A growing cyber threat linked to COVID-19

Nokia Analysis reveals a range of attempts by criminals to exploit the current global health crisis

White Paper

Contents

Introduction 3

Malware directly related to the COVID-19 outbreak 3

“Coronavirus Maps” Trojan 3

CovidLock Android Ransomware 4

COVID-19 themed phishing attacks delivering various malwares 5

PlugX delivered by COVID themed documents 5

HawkEye Info-Stealer distributed as fake COVID19 drug advice 5

Win32.COVID-themed campaign from Kimsuky 5

Android.Corona Safety Mask SMS Scam 5

Android. “corona live 1.1” SpyMax surveillance-ware 5

Ways that help keep users safe 6

Coverage of COVID-19 threats 6

Abbreviations 6

Introduction

As the COVID-19 virus spreads around the world, it's little surprise that cybercriminals are exploiting people's fears in attempts to steal data, gain personal information or deploy ransomware. There are two main threats – malware directly related to the Corona virus outbreak and established malware delivered through Corona-related phishing campaigns.

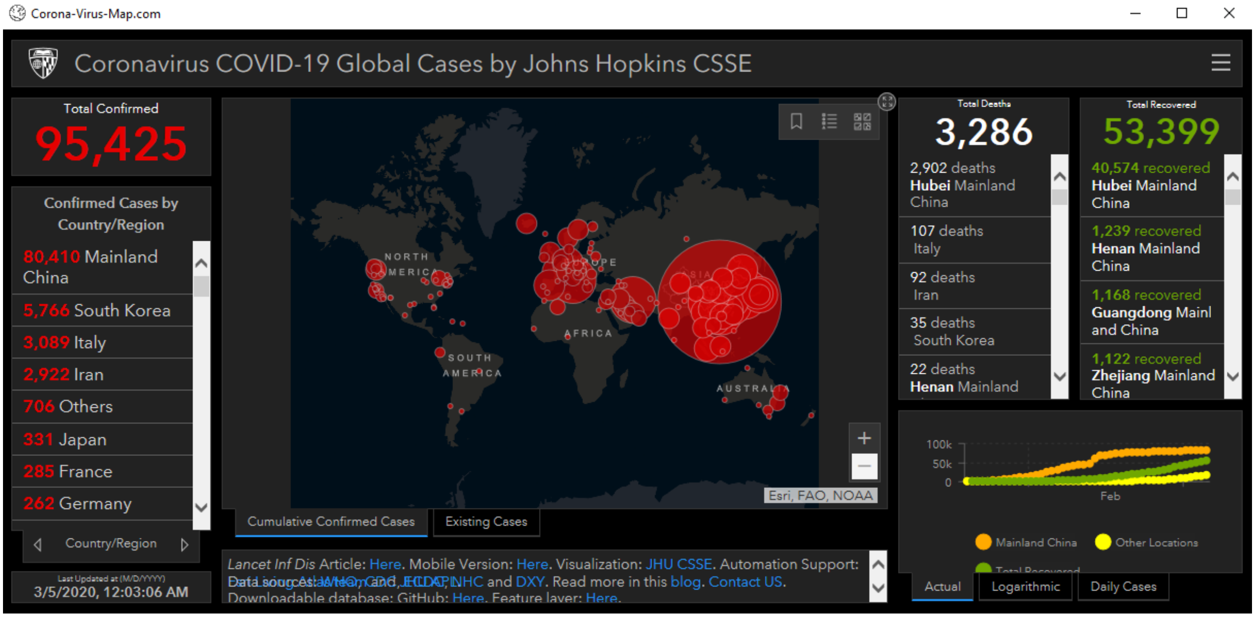
Nokia's Threat Intelligence Lab is monitoring the situation and providing advice on how to detect and remove these threats. In this paper we provide a round up of the most common threats, their behavior and their criminal aims, based on the Lab's own research. We also provide a general guide to help users protect themselves against the threats.

Malware directly related to the COVID-19 outbreak

"Coronavirus Maps" Trojan

A malware disguised as a "Coronavirus Map" is targeting the Windows platform. It takes advantage of the public's demand for accurate information about new Corona-related infections, deaths and transmissions.

The "Coronavirus Map" application is used to plant malware on victims' computers. This malware masquerades as software from Johns Hopkins University, and mimics the university's real map.



Corona-Virus-Map.com

Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE

Total Confirmed
95,425

Confirmed Cases by Country/Region

80,410 Mainland China
5,766 South Korea
3,089 Italy
2,922 Iran
706 Others
331 Japan
285 France
262 Germany

Last Updated at (M/D/YYYY)
3/5/2020, 12:03:06 AM

Total Deaths
3,286

2,902 deaths Hubei Mainland China
107 deaths Italy
92 deaths Iran
35 deaths South Korea
22 deaths Henan Mainland

Total Recovered
53,399

40,574 recovered Hubei Mainland China
1,239 recovered Henan Mainland China
1,168 recovered Guangdong Mainland China
1,122 recovered Zhejiang Mainland China

Lancet Inf Dis Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.
Downloadable database: GitHub: Here. Feature layer: Here.

Figure 1. This false map of the spread of COVID 19 is used to plant malware

How it works: After infecting the computer, the malware immediately contacts its Command and Control (CnC) server with information harvested from the host. The malware aims to steal user credentials, however it will also harvest other information such as credit card numbers, browser history, cookies and usernames and passwords from the browser cache.

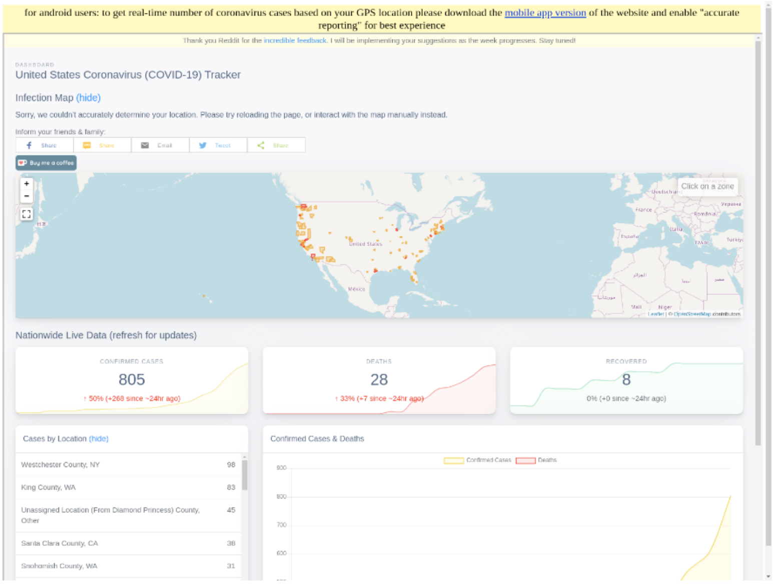
This malware is associated with the AZORult family of malware and is known to open a backdoor on the infected machine using the Remote Desktop Protocol (RDP) and a (new) hidden administrator account. AZORult is widespread among cybercriminals, being popular in underground forums, and is used in a range of malicious campaigns.

Removing malware manually is a complicated task - it is better to use reputable antivirus or anti-malware programs to do this automatically.

CovidLock Android Ransomware

This Android app is a trojan that claims to track the coronavirus spread across the globe and more specifically known COVID-19 patients in the immediate vicinity. In reality, the app is ransomware. It locks out the victim from the device and asks the user to pay to unlock it.

Delivery: Through a phishing e-mail or Google search, the user is drawn to a malicious website that looks like a legitimate COVID-19 information site. The user is encouraged to install an application that will provide real-time updates, but it is actually a ransomware app that locks the phone.



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. I will be 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:

Nationwide Live Data (refresh for updates)

CONFIRMED CASES
805
↑ 50% (+268 since ~24hr ago)

DEATHS
28
↑ 33% (+7 since ~24hr ago)

RECOVERED
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

Figure 2: Seeming to offer real-time updates on COVID-19, this Android app plants ransomware

How it works: As per the AndroidManifest XML file, the CovidLock application requests access to the permission: BIND_DEVICE_ADMIN. If granted access, this permission provides nearly full control of the device to CovidLock.

On starting, CovidLock will check if it is running with administrator permissions and if not, it will request these in order to escalate privileges. A message about enabling notification warnings when a coronavirus patient is near is used to deceive the user into granting this permission.

As soon as the victim clicks on “Scan Area for Coronavirus,” the phone locks itself with a message on the locked screen. It asks for $250 as ransom in the form of bitcoins. The attacker threatens the victim with leaking the their private data, including photos, videos, and more.

For instructions to unlock the phone and remove CovidLock, the user can follow the steps indicated at https://howtoremove.guide/covidlock/

The best option is to restore the encrypted files from the latest backup. If there are no such backups, it is possible to use a data recovery tool or try the manual recovery procedure (such as https://malware-guide.com/blog/remove-covidlock-ransomware).

COVID-19 themed phishing attacks delivering various malwares

In addition to malware that was specifically created or modified to fit the COVID-19 theme, some phishing campaigns are tailored to this theme but deliver existing malware. Below is a list of observed phishing campaigns that exploit the sense of urgency around COVID-19.

PlugX delivered by COVID themed documents

PlugX is a malicious program that targets the Windows platform. This malware is usually distributed through phishing e-mails, infected websites, and malicious software. Its primary goal is to drop malicious payload. After the malware has established persistence on a system, it tries to establish a network connection with the CnC server.

PlugX sends sensitive information from the device to the CnC server, deletes or changes registry entries and changes plugins as directed by the CnC server.

HawkEye Info-Stealer distributed as fake COVID19 drug advice

This is a new HawkEye malware variant distributed in mails spoofing the World Health Organization. The email appears to be sent directly from Dr. Tedros Adhanom Ghebreyesus, Director-General, World Health Organization (WHO).

HawkEye is a malicious information-stealing malware that targets the Windows operating system. The malware is delivered via spam emails containing malicious URL links or macro embedded files. Once installed, the malware steals sensitive information using the technique of browser keylogging. The malware is also able to download additional malware to the compromised system.

Win32.COVID-themed campaign from Kimsuky

KimsukyCOVID malware is delivered as a Microsoft Word file masquerading as information about the COVID-19 pandemic. The document contains a macro that will execute if the user falls for the request to enable additional content downloads to properly view the document. When opened, the malicious macro connects with the CnC and tries to retrieve a file from the site.

Android.Corona Safety Mask SMS Scam

CovidSafetyMask is a malicious info-stealer that targets Android devices. This program masquerades as an application to help users get safety masks. Upon infection, it will ask permission for contacts and SMS messages. Once it gains the permission required, the malware will send fraudulent messages to victims’ contacts in order to spread itself.

Android. “corona live 1.1” SpyMax surveillance-ware

"corona live 1.1" presents itself as a trojanized version of a legitimate corona live application. It is part of the SpyMax surveillance-ware family and has all of the capabilities of SpyMax, such as a call manager, SMS manager and camera manager. It gives the cybercriminal access to sensitive data on the phone and allows the attacker to remotely activate the camera and the microphone.

Ways that help keep users safe

Most of the attacks related to COVID-19 are phishing attacks. The attackers are not exploiting new vulnerabilities, and, in most cases, are not even creating new malware. What they do is use the COVID19 theme in their phishing attacks to increase the success rate of the phishing campaign.

Individual users must be careful and vigilant when visiting websites or opening email attachments. The most important aspects to consider are:

- Visit only reputable sites that are known to be reliable sources of information on these types of pandemics
- Only install applications that are from trusted app stores (Google Play, Apple, Microsoft)
- Use an up-to-date anti-virus program on the mobile device
- Keep applications and operating systems running at the current released patch level
- Don't open email attachments if the sender is not known and the email is unexpected
- Don't grant additional execution privileges if there is no clear reason and need to do so

Coverage of COVID-19 threats

Nokia's Threat Intelligence Lab provides extensive coverage for the Netguard Endpoint Security Appliance, which detects cyber security threats for a multitude of platforms, including Windows, Android and Linux.

For more details, please visit https://www.nokia.com/networks/portfolio/endpoint-security/

The coverage of the COVID-19 related threats includes but is not limited to the above-mentioned threats. The situation is being monitored closely, and the coverage extends to include new threats as soon as they appear, guaranteeing a timely response and accurate detection of these threats.

Abbreviations

CnC	Command and Control
RDP	Remote Desktop Protocol
WHO	World Health Organization
XML	Extensible Markup Language

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

Document code: SR2003042561EN (March) 207324