PROTECTING AGAINST COVID-19 CYBER ATTACKS

A review of COVID-19 related attacks and how to spot and prevent them.

COURSE OBJECTIVES

FIRST OBJECTIVE

Learn the different malicious actors and their motivations: criminals, nation-states, thrill seekers and activists.

SECOND OBJECTIVE

Identify the different methods that malicious actors are using to attack individuals and organizations.

THIRD OBJECTIVE

Provide practical advice on how to reduce your risk and avoid COVID-19 related attacks.

FOURTH OBJECTIVE

Reinforce the importance of asking questions and reporting security concerns to your organization.

DEFINITIONS

A list of cybersecurity terms and their definitions

Term	Definition
Social engineering	The use of expert manipulation via email, text message, phone call or even in-person visits. It is the most common and effective technique used by attackers.
Phishing	The email-based form of social engineering. It is the most used social engineering tactic due to its ease of use and high probability of success.
SMShing	The text message form of social engineering. Less common than email due to aggressive attempts by telecommunications companies to filter malicious content.
DDOS	A form of online attack that floods websites and other online services with malicious traffic, effectively blocking legitimate visitors or users from accessing information.

MALICIOUS ACTORS AND THEIR MOTIVATIONS

The individuals and groups who are leveraging the COVID-19 pandemic to commit cyber attacks and the motivations behind the attacks.

CRIMINALS

Criminal gangs and individuals are primarily interested in identity theft, financial fraud and ransomware attacks.

NATION-STATES

Government hacking teams are seeking to steal intellectual property. Some are engaged in disinformation campaigns to destabilize other nation-states.

THRILL SEEKERS

Individuals who wish to further fear, uncertainty and doubt either for their own entertainment or for profiteering.

ACTIVISTS

Individuals or groups who are not pleased with how individuals, organizations or governments are handling the pandemic.

TYPES OF COVID-19 RELATED CYBER ATTACKS

PHISHING AND SMSHING

The use of email and text messages to send malicious links or malicious files. The purpose is to steal information or install ransomware.

MALICIOUS APPS

Attackers have created fake COVID-19 apps purporting to provide information on infection. Instead they hijack phones and demand a ransom.

MALICIOUS WEBSITES

Attackers have created fake COVID-19 infection maps that are designed to infect devices with malicious software.

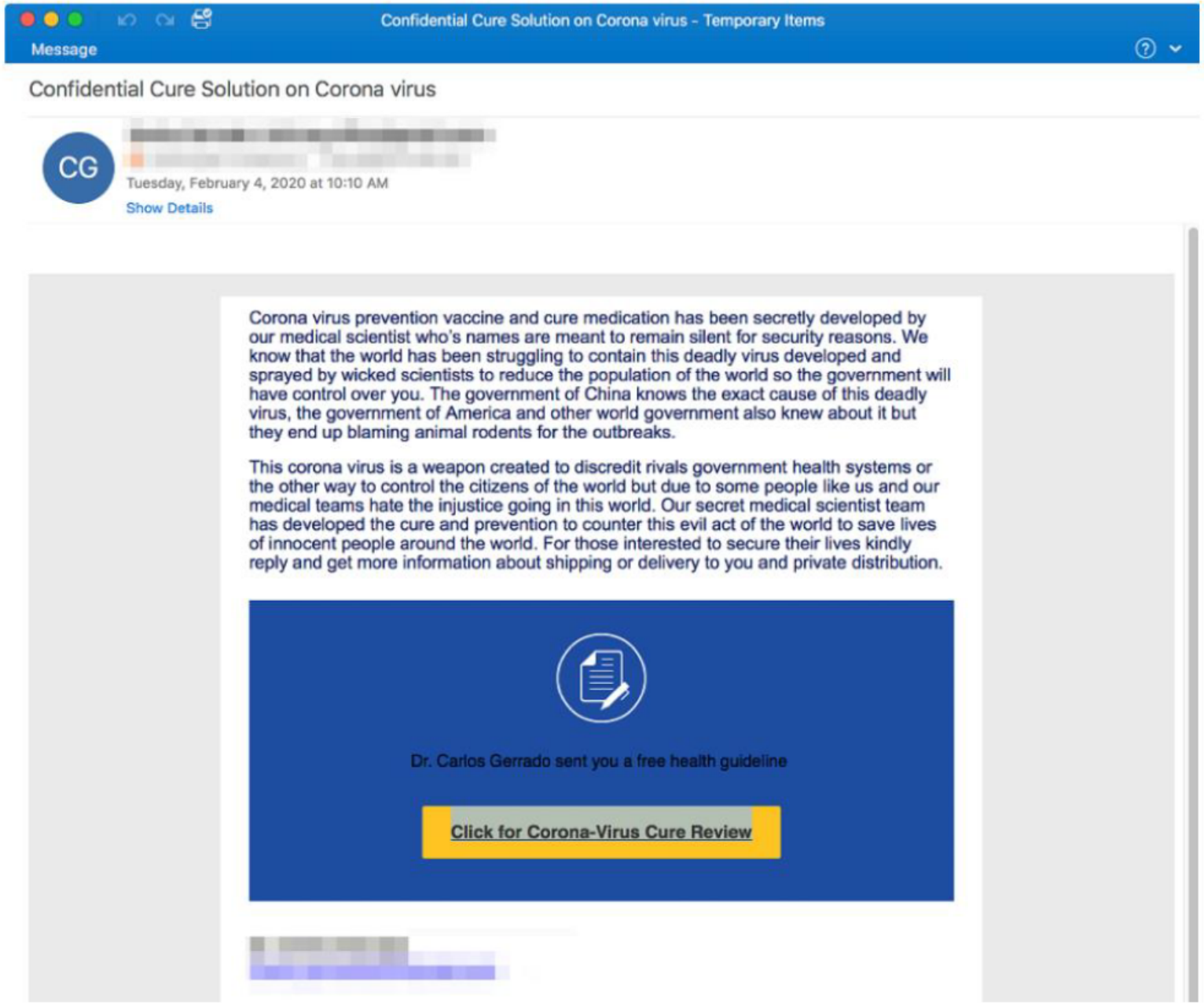
DDOS & DISINFORMATION

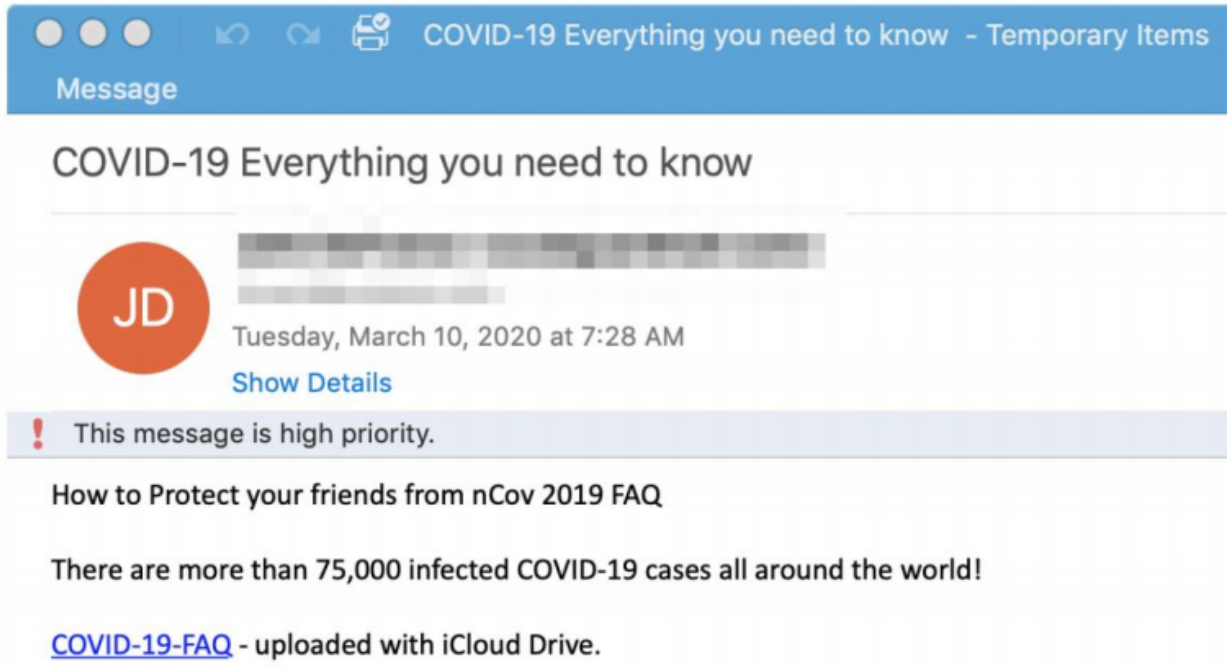
Criminals have launched attacks to disable COVID-19 government websites while simultaneously distributing false information via email, text and social media.

CORONAVIRUS CURE PHISH

This particular phish has a double-barrel: a malicious link and disinformation about the COVID-19 pandemic.

It uses a familiar design and layout from the popular service Docu-Sign as part of its design.



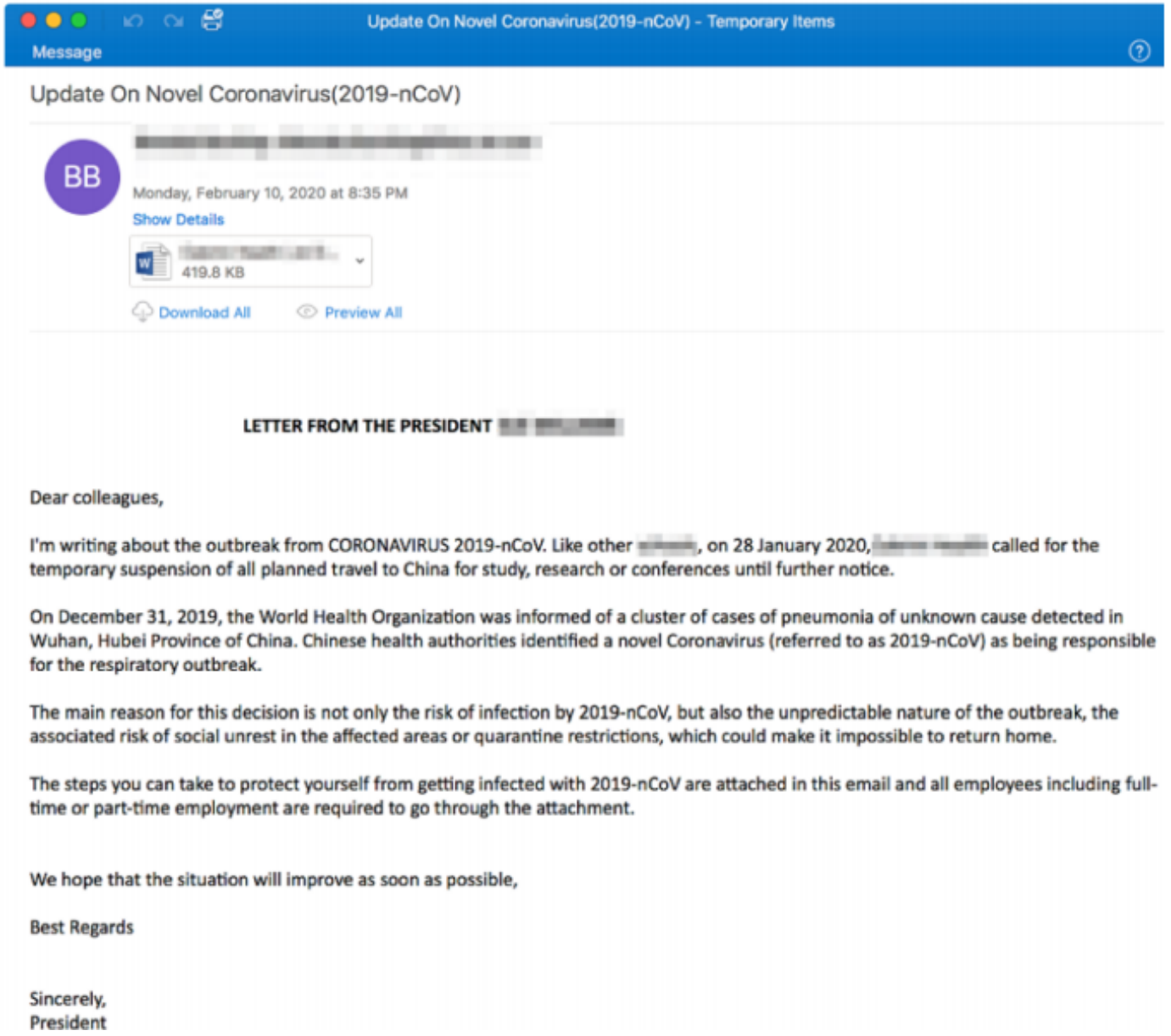


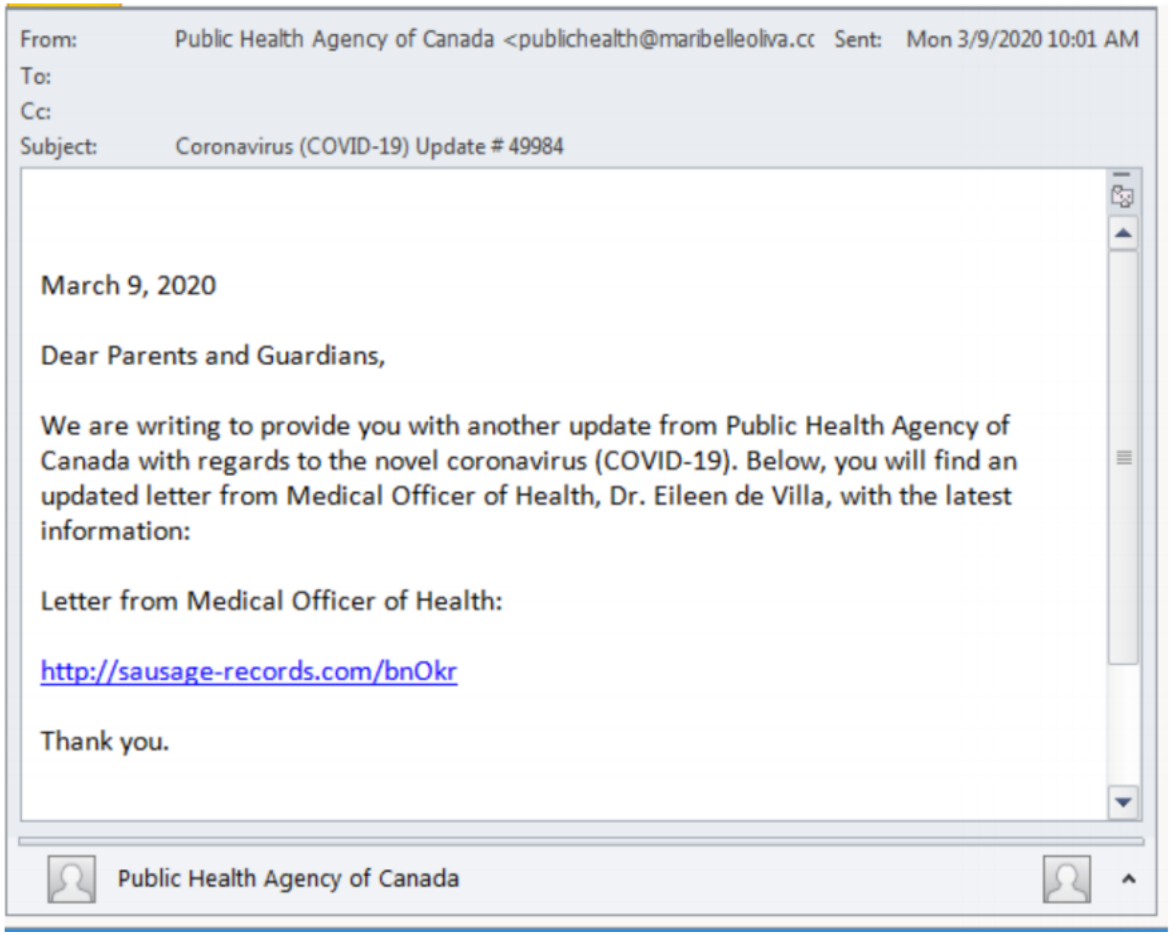
FAKE FREQUENTLY ASKED QUESTIONS PHISH

This link-based phish is designed to trick individuals into visiting a malicious website and to share this link with their family, friends and colleagues.

MESSAGE FROM THE CEO PHISH

In this phish, attackers created a fake message from the company's president. Unlike other link-based attacks, this phish is designed to get individuals to open the malicious attachment that was included in the message.





IMPERSONATING PUBLIC HEALTH AGENCIES

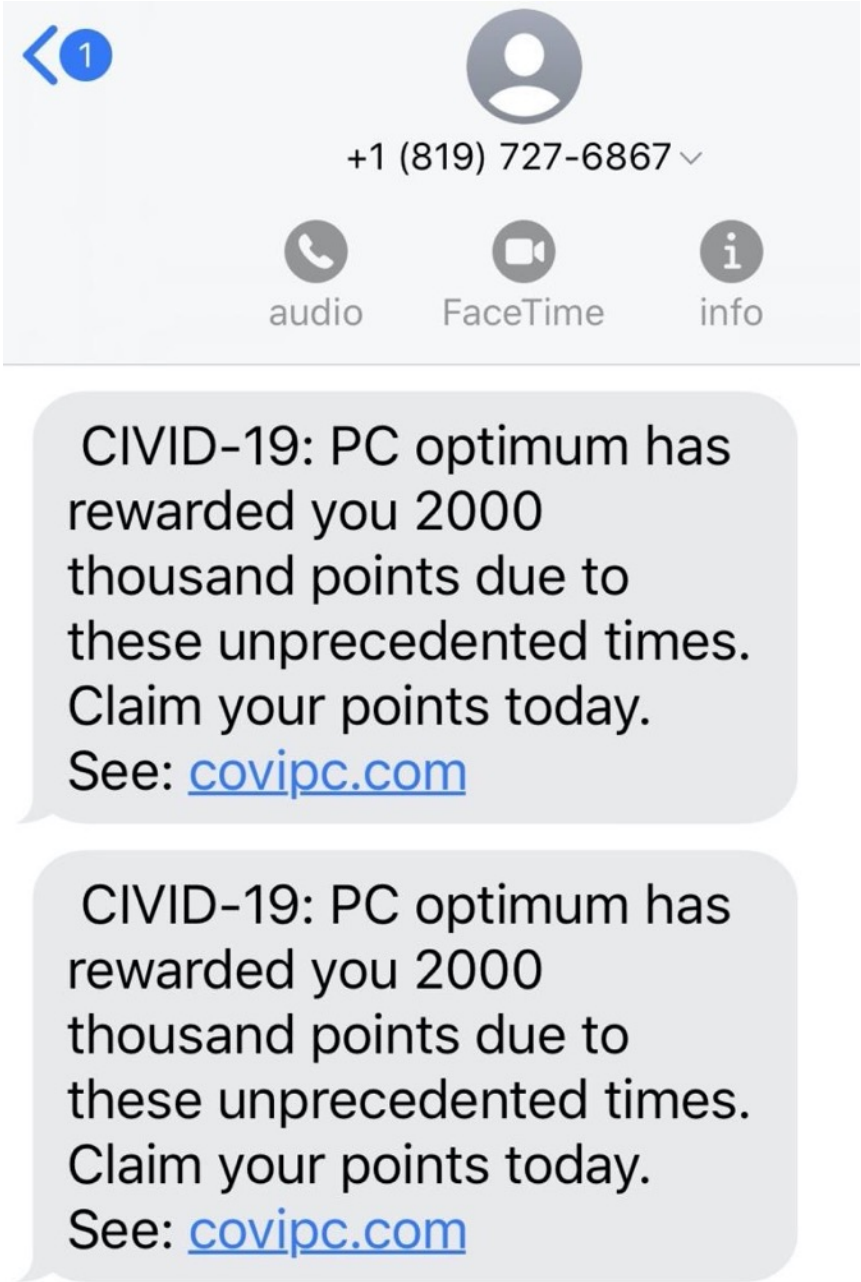
This phish uses known agency names and names of public health officials to provide an air of legitimacy. This phish was targeted at a Toronto-based organization.

This phish used the lure of information to try and trick parents into clicking the link. In this case, the attackers did a poor job hiding that the website was likely fraudulent.

MALICIOUS TEXT MESSAGES

In this example from Canada, attackers impersonated a popular rewards program used by supermarkets, pharmacies and more.

The attackers are using a lure that takes advantage of COVID-19.



MALICIOUS COVID-19 INFECTION MAPS

Attackers have created hundreds of fake websites providing misleading information or interactive maps. These sites attempt to find vulnerabilities in the web browsers of visitors.

They can then use these vulnerabilities to install malicious software designed to steal personal or organizational information, or to encrypt your data or device and hold them for ransom.

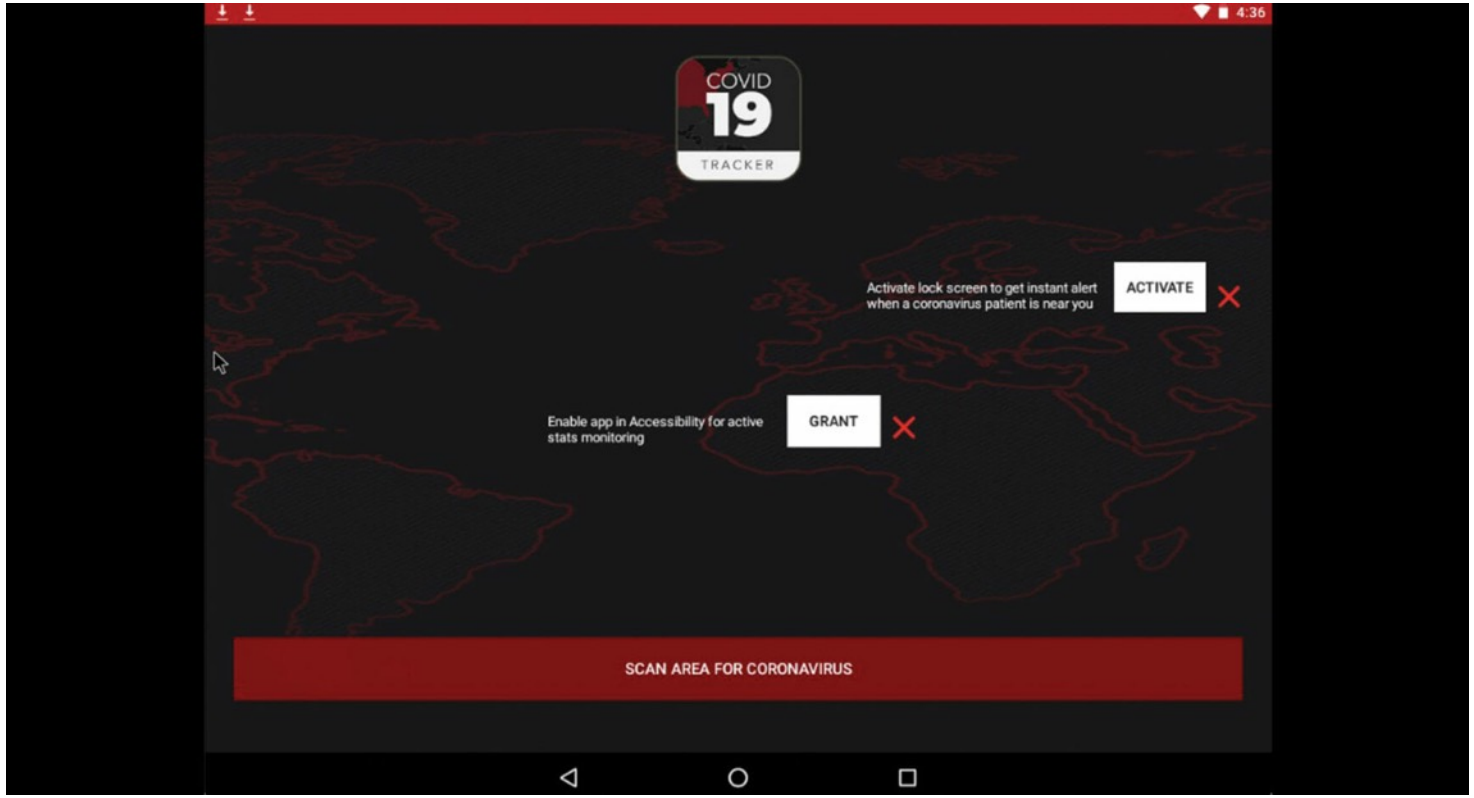
MALICIOUS MOBILE APPS

Attackers created a malicious Android app that falsely told users they could scan to find out the infection rates in their geographical area.

In reality, it gives the app permission to lock the user's screen and demand a ransom.

A note to victims stated that attempts to unlock the device without paying the ransom would result in the device being wiped.

Security researchers have since found a way to unlock devices that were affected by this attack. Similar attacks are likely.



PROTECTING YOURSELF AND YOUR ORGANIZATION

- Be careful clicking on links or opening attachments in emails and texts. Stay calm. Social engineering often preys on our fear and anxiety.
- If you are involved in approving financial transactions or banking, never rely on email alone. Confirm transactions by phone, video chat or secure instant messaging.
- Only visit trusted sites for COVID-19 information such as established news media or government websites.
- Be careful installing new apps on your smartphone or tablet.

HOW YOU CAN HELP

The first step to staying safe online is to remember that you are in control of technology. Stay calm, question unusual emails, texts or phone calls and reach out to your IT team or a trusted advisor about unusual messages or activities.

If you are receiving unusual COVID-19 related emails, please forward them using an email reporting tool or a reporting address that your organization provides. This can help your organization become aware of targeted attacks.

SUMMARY

- There are a wide variety of attackers with different motivations using COVID-19 to launch attacks.
- Knowing how to spot attacks and reacting calmly to messages about COVID-19 can help you avoid succumbing to an attack.
- Reporting suspicious emails and texts to your organization or law enforcement can help in wider efforts to spot and shut down attacks.
- Remember social engineering works by preying on emotions; stay calm and think before you click.

If you're interested in learning more, find us on social media at linkedin.com/company/beauceron-security or Twitter @BeauceronSec or connect with through e-mail at info@beauceronsecurity.com