

Examining the behaviours of recent malware exploiting the COVID19 pandemic



Suleiman Y. Yerima (PhD, CISSP, CEH)

Cyber Technology Institute

De Montfort University, Leicester

United Kingdom

Cybersecurity Education & Research Conference, Kuwait, Nov. 24-25, 2022

Introduction: About the author

- ▶ **Suleiman Yerima (PhD, CEH, CISSP)**
- ▶ Senior Lecturer in Cyber Security @ De Montfort University
- ▶ Member of Cyber Technology Institute (CTI) @ De Montfort University
- ▶ Research Interests: Malware, applied machine Learning, mobile security, behavioral biometrics, network security, digital forensics ...

Outline

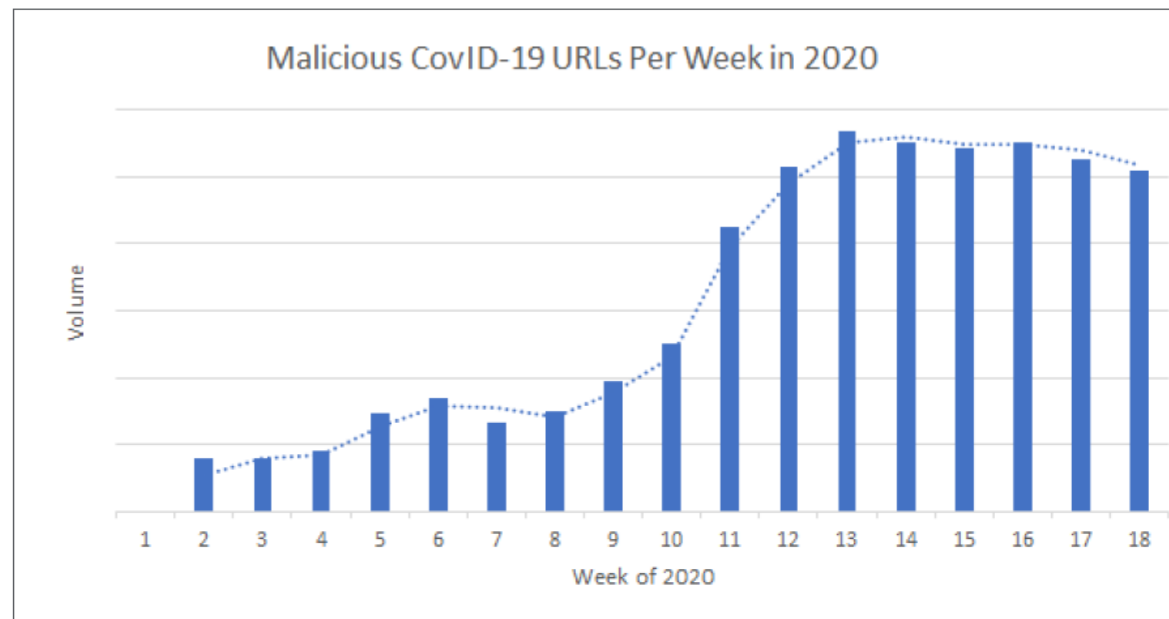
- ▶ Introduction
 - ▶ Covid-19 themed malware
 - ▶ Social engineering-based infection vectors
- ▶ CoronaVirus ransomware behaviour
- ▶ CovidLock ransomware behaviour
- ▶ Conclusion

Introduction

- ▶ The current Covid-19 pandemic is being exploited by cybercriminals taking advantage of peoples' anxieties and changes in working pattern.
- ▶ There's been an increase in the spread of malware through social engineering which is quite effective during a crises.
- ▶ Various Covid-19 themed malware families have emerged targeting PCs and mobile devices.
- ▶ These are spread through Covid19-themed **phishing emails, fake apps, fraudulent websites, and adverts loaded with malware.**

Introduction

- ▶ McAfee detected thousands of Covid19-themed spam emails and websites
- ▶ Malicious URLs with references to COVID-19 and Coronavirus increased dramatically during the start of the pandemic
- ▶ Malicious URLs seen weekly increased exponentially from 1,600 to > 39,000



Source: McAfee rp quarterly threats July 2020

Introduction

- ▶ Several Covid-19 themed malware appeared in the wild
- ▶ These include viruses, Remote Access Trojans (RATs), Ransomware, and malicious apps

Ursnif

Fariet

Emotet

CovidLock

Azorult

Hancitor

NetWalker

KPOT

CoronaVirus

Trickbot

Nanocore

Remcos

Introduction

Example of social engineering based infection vectors:

Fake Covid-19 tests

- ▶ Phishing emails distributed in March that appears to originate from organizations offering Covid19 testing.
- ▶ Users are prompted to open an attached document which will download the information stealing **Trickbot** malware.

Introduction

Example of social engineering based infection vectors:

Fake Covid-19 Precautionary measures

- ▶ In April, phishing email campaigns distributed the **NanoCore RAT** for exfiltration of valuable information.
- ▶ The emails used subject lines such as “***COVID-19 Urgent Precaution Measures***”

Introduction

Example of social engineering based infection vectors:

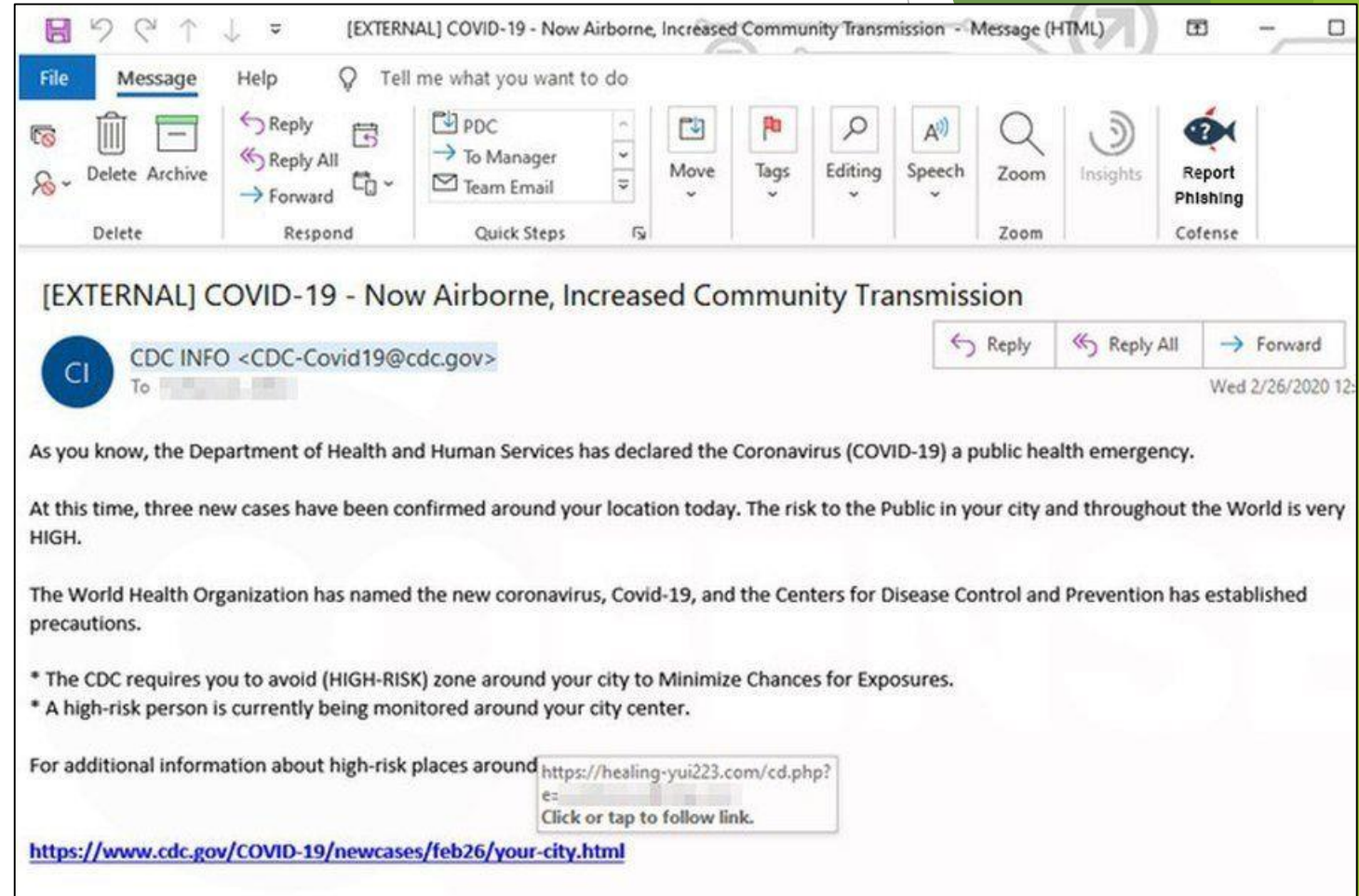
Bogus SBA Loan Emails

- ▶ In March, phishing email campaigns distributed the information stealing **Remcos RAT**
- ▶ The emails appeared to offer small businesses information and guidance on how to apply for Small Business Administration loans
- ▶ The emails claim to originate from the U.S. Government

Samples of fake emails



Source: NBC news



Source: BBC

Samples of fake emails

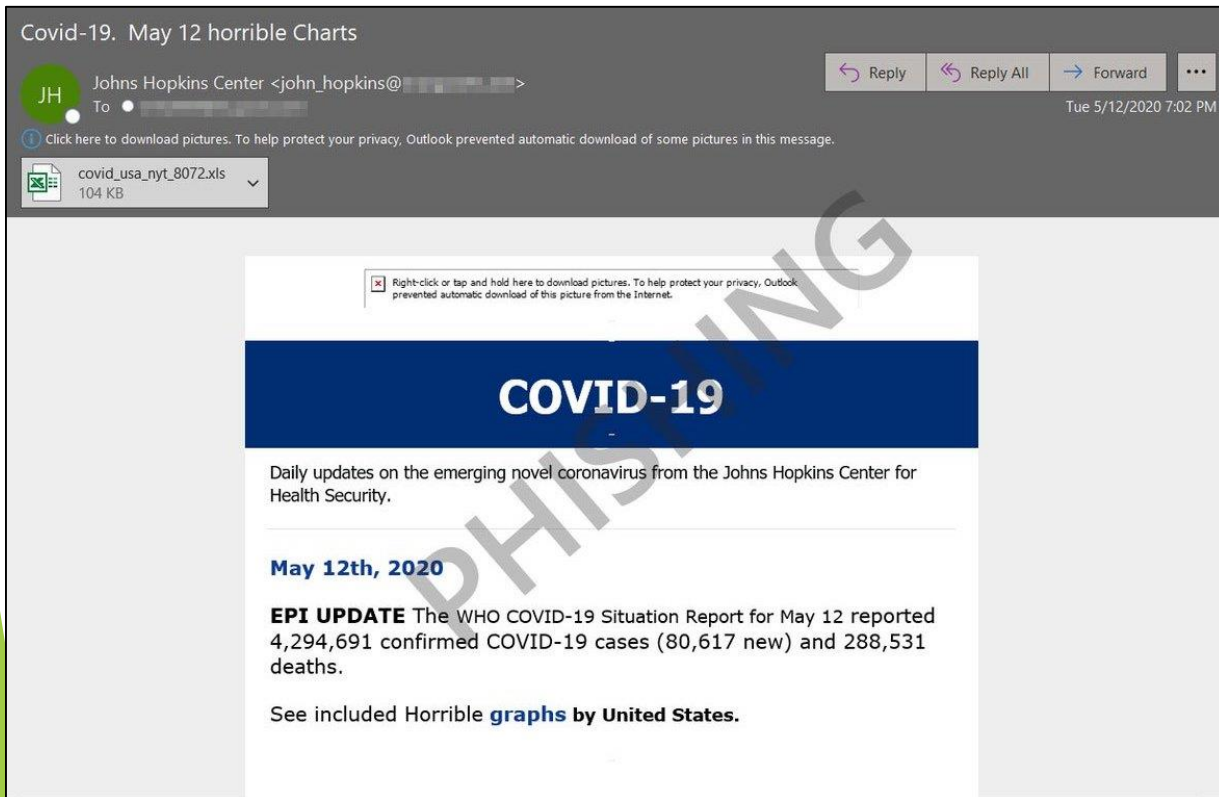


Source: Forbes

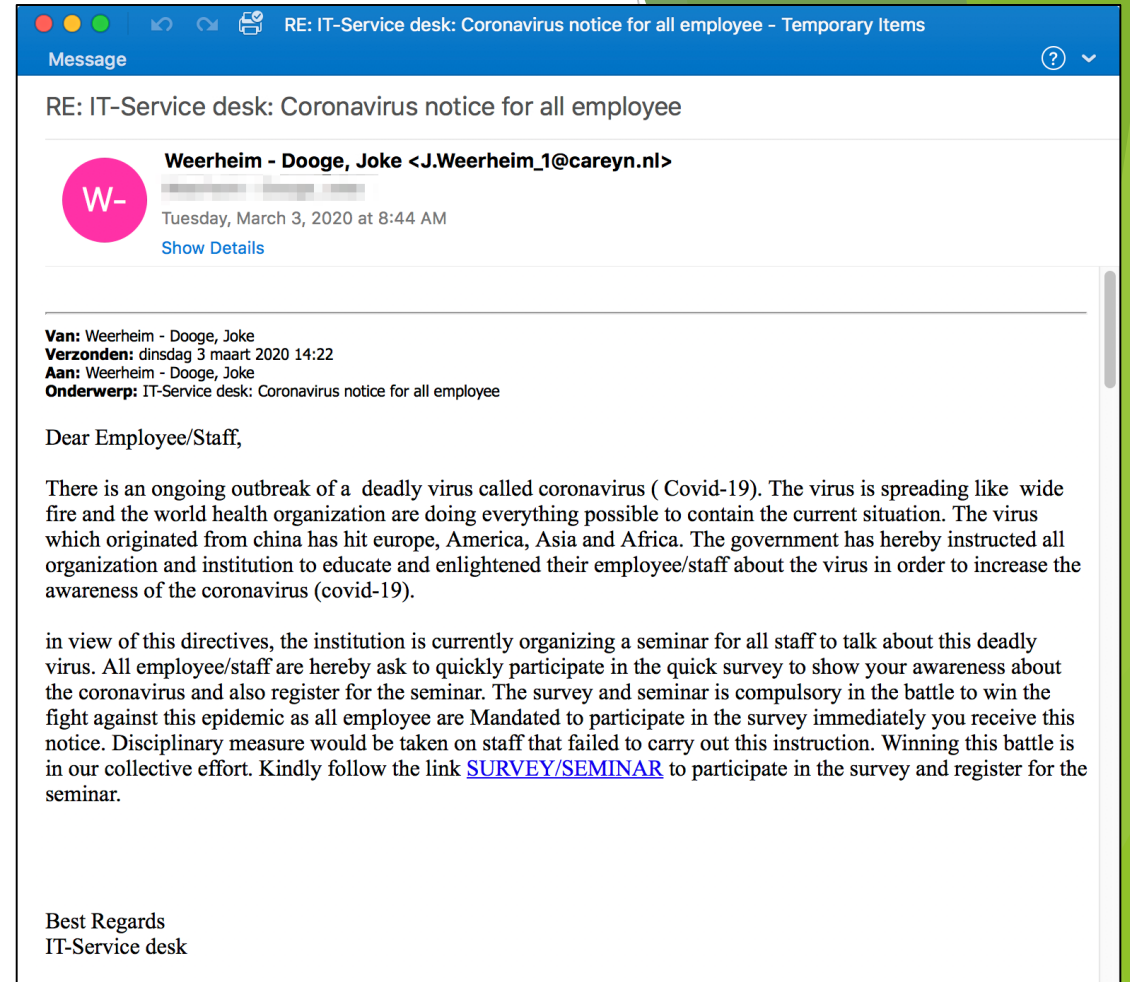


Source: Livemint.com

Samples of fake emails



Source: UT Health San Antonio



Source: proofpoint

CoronaVirus ransomware



- ▶ A file-locker ransomware threatening users worldwide
- ▶ Spread through fake websites that lures users into downloading an executable WSHSetup.exe
- ▶ The file downloads several .exe files from other websites
- ▶ The exe files contain **CoronaVirus** ransomware and **KPOT** trojan
- ▶ It is a ransomware attack bundled with information stealing trojan
- ▶ The primary aim is information theft but ransomware is used as diversionary tactic

CoronaVirus ransomware



- ▶ Encrypts files and override the MBR of a disk
- ▶ Renames the C drive of the computer to 'CoronaVirus'
- ▶ Victim computers do not load the OS on re-boot but displays ransom message

CoronaVirus ransomware



- ▶ Encrypt files:

.bak, .bat, .doc, .jpg, .jpe, .txt, .tex, .dbf, .xls, .cry, .xml, .vsd, .pdf, .csv, .bmp, .tif, .tax, .gif, .gbr, .png, .mdb, .mdf, .sdf, .dwg, .dxf, .dgn, .stl, .gho, .ppt, .acc, .vpd, .odt, .ods, .rar, .zip, .cpp, .pas, .asm, .rtf, .lic, .avi, .mov, .vbs, .erf, .epf, .mxl, .cfu, .mht, .bak, .old

- ▶ Places a ransom note in every folder demanding a payment of **0.008 bitcoins**

- ▶ All encrypted files are renamed to some variation of 'coronaVi2022@protonmail.ch'

CoronaVirus ransomware



```
CORONAVIRUS is there All your file are encrypted.  
Your computer is temporarily blocked on several levels.  
Applying strong military secret encryption algorithm.  
  
To assist in decrypting your files, you must do the following:  
1. Pay 0.008 btc to Bitcoin wallet bclq6ryyex33jxgr946u3jyre66uey07e2xy3v2cah  
or purchase the receipt Bitcoin;  
2. Contact us by e-mail: coronaVi2022@protonmail.ch and tell us this your  
unique ID:  
and send the link to Bitcoin transaction generated or Bitcoin check number.  
After all this, you get in your email the following:  
1. Instructions and software to unlock your computer  
2. Program - decryptor of your files.  
Donations to the US presidential elections are accepted around the clock.  
Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]
```

CoronaVirus ransomware ransom note

CoronaVirus ransomware



- ▶ Changes Windows registry setting to display a lock screen when the computer is rebooted
- ▶ Lock screen shows the same message as ransom note before finally loading the OS.
- ▶ Lock screen changes after 45 minutes but still denies access to the computer
- ▶ Eventually boots into Windows after a further 15 mins. Users will be presented with the same ransom note again after login in:

```
!!!!CORONAVIRUS is there!!!!  
All your file are crypted.  
Your computer is temporarily blocked on several levels.  
Applying strong military secret encryption algorithm.  
  
To assist in decrypting your files, you must  
Pay to Bitcoin wallet: bc1qkk6nwhsxvtp2akunhkke3tjcy2wv2zkk00xa3jcontact us  
via e-mail: coronavi2022@protonmail.ch  
Donations to the US presidential elections are accepted around the clock.  
Desine sperare qui hic intras! [wait timeout 15 min]
```

Coronavirus ransomware alternate lock screen

CoronaVirus ransomware: KPOT activity

- ▶ KPOT trojan steals cookies, passwords, and other credentials.
- ▶ Grabs a screen shot of the active desktop and scans for bitcoin wallets
- ▶ All info gathered by the trojan is sent to another website where it is gathered by attackers
- ▶ The malware basically steals information then encrypts files and overrides the MBR

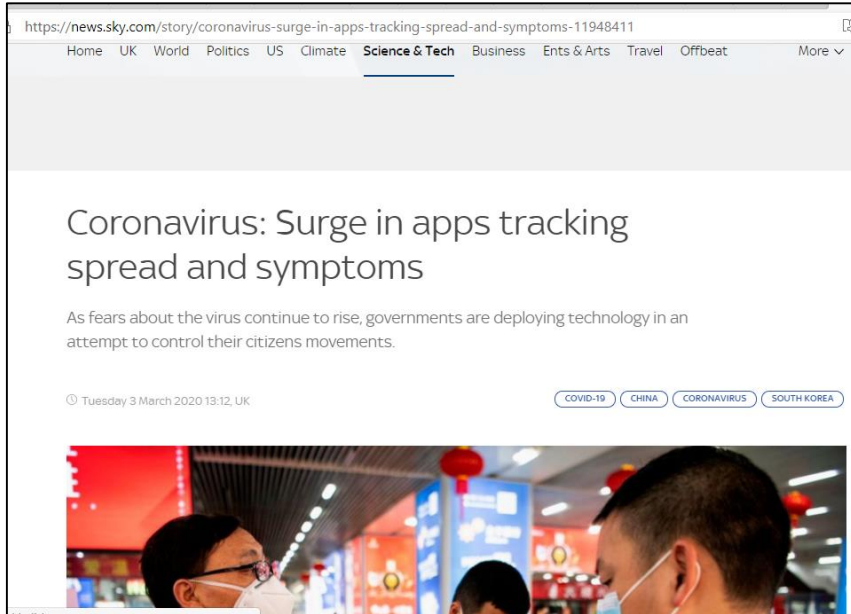


CoronaVirus ransomware

- ▶ Low ransom demand from the ransomware + a static address that received no payment = **Fake ransomware**
- ▶ The ransomware distracts from the information stealing trojan
- ▶ By making victims worried about ransomware it distracts from KPOT activity.



Proliferation of apps for Covid-19



Governments and citizens are using apps in an attempt to learn more about the coronavirus outbreak and prevent it spreading further.

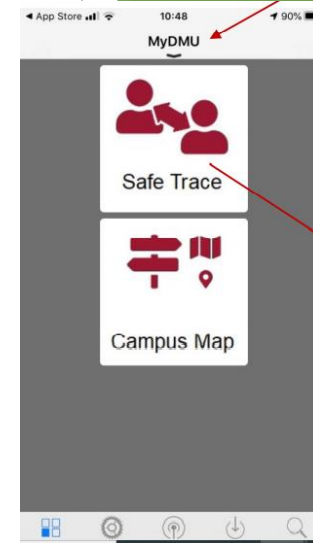
The rush to access new information on [coronavirus](#) shows little sign of slowing. Confirmed infections of [COVID-19](#) now number more than 91,000 people globally, resulting in more than 3,000 deaths.

The majority of these deaths have occurred in China, which has responded to the outbreak by requiring people to download smartphone software called the Alipay Health Code.

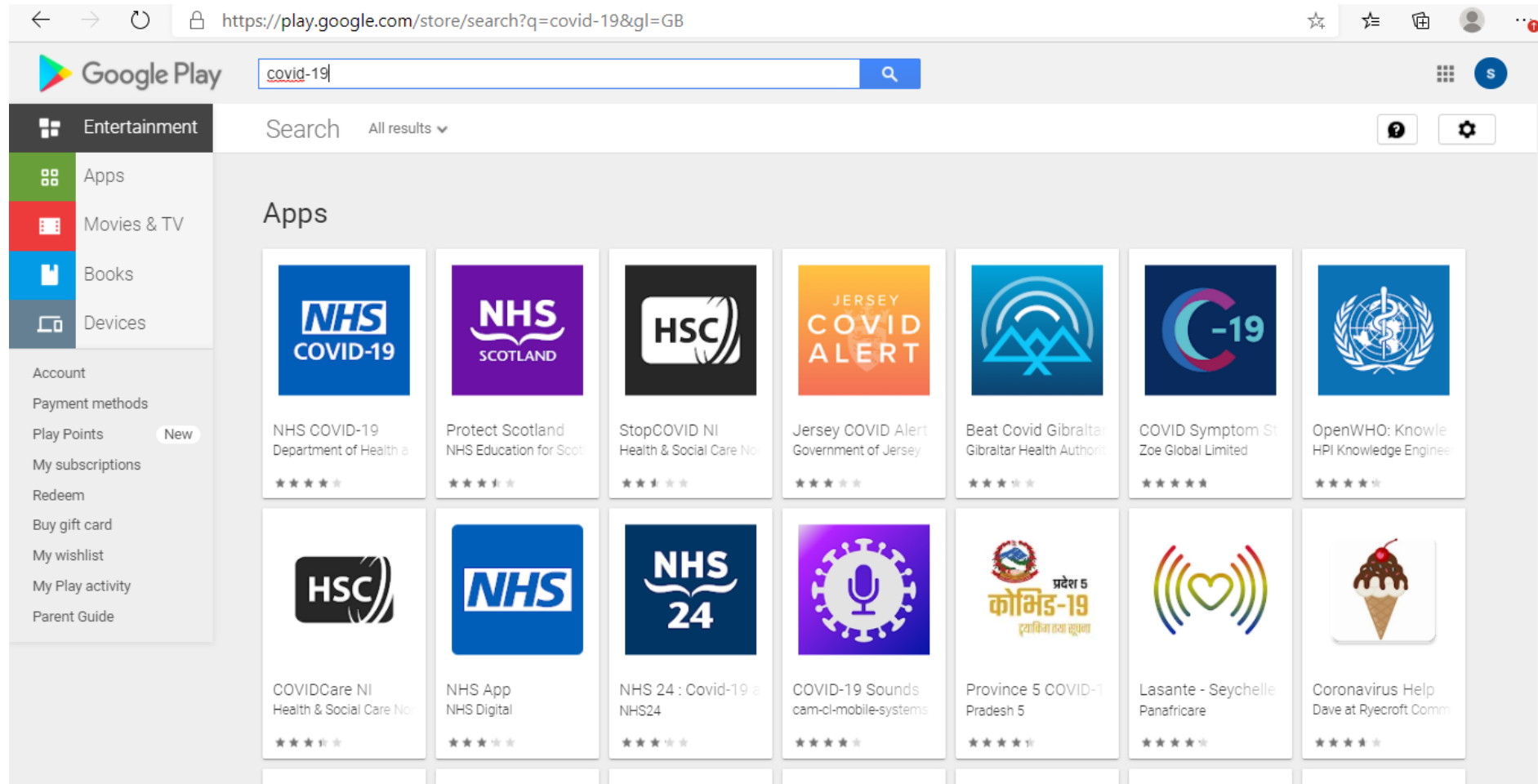


Coronavirus: The infection numbers in real-time

Designed by the Chinese technology giant Alipay, the health-rating app automates decisions on whether individuals should quarantine themselves or be allowed to enter public spaces through colour-



Proliferation of apps for Covid-19



The screenshot shows the Google Play Store search results for 'covid-19'. The search bar at the top contains 'covid-19'. The results are displayed in a grid of app cards. Each card shows the app icon, name, developer, and a star rating. The apps listed include:

- NHS COVID-19 (Department of Health)
- Protect Scotland (NHS Education for Scotland)
- StopCOVID NI (Health & Social Care Northern Ireland)
- Jersey COVID Alert (Government of Jersey)
- Beat Covid Gibraltar (Gibraltar Health Authority)
- COVID Symptom St (Zoe Global Limited)
- OpenWHO: Knowledge HPI (Knowledge Engineering Institute)
- COVIDCare NI (Health & Social Care Northern Ireland)
- NHS App (NHS Digital)
- NHS 24: Covid-19 (NHS24)
- COVID-19 Sounds (cam-cl-mobile-systems)
- Province 5 COVID-19 (Pradesh 5)
- Lasante - Seychelle (Panaficare)
- Coronavirus Help (Dave at Ryecroft Community)



CovidLock ransomware

- ▶ Mobile ransomware spread through websites and applications that claim to provide information about coronavirus.
- ▶ The name of the app is **Coronavirus Tracker**
- ▶ CovidLock was found on the website **coronavirusapp.site**
- ▶ The website recommends users download and install an app to get:
 - ▶ Updates about coronavirus, including notifying users when the virus reaches where they live.
 - ▶ Heatmap visuals that show the spread of infection across an area.
- ▶ The website appears to display information straight from WHO and CDC while hosting the CovidLock ransomware.

CovidLock ransomware



for android users: to get real-time number of coronavirus cases based on your GPS location please download the [mobile app version](#) of the website and enable "accurate reporting" for best experience

Thank you Reddit for the incredible feedback. Please implementing your suggestions as the week progresses. Stay tuned!

DASHBOARD
United States Coronavirus (COVID-19) Tracker

Infection Map ([hide](#))
Sorry, we couldn't accurately determine your location. Please try reloading the page, or interact with the map manually instead.

Inform your friends & family:
f Share WhatsApp Share Email Tweet Share

Buy me a coffee

Nationwide Live Data (refresh for updates)

CONFIRMED CASES	DEATHS	RECOVERED
805 ↑ 50% (+268 since ~24hr ago)	28 ↑ 33% (+7 since ~24hr ago)	8 0% (+0 since ~24hr ago)

Cases by Location ([hide](#))

Westchester County, NY	98
King County, WA	83
Unassigned Location (From Diamond Princess) County, Other	45
Santa Clara County, CA	38
Snohomish County, WA	31

Confirmed Cases & Deaths

Source: domaintools

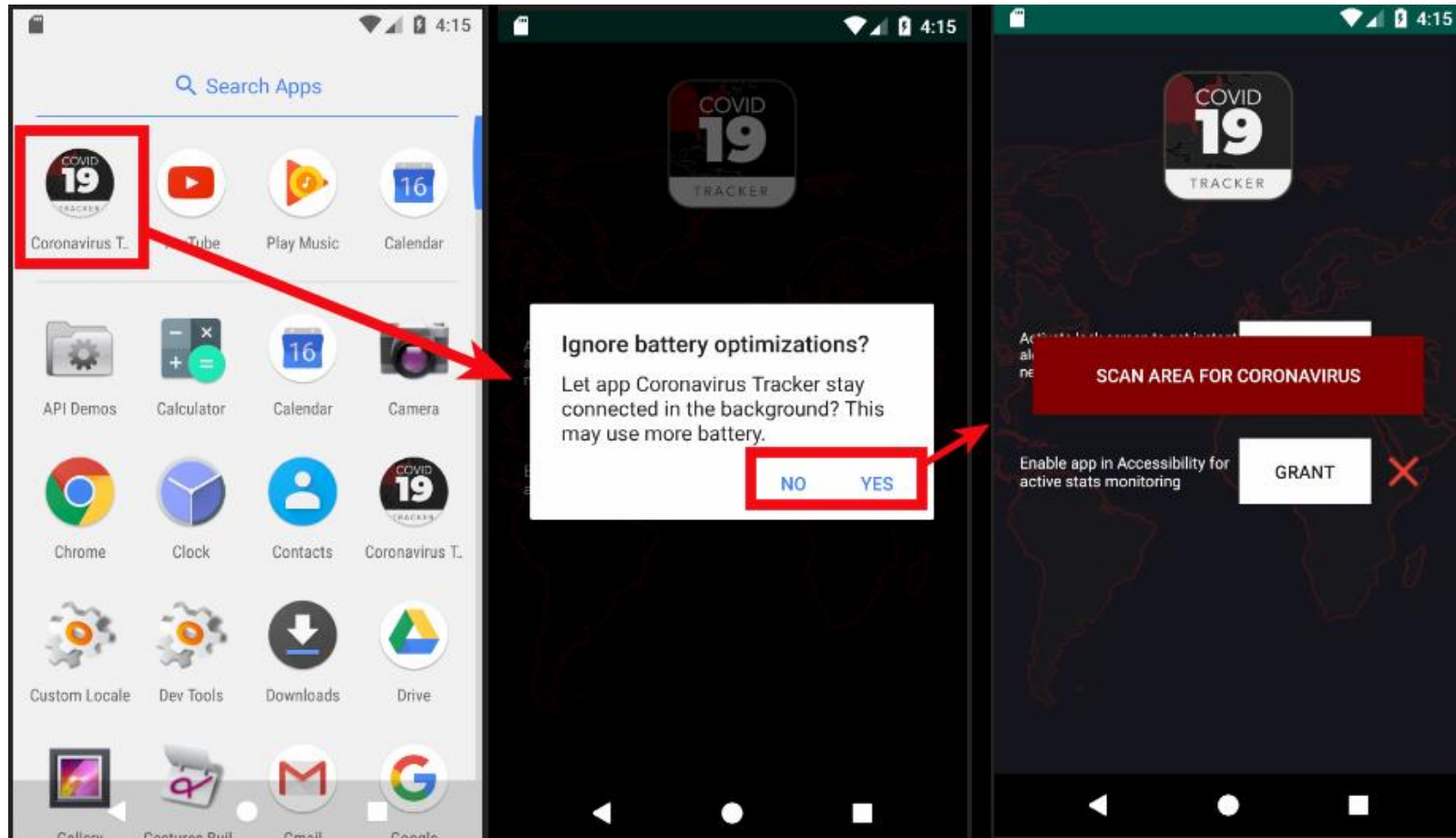
CovidLock ransomware



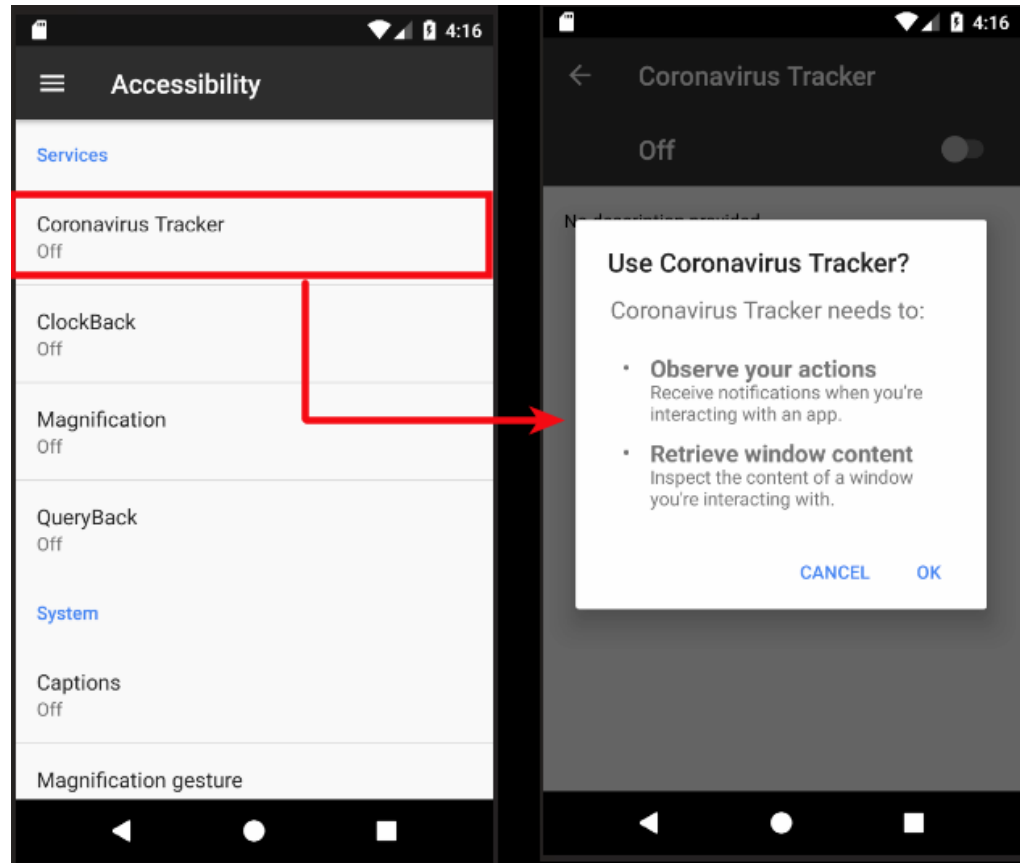
- ▶ CovidLock changes the lockscreen of the infected device
- ▶ Demands a ransom of \$250 in bitcoin for a decryption key to unlock their screen and get back control over their device.
- ▶ Threatens to erase all information on the phone including photos, videos, messages, and contacts if payment isn't received within 48 hours.
- ▶ The ransom note is written to scare victims into complying with the hackers demands.
- ▶ The message reads: “YOUR GPS IS WATCHED AND YOUR LOCATION IS KNOWN. IF YOU TRY ANYTHING STUPID YOUR PHONE WILL BE AUTOMATICALLY ERASED.”



CovidLock ransomware

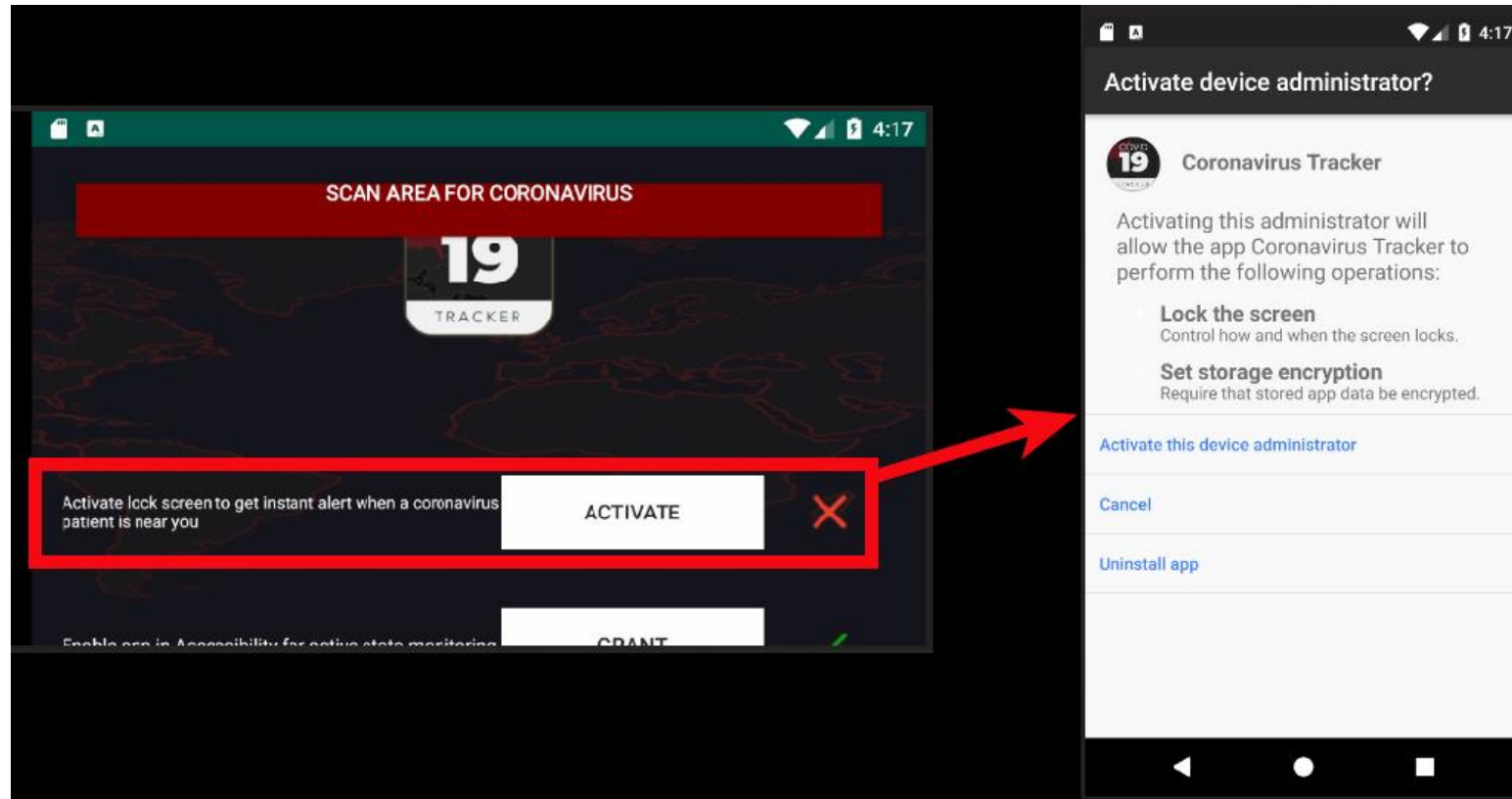


CovidLock ransomware



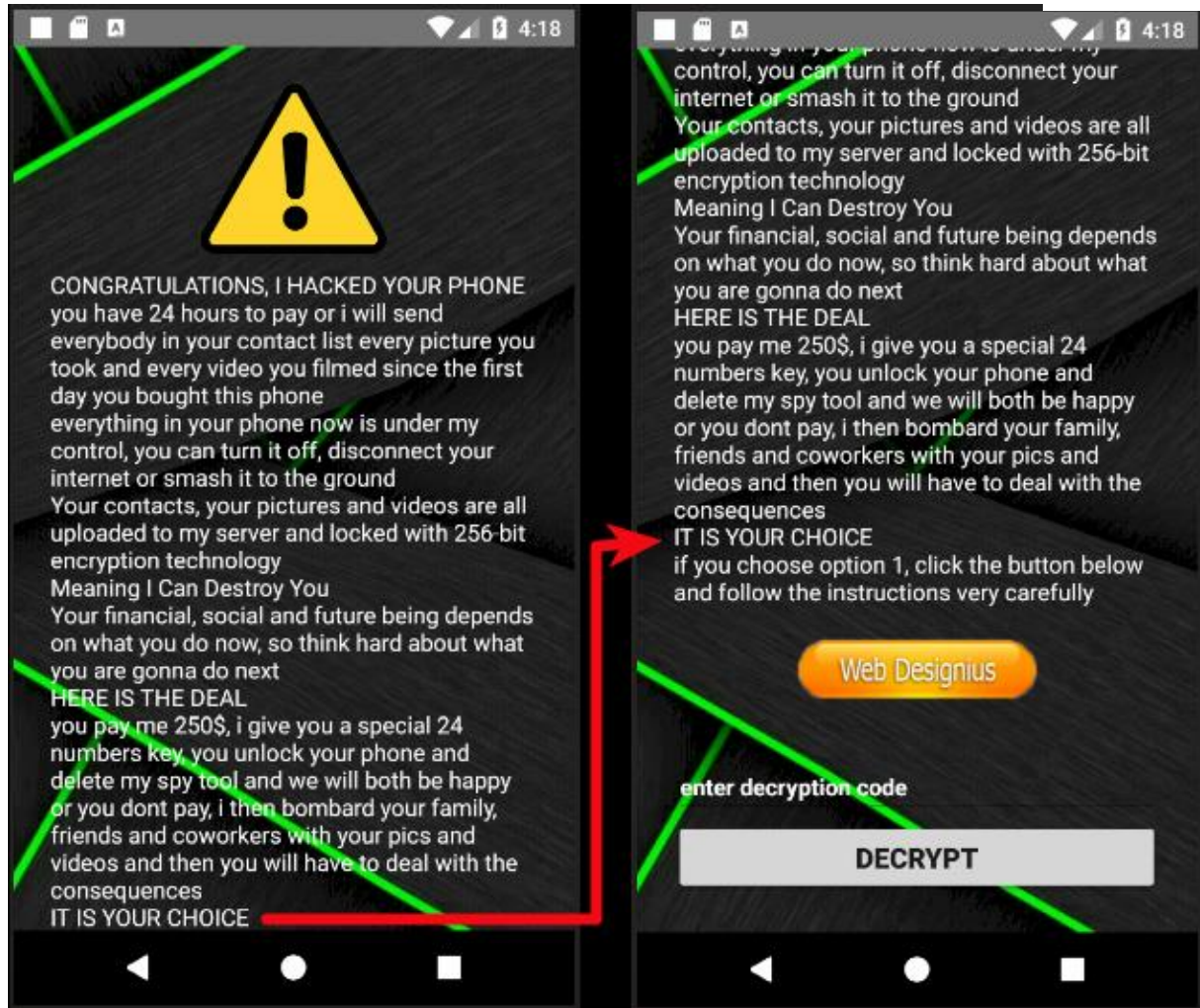
Accessibility request:
To keep the malware persistent

CovidLock ransomware





CovidLock ransomware



CovidLock ransomware



Everything in your phone now is under my control, you can turn it off, disconnect your internet or smash it to the ground
Your contacts, your pictures and videos are all uploaded to my server and locked with 256-bit encryption technology
Meaning I Can Destroy You
Your financial, social and future being depends on what you do now, so think hard about what you are gonna do next
HERE IS THE DEAL
you pay me 250\$, i give you a special 24 numbers key, you unlock your phone and delete my spy tool and we will both be happy or you dont pay, i then bombard your family, friends and coworkers with your pics and videos and then you will have to deal with the consequences
IT IS YOUR CHOICE
if you choose option 1, click the button below and follow the instructions very carefully

Web Designius

enter decryption code

DECRYPT

https://pastebin.com/GK8qrf:

Untitled

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

0.39 KB raw download report

Here is how it works

1. make an account at www.coinbase.com
2. verify your identity
3. plug a payment method, paypal, credit card or else
5. navigate to "Send" page and select "Wallet Address"
6. send 250\$ worth of bitcoin to this address:
185ykfkAPEhoxT8V6gvSLHvC6Lz8bxn3rd
7. once transaction is complete, send the transaction ID to this email: phc859ngge638@inbox.ru
8. wait until i respond

RAW Paste Data

Here is how it works

1. make an account at www.coinbase.com
2. verify your identity
3. plug a p We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the [Cookies Policy](#).
5. navigate
6. send 250
7. once transaction is complete, send the transaction

Conclusion

- ▶ Hackers and cybercriminals are exploiting the pandemic to spread malware
- ▶ This is evident in the rise of spam phishing emails with Covid-19 themes and malicious URLs linked with Covid-19
- ▶ All kinds of malware are being spread: RAT, ransomware, malicious apps
- ▶ While several families like Ursnif, Trickbot, Remcos are being used for information stealing, CoronaVirus adds a level of sophistication by deploying KPOT for information stealing while diverting attention with a file locker.
- ▶ Mobile users also need to beware of malicious apps like the fake Coronavirus Tracker that contains a ransomware designed to trick users into making bogus payments.

Thank you

Any questions?