An investigation of Chrysaor Malware on Android

Posted by Rich Cannings, Jason Woloz, Neel Mehta, Ken Bodzak, Wentao Chang, Megan Ruthven

Google is constantly working to improve our systems that protect users from Potentially Harmful Applications (PHAs). Usually, PHA authors attempt to install their harmful apps on as many devices as possible. However, a few PHA authors spend substantial effort, time, and money to create and install their harmful app on one or a very small number of devices. This is known as a targeted attack.

In this blog post, we describe Chrysaor, a newly discovered family of spyware that was used in a targeted attack on a small number of Android devices, and how investigations like this help Google protect Android users from a variety of threats.

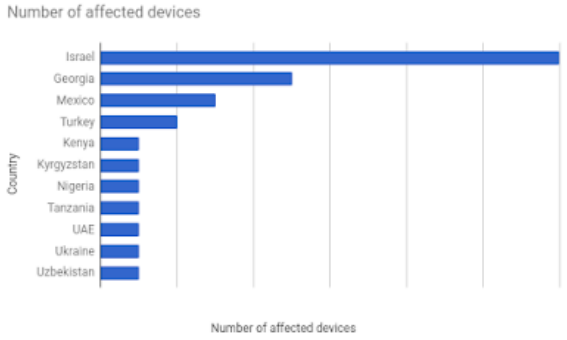
What is Chrysaor?

Chrysaor is spyware believed to be created by NSO Group Technologies, specializing in the creation and sale of software and infrastructure for targeted attacks. Chrysaor is believed to be related to the Pegasus spyware that was first identified on iOS and analyzed by Citizen Lab and Lookout.

Late last year, after receiving a list of suspicious package names from Lookout, we discovered that a few dozen Android devices may have installed an application related to Pegasus, which we named Chrysaor. Although the applications were never available in Google Play, we immediately identified the scope of the problem by using Verify Apps. We gathered information from affected devices, and concurrently, attempted to acquire Chrysaor apps to better understand its impact on users. We've contacted the potentially affected users, disabled the applications on affected devices, and implemented changes in Verify Apps to protect all users.

What is the scope of Chrysaor?

Chrysaor was never available in Google Play and had a very low volume of installs outside of Google Play. Among the over 1.4 billion devices protected by Verify Apps, we observed fewer than 3 dozen installs of Chrysaor on victim devices. These devices were located in the following countries:



How we protect you

To protect Android devices and users, Google Play provides a complete set of security services that update outside of platform releases. Users don't have to install any additional security services to keep their devices safe. In 2016, these services protected over 1.4 billion devices, making Google one of the largest providers of on-device security services in the world:

- Identify PHAs using people, systems in the cloud, and data sent to us from devices
- Warn users about or blocking users from installing PHAs
- Continually scan devices for PHAs and other harmful threats

Additionally, we are providing detailed technical information to help the security industry in our collective work against PHAs.

What do I need to do?

It is extremely unlikely you or someone you know was affected by Chrysaor malware. Through our investigation, we identified less than 3 dozen devices affected by Chrysaor, we have disabled Chrysaor on those devices, and we have notified users of all known affected devices. Additionally, the improvements we made to our protections have been enabled for all users of our security services.
To ensure you are fully protected against PHAs and other threats, we recommend these 5 basic steps:

- **Install apps only from reputable sources:** Install apps from a reputable source, such as Google Play. No Chrysaor apps were on Google Play.
- **Enable a secure lock screen**: Pick a PIN, pattern, or password that is easy for you to remember and hard for others to guess.
- **Update your device**: Keep your device up-to-date with the latest security patches.
- **Verify Apps:** Ensure Verify Apps is enabled.
- **Locate your device**: Practice finding your device with Android Device Manager because you are far more likely to lose your device than install a PHA.

How does Chrysaor work?

To install Chrysaor, we believe an attacker coaxed specifically targeted individuals to download the malicious software onto their device. Once Chrysaor is installed, a remote operator is able to surveil the victim's activities on the device and within the vicinity, leveraging microphone, camera, data collection, and logging and tracking application activities on communication apps such as phone and SMS.

One representative sample Chrysaor app that we analyzed was tailored to devices running Jellybean (4.3) or earlier. The following is a review of scope and impact of the Chrysaor app named `com.network.android` tailored for a Samsung device target, with SHA256 digest:

```
ade8bef0ac29fa363fc9afd958af0074478aef650adeb0318517b48bd996d5d5
```

Upon installation, the app uses known framaroot exploits to escalate privileges and break Android's application sandbox. If the targeted device is not vulnerable to these exploits, then the app attempts to use a superuser binary pre-positioned at `/system/csk` to elevate privileges.

After escalating privileges, the app immediately protects itself and starts to collect data, by:

- Installing itself on the `/system` partition to persist across factory resets
- Removing Samsung's system update app (`com.sec.android.fotaclient`) and disabling auto-updates to maintain persistence (sets `Settings.System.SOFTWARE_UPDATE_AUTO_UPDATE` to 0)
- Deleting WAP push messages and changing WAP message settings, possibly for anti-forensic purpose.
- Starting content observers and the main task loop to receive remote commands and exfiltrate data

The app uses six techniques to collect user data:

- **Repeated commands**: use alarms to periodically repeat actions on the device to expose data, including gathering location data.
- **Data collectors**: dump all existing content on the device into a queue. Data collectors are used in conjunction with repeated commands to collect user data including, SMS settings, SMS messages, Call logs, Browser History, Calendar, Contacts, Emails, and messages from selected messaging apps, including WhatsApp, Twitter, Facebook, Kakoa, Viber, and Skype by making /data/data directories of the apps world readable.
- **Content observers**: use Android's ContentObserver framework to gather changes in SMS, Calendar, Contacts, Cell info, Email, WhatsApp, Facebook, Twitter, Kakao, Viber, and Skype.
- **Screenshots**: captures an image of the current screen via the raw frame buffer.
- **Keylogging**: record input events by hooking `IPCThreadState::Transact` from `/system/lib/libbinder.so` , and intercepting android::parcel with the interface `com.android.internal.view.IInputContext` .
- **RoomTap:** silently answers a telephone call and stays connected in the background, allowing the caller to hear conversations within the range of the phone's microphone. If the user unlocks their device, they will see a black screen while the app drops the call, resets call settings and prepares for the user to interact with the device normally.

Finally, the app can remove itself through three ways:

- Via a command from the server
- Autoremove if the device has not been able to check in to the server after 60 days
- Via an antidote file. If `/sdcard/MemosForNotes` was present on the device, the Chrysaor app removes itself from the device.

Samples uploaded to VirusTotal

To encourage further research in the security community, we've uploaded these sample Chrysaor apps to Virus Total.

Package Name	SHA256 digest	SHA1 certificate
com.network.android	ade8bef0ac29fa363fc9afd958af0074478aef650adeb0318517b48bd996d5d5	44f6d1caa257799e57f0ecaf4e2e2161
com.network.android	3474625e63d0893fc8f83034e835472d95195254e1e4bdf99153b7c74eb44d86	516f8f516cc0fd8db53785a48c0a865

Additional digests with links to Chrysaor

As a result of our investigation we have identified these additional Chrysaor-related apps.

Package Name	SHA256 digest	SHA1 certificate
com.network.android	98ca5f94638768e7b58889bb5df4584bf5b6af56b188da48c10a02648791b30c	516f8f516cc0fd8db53785a48c0a8
com.network.android	5353212b70aa096d918e4eb6b49eb5ad8f59d9bec02d089e88802c01e707c3a1	44f6d1caa257799e57f0ecaf4e2e2
com.binary.sms.receiver	9fae5d148b89001555132c896879652fe1ca633d35271db34622248e048c78ae	7771af1ad3a3d9c0b4d9b55260bb
com.android.copy	e384694d3d17cd88ec3a66c740c6398e07b8ee401320ca61e26bdf96c20485b4	7771af1ad3a3d9c0b4d9b55260bb
com.android.copy	12e085ab85db887438655feebd249127d813e31df766f8c7b009f9519916e389	7771af1ad3a3d9c0b4d9b55260bb
com.android.copy	6348104f8ef22eba5ac8ee737b192887629de987badbb1642e347d0dd01420f8	31a8633c2cd67ae965524d0b2192

Lookout has completed their own independent analysis of the samples we acquired, their report can be viewed here.
