


Mustang Panda, Bronze President - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:46:57 UTC

[Home](#) > [List all groups](#) > Mustang Panda, Bronze President

APT group: Mustang Panda, Bronze President

Names	Mustang Panda (<i>CrowdStrike</i>) Bronze President (<i>SecureWorks</i>) TEMP.Hex (<i>FireEye</i>) HoneyMyte (<i>Kaspersky</i>) Red Lich (<i>PWC</i>) Earth Preta (<i>Trend Micro</i>) Camaro Dragon (<i>Check Point</i>) PKPLUG (<i>Palo Alto</i>) Stately Taurus (<i>Palo Alto</i>) Twill Typhoon (<i>Microsoft</i>) Hive0154 (<i>IBM</i>) G0129 (<i>MITRE</i>)
Country	 China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2012
Description	<p>(CrowdStrike) In April 2017, CrowdStrike Falcon Intelligence observed a previously unattributed actor group with a Chinese nexus targeting a U.S.-based think tank. Further analysis revealed a wider campaign with unique tactics, techniques, and procedures (TTPs). This adversary targets non-governmental organizations (NGOs) in general, but uses Mongolian language decoys and themes, suggesting this actor has a specific focus on gathering intelligence on Mongolia. These campaigns involve the use of shared malware like Poison Ivy or PlugX.</p> <p>Recently, Falcon Intelligence observed new activity from Mustang Panda, using a unique infection chain to target likely Mongolia-based victims. This newly observed activity uses a series of redirections and fileless, malicious implementations of legitimate tools to gain access to the targeted systems. Additionally, Mustang Panda actors reused previously-observed legitimate domains to host files.</p> <p>Also see CeranaKeeper and RedDelta.</p>

Mar 2021	<p>THOR: Previously Unseen PlugX Variant Deployed During Microsoft Exchange Server Attacks by PKPLUG Group</p> <p><https://unit42.paloaltonetworks.com/thor-plugx-variant/></p>
Mid 2021	<p>Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda</p> <p><https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/></p> <p><https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/></p>
Aug 2021	<p>Mustang Panda's Hodur: Old tricks, new Korplug variant</p> <p><https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/></p>
Feb 2022	<p>Mustang Panda or Temp.Hex, a China-based threat actor, targeted European entities with lures related to the Ukrainian invasion.</p> <p><https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/></p>
Feb 2022	<p>Mustang Panda deploys a new wave of malware targeting Europe</p> <p><https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html></p>
Feb 2022	<p>Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets</p> <p><https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets></p>
Mar 2022	<p>BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX</p> <p><https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx></p>
Mar 2022	<p>Earth Preta Spear-Phishing Governments Worldwide</p> <p><https://www.trendmicro.com/en_us/research/22/k/earth-pret-a-spear-phishing-governments-worldwide.html></p>
Jun 2022	<p>BRONZE PRESIDENT Targets Government Officials</p> <p><https://www.secureworks.com/blog/bronze-president-targets-government-officials></p>
2022	<p>Earth Preta's Cyberespionage Campaign Hits Over 200</p> <p><https://www.trendmicro.com/en_us/research/23/c/earth-pret-a-cyberespionage-campaign-hits-over-200.html></p>
Oct 2022	<p>Pack it Secretly: Earth Preta's Updated Stealthy Strategies</p> <p><https://www.trendmicro.com/en_us/research/23/c/earth-pret-a-updated-stealthy-strategies.html></p>
Dec 2022	<p>Operation "SmugX"</p> <p>SmugX: Unveiling a Chinese-Based APT Operation Targeting European</p>

	<p>Governmental Entities: Check Point Research Exposes a Shifting Trend https://blog.checkpoint.com/securing-user-and-access/smugx-unveiling-a-chinese-based-apt-operation-targeting-european-governmental-entities-check-point-research-exposes-a-shifting-trend/</p>
Jan 2023	<p>MQsTTang: Mustang Panda’s latest backdoor treads new ground with Qt and MQTT https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/</p>
Jan 2023	<p>Malware Spotlight: Camaro Dragon’s TinyNote Backdoor https://research.checkpoint.com/2023/malware-spotlight-camaro-dragons-tinynote-backdoor/</p>
Early 2023	<p>Beyond the Horizon: Traveling the World on Camaro Dragon’s USB Flash Drives https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/</p>
Apr 2023	<p>New Mustang Panda’s campaign against Australia https://lab52.io/blog/new-mustang-pandas-campaign-against-australia/</p>
May 2023	<p>Check Point Research reveals a malicious firmware implant for TP-Link routers, linked to Chinese APT group https://blog.checkpoint.com/security/check-point-research-reveals-a-malicious-firmware-implant-for-tp-link-routers-linked-to-chinese-apt-group/</p>
Jul 2023	<p>Operation “SMUGX” Earth Preta Campaign Uses DOPLUGS to Target Asia https://www.trendmicro.com/en_us/research/24/b/earth-pret-a-campaign-targets-asia-doplugs.html</p>
Aug 2023	<p>In August, ESET researchers identified a campaign by Mustang Panda targeting a governmental organization in Slovakia. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2023-q3-2023.pdf</p>
Aug 2023	<p>Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific https://unit42.paloaltonetworks.com/stately-aurus-targets-philippines-government-cyberespionage/</p>
Nov 2023	<p>Stately Taurus Targets Myanmar Amidst Concerns over Military Junta’s Handling of Rebel Attacks https://csirt-cti.net/2024/01/23/stately-aurus-targets-myanmar/</p>
Mar 2024	<p>ASEAN Entities in the Spotlight: Chinese APT Group Targeting https://unit42.paloaltonetworks.com/chinese-aps-target-asean-entities/</p>
Feb 2025	<p>Earth Preta Mixes Legitimate and Malicious Components to Sidestep Detection https://www.trendmicro.com/en_us/research/25/b/earth-pret-a-mixes-legitimate-</p>

	and-malicious-components-to-sidestep-detection.html >
Feb 2025	Stately Taurus Activity in Southeast Asia Links to Bookworm Malware < https://unit42.paloaltonetworks.com/stately-aurus-uses-bookworm-malware/ >
Apr 2025	Latest Mustang Panda Arsenal < https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-toneshell-and-starproxy-p1 > < https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-paklog-corklog-and-splatcloak-p2 >
Jun 2025	Hive0154 aka Mustang Panda shifts focus on Tibetan community to deploy Pubload backdoor < https://www.ibm.com/think/x-force/hive0154-mustang-panda-shifts-focus-tibetan-community-deploy-pubload-backdoor >
Information	< https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/ > < https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/ > < https://www.trendmicro.com/en_us/research/23/f/behind-the-scenes-unveiling-the-hidden-workings-of-earth-preta.html > < https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html >
MITRE ATT&CK	< https://attack.mitre.org/groups/G0129/ >
Playbook	< https://pan-unit42.github.io/playbook_viewer/?pb=statelytaurus >

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=3fb2534ff233-4247-a653-5fc809212951>