Hive0154 Mustang Panda Shifts Focus Tibetan Community Deploy Pubload Backdoor

By Golo Mühr, Joshua Chung

Published: 2025-06-23 · Archived: 2026-04-05 19:00:10 UTC

Joshua Chung

Cyber Threat Intelligence Analyst

IBM Security

Summary

In June 2025, IBM X-Force researchers discovered China-aligned threat actor, Hive0154, spreading Pubload malware featuring lure documents and filenames targeting the Tibetan community. The Tibetan sovereignty dispute is often invoked by Chinese threat groups in their cyber operations, with the latest campaign coinciding with activities leading up to a major event for the Tibetan community, the Dalai Lama's 90th birthday.

Several lures observed feature the following topics related to the Tibetan community:

- The 9th World Parliamentarians' Convention on Tibet (WPCT), held from 06/02 - 06/04 in Tokyo, Japan.
- China’s education policy in the Tibet Autonomous Region (TAR). The topic is of high importance to the Tibetan community, and cultural assimilation in Tibet has been noted by Human Rights Watch in its report.
- The March 2025 book *Voice for the Voiceless*, published by the Tibetan leader-in-exile, the Dalai Lama. The book discusses the Dalai Lama's dialogue with Chinese leaders regarding the independence of Tibet.

Key findings

- China-aligned threat actor Hive0154 has spread numerous phishing lures in targeted campaigns throughout 2025 to deploy the Pubload backdoor
- Hive0154 devises filenames referencing various geopolitical topics tailored to elicit increased interest from the targeted recipients
- As of May 2025, X-Force noticed an increased focus on topics tailored to target the Tibetan community
- The phishing campaigns reference the 9th World Parliamentarians' Convention on Tibet (WPCT) held in Tokyo in June, China’s education policy in the Tibet Autonomous Region (TAR) and the 2025 book *Voice for the Voiceless* by the Dalai Lama

Hive0154 overview

Hive0154 is a well-established China-aligned threat actor with a large malware arsenal, consistent techniques and well-documented activity over the past several years. The group consists of multiple subclusters and engages in

cyberattacks targeting public and private organizations, including think tanks, policy groups, government agencies and individuals. X-Force's observation of the group's use of multiple custom malware loaders, backdoors and USB worm families showcases their advanced capabilities. Hive0154 activity overlaps with threat actors publicly reported as Mustang Panda, Stately Taurus, Camaro Dragon, Twill Typhoon, Polaris and Earth Preta.

Previous activity

X-Force previously detailed extensive activity attributed to a subcluster of Hive0154 targeting the US, Philippines, Pakistan and Taiwan in a suspected espionage campaign from late 2024 to early 2025. The group makes use of weaponized archives originating from spear phishing emails to target entities including the Philippines', the United States' and Pakistan's government, military and diplomatic personnel. The phishing emails, archives and malicious file names use references to various geopolitical topics tailored to their specific audience to elicit increased interest from the recipients. The emails commonly include Google Drive URLs that download weaponized ZIP or RAR archives if the recipient clicks on the link.

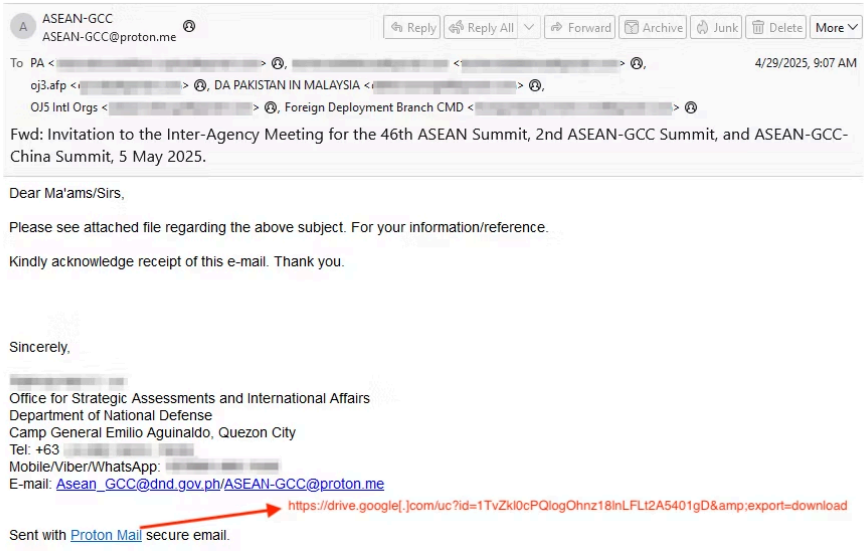
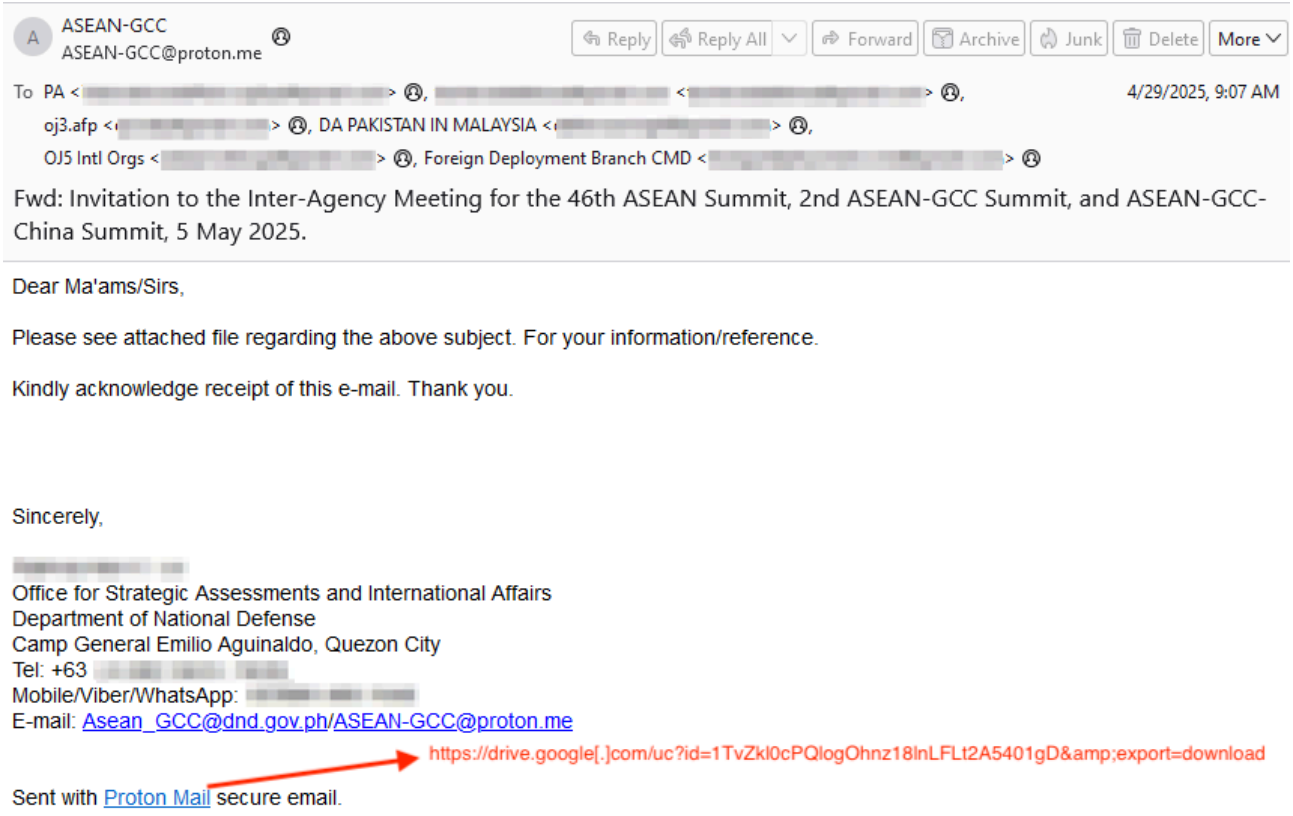


Fig. 1: Example Hive0154 phishing email from a campaign in April 2025.



A ASEAN-GCC
ASEAN-GCC@proton.me

Reply | Reply All | Forward | Archive | Junk | Delete | More

To PA <[redacted]>, [redacted] <[redacted]>, 4/29/2025, 9:07 AM
oj3.afp <[redacted]>, DA PAKISTAN IN MALAYSIA <[redacted]>,
OJ5 Intl Orgs <[redacted]>, Foreign Deployment Branch CMD <[redacted]>

Fwd: Invitation to the Inter-Agency Meeting for the 46th ASEAN Summit, 2nd ASEAN-GCC Summit, and ASEAN-GCC-China Summit, 5 May 2025.

Dear Ma'ams/Sirs,

Please see attached file regarding the above subject. For your information/reference.

Kindly acknowledge receipt of this e-mail. Thank you.

Sincerely,

[redacted]
Office for Strategic Assessments and International Affairs
Department of National Defense
Camp General Emilio Aguinaldo, Quezon City
Tel: +63 [redacted]
Mobile/Viber/WhatsApp: [redacted]
E-mail: Asean_GCC@dnd.gov.ph/ASEAN-GCC@proton.me

https://drive.google[.]com/uc?id=1TvZkl0cPQlogOhnz18lnLFLt2A5401gD&export=download

Sent with Proton Mail secure email.

The archives contain a benign executable vulnerable to DLL sideloading and a malicious Claimloader DLL. The executables are typically renamed to trick victims into opening them, which would immediately trigger the infection chain. The Claimloader malware establishes persistence, decrypts its embedded Pubload payload and injects it into memory. Pubload further downloads Pubshell, a light-weight backdoor facilitating immediate access to the machine via a reverse shell.

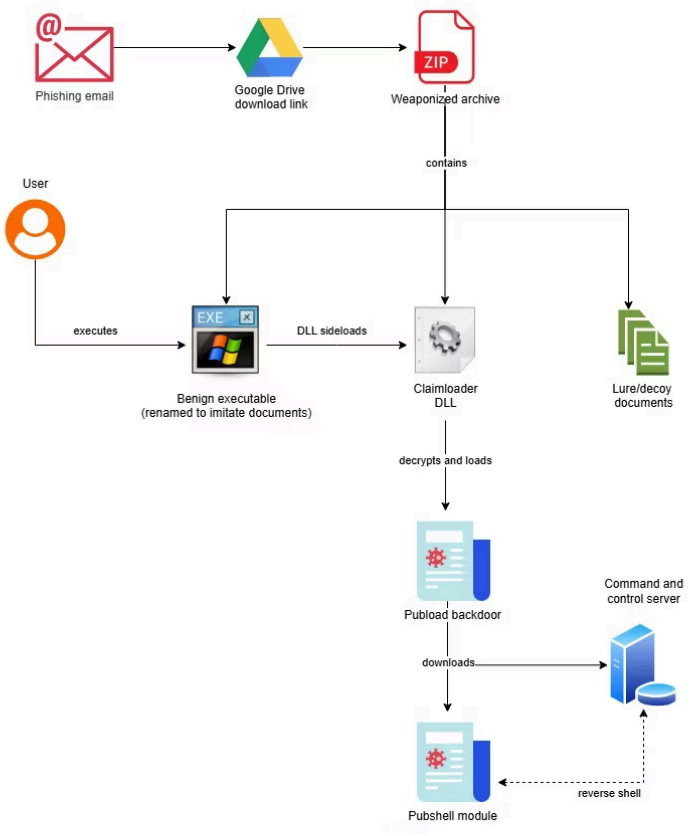
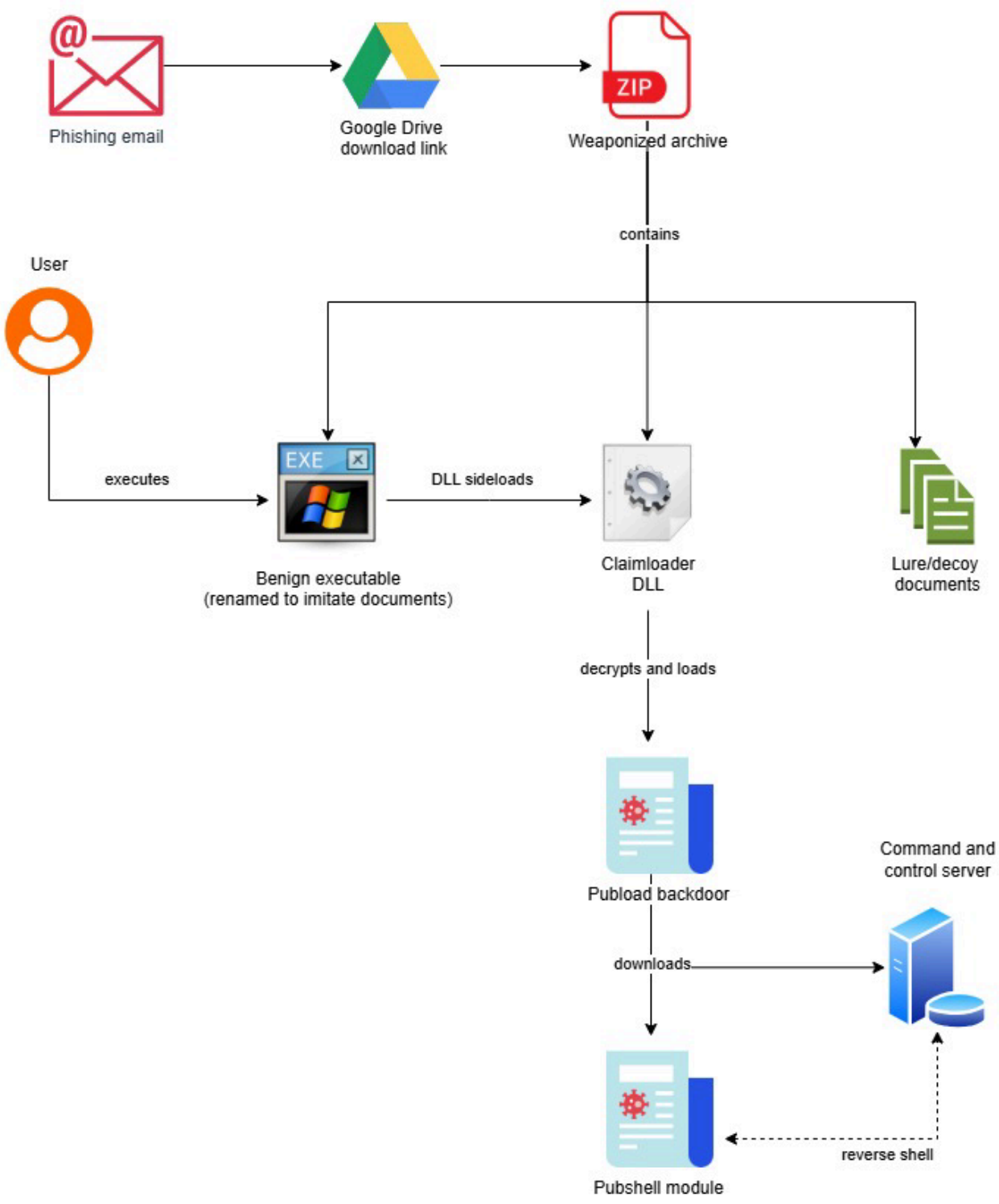


Fig. 2: Pubload infection chain



9th World Parliamentarians' Convention on Tibet (WPCT)

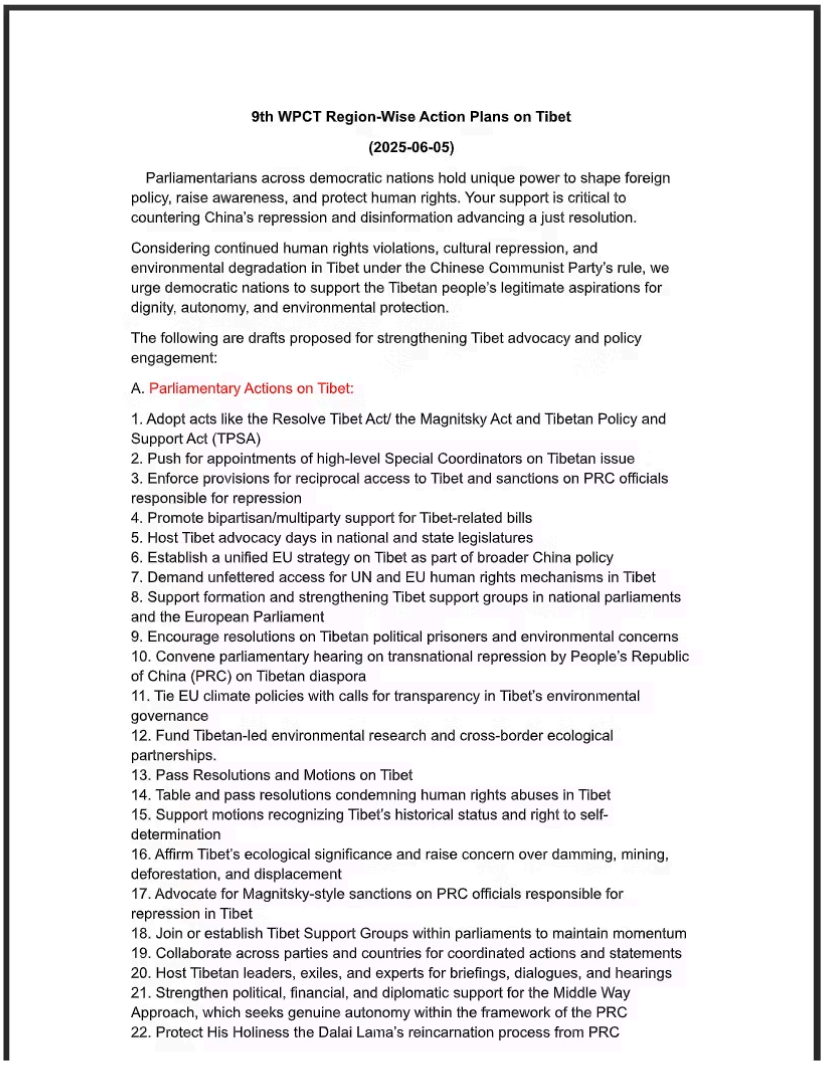
At the time the campaign first began (May 21), the WPCT lure below was likely a reference to the upcoming convention held in Tokyo, Japan, from June 2 to June 4.

Lure name	Submitter country	Claimloader DLL SHA256	Date
(WPCT)-ICT&CTA_Conference /(World_Parliamentarians' _Convention_on _Tibet(WPTC)_in _Japan_tokyo).June 2025.exe	India	2bd60685299c62abe500fe80e9f03a627a1567059ce213d7c0cc762fa32552d7	21 May 2025

The convention is usually held in the U.S. or Europe, and was hosted in Japan for the first time. Overall, 142 parliamentarians and representatives from 29 countries were in attendance, including parliamentary members from Belgium and Japan. The Chinese embassy in Japan issued a strong denouncement over the Central Tibetan Administration's, also known as the Tibetan government-in-exile, involvement in the convention. The convention resulted in the Tokyo Declaration, condemning Chinese government repression in the Tibet region, and calling for international legislation to safeguard Tibetan cultural and religious freedom. X-Force researchers uncovered the Hive0154 campaign devising different lures pre- and post-convention.

After the convention, several declarations were issued, including Wise Action Plans on Tibet. Hive0154 likely copied it from the website and into a benign Microsoft Word document (DOCX) within a weaponized archive. The archive further contains articles directly copied from multiple Tibetan websites (here and here) in relation to the convention, as well as authentic photos from the convention. The presence of legitimate articles and photos among the weaponized executables sharing the same names is likely to trick victims into accidentally opening one of the EXE files and unknowingly triggering the infection.

"9th WPCT Region-Wise Action Plans on Tibet.exe":



9th WPCT Region-Wise Action Plans on Tibet

(2025-06-05)

Parliamentarians across democratic nations hold unique power to shape foreign policy, raise awareness, and protect human rights. Your support is critical to countering China's repression and disinformation advancing a just resolution.

Considering continued human rights violations, cultural repression, and environmental degradation in Tibet under the Chinese Communist Party's rule, we urge democratic nations to support the Tibetan people's legitimate aspirations for dignity, autonomy, and environmental protection.

The following are drafts proposed for strengthening Tibet advocacy and policy engagement:

A. Parliamentary Actions on Tibet:

1. Adopt acts like the Resolve Tibet Act/ the Magnitsky Act and Tibetan Policy and Support Act (TPSA)
2. Push for appointments of high-level Special Coordinators on Tibetan issue
3. Enforce provisions for reciprocal access to Tibet and sanctions on PRC officials responsible for repression
4. Promote bipartisan/multiparty support for Tibet-related bills
5. Host Tibet advocacy days in national and state legislatures
6. Establish a unified EU strategy on Tibet as part of broader China policy
7. Demand unfettered access for UN and EU human rights mechanisms in Tibet
8. Support formation and strengthening Tibet support groups in national parliaments and the European Parliament
9. Encourage resolutions on Tibetan political prisoners and environmental concerns
10. Convene parliamentary hearing on transnational repression by People's Republic of China (PRC) on Tibetan diaspora
11. Tie EU climate policies with calls for transparency in Tibet's environmental governance
12. Fund Tibetan-led environmental research and cross-border ecological partnerships.
13. Pass Resolutions and Motions on Tibet
14. Table and pass resolutions condemning human rights abuses in Tibet
15. Support motions recognizing Tibet's historical status and right to self-determination
16. Affirm Tibet's ecological significance and raise concern over damming, mining, deforestation, and displacement
17. Advocate for Magnitsky-style sanctions on PRC officials responsible for repression in Tibet
18. Join or establish Tibet Support Groups within parliaments to maintain momentum
19. Collaborate across parties and countries for coordinated actions and statements
20. Host Tibetan leaders, exiles, and experts for briefings, dialogues, and hearings
21. Strengthen political, financial, and diplomatic support for the Middle Way Approach, which seeks genuine autonomy within the framework of the PRC
22. Protect His Holiness the Dalai Lama's reincarnation process from PRC

Fig. 3: Screenshot of benign DOCX packaged into weaponized archive together with EXE's sharing the same filename

9th WPCT Region-Wise Action Plans on Tibet

(2025-06-05)

Parliamentarians across democratic nations hold unique power to shape foreign policy, raise awareness, and protect human rights. Your support is critical to countering China's repression and disinformation advancing a just resolution.

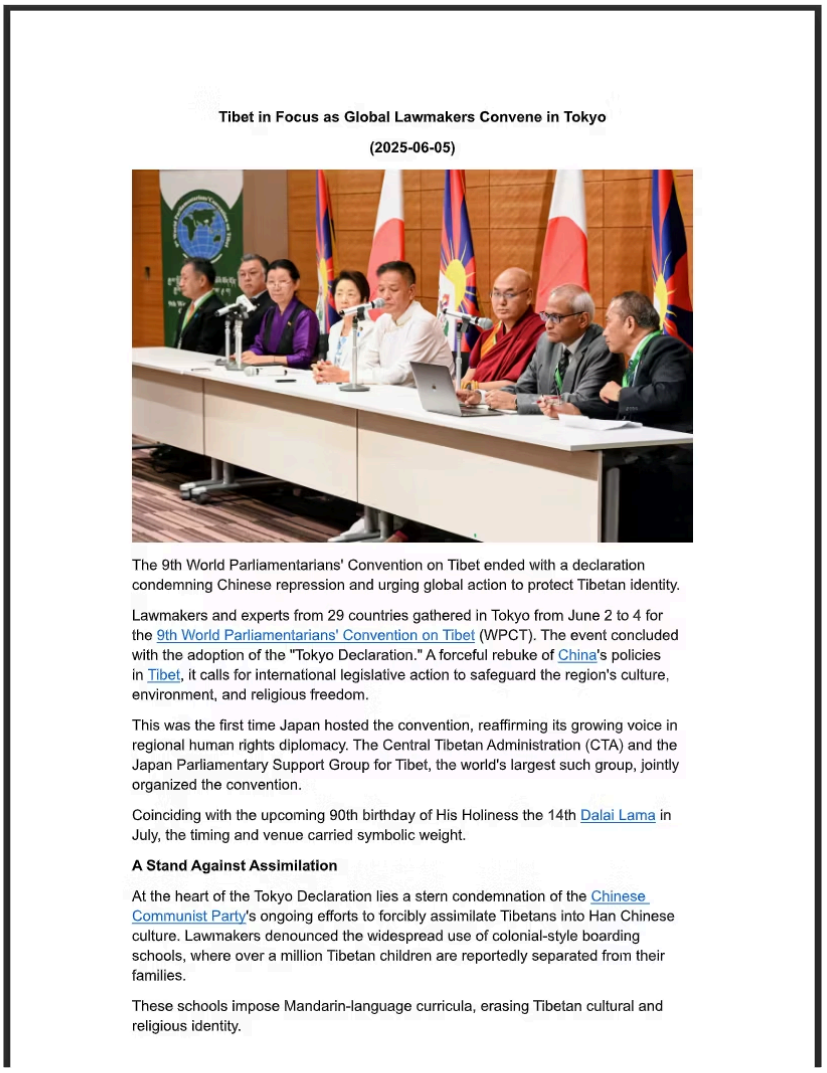
Considering continued human rights violations, cultural repression, and environmental degradation in Tibet under the Chinese Communist Party's rule, we urge democratic nations to support the Tibetan people's legitimate aspirations for dignity, autonomy, and environmental protection.

The following are drafts proposed for strengthening Tibet advocacy and policy engagement:

A. Parliamentary Actions on Tibet:

1. Adopt acts like the Resolve Tibet Act/ the Magnitsky Act and Tibetan Policy and Support Act (TPSA)
2. Push for appointments of high-level Special Coordinators on Tibetan issue
3. Enforce provisions for reciprocal access to Tibet and sanctions on PRC officials responsible for repression
4. Promote bipartisan/multiparty support for Tibet-related bills
5. Host Tibet advocacy days in national and state legislatures
6. Establish a unified EU strategy on Tibet as part of broader China policy
7. Demand unfettered access for UN and EU human rights mechanisms in Tibet
8. Support formation and strengthening Tibet support groups in national parliaments and the European Parliament
9. Encourage resolutions on Tibetan political prisoners and environmental concerns
10. Convene parliamentary hearing on transnational repression by People's Republic of China (PRC) on Tibetan diaspora
11. Tie EU climate policies with calls for transparency in Tibet's environmental governance
12. Fund Tibetan-led environmental research and cross-border ecological partnerships.
13. Pass Resolutions and Motions on Tibet
14. Table and pass resolutions condemning human rights abuses in Tibet
15. Support motions recognizing Tibet's historical status and right to self-determination
16. Affirm Tibet's ecological significance and raise concern over damming, mining, deforestation, and displacement
17. Advocate for Magnitsky-style sanctions on PRC officials responsible for repression in Tibet
18. Join or establish Tibet Support Groups within parliaments to maintain momentum
19. Collaborate across parties and countries for coordinated actions and statements
20. Host Tibetan leaders, exiles, and experts for briefings, dialogues, and hearings
21. Strengthen political, financial, and diplomatic support for the Middle Way Approach, which seeks genuine autonomy within the framework of the PRC
22. Protect His Holiness the Dalai Lama's reincarnation process from PRC

"Tibet in Focus as Global Lawmakers Convene in Tokyo.exe":



Tibet in Focus as Global Lawmakers Convene in Tokyo

(2025-06-05)

The 9th World Parliamentarians' Convention on Tibet ended with a declaration condemning Chinese repression and urging global action to protect Tibetan identity.

Lawmakers and experts from 29 countries gathered in Tokyo from June 2 to 4 for the 9th World Parliamentarians' Convention on Tibet (WPCT). The event concluded with the adoption of the "Tokyo Declaration." A forceful rebuke of China's policies in Tibet, it calls for international legislative action to safeguard the region's culture, environment, and religious freedom.

This was the first time Japan hosted the convention, reaffirming its growing voice in regional human rights diplomacy. The Central Tibetan Administration (CTA) and the Japan Parliamentary Support Group for Tibet, the world's largest such group, jointly organized the convention.

Coinciding with the upcoming 90th birthday of His Holiness the 14th Dalai Lama in July, the timing and venue carried symbolic weight.

A Stand Against Assimilation

At the heart of the Tokyo Declaration lies a stern condemnation of the Chinese Communist Party's ongoing efforts to forcibly assimilate Tibetans into Han Chinese culture. Lawmakers denounced the widespread use of colonial-style boarding schools, where over a million Tibetan children are reportedly separated from their families.

These schools impose Mandarin-language curricula, erasing Tibetan cultural and religious identity.

Fig. 4: Screenshot of benign DOCX packaged into weaponized archive together with EXE's sharing the same filename (Source: Tibet.net)

Tibet in Focus as Global Lawmakers Convene in Tokyo

(2025-06-05)

The 9th World Parliamentarians' Convention on Tibet ended with a declaration condemning Chinese repression and urging global action to protect Tibetan identity.

Lawmakers and experts from 29 countries gathered in Tokyo from June 2 to 4 for the 9th World Parliamentarians' Convention on Tibet (WPCT). The event concluded with the adoption of the "Tokyo Declaration." A forceful rebuke of China's policies in Tibet, it calls for international legislative action to safeguard the region's culture, environment, and religious freedom.

This was the first time Japan hosted the convention, reaffirming its growing voice in regional human rights diplomacy. The Central Tibetan Administration (CTA) and the Japan Parliamentary Support Group for Tibet, the world's largest such group, jointly organized the convention.

Coinciding with the upcoming 90th birthday of His Holiness the 14th Dalai Lama in July, the timing and venue carried symbolic weight.

A Stand Against Assimilation

At the heart of the Tokyo Declaration lies a stern condemnation of the Chinese Communist Party's ongoing efforts to forcibly assimilate Tibetans into Han Chinese culture. Lawmakers denounced the widespread use of colonial-style boarding schools, where over a million Tibetan children are reportedly separated from their families.

These schools impose Mandarin-language curricula, erasing Tibetan cultural and religious identity.

Photos from the convention used as lure: "9th WPCT Region-Wise Action Plans on Tibet(DSC01650.jpg).exe"

Fig. 5: JPG image packaged into weaponized archive (Source: Tibet.net)

Fig. 6: Images from the convention packaged into weaponized archive together with malicious EXE and DLL (Source: Tibet.net)

Further activity targeting the Tibetan community and the U.S.

In another campaign, X-Force uncovered additional malicious Tibet-themed files. These files have names with topics that are of interest to the Tibetan community, such as bilingual education in Tibet or the title of a recently published book by the Dalai Lama. Choosing such topics was probably engineered to entice the recipients to be receptive and click the file. It is notable that the Tibetan-related samples were submitted from India, where the Tibetan government-in-exile currently operates, and this suggests that recipients of the files may have submitted them to VirusTotal. In a parallel campaign, X-Force discovered a file likely targeting the U.S. Navy, potentially discussing ongoing working group meetings between the U.S. Navy and other parties.

Lure name	**Submitter country**	**Claimloader DLL SHA256**	**Date**
DRC Mining, Strategic Minerals Development Policy/April 17/DRC Mining, Strategic Minerals Development Policy.exe	United States	c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444	17 April 2025
སྐད་གཉིས་སྦྱར་སློབ་གསོའི་སྒྱུར་བཅོས་སྙན་ཞུ/སྐད་གཉིས་སྦྱར་སློབ་གསོའི་སྒྱུར་བཅོས་སྙན་ཞུ.exe (translated Tibetan: Bilingual Education Reform Report/Bilingual Education Reform Report.exe)	India	93f1fd31e197a58b03c6f5f774c1384ffd03516ab1172d9b26ef5a4a32831637	26 May 2025

Voice for the Voiceless photos/Voice for the Voiceless photos.exe	India	3e7384c5e7c5764258947721c7729f221fb47ef53d447a7af5db5426f1e7c13d	28 May 2025
(USPACFLT) Working_Group_ Meeting/DF for After Activity Report on the conduct of 4th PN-United States Pacific Fleet (USPACFLT) Working Group Meeting (WGM).exe	United States	8cd4324e1e764aafba4ea0394a82943cefd7deeee28a6cbd19f2ba69de6a5766	9 June 2025

སྐད་གཉིས་སློབ་གསོ་བསྒྱུར་བཅོས་སྙན་ཞུ/སྐད་གཉིས་སློབ་གསོ་བསྒྱུར་བཅོས་སྙན་ཞུ.exe" (translated Tibetan: Bilingual Education Reform Report/Bilingual Education Reform Report.exe): The topic is of high importance to the Tibetan community and cultural assimilation in Tibet has been noted by Human Rights Watch in its report.

"Voice for the Voiceless photos/Voice for the Voiceless photos.exe": This is a reference to a book published by the Tibetan leader-in-exile, the Dalai Lama, in March 2025. He writes about his dialogue with Chinese leaders regarding the independence of Tibet.

"DRC Mining, Strategic Minerals Development Policy/April 17/DRC Mining, Strategic Minerals Development Policy.exe": This file may be a reference to the Democratic Republic of Congo (DRC) mining deal with the U.S. and efforts to gain its support for such a deal after observing Ukraine reaching a similar deal with the U.S. As of June 2025, the DRC is about to finalize the deal with the U.S. in return for military and diplomatic assistance against M23 rebels who are being supported by neighboring Rwanda.

"(USPACFLT) Working_Group_Meeting/DF for After Activity Report on the conduct of 4th PN-United States Pacific Fleet (USPACFLT) Working Group Meeting (WGM).exe": This may be a reference to the U.S. Navy's Pacific Fleet and its outreach activities to Pacific Rim countries. The fleet provides naval forces to the U.S. Indo-Pacific Command and may be called upon in the event of a conflict in Taiwan.

Technical details: Claimloader updates

Claimloader is a family of loaders that have evolved significantly over the past years. They contain an encrypted shellcode payload, which is decrypted and injected at runtime. Our previous blog provides more technical details on previous variants used by Hive0154.

On the first execution, Claimloader begins by creating a new mutex object to ensure only a single instance of Claimloader is running. It then moves itself and its processes' EXE used for DLL sideloading into a new directory under a new name, such as:

C:\ProgramData\AdobeLicensingPlugin\WF_Adobe_licensing_helper.exe
C:\ProgramData\AdobeLicensingPlugin\libjyy.dll

Next, Claimloader uses the API *SHSetValueA()* to establish persistence for the EXE via a registry key below:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

This will cause the EXE to be executed every time the current user logs onto the machine. The process is executed with a predefined argument, such as "Licensing", which is used to invoke the main functionality of Claimloader.

On the second Claimloader execution with the specified argument, the latest Claimloader variant begins to decrypt an embedded payload via the TripleDES algorithm. This algorithm has only been observed in Claimloader variants starting late April 2025. The updated variants also use XOR-encrypted API names and native APIs *LdrLoadDll()* and *LdrGetProcedureAddress()* to resolve imports dynamically.

After sleeping for five seconds, Claimloader allocates a new executable buffer in memory and copies the shellcode payload into it. The malware sleeps for another 10 seconds and then calls the API's *GetDC()* and *EnumFontsW(),* which it uses to execute the payload in memory by passing its entry point as a callback function.

Pubload backdoor

The Pubload shellcode payload has not undergone any updates since our last reporting. It contains a simple self-decrypting routine before executing its main functionality. Pubload is a simple backdoor capable of downloading encrypted shellcode payloads, which are injected into memory. One of the first payloads is the Pubshell module, which implements a reverse shell to facilitate immediate access to the infected machine.

Conclusion

Hive0154 remains a highly capable threat actor with multiple active subclusters and frequent development cycles. X-Force assesses with high confidence that China-aligned groups like Hive0154 will continue to refine their large malware arsenal and target public and private organizations worldwide. Entities at risk of Hive0154 activity should remain at a heightened state of defensive security and remain vigilant with regard to the techniques mentioned in this report.

Recommendations

- Exercise caution with emails containing a Google Drive download link
- Exercise caution with downloaded archives, even if they do contain expected documents. Train staff to display and recognize unexpected file extensions.
- Monitor and hunt in networks for TLS 1.2 Application Data packets (header: 17 03 03) without a previous TLS handshake as a sign of a Pubload or Toneshell beacon
- Monitor and hunt for USB drives containing suspicious executable names, DLLs and hidden directories which could indicate a device infected with a USB worm
- Monitor and hunt for suspicious and unknown directories in C:\ProgramData* which contain a legitimate EXE vulnerable to DLL sideloading and a corresponding DLL
- Monitor and hunt for persistence techniques in the registry and scheduled tasks
- Monitor any unusual network, persistence or file modification activity coming from seemingly benign process executables that sideload a malicious DLL

Indicators of compromise

Indicator	Indicator Type	Context
2bd60685299c62abe500fe80e9f03a627a1567059ce213d7c0cc762fa32552d7	SHA256	Claimloader DLL
c80dfc678570bde7c19df21877a15cc7914d3ef7a3cef5f99fce26fcf696c444	SHA256	Claimloader DLL
93f1fd31e197a58b03c6f5f774c1384ffd03516ab1172d9b26ef5a4a32831637	SHA256	Claimloader DLL
3e7384c5e7c5764258947721c7729f221fb47ef53d447a7af5db5426f1e7c13d	SHA256	Claimloader DLL
8cd4324e1e764aafba4ea0394a82943cefd7deeee28a6cbd19f2ba69de6a5766	SHA256	Claimloader DLL
7979686bf73c2988ab5d57f9605dcef2231ca87580f6ecedc75b2cbe81669ba0	SHA256	Weaponized archive
ea991719885b2fe91502218ff3be12c9f990a24c7e007e4ffb5a5c5c52b3a0b5	SHA256	Weaponized archive
6e408aada775eaf19c524792344cabca0b406247154e2b03ed03a929e0feee5a	SHA256	Weaponized archive

57770ede7015734e2d881430423b cc76c160b90448f5e67334e56b9747 ff874c	SHA256	Weaponized archive
fb33f222b3d4d5edc9b743e6428 2de561ef51e42db150dd8086203c5 3b25ff79	SHA256	Weaponized archive
218.255.96[.]245:443	IPv4	Pubload C2 server

IBM X-Force Premier Threat Intelligence is now integrated with OpenCTI by Filigran, delivering actionable threat intelligence about this threat activity and more. Access insights on threat actors, malware, and industry risks. Install the X-Force OpenCTI Connector to enhance detection and response, strengthening your cybersecurity with IBM X-Force's expertise. Get a 30-Day X-Force Premier Threat Intelligence trial today!
