Corona Virus (COVID-19) Scams

During any crisis there are those that would take advantage of a lower security stance by many individuals, businesses and organizations. Whether it is an individual malicious actor, group, or government sponsored hacking group.

Recorded Future has noticed a large increase of domain registrations specifically to emulate government health agencies or Corona virus specific sites. These domain registrations will be used to legitimize Phishing emails top make them appear to come from the CDC or WHO as well as many other foreign health organizations. The emails claim to have new information about COVID-19 and include attached files (Word Documents, PDF files, etc). These files contain a variety of computer malware. Other malicious actors are setting up fake websites in order trick individuals into exposing information such as credit card, Social Security, login info or other personal information to be used in later hacking schemes. There are also those that ask for money directly for immunity boosting supplements, or even a cure.

Things to look for:

Beware of online requests for personal information. A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.

Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.

Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.

Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.

Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete the message.

Below is a small list of example malicious domains, security services monitoring the domain registrars have seen as many as 17,000 new COVID-19 related domains registered in a day some are legitimate sites, but a large percentage are not:

acccorona.com

alphacoronavirusvaccine.com

anticoronaproducts.com

beatingcorona.com

beatingcoronavirus.com

bestcorona.com

betacoronavirusvaccine.com

buycoronavirusfacemasks.com

byebyecoronavirus.com

cdc-coronavirus.com

combatcorona.com

contra-coronavirus.com

corona-armored.com

corona-crisis.com

corona-emergency.com

corona-explained.com

corona-iran.com

corona-ratgeber.com

coronadatabase.com

coronadeathpool.com

coronadetect.com

coronadetection.com

cdc-gov.org

Here are a couple examples of Phishing Scams that have been distributed:

Email

"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear ████████████

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [[current_date_1]].

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization·

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

[Safety measures]

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

There have also been Text Messages, Facebook ads, Twitter posts, and many other social outlets targeted by malicious actors.

Text Message
Today 1:17 PM

Because of the COVID-19 outbreak we are giving out free iPhone 11 smartphones to help you spend time at home: Katie, go to appie10.info/Dl7uxPFI0t