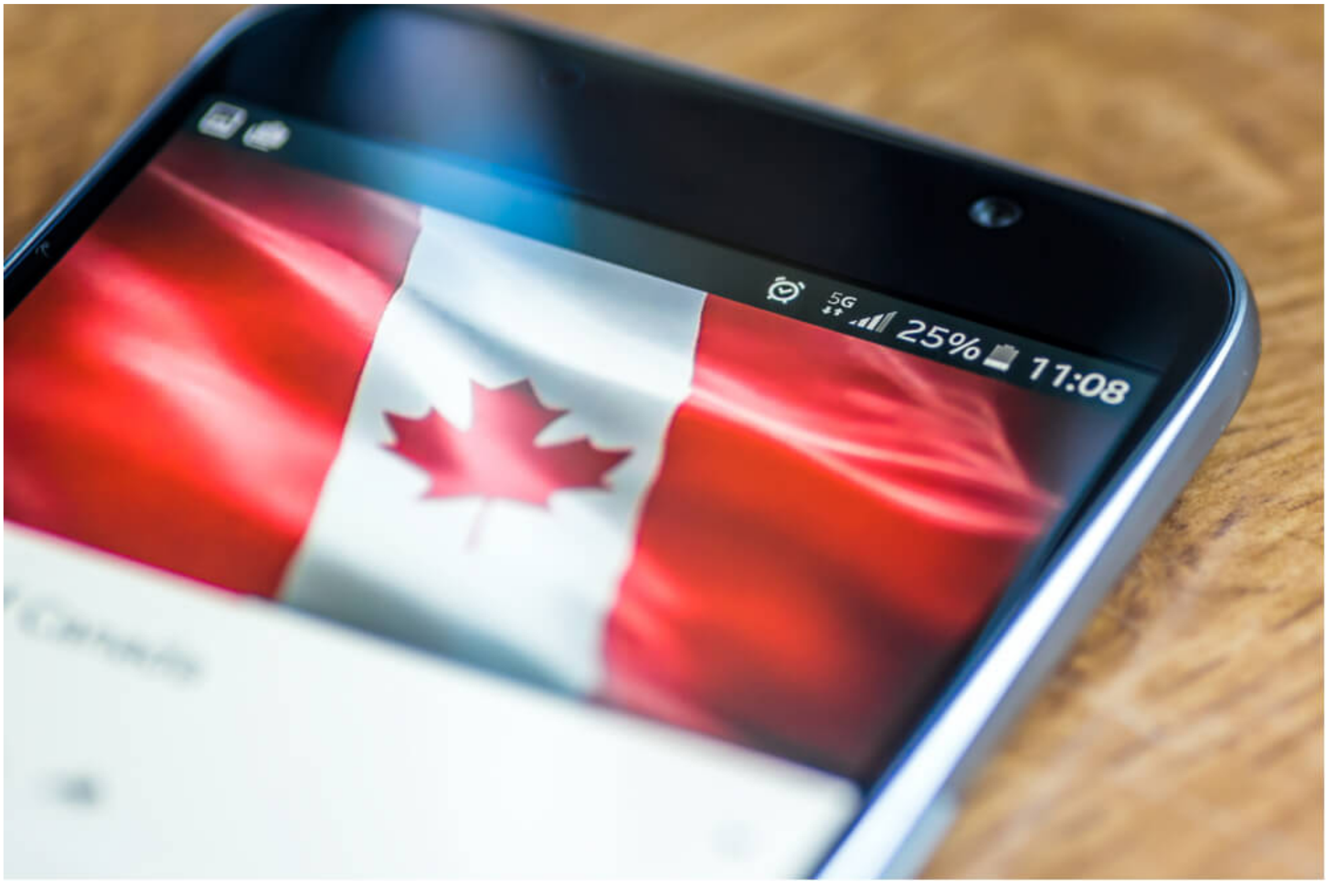
New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor

welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

June 23, 2020



ESET researchers dissect an Android app that masquerades as an official COVID-19 contact-tracing app and encrypts files on the victim's device

Lukas Stefanko
24 Jun 2020 - 12:36AM

ESET researchers dissect an Android app that masquerades as an official COVID-19 contact-tracing app and encrypts files on the victim’s device

New ransomware CryCryptor has been targeting Android users in Canada, distributed via two websites under the guise of an official COVID-19 tracing app provided by Health Canada. ESET researchers analyzed the ransomware and created a decryption tool for the victims.

CryCryptor surfaced just a few days after the Canadian government officially announced its intention to back the development of a nation-wide, voluntary tracing app called COVID Alert. The official app is due to be rolled out for testing in the province of Ontario as soon as next month.

ESET informed the Canadian Centre for Cyber Security about this threat as soon as it was identified.

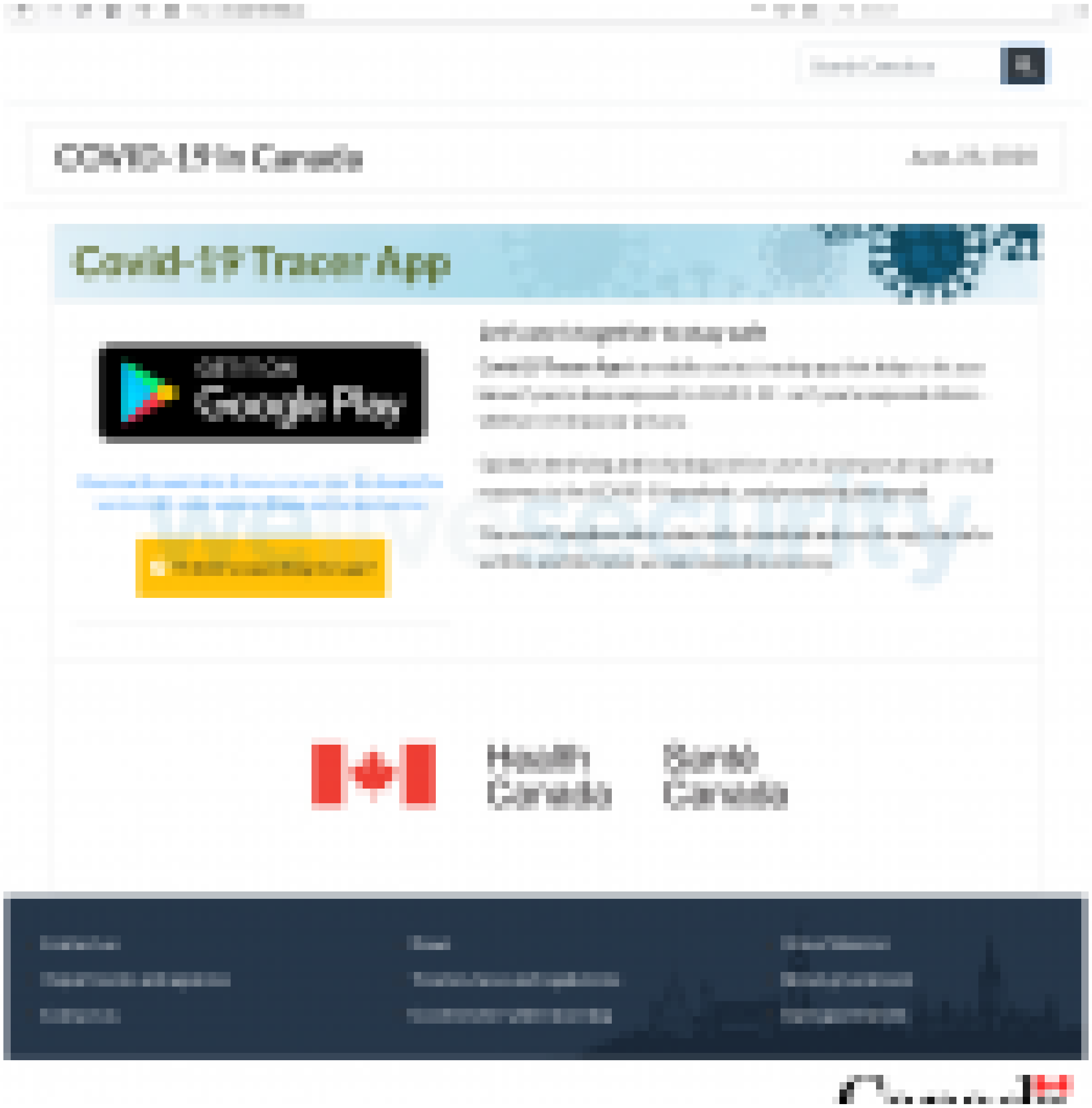


Figure 1. One of the malicious distribution websites; the other one has identical design and differs only in its domain, covid19tracer[.]ca.

Once the user falls victim to CryCryptor, the ransomware encrypts the files on the device – all the most common types of files – but instead of locking the device, it leaves a “readme” file with the attacker’s email in every directory with encrypted files.

Fortunately, we were able to create a decryption tool for those who fall victim to this ransomware.

RELATED READING: Mobile security threats amid COVID-19 and beyond: A Q&A with Lukas Stefanko

After we spotted the tweet that brought this ransomware to our radar (the researcher who discovered it mistakenly labeled the malware as a banking trojan), we analyzed the app. We discovered a bug of the type “Improper Export of Android Components” that MITRE labels as CWE-926.

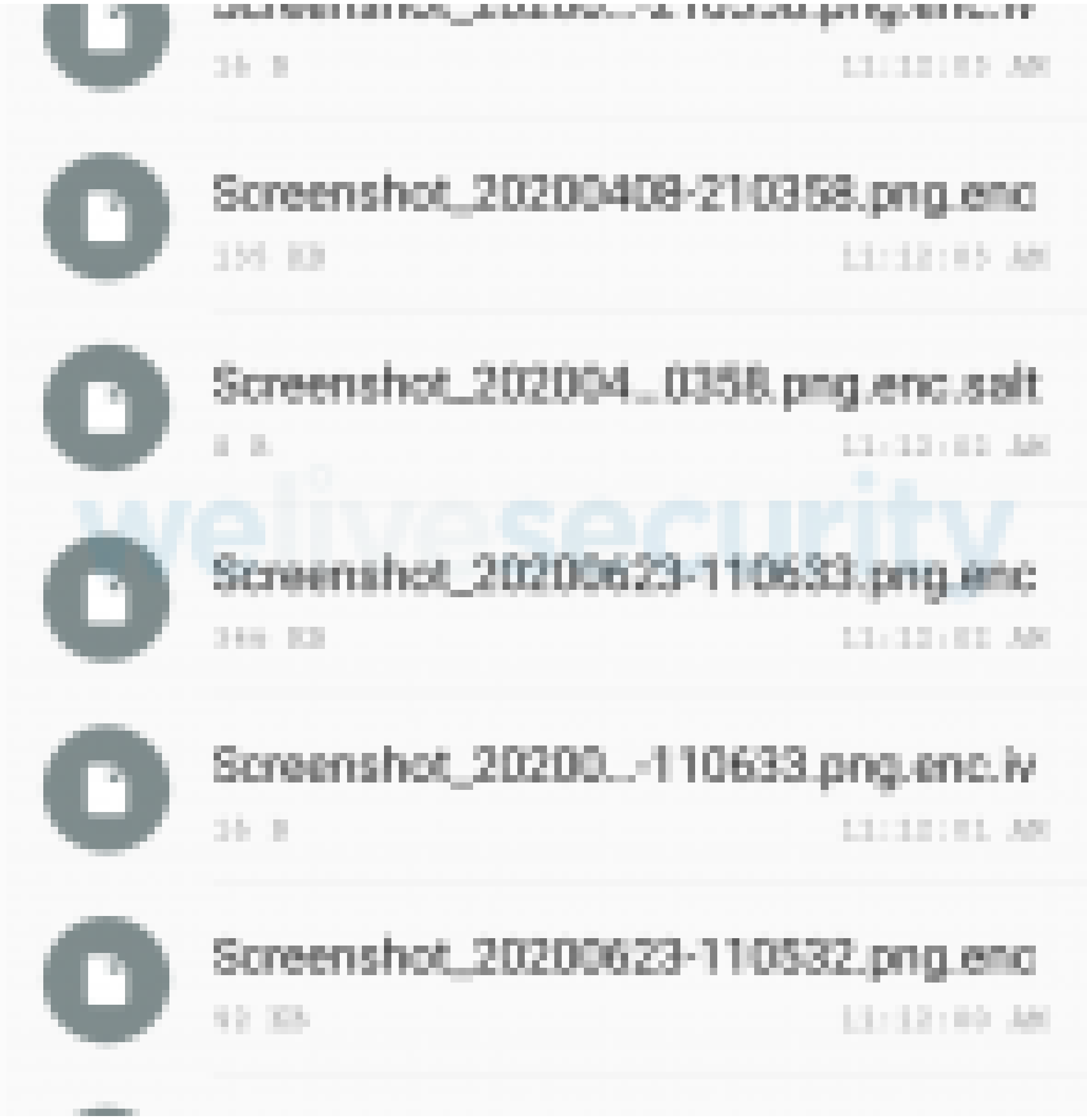
Due to this bug, any app that is installed on the affected device can launch any exported service provided by the ransomware. This allowed us to create the decryption tool – an app that launches the decrypting functionality built into the ransomware app by its creators.

Encryption/functionality

After launch, the ransomware requests to access files on the device. After obtaining that permission, it encrypts files on external media with certain extensions, which are shown in Figure 2.

Figure 2. File extensions to be encrypted

Selected files are encrypted using AES with a randomly generated 16-character key. After CryCryptor encrypts a file, three new files are created, and the original file is removed. The encrypted file has the file extension **“.enc”** appended, and the algorithm generates a salt unique for every encrypted file, stored with the extension **“.enc.salt”**; and an initialization vector, **“.enc.iv”**



Screenshot_20200409-210358.png.enc
[illegible]

Screenshot_202004...0358.png.enc.salt
8 B

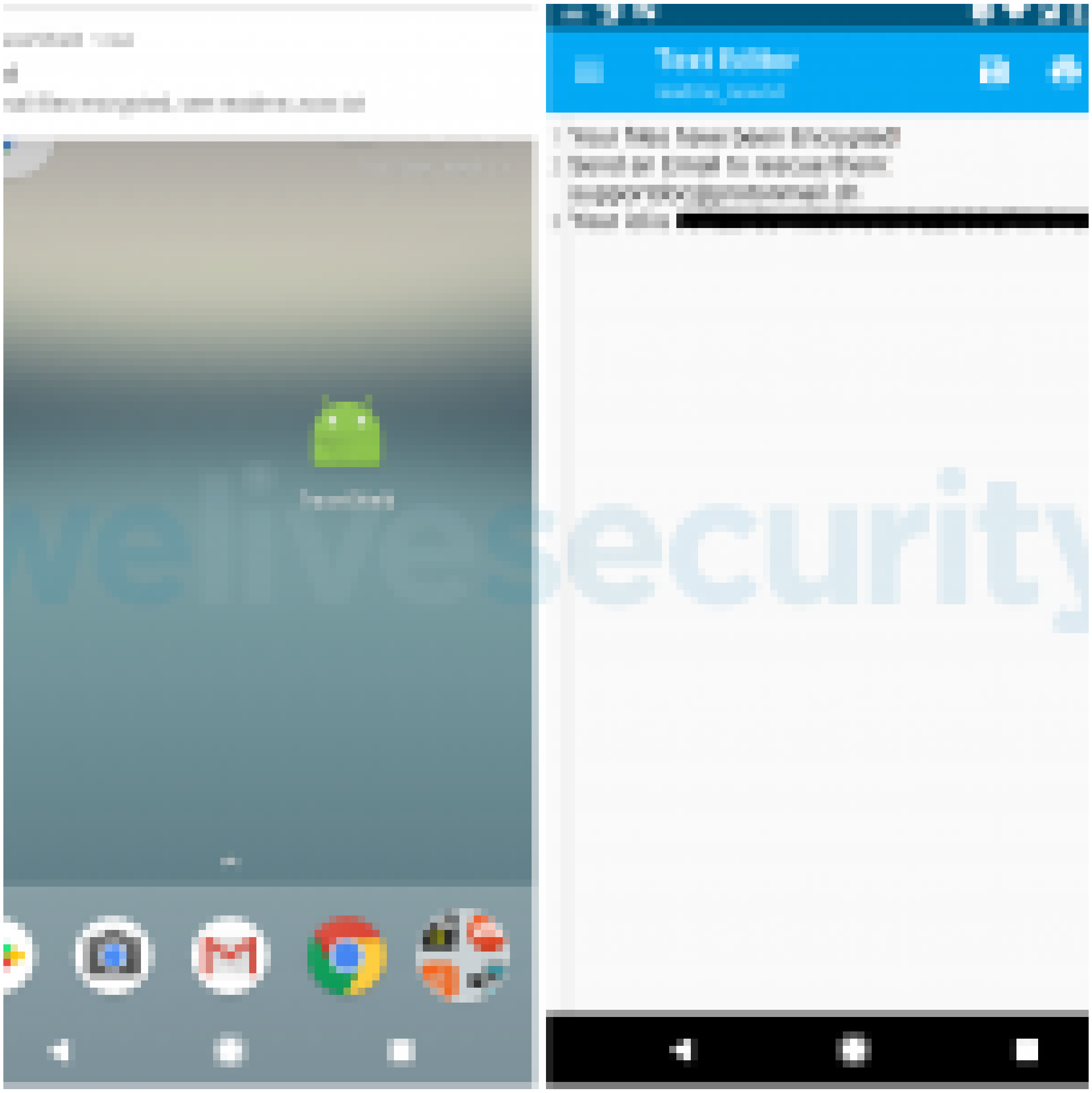
Screenshot_20200623-110633.png.enc
[illegible]

Screenshot_20200...-110633.png.enc.iv
16 B

Screenshot_20200623-110532.png.enc
[illegible]

Figure 3. Files after encryption

After all the target files are encrypted, CryCryptor displays a notification “Personal files encrypted, see readme_now.txt”. The readme_now.txt file is placed in every directory with encrypted files.



"Your files have been Encrypted!
Send an Email to recover them:
[illegible]
"Your id is [redacted]

Figure 4. File encryption notification (left) and contents of the readme_now.txt file (right)

Decryption

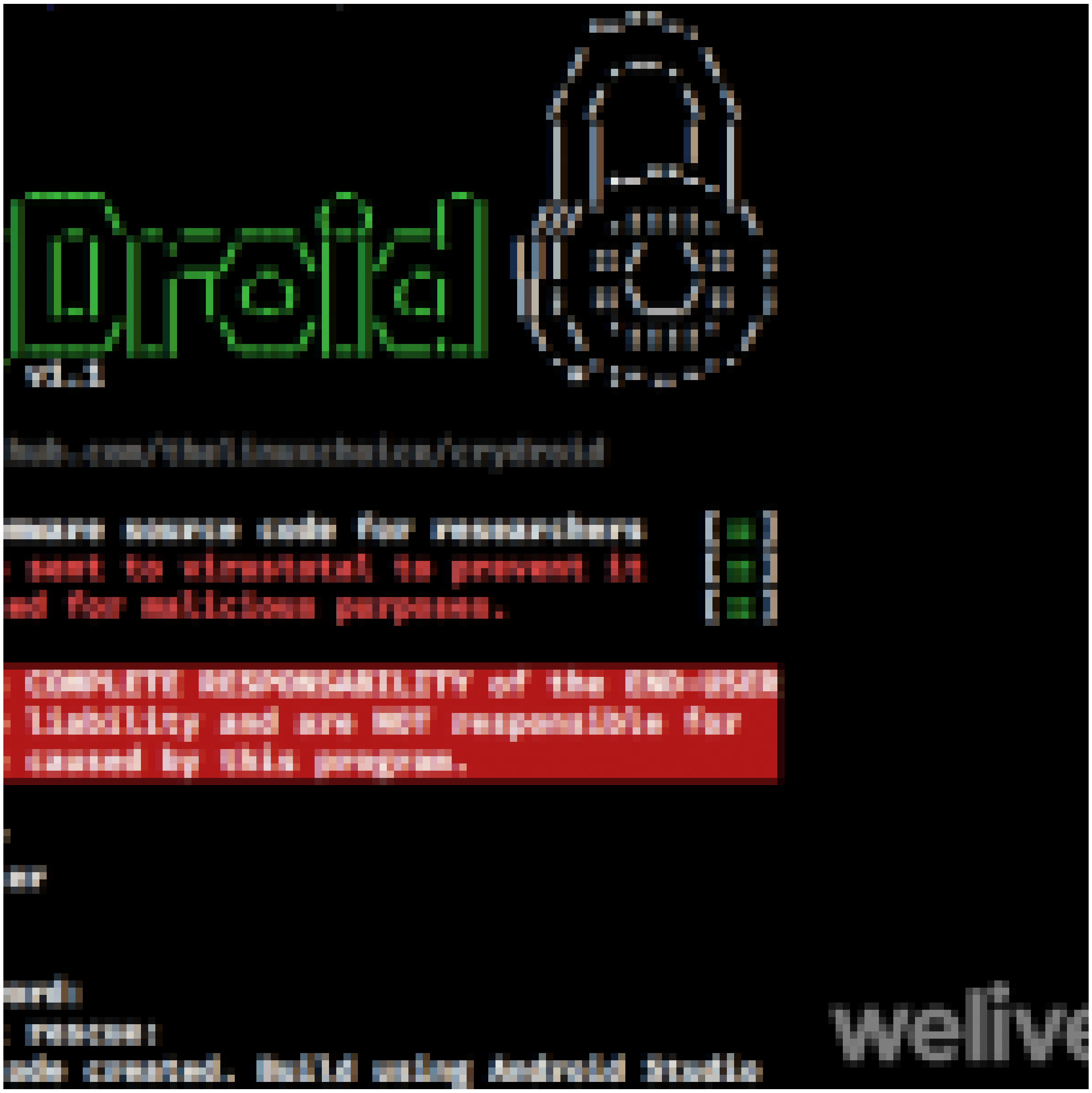
The service responsible for file decryption in CryCryptor has the encryption key stored in shared preferences, meaning it doesn't have to contact any C&C to retrieve it. Importantly, the service is exported without any restriction in the Android Manifest (security weakness CWE-926), which means it is possible to launch it externally.

Based on this, we created an Android decryption app for those affected with the CryCryptor ransomware. Naturally, the decryption app works only on this version of CryCryptor.

A new ransomware family

The CryCryptor ransomware is based on open source code on GitHub. We discovered it there using a simple search based on the app's package name and a few strings that looked unique.

The developers of the open source ransomware, who named it CryDroid, must have known the code would be used for malicious purposes. In an attempt to disguise the project as research, they claim they uploaded the code to the VirusTotal service. While it’s unclear who uploaded the sample, it indeed appeared on VirusTotal the same day the code was published on GitHub.



```
Droid
 v1.1

hub.com/thelinuxchoice/crydroid

mware source code for researchers     [+]
 sent to virustotal to prevent it     [+]
ed for malicious purposes.            [+]

 COMPLETE RESPONSABILITY of the END-USER
 liability and are NOT responsible for
 caused by this program.

er

ord:
 reason:
ode created. Build using Android Studio
```

Figure 5. The open source ransomware

We dismiss the claim that the project has research purposes – no responsible researcher would publicly release a tool that is easy to misuse for malicious purposes.

We notified GitHub about the nature of this code.

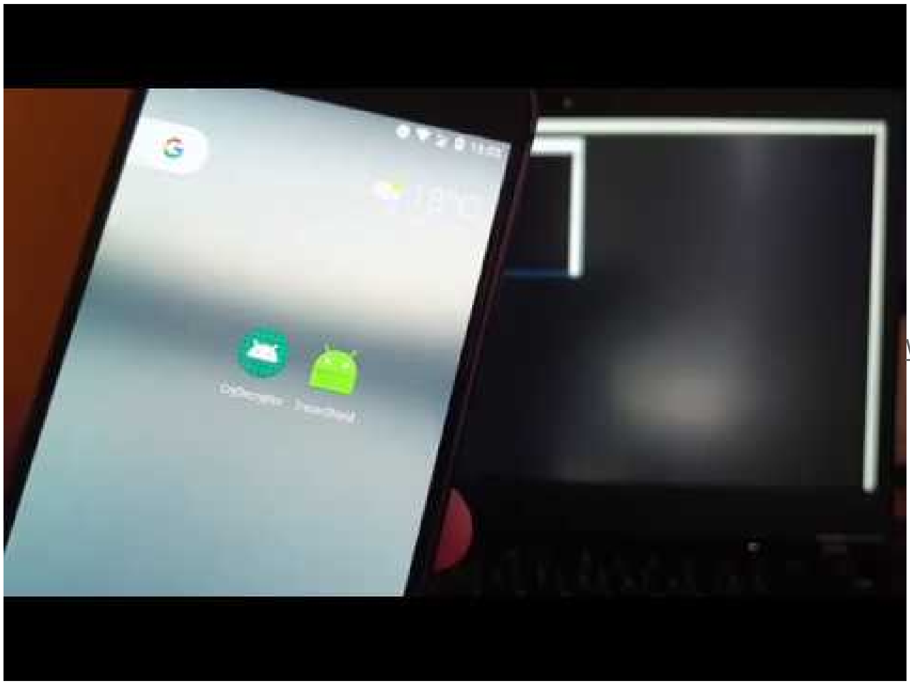
ESET products provide protection against the CryCryptor ransomware, detecting it as Trojan.Android/CryCryptor.A. On top of using a quality mobile security solution, we advise Android users to install apps only from reputable sources such as the Google Play store.

Timeline:

- Jun 11, 2020: source code published– CryDroid v1.1
- Jun 11, 2020: code uploaded to VirusTotal

- Jun 12, 2020: first malicious domain that distributed this sample was registered
- Jun 18, 2020: malicious app (this Android ransomware) was compiled (based on its certificate)
- Jun 21, 2020: second malicious domain that distributed this sample was registered
- Jun 23, 2020: ESET informs Canadian Center for Cyber Security
- Jun 23, 2020: the two domains stopped responding

We have prepared a video that that shows the process of encryption and decryption, along with our explanation.



Watch Video At:

https://youtu.be/llG_YFVLXyo

Indicators of Compromise (IoCs)

Package name	Hash	ESET detection name
com.crydroid	322AAB72228B1A9C179696E600C1AF335B376655	Trojan.Android/CryCryptor.A

Distribution links

https://covid19tracer[.]ca/
https://tracershield[.]ca/

MITRE ATT&CK techniques

Tactic	ID	Name	Description

Tactic	ID	Name	Description
Initial Access	T1476	Deliver Malicious App via Other Means	The malware is downloaded from a fake website
Initial Access	T1444	Masquerade as Legitimate Application	It impersonates COVID-19 tracking app
Persistence	T1402	App Auto-Start at Device Boot	It listens for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts
Impact	T1471	Data Encrypted for Impact	Encrypts files with particular file extensions found on external media

24 Jun 2020 - 12:36AM

Newsletter

Discussion