Operation Celestial Force employs mobile and desktop malware to target Indian entities

By Cisco Talos

Published: 2024-06-13 · Archived: 2026-04-05 17:32:05 UTC

Thursday, June 13, 2024 06:00

By Gi7w0rm, Asheer Malhotra and Vitor Ventura.

- Cisco Talos is disclosing a new malware campaign called “Operation Celestial Force” running since at least 2018. It is still active today, employing the use of GravityRAT, an Android-based malware, along with a Windows-based malware loader we track as “HeavyLift.”
- All GravityRAT and HeavyLift infections are administered by a standalone tool we are calling “GravityAdmin,” which carries out malicious activities on an infected device. Analysis of the panel binaries reveals that they are meant to administer and run multiple campaigns at the same time, all of which are codenamed and have their own admin panels.
- Talos attributes this operation with high confidence to a Pakistani nexus of threat actors we’re calling “Cosmic Leopard,” focused on espionage and surveillance of their targets. This multiyear operation continuously targeted Indian entities and individuals likely belonging to defense, government and related technology spaces. Talos initially disclosed the use of the Windows-based GravityRAT malware by suspected Pakistani threat actors in 2018 — also used to target Indian entities.
- While this operation has been active for at least the past six years, Talos has observed a general uptick in the threat landscape in recent years, with respect to the use of mobile malware for espionage to target high-value targets, including the use of commercial spyware.

Operation Celestial Force: A multi-campaign, multi-component infections operation

Talos assesses with high confidence that this series of campaigns we're clustering under the umbrella of "Operation Celestial Force" is conducted by a nexus of Pakistani threat actors. The tactics, techniques, tooling and victimology of Cosmic Leopard contain some overlaps with those of Transparent Tribe, another suspected Pakistani APT group, which has a history of targeting high-value individuals from the Indian subcontinent. However, we do not have enough technical evidence to link both the threat actors together for now, therefore we track this cluster of activity under the "Cosmic Leopard" tag.

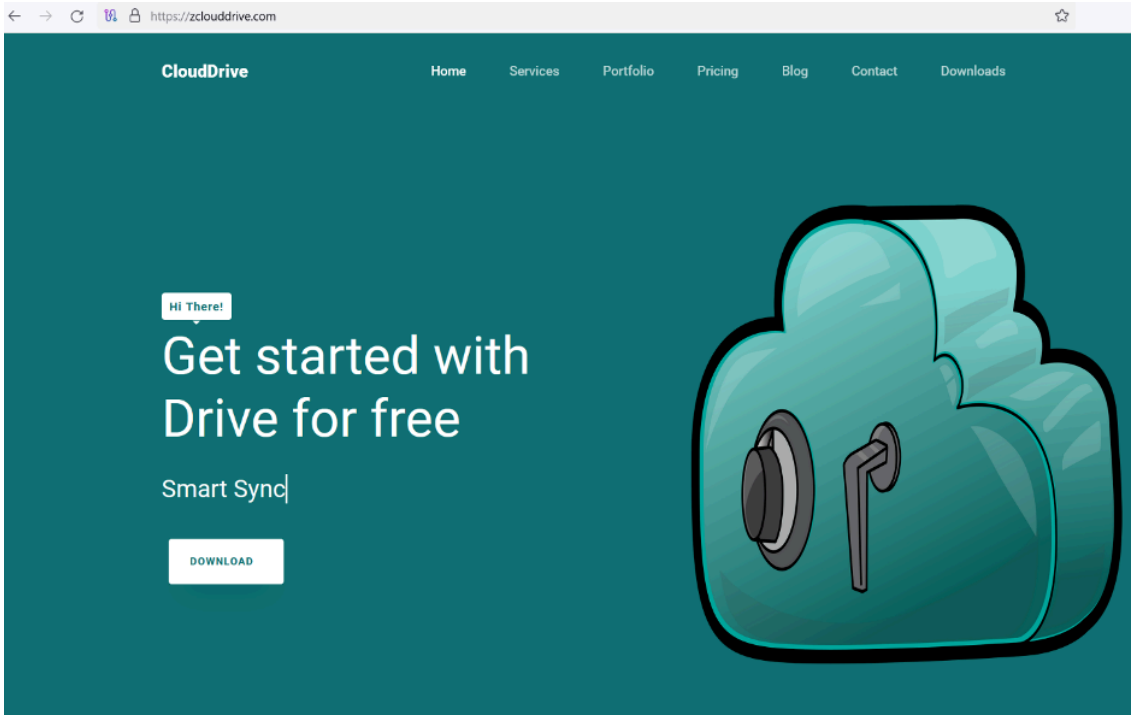
Operation Celestial Force has been active since at least 2018 and continues to operate today — increasingly utilizing an expanding and evolving malware suite — indicating that the operation has likely seen a high degree of success targeting users in the Indian subcontinent. Cosmic Leopard initially began the operation with the creation and deployment of the Windows-based GravityRAT malware family distributed via malicious documents (maldocs). Cosmic Leopard then created Android-based versions of GravityRAT to widen their net of infections to begin targeting mobile devices around 2019. During the same year, Cosmic Leopard also expanded their arsenal to use the HeavyLift malware family as a malware loader. HeavyLift is primarily wrapped in malicious installers sent to targets tricked into running the into running the malware via social engineering techniques.

Some campaigns from this multi-year operation have been disclosed and loosely attributed to Pakistani threat actors in previous reporting. However, there has been little evidence to tie all of them together until now. Each campaign in the operation has been codenamed by the threat actor and managed/administered using custom-built panel binaries we call "GravityAdmin."

Adversaries like Cosmic Leopard may use low-sophistication techniques such as social engineering and spear phishing, but will aggressively target potential victims with various TTPs. Therefore, organizations must remain vigilant against such motivated adversaries conducting targeted attacks by educating users on proper cyber hygiene and implementing defense-in-depth models to protect against such attacks across various attack surfaces.

This campaign primarily utilizes two infection vectors — spear phishing and social engineering. Spear phishing consists of messages sent to targets with pertinent language and maldocs that contain malware such as GravityRAT.

The other infection vector, gaining popularity in this operation, and now a staple tactic of the Cosmic Leopard's operations consists of contacting targets over social media channels, establishing trust with them and eventually sending them a malicious link to download either the Windows- or Android-based GravityRAT or the Windows-based loader, HeavyLift.



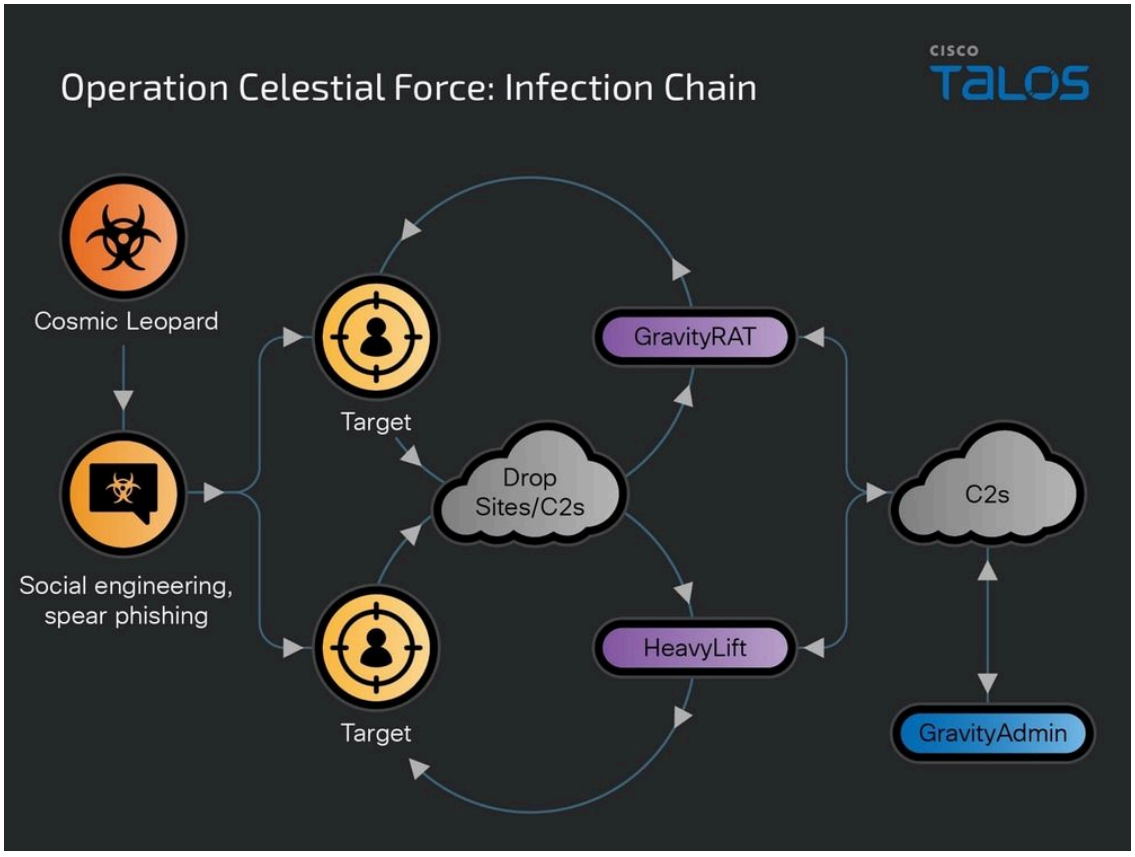
Malicious drop site delivering HeavyLift.

Operation Celestial Force's malware and its management interfaces

Talos' analysis reveals the use of multiple components, including Android- and Windows-based malware, and administrative binaries supporting multiple campaign panels used by Operation Celestial Force.

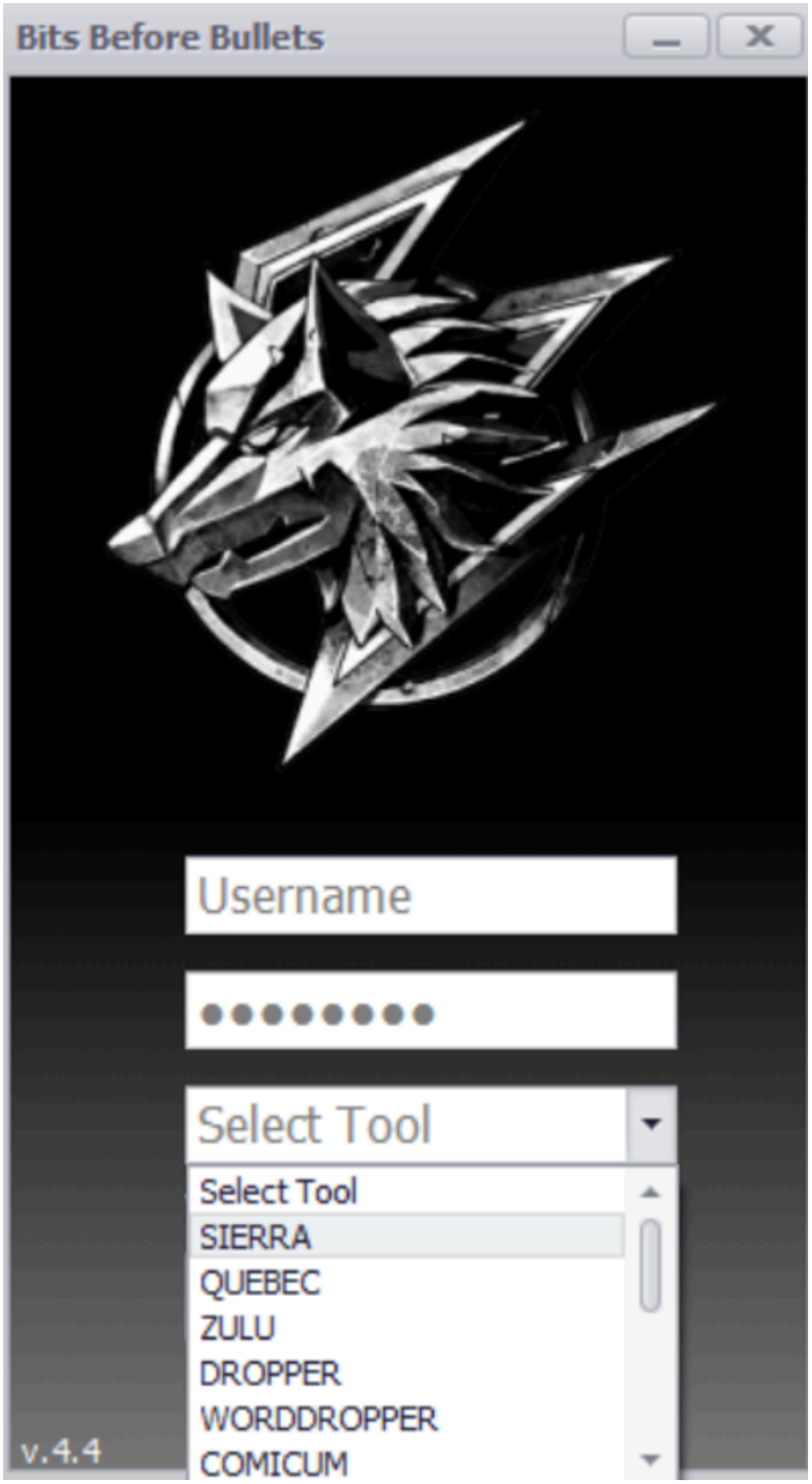
- **GravityRAT**: GravityRAT, a closed-source malware family, first disclosed by Talos in 2018, is a Windows- and Android-based RAT used to target Indian entities.
- **HeavyLift**: A previously unknown Electron-based malware loader family distributed via malicious installers targeting the Windows operating system.
- **GravityAdmin**: A tool to administer infected systems (panel binary), used by operators since at least 2021, by connecting to GravityRAT's and HeavyLift's C2 servers. GravityAdmin consists of multiple inbuilt User Interfaces (UIs) that correspond to specific, codenamed, campaigns being operated by malicious operators.

Operation Celestial Force's infection chains are:



GravityAdmin: Panel binaries administering the campaigns

The Panel binaries we analyzed consist of multiple versions with the earliest compiled in August 2021. The panel binary asks for a user ID, password and campaign ID (from a drop-down menu) from the operator when it runs.

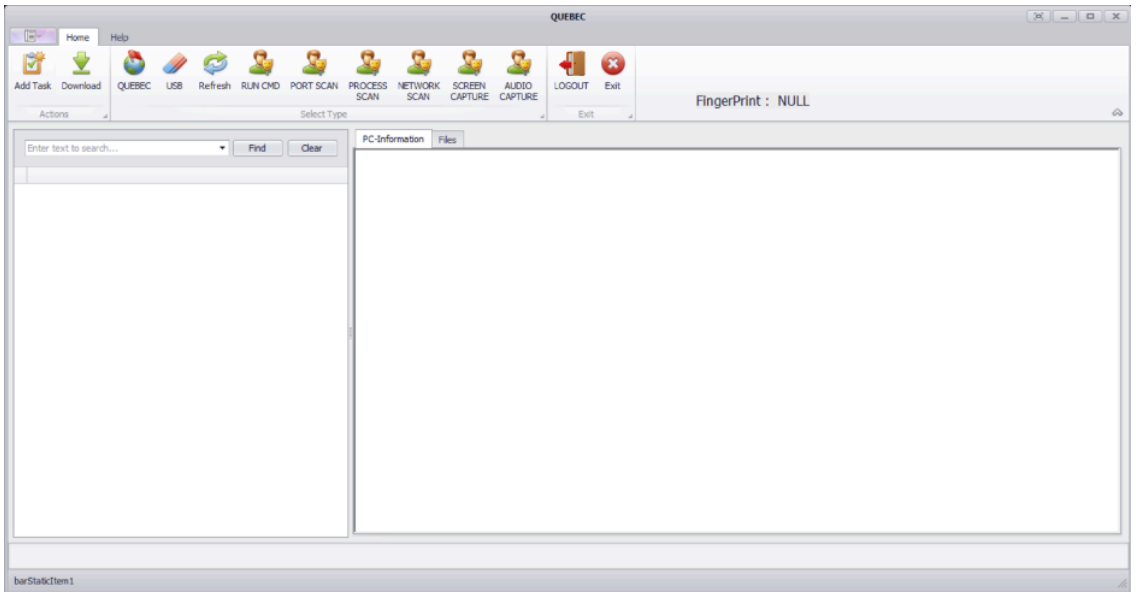

Bits Before Bullets
Username
Select Tool
Select Tool
SIERRA
QUEBEC
ZULU
DROPPER
WORDDROPPER
COMICUM
v.4.4

Login screen for GravityAdmin titled “Bits Before Bullets.”

When the operator clicks the login button, the executable will check if it is connected to the internet by sending a ping request to www[.]google[.]com. Then, the user ID and password are authenticated with an authentication server which sends back:

- A code to direct the panel binary to open the panel UI for the specified panel.
- Also sends a value back via the HTTP “Authorization” Header. This value acts as an authentication token when communicating with campaign-specific[C2 servers to load data such as a list of infected machines, etc.

A typical Panel screen will list the machines infected as part of the specific campaign. It also has buttons to trigger various malicious actions against one or more infected systems.



Different panels have different capabilities, however, some core capabilities are common across all campaigns.

The various campaigns configured in the Panel binaries are code named as:

- "SIERRA"
- "QUEBEC"
- "ZULU"
- "DROPPER"
- "WORDDROPPER"
- "COMICUM"
- "ROCKAMORE"
- "FOXTROT"
- "CLOUDINFINITY"
- "RECOVERBIN"
- "CVSCOUT"
- "WEBBUCKET"

- "CRAFTWITHME"
- "SEXYBER"
- "CHATICO"

Each of the codenamed campaigns from the Panel binaries consists of its own infection mechanisms. For example, “FOXTROT,” “CLOUDINFINITY” and “CHATICO” are names given to all Android-based GravityRAT infections whereas “CRAFTWITHME,” “SEXYBER” and “CVSCOUT” are named for attacks deploying HeavyLift. Our analysis correlates the campaigns listed above with the Operating Systems being targeted with respective malware families.

Campaign Name	Platform targeted and Malware Used
SIERRA	Windows, GravityRAT
QUEBEC	Windows, GravityRAT
ZULU	Windows, GravityRAT
DROPPER / WORDDROPPER / COMICUM	Windows, GravityRAT
ROCKAMORE	Windows, GravityRAT
FOXTROT / CLOUDINFINITY / RECOVERBIN / CHATICO	Android, GravityRAT
CVSCOUT	Windows, HeavyLift
WEBBUCKET / CRAFTWITHME	Windows, HeavyLift
SEXYBER	Windows, HeavyLift

Most campaigns consist of infrastructure overlaps between each other mostly to host malicious payloads or maintain a list of infected systems.

	Campaigns using the domain

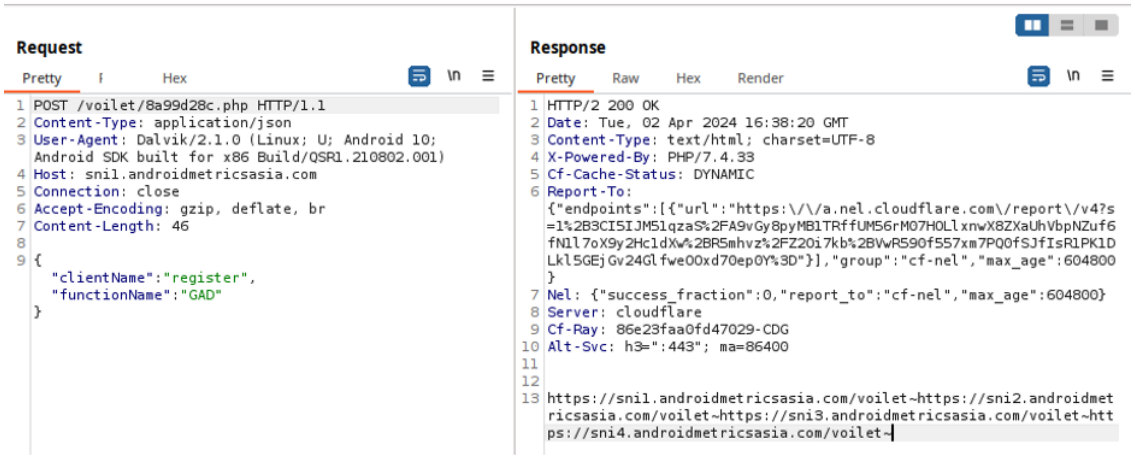
GravityRAT: A multi-platform remote access trojan

GravityRAT is a Windows-based remote access trojan first disclosed by Talos in 2018. GravityRAT was later ported to the Android operating system to target mobile devices around 2019. Since 2019, we've observed a continuous addition of a multitude of capabilities in GravityRAT and its associated infrastructure. So far, we have observed the use of GravityRAT exclusively by suspected Pakistani threat actors to target entities and individuals in India. There is currently no publicly available evidence to suggest that GravityRAT is a commodity/open-source malware, suggesting its potential use by multiple, disparate threat actors.

Our analysis of the entire ecosystem of Operation Celestial Force revealed that GravityRAT's use in this campaign likely began as early as 2016 and continues to this day.

The latest variants of GravityRAT are distributed through malicious websites, some registered and set up as late as early January 2024, pretending to distribute legitimate Android applications. Malicious operators will distribute the download links to their targets over social media channels asking them to download and install the malware.

The latest variants of GravityRAT use the previously mentioned code names to define the campaigns. The screenshot below shows the initial registration of a victim into the C2, getting back a list of alternative C2 to be used, if needed.

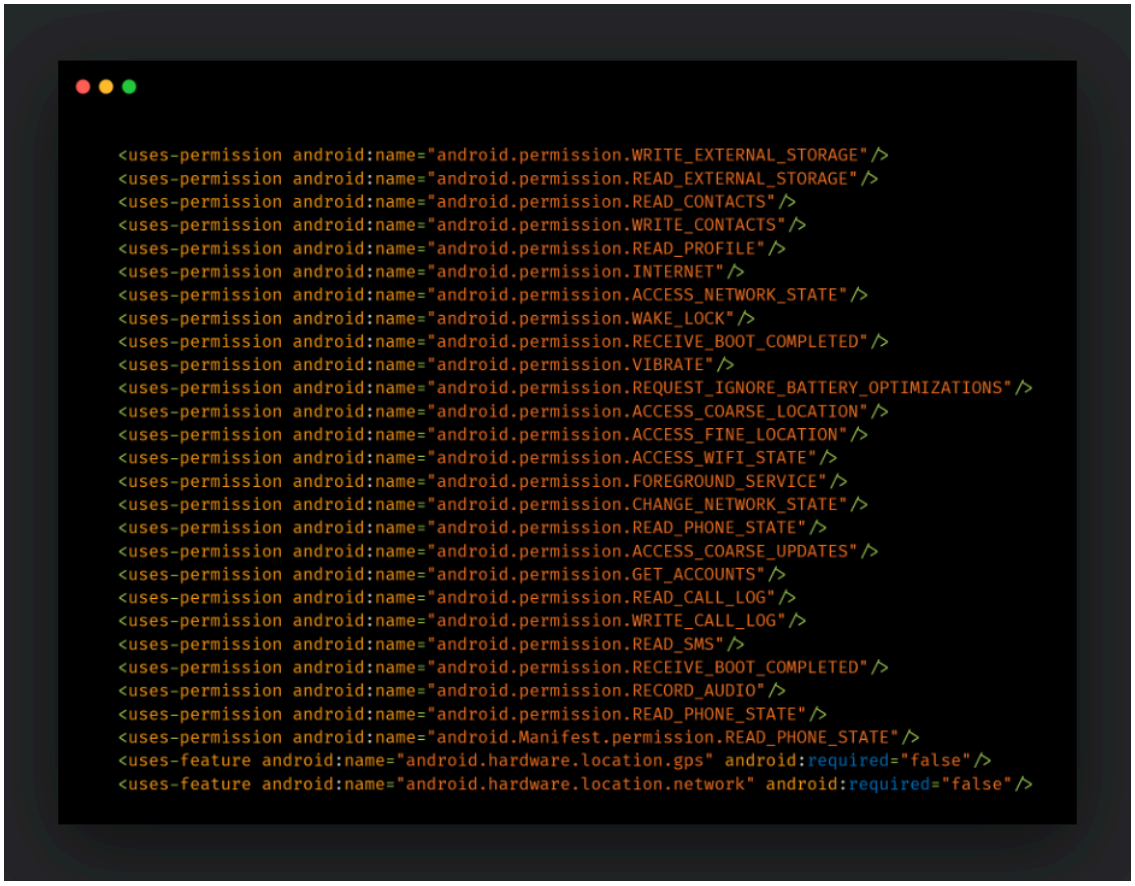


The group uses Cloudflare service to hide the true location of their C2 servers.

After registration, the trojan requests tasks to execute to the C2 followed by uploading a file containing the device's location.

The trojan will use a different user-agent for each request — it's unclear if this is done on purpose, or if this anomaly is just the result of cut-and-paste code from other projects to tie together this trojan's features.

GravityRAT requests the following permissions on the device for stealing information and housekeeping tasks.



These variants of GravityRAT are similar to previously disclosed versions from ESET and Cyble and consist of the following capabilities:

1. Send preliminary information about the device to the C2. This information includes IMEI, phone number, network country ISO code, network operator name, SIM country ISO code, SIM operator name, SIM serial number, device model, brand, product and manufacturer, addresses surrounding the obtained longitude and latitude of the device and the current build information, including release, host, etc.
2. Read SMS data and content and upload to the C2.
3. Read specific file formats and upload them to the C2.
4. Read call logs and upload them to the C2.
5. Obtain IMEI information including associated email ID and send it to C2.
6. Delete all contacts, call logs and files related to the malware.

HeavyLift: Electron-based malware loader

Some of the campaigns in this operation use Electron-based malware loaders we're calling "HeavyLift," which consist of JavaScript code communicating and controlled by C2 servers. These are the same C2 servers that interact with GravityAdmin, the panel tool used by the operators to govern infected systems. HeavyLift is essentially a stage one malware component that downloads and installs other malicious implants whenever available on the C2 server. HeavyLift bears some similarities with GravityRAT's Electron versions disclosed previously by Kaspersky in 2020.

A HeavyLift infection begins with an executable masquerading as an installer for a legitimate application. The installer installs a dummy application but also installs and sets up a malicious Electron-based desktop application. This malicious application is, in fact, HeavyLift and consists of JavaScript code that carries out malicious operations on the infected system.

On execution, HeavyLift will check if it is running on a macOS or Windows system. If it is running on macOS, and not running as root, it will execute with admin privileges using the command:

```
/usr/bin/osascript -e 'do shell script "bash -c " _process_path " with administrator privileges'
```

If it is running as root, it will set the default HTTP User-Agent to "M_9C9353252222ABD88B123CE5A78B70F6", then get system info using the commands:

```
system_profiler SPHardwareDataType | grep 'Model Name'

system_profiler SPHardwareDataType | grep 'SMC'

system_profiler SPHardwareDataType | grep 'Model Identifier'

system_profiler SPHardwareDataType | grep 'ROM'

system_profiler SPHardwareDataType | grep 'Serial Number'
```

For a Windows-based system, the HTTP User-Agent is set to "W_9C9353252222ABD88B123CE5A78B70F6". The malware will then obtain preliminary system information such as:

- Processor ID
- MAC address
- Installed anti-virus product name
- Username
- Domain name
- Platform information
- Process, OS architecture
- Agent (hardcoded value)
- OS release number

All this preliminary information is sent to the hardcoded C2 server URL to register the infection with the C2.

HeavyLift will then reach out to the C2 server to poll for any new payloads to execute on the infected system. A payload received from the C2 will be dropped to a directory in the "AppData" directory and persisted on the system.

On macOS, the payload is a ZIP file that is extracted, and the resulting binary persists using crontab via the command:

```
crontab -l 2>/dev/null; echo ' */2 * * * * "_filepath_" _arguments_ ' | crontab -
```

For Windows, the payload received is an EXE file that persists on the system via a scheduled task. The malware will create an XML file for the scheduled tasks with the payload path, arguments and working directory and then use the XML to set up the schedtask:

```
SCHTASKS /Create /XML "_xmlpath_" /TN "_taskname_" /F
```

The malware will then open the accompanying HTML file via web view to appear legitimate.

In some cases, the malware will also perform anti-analysis checks to see if it's running in a virtual environment.

It checks for the presence of specific keywords before closing if there is a match:

- Innotek GmbH
- VirtualBox
- VMware
- Microsoft Corporation
- HITACHI

These keywords are checked against model information, SMC, ROM and serial numbers on macOS and Windows against manufacturer information, such as product, vendor, processor and more.

Coverage

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

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
✓	✓	✓	✓

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.

HeavyLift

8e9bcc00fc32ddc612bdc0f1465fc79b40fc9e2df1003d452885e7e10feab1ee
ceb7b757b89693373ffa1c46dd96544bdc25d1a47608c2ea24578294bcf1db37
06b617aa8c38f916de8553ff6f572dcaa96e5c8941063c55b6c424289038c3a1
da3907cf75662c3401581a5140831f8b2520a4c3645257b3860c7db94295af88
838fd5d269fa09ef4f7e9f586b6577a9f46123a0af551de02de78501d916236d
12d98137cd1b0cf59ce2fafbfe3a9c3477a42dae840909adad5d4d9f05dd8ede
688c8e4522061bb9d82e4c3584f7ef8afc6f9e07e2374567755faad2a22e25b8
5695c1e5e4b381844a36d8281126eef73a9641a315f3fdd2eb475c9073c5f4da
8d458fb59b6da20e1ba1658bb4a1f7dbb46d894530878e91b64d3c675d3d4516

GravityRAT Android

36851d1da9b2f35da92d70d4c88ea1675f1059d68fafd3abb1099e075512b45e
4ebdfa738ef74945f6165e337050889dfa0aad61115b738672bbeda648a59dab
1382997d3a5bb9bdbb9d41bb84c916784591c7cdae68305c3177f327d8a63b71
c00cedd6579e01187cd256736b8a506c168c6770776475e8327631df2181fae2
380df073825aca1e2fdbea379431c2f4571a8c7d9369e207a31d2479fbc7be88

GravityAdmin

63a76ca25a5e1e1cf6f0ca8d32ce14980736195e4e2990682b3294b125d241cf
69414a0ca1de6b2ab7b504a507d35c859fc5a1b8e0b3cf0c6a8948b2f652cbe9

04e216f4780b6292ccc836fa0481607c62abb244f6a2eedc21c4a822bcf6d79f

Network IOCs

androidmetricsasia[.]com
dl01[.]mozillasecurity[.]com
officelibraries[.]com
javacdnlib[.]com
windowsupdatecloud[.]com
webbucket[.]co[.]uk
craftwithme[.]uk
sexyber[.]net
rockamore[.]co[.]uk
androidsdkstream[.]com
playstoreapi[.]net
sdklibraries[.]com
cvscout[.]uk
zclouddrive[.]com
jdklibraries[.]com
cloudieapp[.]net
androidadbserver[.]com
androidwebkit[.]com
teraspace[.]co[.]in

hxxps[://]zclouddrive[.]com/downloads/CloudDrive_Setup_1[.]0[.]1[.]exe
hxxps[://]www[.]sexyber[.]net/downloads/7ddf32e17a6ac5ce04a8ecbf782ca509/Sexyber-1[.]0[.]0[.]zip
hxxps[://]sexyber[.]net/downloads/7ddf32e17a6ac5ce04a8ecbf782ca509/Sexyber-1[.]0[.]0[.]zip
hxxps[://]cloudieapp[.]net/cloudie[.]zip
hxxps[://]sni1[.]androidmetricsasia[.]com/voilet/8a99d28c[.]php
hxxps[://]dev[.]androidadbserver[.]com/jurassic/6c67d428[.]php
hxxps[://]adb[.]androidadbserver[.]com/jurassic/6c67d428[.]php
hxxps[://]library[.]androidwebkit[.]com/kangaroo/8a99d28c[.]php
hxxps[://]ux[.]androidwebkit[.]com/kangaroo/8a99d28c[.]php
hxxps[://]jupiter[.]playstoreapi[.]net/indigo/8a99d28c[.]php
hxxps[://]moon[.]playstoreapi[.]net/indigo/8a99d28c[.]php
hxxps[://]sni1[.]androidmetricsasia[.]com/voilet/8a99d28c[.]php
hxxps[://]moon[.]playstoreapi[.]net/indigo/8a99d28c[.]php
hxxps[://]moon[.]playstoreapi[.]net/indigo/8a99d28c[.]php
hxxps[://]jre[.]jdklibraries[.]com/hotriculture/671e00eb[.]php
hxxps[://]jre[.]jdklibraries[.]com/hotriculture/671e00eb[.]php
hxxps[://]cloudinfinity-d4049-default-rtdb[.]firebaseio[.]com/
hxxps[://]dl01[.]mozillasecurity[.]com/
hxxps[://]dl01[.]mozillasecurity[.]com/Sier/resauth[.]php

hxxps[://]dl01[.]mozillasecurity[.]com/resauth[.]php/
hxxps[://]tl37[.]officelibraries[.]com/Sier/resauth[.]php
hxxps[://]tl37[.]officelibraries[.]com/resauth[.]php/
hxxps[://]jun[.]javacdnlib[.]com/Quebec/5be977ac[.]php
hxxps[://]dl01[.]mozillasecurity[.]com/resauth[.]php/
hxxps[://]dl01[.]mozillasecurity[.]com/MicrosoftUpdates/6efbb147[.]php
hxxps[://]tl37[.]officelibraries[.]com/MicrosoftUpdates/741bbfe6[.]php
hxxps[://]tl37[.]officelibraries[.]com/MsWordUpdates/c47d1870[.]php
hxxps[://]dl01[.]windowsupdatecloud[.]com/opex/7ab24931[.]php
hxxps[://]tl37[.]officelibraries[.]com/opex/13942BA7[.]php
hxxp[://]dl01[.]windowsupdatecloud[.]com/opex/7ab24931[.]php
hxxps[://]tl37[.]officelibraries[.]com/opex/13942BA7[.]php
hxxps[://]download[.]rockamore[.]co[.]uk/m2c/m_client[.]php
hxxps[://]api1[.]androidsdkstream[.]com/foxtrot/
hxxps[://]api1[.]androidsdkstream[.]com/foxtrot/61c10953[.]php
hxxps[://]jupiter[.]playstoreapi[.]net/RB/e7a18a38[.]php
hxxps[://]sdk2[.]sdklibraries[.]com/golf/c6cf642b[.]php
hxxps[://]jre[.]jdklibraries[.]com/hotriculture/671e00eb[.]php
hxxps://hxxp[://]api1[.]androidsdkstream[.]com/foxtrot//DataX/
hxxps[://]download[.]cvscout[.]uk/cvscout/cvstyler_client[.]php
hxxps[://]download[.]webbucket[.]co[.]uk/webbucket/strong_client[.]php
hxxps[://]www[.]craftwithme[.]uk/cwmb/craftwithme/strong_client[.]php
hxxps[://]download[.]sexyber[.]net/sexyber/sexyberC[.]php
hxxps[://]download[.]webbucket[.]co[.]uk/A0B74607[.]php
hxxps[://]zclouddrive[.]com/system/546F9A[.]php
hxxps[://]download[.]cvscout[.]uk/cvscout/
hxxps[://]download[.]cvscout[.]uk/c9a5e83c[.]php
hxxps[://]zclouddrive[.]com/downloads/CloudDrive_Setup_1[.]0[.]1[.]exe
hxxps[://]zclouddrive[.]com/system/clouddrive/
hxxps[://]www[.]sexyber[.]net/downloads/7ddf32e17a6ac5ce04a8ecbf782ca509/Sexyber-1[.]0[.]0[.]zip
hxxps[://]sexyber[.]net/downloads/7ddf32e17a6ac5ce04a8ecbf782ca509/Sexyber-1[.]0[.]0[.]zip
hxxps[://]download[.]sexyber[.]net/0fb1e3a0[.]php
hxxps[://]www[.]craftwithme[.]uk/cwmb/d26873c6[.]php
hxxps[://]download[.]teraspace[.]co[.]in/teraspace/
hxxps[://]download[.]teraspace[.]co[.]in/78181D14[.]php
hxxps[://]www[.]craftwithme[.]uk/cwmb/craftwithme/
hxxps[://]download[.]webbucket[.]co[.]uk/webbucket/

Source: https://blog.talosintelligence.com/cosmic-leopard/