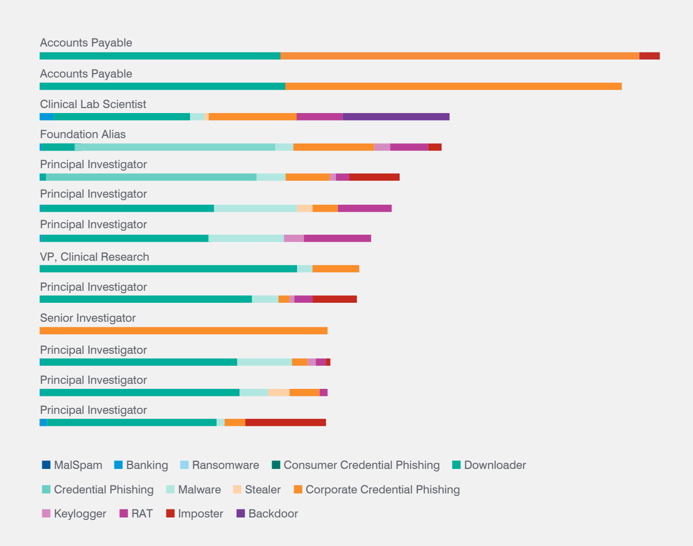
Children's Hospitals

The title "physician" was the most attacked title for the first children's hospital VAP analysis we performed, while "research" titles were a highly attacked category in the second example. Privacy concerns are heightened with children because they are a popular target for identity theft. A minor patient's record is extremely valuable on the dark web or underground economy.

Most children have not established a credit history and will not be applying for loans or credit cards at the time of breach. Cyber crime actors know most people are not monitoring if these data are being used for fraud.

In the first example, the volume of backdoor activity was highest in facilities management, which often have weak security controls. Given that these environments employ permissive assets such as Internet of Things (IoT) devices and HVAC systems, attacks against these targets can often use these as network pivot points to attack the corporate IT enterprise.



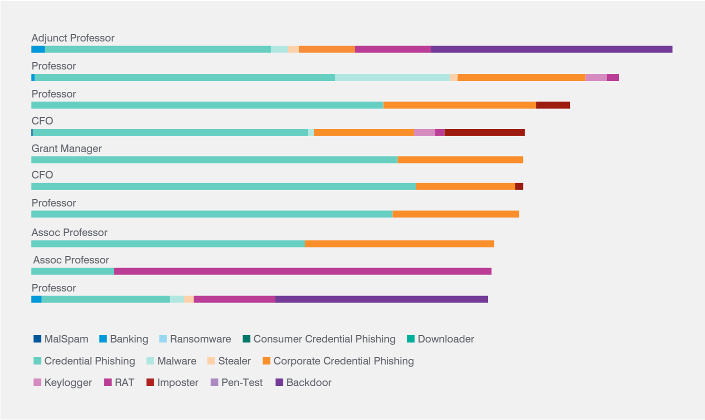


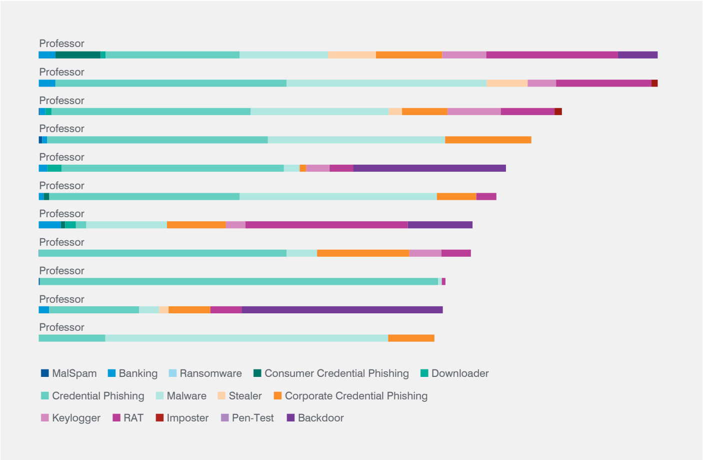
Teaching Hospitals

In comparing two teaching hospitals, the hospital email accounts most targeted by attackers are professors who have access to academic research often under research grants from third-party medical or commercial organizations. Faculty often conduct original research as part of their positions.

A VAP analysis conducted for a large university education, research and patient care health system in the American southeast is interesting because professors were highly attacked, and three finance email addresses made the top 10 list of VAPs. Finance departments are likely information rich, given that teaching and research hospitals handle large amounts of financial data from government loans, grants and work-study positions.

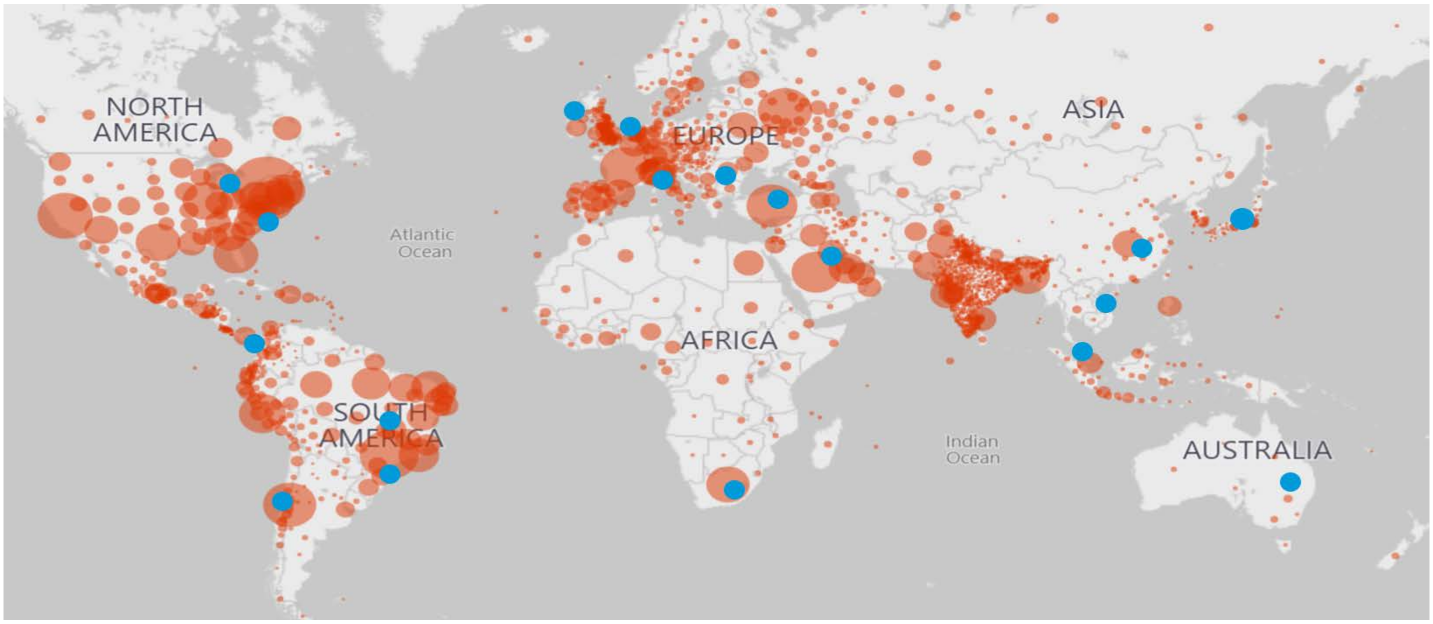
In the second VAP example from a major research hospital in California, all VAPs were professors, a validation that faculty of medicine are susceptible to larger volumes of phishing, especially given the nature of the research environment—open knowledge sharing and collaboration among third parties.





How COVID-19 Affected Cybersecurity

By the summer of 2020, nearly 20 countries were seeing COVID-19-themed lures (marked in blue on the map), or the lure languages represented an interest in users with that language preference. To further increase vulnerability, users were in many cases now working from home outside the security controls of corporate networks and relying heavily on host-based security protections. As the pandemic grew globally, the subjects and lure content began to take advantage of different local, national, regional and international themes.



Source: Microsoft Bing – accessed October 9th, 2020

Proofpoint researchers have observed the following trends in regard to COVID-19 themed attacks generally.

- By mid-March, a significant portion of scanned attachment threats were making use of COVID-19 themes, from commodity criminals to nation-state threat actors.
- Threat actors continued distributing the same malware or phishing campaigns to their regularly intended victims they did prior to COVID-19 but now with COVID-19 content.
- Early-stage COVID-19-themed lure content centered on stoking a strong emotional response with themes such as ventilator and mask shortages and a neighbor being infected.
- As information updates from credible international, national, state and local authorities developed, threat actors developed malicious messages aligned to those authorities' legitimate messages around government policy, regulation, tax rebates and incentives and how to stay safe working from home.
- Later, the above lure themes were followed by shipping-related, work from home-related, and even local grocery store delivery-related themes. These themes leveraged the new conditions of living.
- As shown in Figure 10, there was a clear trend in COVID-19 themed campaigns reaching a peak in March 2020 and steadily declining from March 2020 through July 2020. It's notable that April and May 2020 saw the most rapid decline in COVID-19-themed campaign volume. Since May 2020, COVID-19-themed campaign volume has continued a slow but steady decline.

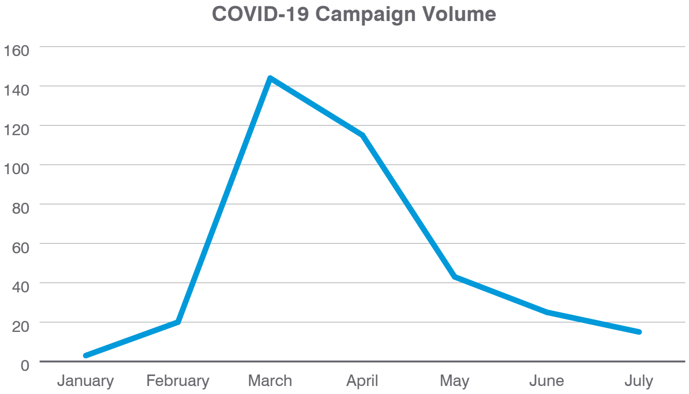
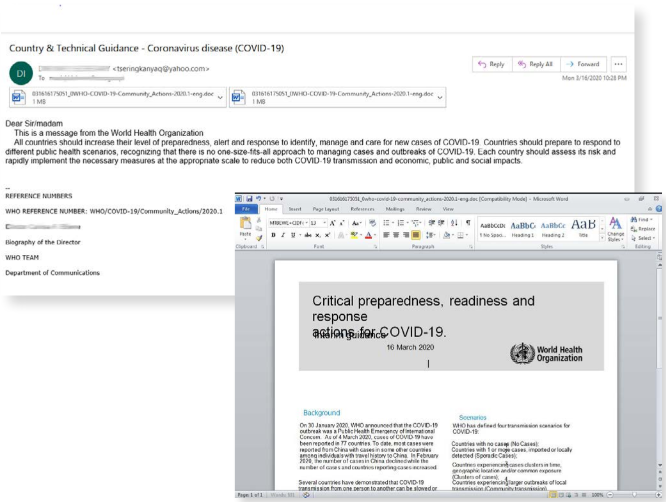


Figure 10. Volume of COVID-19 Themed Campaigns January – July 2020

COVID-19 campaign examples

In March 2020, our researchers observed a Chinese APT actor, TA413, a phishing campaign impersonating the World Health Organization's guidance on COVID-19 critical preparedness to deliver a new malware family that researchers have dubbed "Sepulcher". This campaign targeted European diplomatic and legislative bodies, non-profit policy research organizations and global organizations dealing with economic affairs.[3]



Country & Technical Guidance - Coronavirus disease (COVID-19)

DI [redacted] <tseringkanyaq@yahoo.com>
To [redacted]

Mon 3/16/2020 10:28 PM

031616175051_0WHO-COVID-19-Community_Actions-2020.1-eng.doc 1 MB
031616175051_0WHO-COVID-19-Community_Actions-2020.1-eng.doc 1 MB

Dear Sir/madam
This is a message from the World Health Organization
All countries should increase their level of preparedness, alert and response to identify, manage and care for new cases of COVID-19. Countries should prepare to respond to different public health scenarios, recognizing that there is no one-size-fits-all approach to managing cases and outbreaks of COVID-19. Each country should assess its risk and rapidly implement the necessary measures at the appropriate scale to reduce both COVID-19 transmission and economic, public and social impacts.

--
REFERENCE NUMBERS

WHO REFERENCE NUMBER: WHO/COVID-19/Community_Actions/2020.1

[redacted]

Biography of the Director

WHO TEAM

Department of Communications

031616175051_0who-covid-19-community_actions-2020.1-eng.doc [Compatibility Mode] - Microsoft Word

Critical preparedness, readiness and response
actions for COVID-19.
Interim guidance
16 March 2020

World Health Organization

Background

On 30 January 2020, WHO announced that the COVID-19 outbreak was a Public Health Emergency of International Concern. As of 4 March 2020, cases of COVID-19 have been reported in 77 countries. To date, most cases were reported from China with cases in some other countries among individuals with travel history to China. In February 2020, the number of cases in China declined while the number of cases and countries reporting cases increased.

Several countries have demonstrated that COVID-19 transmission from one person to another can be slowed or

Scenarios

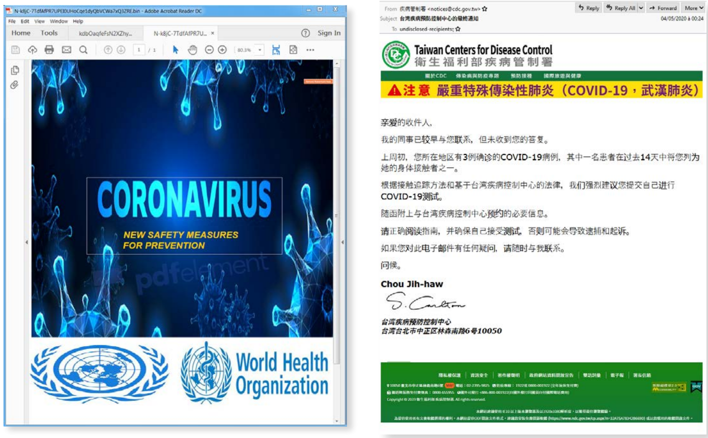
WHO has defined four transmission scenarios for COVID-19:

1 Countries with no cases (No Cases);
2 Countries with 1 or more cases, imported or locally detected (Sporadic Cases);
3 Countries experiencing cases clusters in time, geographic location and/or common exposure (Clusters of cases);
4 Countries experiencing larger outbreaks of local transmission (Community transmission).

Figure 11. COVID-19-Themed Email Abusing World Health Organization Name and Logo

Our researchers have seen multiple instances where cybercriminals attempted to use COVID-19 as a basis to launch central theme for their attacks. The World Health Organization (WHO) and US Centers for Disease Control (CDC) are not only two of the most prominent institutions for learning about pandemics such as COVID-19 but also institutions that regularly have their brand abused by cybercriminals as they look to launch attacks.

As campaigns developed globally, similar lure themes were adopted leveraging abusing the Taiwanese CDC name and logo. These lures leveraged safety themes and announcements of vaccines to entice users.



From 疾病管制署 <notices@cdc.gov.tw>
Subject 台灣疾病預防控制中心的最終通知
To undisclosed-recipients;

04/05/2020 à 00:24

Taiwan Centers for Disease Control
衛生福利部疾病管制署

⚠注意 嚴重特殊傳染性肺炎（COVID-19，武漢肺炎）

亲爱的收件人，

我的同事已较早与您联系，但未收到您的答复。

上周初，您所在地区有3例确诊的COVID-19病例，其中一名患者在过去14天中将您列为她的身体接触者之一。

根据接触追踪方法和基于台湾疾病控制中心的法律，我们强烈建议您提交自己进行COVID-19测试。

随函附上与台湾疾病控制中心预约的必要信息。

请正确阅读指南，并确保自己接受测试，否则可能会导致逮捕和起诉。

如果您对此电子邮件有任何疑问，请随时与我联系。

问候。

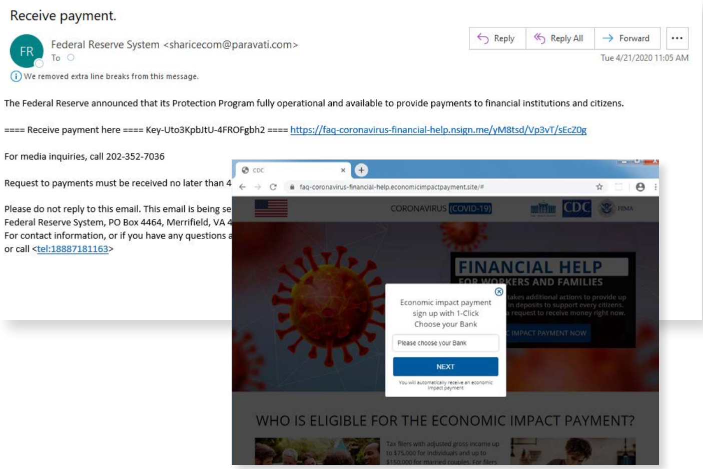
Chou Jih-haw

S. Carlton

台湾疾病预防控制中心
台湾台北市中正区林森南路6号10050

Figure 12. COVID-19-Themed Email Abusing World Health Organization Name and Logo and COVID-19-Themed Email Abusing Taiwan CDC Name and Logo

As the focus of cybercriminal activity is monetization, threat actors also adopted lures impersonating the Federal Relief Protection Act from the U.S. Federal Reserve Bank.



Receive payment.

FR Federal Reserve System <sharicecom@paravati.com>
To

Tue 4/21/2020 11:05 AM

We removed extra line breaks from this message.

The Federal Reserve announced that its Protection Program fully operational and available to provide payments to financial institutions and citizens.

==== Receive payment here ==== Key-Uto3KpbJtU-4FROFgbh2 ==== https://faq-coronavirus-financial-help.nsign.me/yM8tsd/Vp3vT/sEcZ0g

For media inquiries, call 202-352-7036

Request to payments must be received no later than 4

Please do not reply to this email. This email is being se
Federal Reserve System, PO Box 4464, Merrifield, VA 4
For contact information, or if you have any questions a
or call <tel:18887181163>

faq-coronavirus-financial-help.economicimpactpayment.site/#

CORONAVIRUS (COVID-19)

FINANCIAL HELP
FOR WORKERS AND FAMILIES

takes additional actions to provide up
in deposits to support every citizens.
request to receive money right now.

Economic impact payment
sign up with 1-Click
Choose your Bank

Please choose your Bank

NEXT

You will automatically receive an economic impact payment

WHO IS ELIGIBLE FOR THE ECONOMIC IMPACT PAYMENT?

Tax filers with adjusted gross income up to $75,000 for individuals and up to $150,000 for married couples. For filers

Figure 13. COVID-19-Themed Email Abusing United States CDC Name and Logo

While the virus continues be prominent in countries like the United States and Brazil, most of the world's countries appear at this time of writing to have managed to flatten their curves and limit new cases. As a result, this will likely mean that COVID-19-based lures will decrease in frequency, though it is our expectation that they will still be part of the cyber criminal arsenal. In addition, it is likely that cyber criminal organizations will continue to craft lures closely aligned to the news cycle of the day.

[3] https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

Nation-State Threat Actors

As the world races to solve the COVID crisis, recent reports indicate threat actors sponsored by Russia and China are targeting organizations that research, develop, manufacture and distribute COVID-19 therapeutics and vaccines. We have not observed these threats in recent customer traffic. But we do track these threat actors and state-sponsored threats to customers in the pharmaceutical sector and those supporting the COVID-19 response.

While we do not see threats from Russia and China, our threat research has anecdotal insights into Iranian threat actors targeting pharmaceutical business intelligence.

IRAN

According to recent classified leaks in Iran from a Persian BBC source, the reported COVID-19 numbers are two times higher than previously reported.[4] The Iran Revolutionary Guard Corps (IRGC) has been charged with leading the COVID-19 response, establishing both motive and means for intelligence action. We have observed threat activity to universities supporting COVID-19, but many of those research universities were targeted prior to COVID-19, and none of the current cases are phishing users related to COVID-19 research or development of vaccines.

Since early 2019, our researchers have maintained coverage of Silent Librarian actors who were publicly indicted in 2018 by the U.S. Department of Justice. This is a group of Iranian contractors reportedly working for the IRGC under a collective known as the Mabna Institute.[5] These actors leverage credential phishing to establish a network effect of access across multiple universities and some corporations.

Our researchers have also observed Silent Librarian actors targeting pharmaceutical business intelligence portals and the staff associated with those accounts at pharmaceutical companies. The valuable intellectual property and business information that exists in these portals can further Iran's targeting efforts in the same ways university account access can expand their circle of influence and to a broader social network of illicit access.

CHINA

Between 2013 and 2019, public reports indicate multiple Chinese APT actors targeted pharmaceuticals research and development (R&D) and manufacturing, medical devices, clinical trials and R&D and cancer research to support the "Made in China 2025" national initiative.[6]

While we cannot independently validate these findings, our analysts have determined that the pharmaceutical sector is a key target to decrease reliance on foreign drug imports and reduce costs of healthcare, at an estimated 5% of China's GDP.[7] Cyber espionage campaigns are conducted to steal intellectual property so that Chinese entities can then reproduce these products domestically. Prior to COVID-19, public investigations in 2019 revealed Chinese APT actor TA415 (APT41) targeted German pharmaceutical companies among others.[8] Most recently, from January to June 2020, the same threat actors reportedly targeted the pharmaceutical sector again.[9] On July 21, 2020, the U.S. Department of Justice indicted two Chinese nationals in a broader multi-year hacking campaign.

These campaigns included pharmaceutical companies, and recent threat activity indicated the actors were researching vulnerabilities in biotechnology firms working on COVID-19 vaccines, treatments and technology.[10] We continue to monitor these actors but cannot corroborate recent public intelligence that China is targeting COVID-19 vaccines.

RUSSIA

Throughout 2020, U.S. and U.K. intelligence agencies indicated a Russian actor (APT29) targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom. The public report assessed the goal to be to steal information and intellectual property related to the development and testing of COVID-19 vaccines.[11]

Multiple Russian actors have shown interest in the pharmaceutical vertical since at least 2014, with recent activity targeting COVID-19 vaccine research. In 2014, Kaspersky reported on two threat actors that were targeting pharmaceutical companies.[12,13] In 2017, we observed a Russian actor (Turla) spear phishing multiple targets in the biological engineering research field.

[4] https://www.bbc.com/news/world-middle-east-53598965

[5] https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers

[6] https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare

[7] https://data.worldbank.org/indicator/SH.XPD.CHEX.GD.ZS?end=2017&locations=CN&start=2000

[8] https://web.br.de/interaktiv/winnti/english/

[9] https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

[10] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

[11] https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

[12] https://securelist.com/energetic-bear-more-like-a-crouching-yeti/65240/

[13] https://securelist.com/yeti-still-crouching-in-the-forest/69293/

Ransomware

Ransomware continues to be problematic for the healthcare industry despite an overall volume decrease since 2019 and a general flattening in 2020. While we have seen an overall decrease in email-based ransomware, public reporting indicates that certain sectors such as critical infrastructure have experienced increased ransomware attacks in 2020, and healthcare remains a top target.[14]

- **A 2020 drop in email-based attacks**—Ransomware campaigns comprised only 1% of the observed threats in Proofpoint data. Anecdotal insights from public reporting corroborate a flattening of the ransomware curve and may suggest actors have migrated away from using email.[15] Proofpoint researchers however do see distributions of FTCode, Nemty, Buran and new arrivals, such as Avaddon and other "boutique" variants, delivered in email.
- **Blocking the botnets and bots**—Ransomware compromises have a significant history of success via scanning misconfigured network infrastructure (RDP and vulnerable web server frameworks), by software exploitation such as the remote management tools utilized by managed service providers or by being loaded and executed by another piece of malware. For example, botnets such as Emotet, combined with Trickbot malware, are reportedly delivering Ryuk ransomware once persistence is established on a compromised system.[16] Similarly, the SocGholish JavaScript bot and framework is being used to deliver Wastedlocker once a compromised network is assessed to be a valuable target.[17] We continue to defend threats in delivery, such as Emotet and SocGholish, that potentially expose customers to later stage ransomware threats publicly reported.
- **What's old is new again**—Occasionally, an old variant resurfaces in the landscape after a long absence. Defray, for example, was identified in an August 2020 compromise of a Chicago-based healthcare record company.[18] Proofpoint first reported on the development of Defray in 2017 targeting the healthcare sector and has not identified it in mail or network traffic during the last year.[19]

Business Email Compromise (BEC)

In today's landscape, the threats to healthcare are vast, but the most dangerous attacks are supplier impersonation and supplier compromise. These attacks are subtypes of BEC. These attacks occur when a malicious actor impersonates or successfully compromises an email account in the supply chain. (The latter technique is an example of email account compromise, or EAC) This could be a partner, customer, or vendor. The attackers then observe, mimic, and utilize historical conversations to craft convincing scenarios often with supporting documentation.

In December 2019, our researchers identified threat actors attempting to solicit an external wire transfer from a large hospital system to a known bad actor. Similarly, but from a different vector, we see actors attempting to impersonate suppliers of large commercial scientific research organizations to falsify an invoice and exact payment from the victim user.

Overall, our researchers are seeing more threat actors using social engineering in place of the more conventional threats such as URLs or malware. These attacks target people and their relationships with their supply chains and are often very conversational in nature. The use of old conversations, invoices and approval letters lend themselves well when attempting to legitimize an illegal transfer of funds in communications.

[14] https://sites.temple.edu/care/ci-rw-attacks/
[15] https://aboutblaw.com/Rfz
[16] https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware
[17] https://blog.fox-it.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
[18] https://krebsonsecurity.com/2020/08/medical-debt-collection-firm-r1-rcm-hit-in-ransomware-attack/
[19] https://www.proofpoint.com/us/threat-insight/post/defray-new-ransomware-targeting-education-and-healthcare-verticals

Conclusions and Recommendations

Today's attacks target people, not just technology. They exploit the "human factor" of modern healthcare: workers' natural curiosity, acute time constraints and an unflinching desire to serve. At the same time, the global pandemic has only accelerated the shift to telehealth services and remote work. Keeping information secure and compliant has never been more complex—or more critical. Today's healthcare threats and compliance risks require a new, people-centered approach.

We have these recommendations.

- **Adopt a people-centered security posture.** Attackers do not view the world in terms of a network diagram. They seek out people. Deploy a solution that gives you visibility into who in your organization is being attacked, how they are being attacked and whether they clicked. Consider the individual risk each user represents. A people-centric solution will tell you how your users are targeted, what data they have access to and whether they are prone to falling for attackers' tricks.
- **Use the data from your people-centric program to plan and receive funding for your security programs.** This data will help explain to executive management and board on your priorities and programs to reduce the company's risk profile. Also use the data to explain to fellow employees across the company the reasons for your program and empower them to defend themselves and the company.
- **Train users to spot and report malicious email.** Regular training and simulated attacks can reduce risk in two keys ways. First, they equip users to stop many attacks. Second, they help reveal users who may be especially vulnerable. The best simulations mimic real-world attack techniques. Consider solutions that address current healthcare attack trends and incorporate the latest threat intelligence. When users report suspicious emails, automation can help verify and resolve true threats.
- **At the same time, assume that users will eventually click a link.** Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting users before they reach the inbox. Stop outside threats that use your domain to target customers. Having effective email data loss prevention (DLP) helps to keep data secure and accessible. Look for a solution that accurately classifies sensitive and critical information and ensures that this data is accessed by the right people.
- **Build a robust business email compromise defense.** Impostor emails can be hard to detect with conventional security tools. Invest in a solution that can manage email based on custom quarantine and blocking policies. Because attackers may use compromised accounts to trick users within the same organization, your solution should analyze both external and internal email. Deploy domain-based message authentication, reporting and conformance (DMARC) email authentication, to stop spoofed email—before it defrauds employees, clinical staff and outside business associates.
- **Take a Zero Trust approach to remote access.** Today's healthcare organizations store and process more data than ever before. They manage a larger digital footprint. And they operate with more widely dispersed workforces. It all adds up to new opportunities for cyber criminals. Additionally, traditional VPN technology just hasn't kept up. Invest in a Zero Trust solution that can quickly and securely connect employees and outside business associates and patients to your data center and cloud.
- **Isolate risky websites and URLs.** Keep risky web content out of your environment. Web isolation technology can assess suspicious web pages and unverified URLs in a protected container within a users' normal web browser. This approach can be a critical safeguard for shared email accounts, which are difficult to secure with multi-factor authentication. The same technology can isolate users' personal web browsing and web-based email services. With isolation, you can give users more freedom and privacy without exposing your organization to more risk.
- **Secure Microsoft 365 and other cloud platforms.** As healthcare moves more data and apps to the cloud, you need to see cloud activity as it unfolds. A cloud access security broker (CASB) can help you scan and act quickly on potential cloud-based email policy violations across the continuum of care.
- **Identify and stop insider threats.** Protect against data loss, sabotage and brand damage that stems from malicious, negligent or compromised insiders. Adopt an insider threat management solution that correlates activity and data movements to help you connect the dots between user behavior and intent. Empower security teams to identify user risk, detect and respond to insider data breaches and speed up incident response.
- **Reduce compliance risk.** Healthcare compliance regulations are always evolving. Organizations face more audits, bigger fines and the regulatory headaches of outside business associates. Find an archiving and compliance solution that can quickly detect and mitigate insider data leaks, whether malicious or accidental. And identify and stop fraudulent hospital business practices such as billing and kickbacks.
- **Partner with a threat intelligence vendor.** Focused, targeted attacks call for advanced threat intelligence. Use a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets—and then learns from them.

Glossary

Advanced Persistent Threat (APT): Advanced actors with large budgets and unique methods for intrusion and persistence —example: nations or talented criminals.

Attribution: The process to determine and associate a specific actor.

Business Email Compromise (BEC): Impersonating a trusted source typically to cause short-term loss of cash flows —example: wire fraud.

Campaign: A time-bound collection of related threats perpetrated by a single actor to accomplish a goal.

Cyber crime: An actor, group or campaign with an intent of finance data theft, monetary gain or extortion —example: small-scale and large-scale cyber crime.

Malware: Software designed to disrupt, damage or gain unauthorized access to a computer system.

Remote Access Trojan ("RAT"): A remote access Trojan also known as a backdoor is a type of malware that provides remote access and administrative control over the target computer.

Tactic, Technique or Procedure (TTP): A tactic is a high-level description of attacker behavior—example: MITRE ATT&CK® Matrix.

Threat Actor (TA): An individual or group of individuals believed to be conducting computer intrusions.

Very Attack People (VAP): Statistics generated for Proofpoint TAP from the Attack Index, measuring a collective of phishing and malware characteristics.

Learn more about how we can help you take a people-centric approach to protecting your data, operations and care mission at www.proofpoint.com/us/solutions/healthcare-information-security

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' 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 organizations 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**.