THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Pubload Malware Campaign

by Hive0154 Threat Actor

CATEGORY

Malware

SEVERITY

Critical

Platforms

Windows

IMPACT

- Cyber Espionage
- Cultural Destabilization
- Cross-regional Threat

Description

Pubload Malware Campaign by (Hive0154 Threat Actor)

Researchers have reported a sophisticated phishing campaign conducted by China-aligned threat actor **Hive0154** in mid-2025. The campaign delivers the **Pubload** malware via spear-phishing emails using lure documents themed around sensitive Tibetan-related events such as the **9th World Parliamentarians' Convention on Tibet** and publications by the **Dalai Lama**.

This activity aligns with the Chinese geopolitical interest in suppressing Tibetan autonomy and appears timed to influence or disrupt community awareness around the **Dalai Lama's 90th birthday** and related international events.

Technical Summary:

Initial Vector: Phishing emails with links to weaponized archives on Google Drive

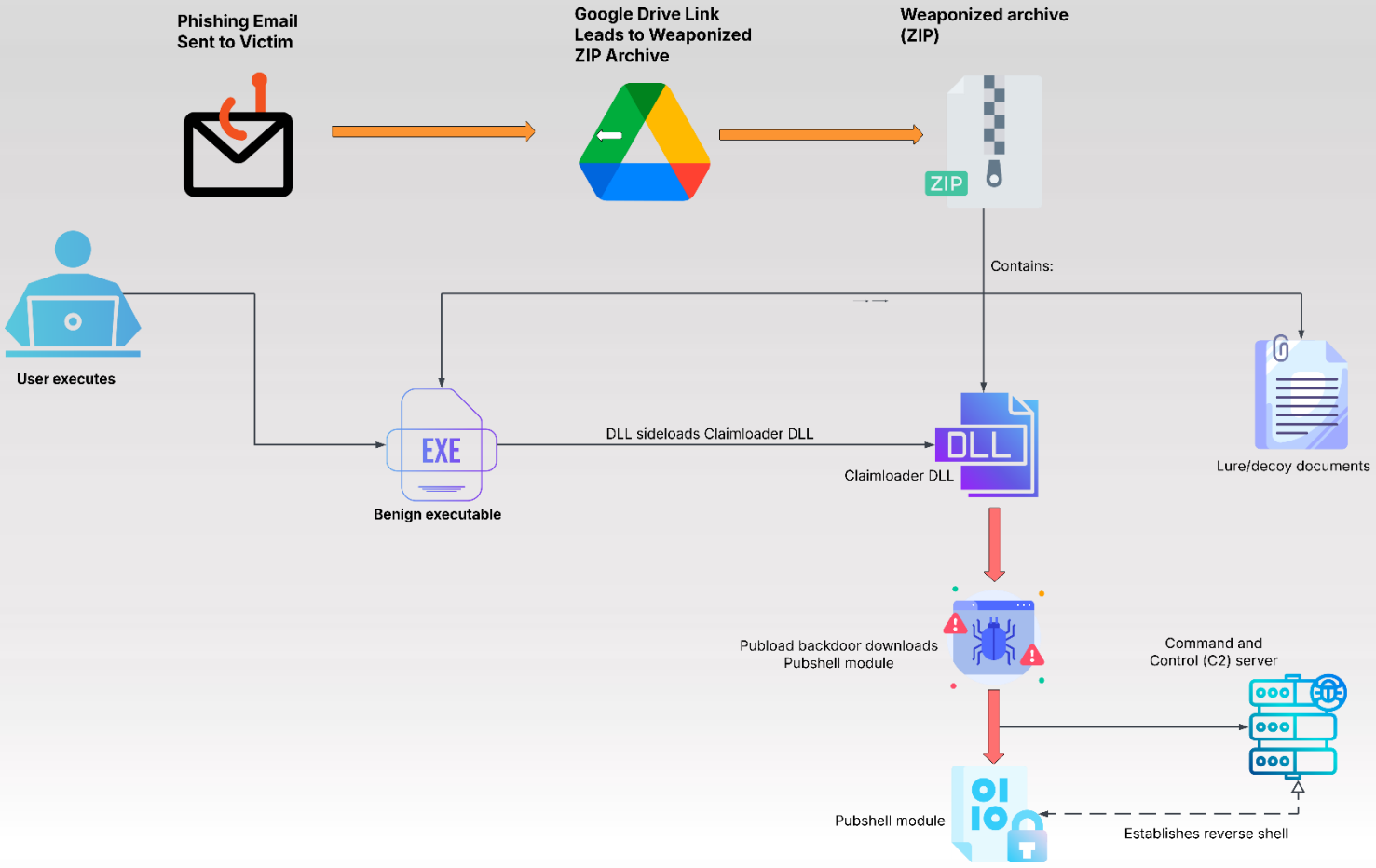
Loader: *Claimloader*

- Persists using HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Decrypts shellcode using TripleDES
- Uses LdrLoadDll() and LdrGetProcedureAddress() for import resolution

Payload: *Pubload*

- Loads *Pubshell* reverse shell module
- Capable of in-memory payload execution and remote access

Infection chain and technical analysis



Indicator of Compromise

SHA-256

2bd60685299c62abe500fe80e9f03a627a1567059ce213d7c0cc762fa32552d7
c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444
93f1fd31e197a58b03c6f5f774c1384ffd03516ab1172d9b26ef5a4a32831637
3e7384c5e7c5764258947721c7792f221fb47ef53d447a7af5db5426f1e7c13d
8cd4324e1e764aafba4ea0394a82943cefd7deeee28a6cbd19f2ba69de6a5766
7979686bf73c298ab5d57f9605dcef2231ca87580f6ceecd75b2cbe81669ba0
ea991719885b2fe91502218ff3be12c9f990a24c7e007e4ffb5a5c5c52b3a0b5
6e408aada775eaf19c524792344cabca0b406247154e2b03ed03a929e0feee5a
57770ede7015734e2d881430423bcc76c160b90448f5e67334e56b9747ff874c
fb33f222b3d4d5edc9b743e64282de561ef51e42db150dd8086203c53b25ff79

MD5

f8099461ca9098bc6a1e7a9de9f989ec
2123eab51aa468d5140c3bfe2bbe7775
5d88adf862e6944b995ac6dd5151588d
668d0cbedde9edd87823f3ed08569a6c
af5cbc0d6d26064ca8d4ecf64eeca7fa0
4d65961f06157b3dd87bfc494142c055
6007561fb40a25e797f3461b867427cc
5a47c6b4bdb2964285dfb0233ab75924

SHA-1

684c53a07ca0928f5bc4a31e15be7be6ca25b2bd
eee8b975bfb640ffb99a2d3065998b4edab704c8
8329dc43b776bf040aa646154016748b688d8ee9
034ec391503041836fcc1e0d8d52ecfeea41f8f1
eacb62b12852793552412e0cec7fd0fe17e58599
f205d2a3bc6e0551c6a9673c82836b89adc8e3eb
69c4087b7992fbaeb66c3a51a712dc66afbe1de4
5bd9b1698dc885ec18b6ad5e97ff6529815ae337
f70b2e8fe1bdea492bbec231c6ae0982c667ac16
d2609e8a7c65c33b6182936d6322625d8015c010

Recommended Immediate Actions

- Block suspicious Google Drive URLs in email security appliances
- Train employees to detect archive-based phishing with executable payloads

Monitor:

- C:\ProgramData* directories for unauthorized EXE/DLL pairs
- Registry Run keys and unsanctioned persistence mechanisms
- TLS 1.2 AppData packets (without handshake) indicating Pubload beacons
- Implement threat hunting for:
- DLL sideloading behavior
- XOR-encoded API calls and unusual Ldr* function usage
- Unusual scheduled tasks or font-related API executions (EnumFontsW)

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world

Pubload Malware Campaign by (Hive0154 Threat Actor)

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net