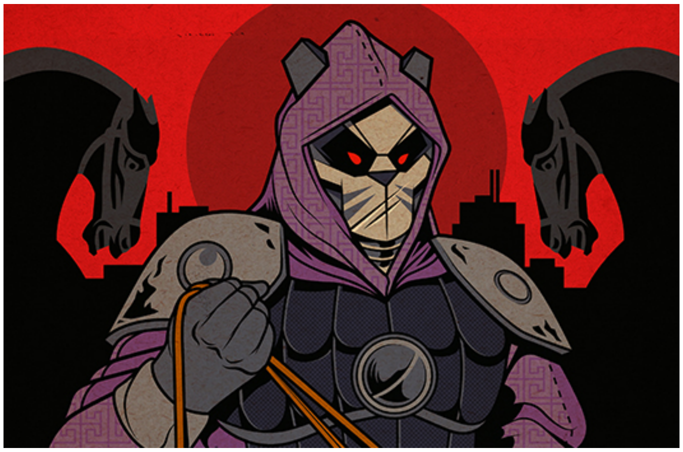
Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA

June 15, 2018 | AdamM | Counter Adversary Operations



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

Featured
Recent
Video
Category
Start Free Trial

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'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**

Featured
Recent
Video
Category
Start Free Trial

- Deep Panda
- Goblin 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.*

Tweet Share

Related Content

Featured
Recent
Video
Category
Start Free Trial

Sudan for Prominent DDoS

INDRIK SPIDER Members and Detail Ties to

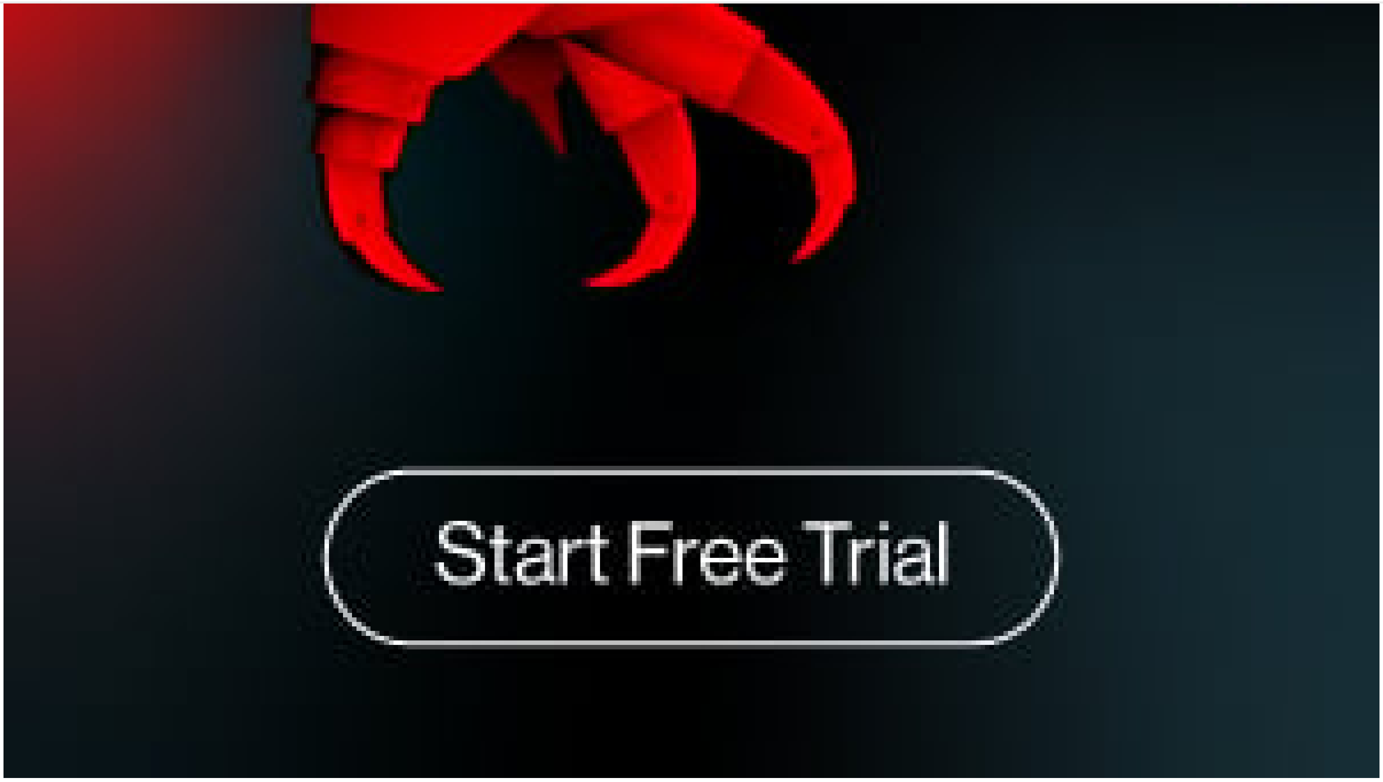
Cloud-Focused Threats

CATEGORIES

Cloud & Application Security	104
Counter Adversary Operations	184
Endpoint Security & XDR	306
Engineering & Tech	78
Executive Viewpoint	162
Exposure Management	84
From The Front Lines	190
Identity Protection	37
Next-Gen SIEM & Log Management	91
Public Sector	37
Small Business	8

Featured
Recent
Video
Category
Start Free Trial

Featured
Recent
Video
Category
Start Free Trial



Featured
Recent
Video
Category
Start Free Trial

October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

« Meet CrowdStrike's Adversary of the Month for April: STARDUST CHOLLIMA

Meet CrowdStrike's Adversary of the Month for July: WICKED SPIDER »