Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

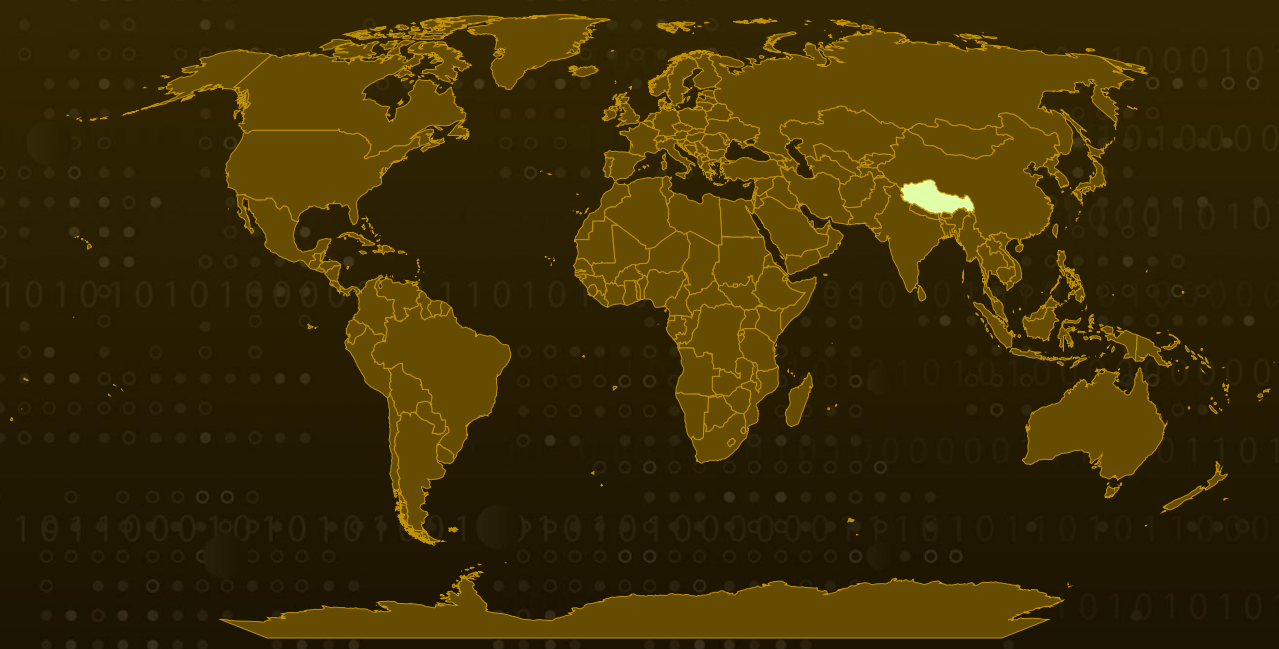
Operation GhostChat and PhantomPrayers Breach Tibetan Trust

Date of Publication	Admiralty Code	TA Number
July 29, 2025	A1	TA2025234

Summary

Attack Discovered: June 2025
Targeted Region: Tibet
Malware: Ghost RAT, PhantomNet (SManager)
Campaign: Operation GhostChat and Operation PhantomPrayers
Attack: In June 2025, cyber attackers linked to China ramped up espionage campaigns against the Tibetan community, especially around the Dalai Lama's 90th birthday. Disguising malware as chat apps and prayer tools, the attackers tricked users into downloading trojanized software from fake websites designed to look legitimate. These malicious tools secretly installed malware like Ghost RAT and PhantomNet, giving the attackers control over victims' devices. The campaigns dubbed Operation GhostChat and Operation PhantomPrayers used clever social engineering, fake GUIs, and tailored malware to gather sensitive information and maintain long-term surveillance, highlighting a calculated attempt to exploit trust and community sentiment for political spying.

Attack Regions



Attack Details

#1 In June 2025, a wave of sophisticated cyberattacks targeted the Tibetan community, timed strategically around the Dalai Lama's 90th birthday to exploit heightened online activity. Two distinct campaigns, Operation GhostChat and Operation PhantomPrayers were identified and attributed to China-linked APT groups.

#2 In Operation GhostChat, attackers hijacked a legitimate Tibetan community website that originally invited users to send birthday greetings to the Dalai Lama. Instead of reaching the original page, visitors were redirected to a spoofed domain that mimicked the look and feel of the legitimate site. The fake page encouraged users to download what appeared to be a secure, encrypted messaging app to chat with other community members. However, the download was a trap: it led to a trojanized version of the popular Element chat app bundled in a ZIP file named TBElement.zip.

#3 Once opened, this file contained both legitimate components and a maliciously modified ffmpeg.dll library. This DLL acted as the entry point for the malware, initiating a multi-stage infection chain. First, it loaded shellcode that stealthily injected itself into a system process. This was followed by a reflective loader designed to evade antivirus detection using NRV2D compression. Finally, the Ghost RAT backdoor was deployed capable of remote spying, file theft, and system control communicating silently with its command-and-control (C2) server via a binary TCP protocol.

#4 The campaign also embedded surveillance tactics directly into the malicious website. JavaScript code harvested users' IP addresses and browser details, while WebRTC functionality exposed real-time IP data, all silently transmitted to a script on the attacker's server.

#5 Simultaneously, a separate but related campaign, Operation PhantomPrayers, leveraged similar techniques but with new delivery mechanisms. Victims were lured with a seemingly spiritual application disguised as a "special prayer check-in" tool, hosted on malicious domain. The application, built using Python tools featured a polished interface displaying an interactive map of other supposed participants adding a layer of social credibility. Users were asked to input personal details, which were then sent back to the attackers.

#6 This application deployed a second-stage loader that decrypted and executed a variant of the PhantomNet backdoor. This malware was configured to communicate over TCP or HTTPS, using AES encryption for its C2 traffic. It also featured advanced capabilities such as plugin-based functionality and time-based execution though in this instance, timed execution was not activated. Together, these two campaigns showcase a targeted, calculated effort by state-sponsored threat actors to infiltrate and monitor the Tibetan community.

Recommendations

- **Be cautious of links on community websites:** Always double-check the web address (URL) before clicking any link, even if it's on a site you trust. Attackers can replace legitimate links with malicious ones that look similar.
- **Avoid downloading unfamiliar software**: Even if it looks community-related Don't install applications or tools like "chat" apps or "check-in" tools unless they come from official sources. Malware is often hidden in seemingly helpful programs.
- **Use VPNs and secure messaging platforms:** Communicate using well-known, vetted encrypted apps, and use a VPN to protect your online identity and location.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
TA0040 Impact	**T1041** Exfiltration Over C2 Channel	**T1106** Native API	**T1204** User Execution
T1204.002 Malicious File	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1574** Hijack Execution Flow
T1574.001 DLL	**T1055** Process Injection	**T1055.002** Portable Executable Injection	**T1036** Masquerading

T1027 Obfuscated Files or Information	**T1027.007** Dynamic API Resolution	**T1027.009** Embedded Payloads	**T1027.015** Compression
T1620 Reflective Code Loading	**T1070** Indicator Removal	**T1070.001** Clear Windows Event Logs	**T1056** Input Capture
T1056.001 Keylogging	**T1083** File and Directory Discovery	**T1057** Process Discovery	**T1012** Query Registry
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1082** System Information Discovery	**T1033** System Owner/User Discovery
T1123 Audio Capture	**T1115** Clipboard Data	**T1005** Data from Local System	**T1113** Screen Capture
T1125 Video Capture	**T1573** Encrypted Channel	**T1573.001** Symmetric Cryptography	**T1095** Non-Application Layer Protocol
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1529** System Shutdown/Reboot	**T1189** Drive-by Compromise
T1059 Command and Scripting Interpreter	**T1059.007** JavaScript		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	42d83a46250f788eef80ff090d9d6c87, 5b63a01a0b3f6e06dd67b42ad4f18266, 998dd032b0bb522036706468eca62441, a17092e3f8200996bdcaa4793981db1f, 1244b7d19c37baab18348fc2bdb30383, a139e01de40d4a65f4180f565de04135, 81896b186e0e66f762e1cb1c2e5b25fc, 5ad61fe6a92d59100dc6f928ef780adb, 32308236fa0e3795df75a31bc259cf62, 26240c8cfbb911009a29e0597aa82e6c, a74c5c49b6f1c27231160387371889d3

TYPE	VALUE
SHA1	ff9fddb016ec8062180c77297d478b26d65a7a40, 71f09721792d3a4f1ea61d1f3664e5a503c447b2, 25cb602e89b5d735776e2e855a93915714f77f01, ca6845e4ac8c0e45afc699557ad415339419bfe0, 365888661b41cbe827c630fd5eea05c5ddc2480d, e089daa04cceb8306bc42e34a5da178e89934f45, 10a440357e010c9b6105fa4cbb37b7311ad574ea, 11be5085f6ddc862cabae37c7dbd6400fb8b1498, 40ef100472209e55877b63bf817982e74933b3f8, a03527b2a2f924d3bc41636aa18187df72e9fe03, Fb32d8461ddb6ca2f03200d85c09f82fb6c5bde3
SHA256	0ad4835662b485f3a1d0702f945f1a3cf17e0a5d75579bea165c19afd1f8ea00, d896953447088e5dc9e4b7b5e9fb82bcb8eb7d4f6f0315b5874b6d4b0484bd69, 037d95510c4aa747332aa5a2e33c58828de4ad0af8a1e659a20393f2448e48d7, 98d30b44560a0dde11927b477b197daf75fb318c40bdeed4f9e27235954f9e71, 1e5c37df2ace720e79e396bbb4816d7f7e226d8bd3ffc3cf8846c4cf49ab1740, a0b5d6ea1f8be6dbdbf3c5bb469b111bd0228bc8928ed23f3ecc3dc4a2c1f480, 9ffb61f1360595fc707053620f3751cb76c83e67835a915ccd3cbff13cf97bed, f6b42e4d0e810ddbd0c1649abe74497dad7f0e9ada91e8e0e4375255925dd4d2, 45fd64a2e3114008f400bb2d9fa775001de652595ffe61c01521eb227a0ba320, 8809b874da9a23e5558cc386dddf02ea2b9ae64f84c9c26aca23a1c7d2661880, c9dac9ced16e43648e19a239a0be9a9836b80ca592b9b36b70d0b2bdd85b5157
Filenames	TBElement.zip, Element.exe, ffmpeg.dll, DalaiLamaCheckin.exe, VLC.exe, libvlc.dll, .tmp
Domains	thedalailama90[.]niccenter[.]net, tbelement[.]niccenter[.]net, beijingspring[.]niccenter[.]net, penmuseum[.]niccenter[.]net

TYPE	VALUE
URLs	tbelement[.]niccenter[.]net/Download/TBElement[.]zip, hxxp[:]//hhthedalailama90[.]niccenter[.]net/DalaiLamaCheckin[.]exe, hxxp[:]//104[.]234[.]15[.]90[:]59999/api
IPv4:Port	104[.]234[.]15[.]90[:]19999, 45[.]154[.]12[.]93[:]2233

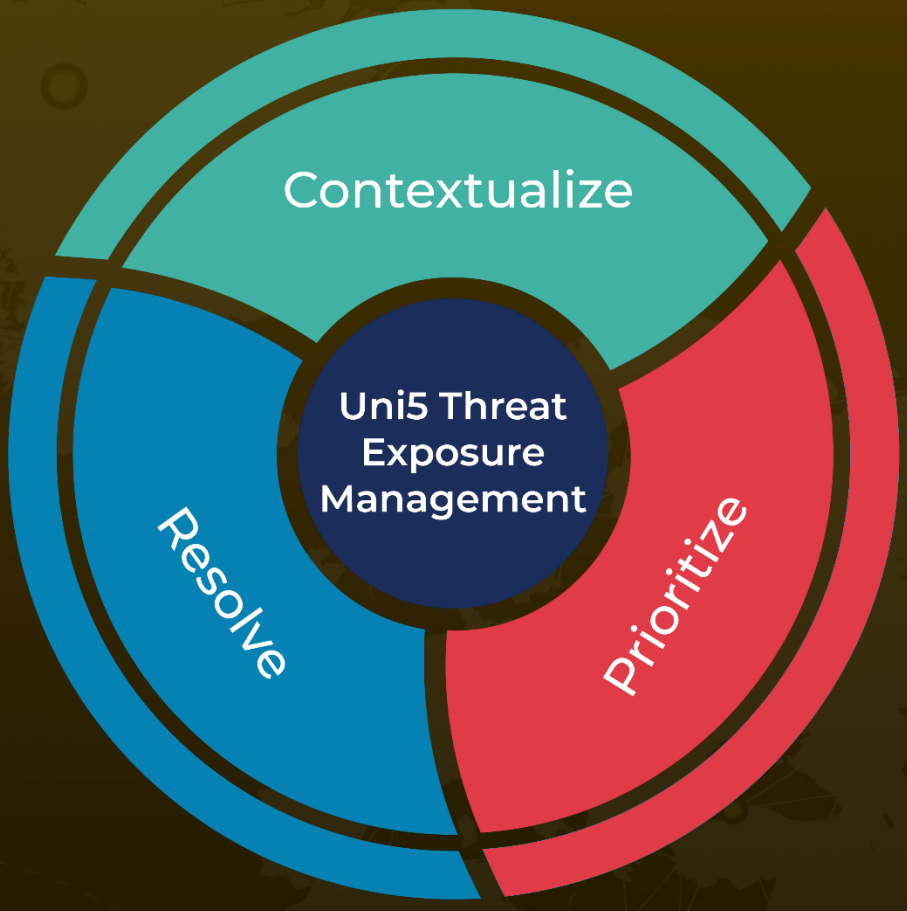
References

https://www.zscaler.com/blogs/security-research/illusory-wishes-china-nexus-apt-targets-tibetan-community

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 29, 2025 • 6:30 AM

More at www.hivepro.com