China-Nexus TAG-112 Compromises Tibetan Websites to Distribute Cobalt Strike

By Insikt Group®

Archived: 2026-04-05 13:17:46 UTC

Summary

In a recent cyber campaign, the Chinese state-sponsored threat group TAG-112 compromised two Tibetan websites, Tibet Post and Gyudmed Tantric University, to deliver the Cobalt Strike malware. Recorded Future's Insikt Group discovered that the attackers embedded malicious JavaScript in these sites, which spoofed a TLS certificate error to trick visitors into downloading a disguised security certificate. This malware, often used by threat actors for remote access and post-exploitation, highlights a continued cyber-espionage focus on Tibetan entities. TAG-112's infrastructure, concealed using Cloudflare, links this campaign to other China-sponsored operations, particularly TAG-102 (Evasive Panda).

Cyberattacks targeting ethnic and religious minority groups in China continue, with new developments pointing to a targeted campaign against Tibetan organizations. In a recent investigation, Recorded Future's Insikt Group discovered a Chinese state-sponsored threat actor group, designated TAG-112, responsible for compromising Tibetan community websites and delivering Cobalt Strike, a potent cyber-espionage tool.

Key Findings

In late May 2024, TAG-112 compromised at least two Tibetan community websites: Tibet Post (tibetpost[.]net) and Gyudmed Tantric University (gyudmedtantricuniversity[.]org). The attackers exploited vulnerabilities in the Joomla content management system (CMS) used by these sites to implant malicious JavaScript. This JavaScript prompted visitors to download a fake security certificate, which, when opened, deployed the Cobalt Strike payload.

TAG-112's infrastructure shows notable overlap with TAG-102 (Evasive Panda), a more sophisticated Chinese state-sponsored group known for targeting Tibetan entities. However, Insikt Group has identified TAG-112 as a separate entity due to differences in attack maturity and tactics, such as using Cobalt Strike rather than custom malware and foregoing JavaScript obfuscation.

Malicious JavaScript and Spoofed TLS Error

The attack begins with the malicious JavaScript embedded in the compromised websites. When a user visits one of these sites, the script detects the operating system and browser type, confirming compatibility with Windows. If

compatible, the script initiates a connection with TAG-112's command-and-control (C2) domain, update[.]maskrisks[.]com, which then returns an HTML page spoofing a legitimate TLS certificate error.

This spoofed error page is crafted to mimic Google Chrome's TLS certificate warning, deceiving users into clicking a link to "download a security certificate." Upon clicking, users unknowingly initiate the download of Cobalt Strike, a legitimate tool commonly used by security testers but often exploited by attackers for remote access and command execution.

Exploiting Website Vulnerabilities

TAG-112 likely gained access to the compromised Tibetan websites through vulnerabilities in Joomla, a popular CMS. Websites built on Joomla are frequently targeted by attackers if they are not adequately maintained and updated. Likely by exploiting these weaknesses, TAG-112 was able to upload the malicious JavaScript file, which remains active on these sites as of early October 2024.

Infrastructure and Obfuscation Tactics

TAG-112's infrastructure shows a level of sophistication in concealing its origins. The group used Cloudflare to shield its servers' IP addresses, complicating efforts to trace the infrastructure back to its origin. Insikt Group identified multiple IP addresses linked to TAG-112's C2 servers, some active as early as March 2024. The primary domain, maskrisks[.]com, was registered in March 2024 through Namecheap, with subdomains such as mail[.]maskrisks[.]com and checkupdate[.]maskrisks[.]com added for further operational flexibility.

TAG-112's Use of Cobalt Strike

Cobalt Strike is a commercial penetration testing tool that has become a favorite among threat actors due to its versatility and powerful capabilities for remote access, lateral movement, and command-and-control. Insikt Group identified six distinct Cobalt Strike Beacon samples linked to TAG-112, with their C2 communication directed to mail[.]maskrisks[.]com. This malware enables TAG-112 to monitor and control compromised systems, gathering intelligence and potentially leveraging these infected systems for further espionage activities.

Connections to TAG-102 (Evasive Panda)

TAG-112 shares several operational characteristics with TAG-102 (Evasive Panda), another Chinese APT known for targeting the Tibetan community. Both groups have used similar methods, including spoofed error pages to deliver malicious files. However, TAG-112's operations are less sophisticated than TAG-102, indicating that it may be a subgroup or less experienced branch. For instance, while TAG-102 has deployed customized malware and used obfuscation techniques, TAG-112 relies on the readily available Cobalt Strike tool without obfuscating its JavaScript.

Despite the lack of obfuscation, TAG-112's tactics and overlaps with TAG-102 highlight the Chinese government's ongoing interest in Tibetan and other ethnic and religious minority communities. Such campaigns are part of a broader strategy of surveillance and control, targeting groups perceived as threats to the stability and control of the Chinese Communist Party (CCP).

Mitigation Recommendations

TAG-112's campaign underscores the importance of proactive cybersecurity measures, particularly for organizations that may be high-value targets for state-sponsored actors. Recorded Future recommends the following steps:

1. **Intrusion Detection and Prevention**: Configure intrusion detection (IDS) and intrusion prevention systems (IPS) to alert on any indicators of compromise (IoCs) associated with TAG-112. Consider blocking connections to known TAG-112 infrastructure after a thorough review.
2. **User Training**: Educate users to exercise caution when handling files downloaded from untrusted sources. Advise users against opening files that download automatically without input, as these could be part of phishing or drive-by download attacks.
3. **Cobalt Strike Detection**: Enable real-time monitoring for malicious Cobalt Strike C2 servers using threat intelligence modules such as Recorded Future's Intelligence Cloud.
4. **Network Monitoring**: Regularly monitor network traffic for signs of compromise, particularly for connections to known threat infrastructure. Malicious Traffic Analysis (MTA) can help detect unusual activity, alerting security teams to potential C2 communications.

Outlook

TAG-112's operations against Tibetan organizations reflect a longstanding objective within Chinese cyber-espionage campaigns to monitor and control ethnic and religious minorities, especially those seen as potentially destabilizing. Other groups and regions with similar CCP-designated risk profiles are likely targets of similar state-sponsored attacks.

To read the entire analysis, click here to download the report as a PDF.

Appendix A — Indicators of Compromise

Appendix B — Mitre ATT&CK Techniques
