

Mustang Panda | Threat Actor Profile | CrowdStrike

By Adam Meyers

Archived: 2026-04-05 13:10:16 UTC

The June 2018 adversary spotlight is on **MUSTANG PANDA, a China-based adversary that has demonstrated an ability to rapidly assimilate new tools and tactics into its operations**, as evidenced by its use of exploit code for CVE-2017-0199 within days of its public disclosure. 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**. 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.

Mustang Panda's Methods

Mustang Panda's unique infection chain often takes the following steps:

1. **The infection chain used in this attack begins with a weaponized link to a Google Drive folder**, obfuscated using the goo.gl link shortening service.
2. **When contacted, the Google Drive link retrieves a zip file, which contains a .lnk file** obfuscated as a .pdf file using the double extension trick.
3. This file **requires the target to attempt to open the .lnk file, which redirects the user to a Windows Scripting Component (.wsc) file**, hosted on an adversary-controlled microblogging page. MUSTANG PANDA has previously used the observed microblogging site to host malicious PowerShell scripts and Microsoft Office documents in targeted attacks on Mongolia-focused NGOs.
4. **The .lnk file uses an embedded VBScript component to retrieve a decoy PDF file and a PowerShell script** from the adversary-controlled web page.
5. **The PowerShell script creates a Cobalt Strike stager payload**. This PowerShell script also retrieves an XOR-encoded Cobalt Strike beacon payload from an adversary-controlled domain.
6. **The Cobalt Strike Beacon implant beacons to the command-and-control (C2) IP address, which is used to remotely control the implant**.

There are no known community or industry names associated with this actor.

Other Known China-based Adversaries

- [Anchor Panda](#)

- [Deep Panda](#)
- [Goblin Panda](#)
- [Samurai Panda](#)

Curious about other nation-state adversaries? Visit our [threat actor hub](#) to learn about the new adversaries that the CrowdStrike team discovers.

Learn More

To learn more about how to incorporate intelligence on threat actors like MUSTANG PANDA into your security strategy, please visit the [Falcon threat intelligence product page](#). **Want the insights on the latest adversary tactics, techniques, and procedures (TTPs)?** Download the [CrowdStrike 2020 Global Threat Report](#).

Source: <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/>