Coronavirus Update App Leads to Project Spy Android and iOS Spyware

By Tony Bao, Junzhi Lu (words)

Published: 2020-04-14 · Archived: 2026-04-05 23:01:12 UTC

We discovered a potential cyberespionage campaign, which we have named Project Spy, that infects Android and iOS devices with spyware (detected by Trend Micro as AndroidOS_ProjectSpy.HRX and IOS_ProjectSpy.A, respectively). Project Spy uses the ongoing coronavirus pandemic as a lure, posing as an app called Coronavirus Updates. We also found similarities in two older samples disguised as a Google service and, subsequently, as a music app after further investigation. However, we have noted a significantly small number of downloads of the app in Pakistan, India, Afghanistan, Bangladesh, Iran, Saudi Arabia, Austria, Romania, Grenada, and Russia.

Project Spy routine

At the end of March 2020, we came across an app masquerading as a coronavirus update app, which we named Project Spy based on the login page of its backend server.

 Coronavirus_Update_App_ProjectSpy_Fig1open on a new tabFigure 1. Project Spy as an app called Corona Updates

 Coronavirus_Update_App_ProjectSpy_Fig2open on a new tab

Figure 2. The Project Spy server login page. The address and login credentials to the server are found in the app's code.

This app carries a number of the capabilities:

- Upload GSM, WhatsApp, Telegram, Facebook, and Threema messages
- Upload voice notes, contacts stored, accounts, call logs, location information, and images
- Upload the expanded list of collected device information (e.g., IMEI, product, board, manufacturer, tag, host, Android version, application version, name, model brand, user, serial, hardware, bootloader, and device ID)
- Upload SIM information (e.g., IMSI, operator code, country, MCC-mobile country, SIM serial, operator name, and mobile number)
- Upload wifi information (e.g., SSID, wifi speed, and MAC address)
- Upload other information (e.g., display, date, time, fingerprint, created at, and updated at)

The app is capable of stealing messages from popular messaging apps by abusing the notification permissions to read the notification content and saving it to the database. It requests permission to access the additional storage.

 Coronavirus_Update_App_ProjectSpy_Fig3open on a new tab

Figure 3. The app intercepts received broadcasts and saves notification content in a database


Coronavirus_Update_App_ProjectSpy_Fig4open on a new tab

Figure 4. Abusing notification permissions to read the notification content

Project Spy's earlier versions

Searching for the domain in our sample database, we found that the coronavirus update app appears to be the latest version of another sample that we detected in May 2019.


Coronavirus_Update_App_ProjectSpy_Fig5open on a new tab

Figure 5. The May 2019 (first) version contains the same domain as the March 2020 (third) version

The first version of Project Spy (detected by Trend Micro as AndroidOS_SpyAgent.HRXB) had the following capabilities:

- Collect device and system information (i.e., IMEI, device ID, manufacturer, model and phone number), location information, contacts stored, and call logs
- Collect and send SMS
- Take pictures via the camera
- Upload recorded MP4 files
- Monitor calls

Searching further, we also found another sample that could be the second version of Project Spy. This version appeared as *Wabi Music*, and copied a popular video-sharing social networking service as its backend login page. In this second version, the developer's name listed was "concipit1248" in Google Play, and may have been active between May 2019 to February 2020. This app appears to have become unavailable on Google Play in March 2020.


Coronavirus_Update_App_ProjectSpy_Fig6open on a new tab

Figure 6. Project Spy's second version (left) and login page (right)

The second Project Spy version has similar capabilities to the first version, with the addition of the following:

- Stealing notification messages sent from WhatsApp, Facebook, and Telegram
- Abandoning the FTP mode of uploading the recorded images

Aside from changing the app's supposed function and look, the second and third versions' codes had little differences.

Potentially malicious iOS connection

Using the codes and "Concipit1248" to check for more versions, we found two other apps in the App Store.


Coronavirus_Update_App_ProjectSpy_Fig7open on a new tab

Figure 7. Apps available in the App Store, the developer is “Concipit Shop”

Further analysis of the iOS app “Concipit1248” showed that the server used, spy[.]cashnow[.]ee, is the same one used in the Android version of Project Spy.


Coronavirus_Update_App_ProjectSpy_Fig8open on a new tab

Figure 8. Concipit1248 iOS app’s code showing the server address

However, although the “Concipit1248” app requested permissions to open the device camera and read photos, the code only can upload a self-contained PNG file to a remote sever. This may imply the “Concipit1248” app is still incubating.


Coronavirus_Update_App_ProjectSpy_Fig9open on a new tab

Figure 9. iOS app Concipit1248’s permissions

The other iOS app “Concipit Shop” from the same developer appeared normal and was last updated on November 2019. Apple has confirmed that the iOS apps are not functioning based on analysis of the codes, and stated that the sandbox is able to detect and block these malicious behaviors.

Conclusion

The “Corona Updates” app had relatively low downloads in Pakistan, India, Afghanistan, Bangladesh, Iran, Saudi Arabia, Austria, Romania, Grenada, and Russia. Perhaps the app’s false capabilities also fueled the low number of downloads. It also appears the apps may still be in development or incubation, maybe waiting for a “right time” to inject the malicious codes. It’s also possible that the apps are being used to test other possible techniques. A possible indication for timing might be when the app reaches a specific number of downloads or infected devices.

The coding style suggests that the cybercriminals behind this campaign are amateurs. The incomplete iOS codes used in this campaign may have been bought while other capabilities appear to have been added. This may also explain the timing in between the apps becoming fully functional and “incubation.” As this is a group we have not observed before, we will continue monitoring this campaign for further developments.

Users are cautioned to research and check reviews before they download apps. Observe and look at the app’s display and text, stated functions, reviews from other users, and requested permissions before downloading. Make sure that all other apps installed and the device operating systems are updated to the latest version.

Trend Micro solutions

Users can install security solutions, such as the Trend Micro™ Mobile Security for iOSopen on a new tab and Trend Micro™ Mobile Security for Android™open on a new tab (also available on Google Playopen on a new tab) solutions, that can block malicious apps. End users can also benefit from their multilayered security capabilities that secure the device owner’s data and privacy, and features that protect them from ransomware, fraudulent websites, spyware, and identity theft.

For organizations, the Trend Micro™ Mobile Security for Enterpriseopen on a new tab suite provides device, compliance and application management, data protection, and configuration provisioning. The suite also protects devices from attacks that exploit vulnerabilities, prevents unauthorized access to apps and detects and blocks malware. Trend Micro's Mobile App Reputation Serviceopen on a new tab (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Indicators of Compromise (IoCs)

SHA256	Detection
e394e53e53cd9047d6cff184ac333ef7698a34b777ae3aac82c2c669ef661dfe	AndroidOS_SpyAgent.HRXB
e8d4713e43241ab09d40c2ae8814302f77de76650ccf3e7db83b3ac8ad41f9fa	AndroidOS_ProjectSpy.HRX
29b0d86ae68d83f9578c3f36041df943195bc55a7f3f1d45a9c23f145d75af9d	AndroidOS_ProjectSpy.HRX
3a15e7b8f4e35e006329811a6a2bf291d449884a120332f24c7e3ca58d0fbbdb	IOS_ProjectSpy.A

URLs

cashnow[.]ee Backend server

ftp[.]XXXX[.]com Backend server

spy[.]cashnow[.]ee Backend server

xyz[.]cashnow[.]ee Backend server

MITRE ATT&CK Framework

Android

iOS