Starry Addax targets human rights defenders in North Africa with new malware

By Cisco Talos

Published: 2024-04-09 · Archived: 2026-04-05 18:39:48 UTC

- Cisco Talos is disclosing a new threat actor we deemed “Starry Addax” targeting mostly human rights activists associated with the Sahrawi Arab Democratic Republic (SADR) cause with a novel mobile malware.
- Starry Addax conducts phishing attacks tricking their targets into installing malicious Android applications we’re calling “FlexStarling.”
- For Windows-based targets, Starry Addax will serve credential-harvesting pages masquerading as login pages from popular media websites.

Talos would like to thank the Yahoo! Paranoids Advanced Cyber Threats Team for their collaboration in this investigation.

Starry Addax has a special interest in Western Sahara

The malicious mobile application (APK), “FlexStarling,” analyzed by Talos recently masquerades as a variant of the Sahara Press Service (SPSRASD) App. The Sahara Press Service is a media agency associated with the Sahrawi Arab Democratic Republic. The malware will serve content in the Spanish language from the SPSRASD website to look legitimate to the victim. However, in actuality, FlexStarling is a highly versatile malware capable of deploying additional malware components and stealing information from the infected devices.

Splash screen for the malicious application.

Starry Addax's infrastructure can be used to target Windows- and Android-based users. This campaign's infection chain begins with a spear-phishing email sent to targets, consisting of individuals of interest to the attackers, especially human rights activists in Morocco and the Western Sahara region. The email contains content that requests the target to install the Sahrawi News Agency's Mobile App or include a topical theme related to the Western Sahara.

Some examples of the subject lines of the phishing emails consist of:

طلب تثبيت التطبيق على هواتف متابعي وكالة الأنباء الصحراوية	Request to install the application on the phones of Sahrawi News Agency followers
الوفد برلماني الأوروبي يدلي بتصريحات	The European Parliament delegation makes statements
الوفد برلماني يدلي بتصريحات	A parliamentary delegation makes statements
عاجل وبالفيديو ونقلاً عن جريدة إلبايس	Urgent, video, and quoted from El Pais newspaper

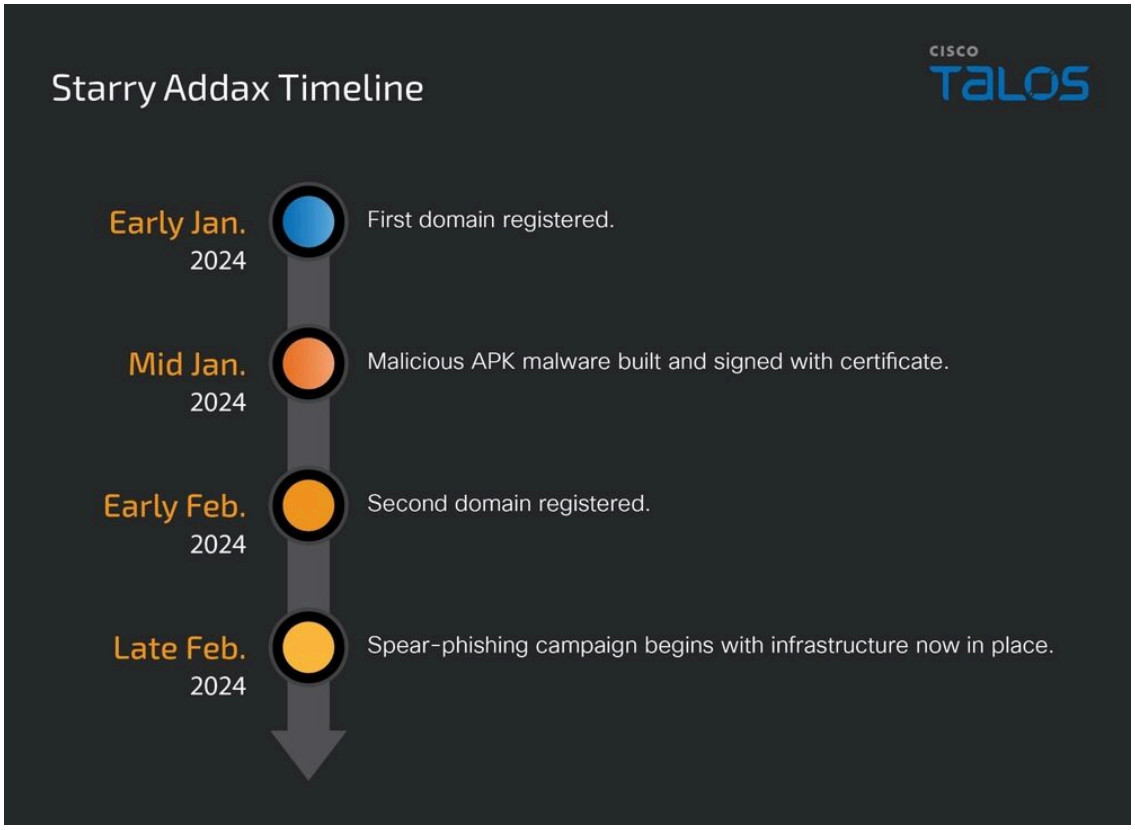
The email originating from an attacker-owned domain, ondroid[.]site, consists of a shortened link to an attacker-controlled website and domain. Depending on the requestor's operating system, the website will either serve the FlexStarling APK for Android devices or redirect the victim to a social media login page to harvest their credentials. The links observed by Talos so far are:

	www[.]ondroid[.]store/aL2mohh1
	www[.]ondroid[.]store/ties5shizooQu1ei/

Starry Addax likely to escalate momentum

Campaigns like this that target high-value individuals usually intend to sit quietly on the device for an extended period. All components from the malware to the operating infrastructure seem to be bespoke/custom-made for this specific campaign indicating a heavy focus on stealth and conducting activities under the radar. The use of FlexStarling with a Firebase-based C2 instead of commodity malware or commercially available spyware indicates the threat actor is making a conscious effort to evade detections and operate without being detected.

The timelines connected to various artifacts used in the attacks indicate that this campaign is just starting and may be in its nascent stages with more infrastructure and Starry Addax working on additional malware variants.



FlexStarling – A highly capable implant

The FlexStarling malware app requests a plethora of permissions from the Android OS to extract valuable information from the infected mobile device. The following list contains the permissions acquired by FlexStarling via its AndroidManifest[.]xml:

```
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_CALL_LOG" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.RECORD_AUDIO" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.ACCESS_NOTIFICATION_POLICY" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES" />
    <uses-permission android:name="android.permission.GET_TASKS" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="android.permission.QUICKBOOT_POWERON" />
    <uses-permission android:name="android.permission.RECEIVE_LAUNCH_BROADCASTS" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
    <uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES" />
    <uses-permission android:name="android.permission.CALL_PHONE" />
    <uses-permission android:name="android.permission.QUERY_ALL_PACKAGES" />
    <uses-permission android:name="android.permission.MANAGE_EXTERNAL_STORAGE" />
    <uses-permission
android:name="android.permission.ACTION_MANAGE_OVERLAY_PERMISSION" />
    <uses-permission
android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
    <uses-permission android:name="android.permission.READ_PHONE_NUMBERS" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.DISABLE_KEYGUARD" />
    <uses-permission android:name="android.permission.READ_CALENDAR" />
    <permission
android:name="google.android.services.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"
android:protectionLevel="signature" />
    <uses-permission
android:name="google.android.services.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION" />
```

Some of these permissions are dynamically requested at runtime: READ_CALL_LOG, READ_EXTERNAL_STORAGE, READ_SMS, READ_CONTACTS, WRITE_EXTERNAL_STORAGE, INTERNET, ACCESS_NETWORK_STATE, RECORD_AUDIO, READ_PHONE_STATE.

Anti-emulation checks

When the implant runs, it checks the BUILD information for keywords or phrases that indicate that it is running on an emulator or analysis tool. The implant checks for the following keywords:

- BUILD[MANUFACTURER] does not contain: “Genymotion”.
- BUILD[MODEL] does not contain any of: “google_sdk”, “droid4x”, “Emulator”, "Android SDK built for x86"
- BUILD[HARDWARE] does not contains any of: “goldfish”, “vbox86”, “nox”.
- BUILD[FingerPrint] does not start with “generic”.
- BUILD[Product] does not consist of any of: “sdk”, “google_sdk”, “sdk_x86”, “vbox86p”, “nox”.
- BUILD[Board] does not contain: “nox”.

- BUILD[Brand] or Device does not start with “generic”.

The implant also checks for the presence of the following emulation/virtualization-related files in the filesystem:

- /dev/socket/genyd
- /dev/socket/baseband_genyd
- /dev/socket/qemud
- /dev/qemu_pipe
- ueventd.android_x86.rc
- X86.prop
- ueventd.ttVM_x86.rc
- init.ttVM_x86.rc
- fstab.ttVM_x86
- fstab.vbox86
- init.vbox86.rc
- ueventd.vbox86.rc
- fstab.andy
- ueventd.andy.rc
- fstab.nox
- init.nox.rc
- Ueventd.nox.rc

If none of the keywords or files are found or all checks are passed, the malicious app tries to gain permissions for managing external storage areas (shared storage space) on the device using the permission “MANAGE_EXTERNAL_STORAGE”. The actor wants to gain the ability to read, write, modify, delete and manage files on external storage locations.

Stealing information and executing arbitrary code

The malware obtains command codes and accompanying information from the C2 server. It then generates the MD5 hash string of the command code and compares its list of hardcoded hashes. The corresponding activity is carried out by the implant once a match is found.

The various commands supported by the sample are:

Command code MD5 hash	Decode command code	Intent
801ab24683a4a8c433c6eb40c48bcd9d	Download	Download a file specified by a URL to the Downloads directory.

e8606d021da140a92c7eba8d9b8af84f	unknown	Copy files from the download's directory to the application package directory
725888549d44eb5a3a676c018df55943	unknown	Decrypt a dex file located in the application package directory and reflectively load it.
3a884d7285b2caa1cb2b60f887571d6c	unknown	Cleanup directories – remove all files: • Cache directory. • Application package directory (including "/oat/"). • External Cache Directory.
f2a6c498fb90ee345d997f888fce3b18	Delete	Delete a specified filepath.
3e679cff5b3a6f6f8f32aead541a0a12	Drop	Upload a local file to the attacker's dropbox folders using the Dropbox API. The ACCESS TOKEN, local filepath and remote upload path is specified by the C2.
fb84708d32d00fca5d352e460776584c	DECRYPT	AES Decrypt a file from the application package directory using the secret key and IV specified and write it to a file named ".EXEC.dex"

0ba4439ee9a46d9d9f14c60f88f45f87	check	Check if a file inside the application package directory exists.

These commands are supported by accompanying information and consist of the following variables being sent across by the C2:

DURL: Indicates the download URL used by the “Download” command above.

APPNAME: Indicates the filename to use for the destination file during the “Download” command.

DEX: Contains the source file name to be used during the Decrypt (and reflectively load) commands.

ky1: Indicates a value to be used in the context of specific command codes:

- Delete = File to be deleted.
- Drop = File to be read and uploaded to Dropbox.
- DECRYPT = Secret key used for AES decryption.
- Check = Filename to be whose presence is to be checked in the application package directory.

ky2: Indicates a value to be used in the context of specific command codes:

- Drop = Remote file location where the local file needs to be uploaded on Dropbox.
- DECRYPT = IV used for AES decryption.

ky3: Indicates a value to be used in the context of specific command codes:

- Drop = Dropbox ACCESS TOKEN value to be used during file upload.
- DECRYPT = IV used for AES decryption.

fl: Filename used during the DEX reflective load process.

ky4: Used as a parameter during reflective loading of the DEX file.

ky5: Secret key used for AES decryption as part of the implant’s DEX decrypt and reflective load.

ky6: IV used for AES decryption as part of the implant’s DEX decrypt and reflective load.

ky7: Contains the source file name to be used during the AES decryption as part of the implant’s DEX decrypt and reflective load.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

IOCs for this research can also be found at our GitHub repository here.

Hashes

f7d9c4c7da6082f1498d41958b54d7aeffd0c674aab26db93309e88ca17c826c

ec2f2944f29b19ffd7a1bb80ec3a98889ddf1c097130db6f30ad28c8bf9501b3

Network IOCs

hxxps[://]runningapplications-b7dae-default-rtdb[.]firebaseio[.]com

ondroid[.]site

ondroid[.]store

bit[.]ly/48wdj1m

www[.]ondroid[.]store/aL2mohh1

bit[.]ly/48E4W3N

www[.]ondroid[.]store/ties5shizooQu1ei/
