Goblin Panda Adversary | Threat Actor Profile

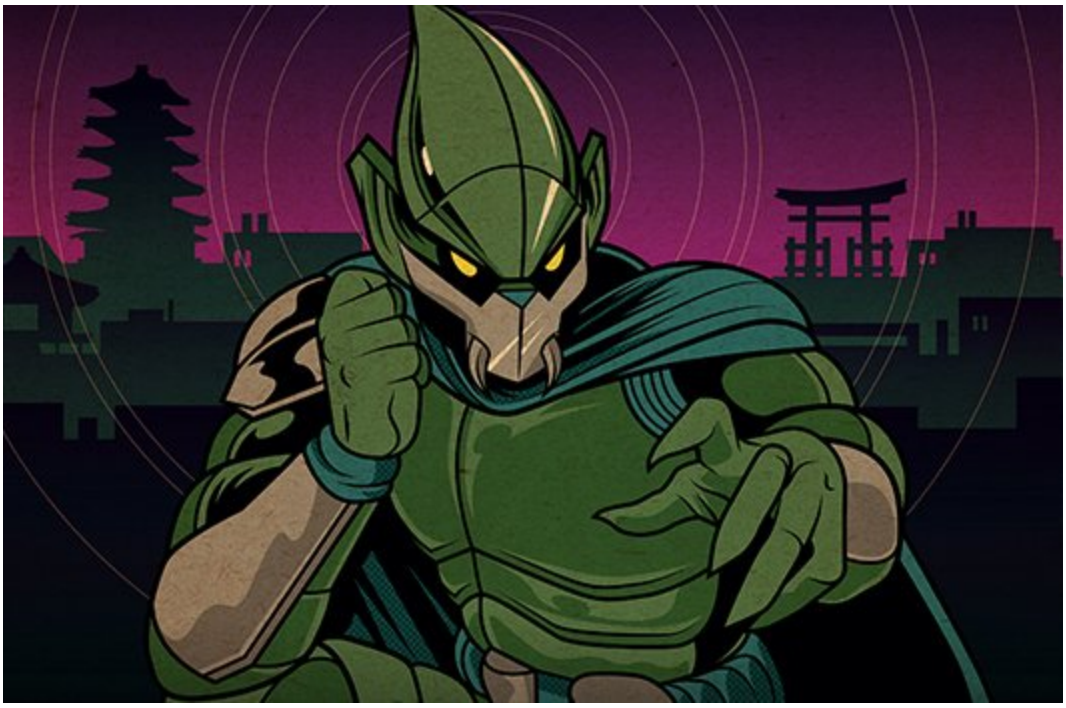
crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/

August 29, 2018

Meet CrowdStrike's Adversary of the Month for August: GOBLIN PANDA

August 29, 2018

Adam Meyers Research & Threat Intel



CrowdStrike® first observed GOBLIN PANDA activity in September 2013 when indicators of its activity were discovered on the network of a technology company operating in multiple sectors.

Malware variants primarily used by this actor include PlugX and HttpTunnel. This actor focuses a **significant amount of its targeting activity on entities in Southeast Asia, particularly Vietnam**. Heavy activity was observed in the late spring and early summer of 2014 when tensions between China and other Southeast Asian nations were high, due to conflict over territory in the South China Sea. **GOBLIN PANDA targets have been primarily observed in the defense, energy, and government sectors.**

Last month, CrowdStrike Intelligence observed renewed activity from GOBLIN PANDA targeting Vietnam. As part of this campaign, new exploit documents were identified with Vietnamese-language lures and themes, as well as Vietnam-themed, adversary-controlled

infrastructure.

Two exploit documents with Vietnamese-language file names were observed with file metadata unique to the GOBLIN PANDA adversary. Decoy content displayed in these incidents used Vietnamese-language Microsoft Office Word documents with training-related themes. These documents did not specifically reference Vietnamese government projects or departments, however they could still be directed towards Government of Vietnam personnel.

When opened, both documents use CVE-2012-0158 exploit code to drop malicious files associated with a previously identified side-loading malware implant, tracked as QCRat by CrowdStrike Falcon® Intelligence™.

Both exploit documents used a previously identified legitimate executable, and a side-loading implant Dynamic Link Library (DLL), as well as new implant configuration files stored as a *.tlb* file.

Analysis of command and control infrastructure suggests that GOBLIN PANDA is targeting entities in Laos, as well. CrowdStrike Intelligence has not directly observed Laotian targeting, and cannot confirm targets in Laos for this campaign, however, previous activity linked to GOBLIN PANDA has targeted this country.

Given major economic initiatives by China, such as the Belt and Road Initiative and continued dispute over the Paracel Islands, it is unlikely that GOBLIN PANDA will abandon efforts to collect intelligence from South East Asian neighbors and businesses operating in that region.

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

Other Known China-based Adversaries

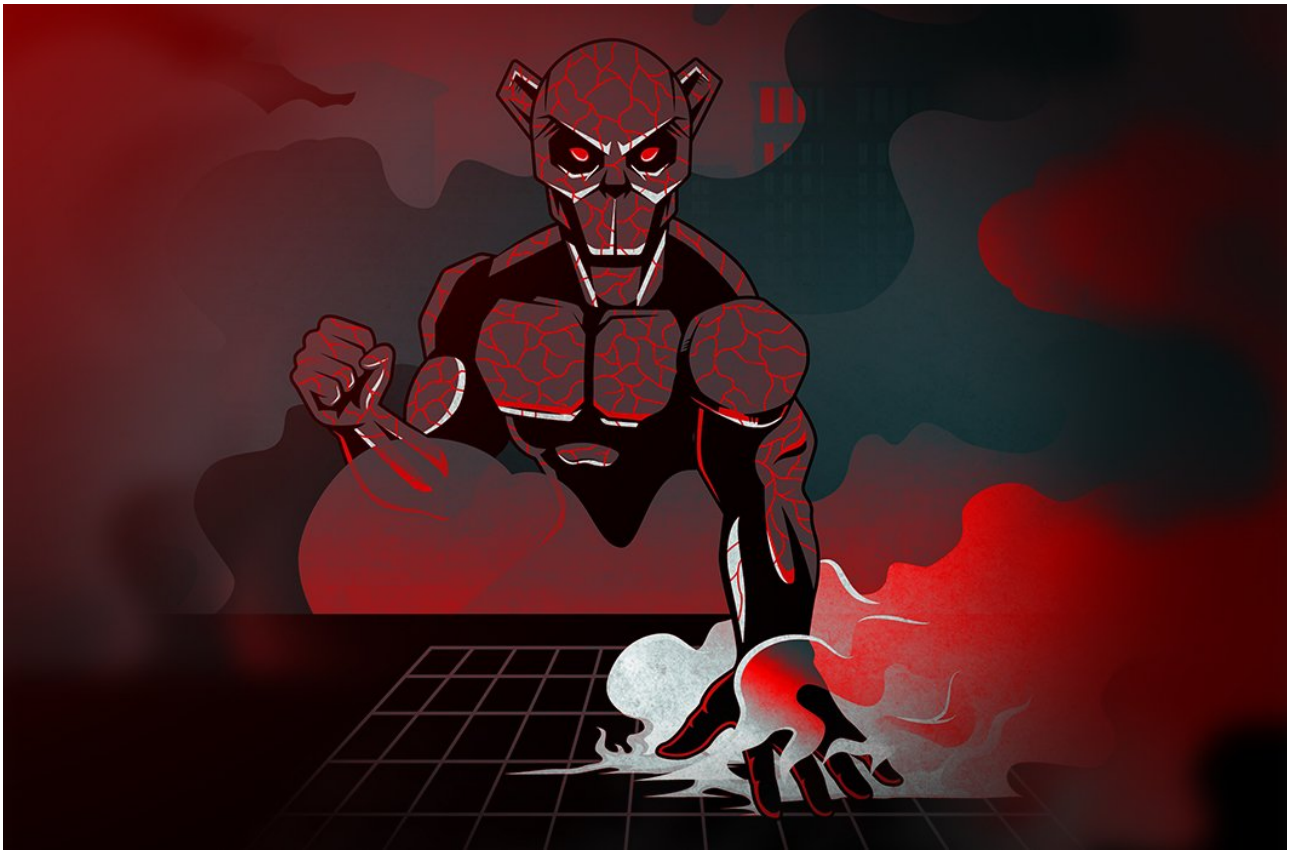
- Anchor Panda
- Deep Panda
- Mustang Panda
- Samurai Panda

Curious about other nation-state adversaries? *Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.*

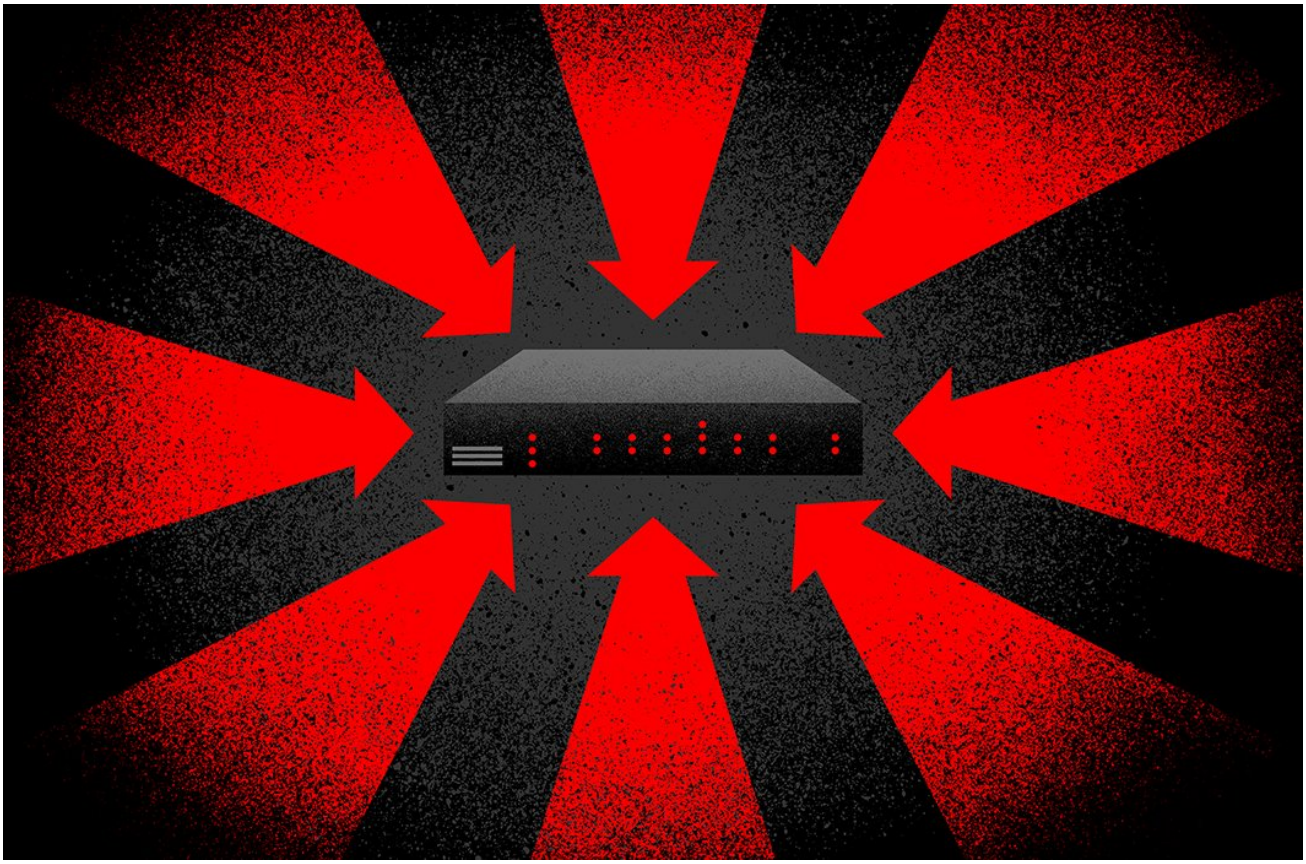
Learn More

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

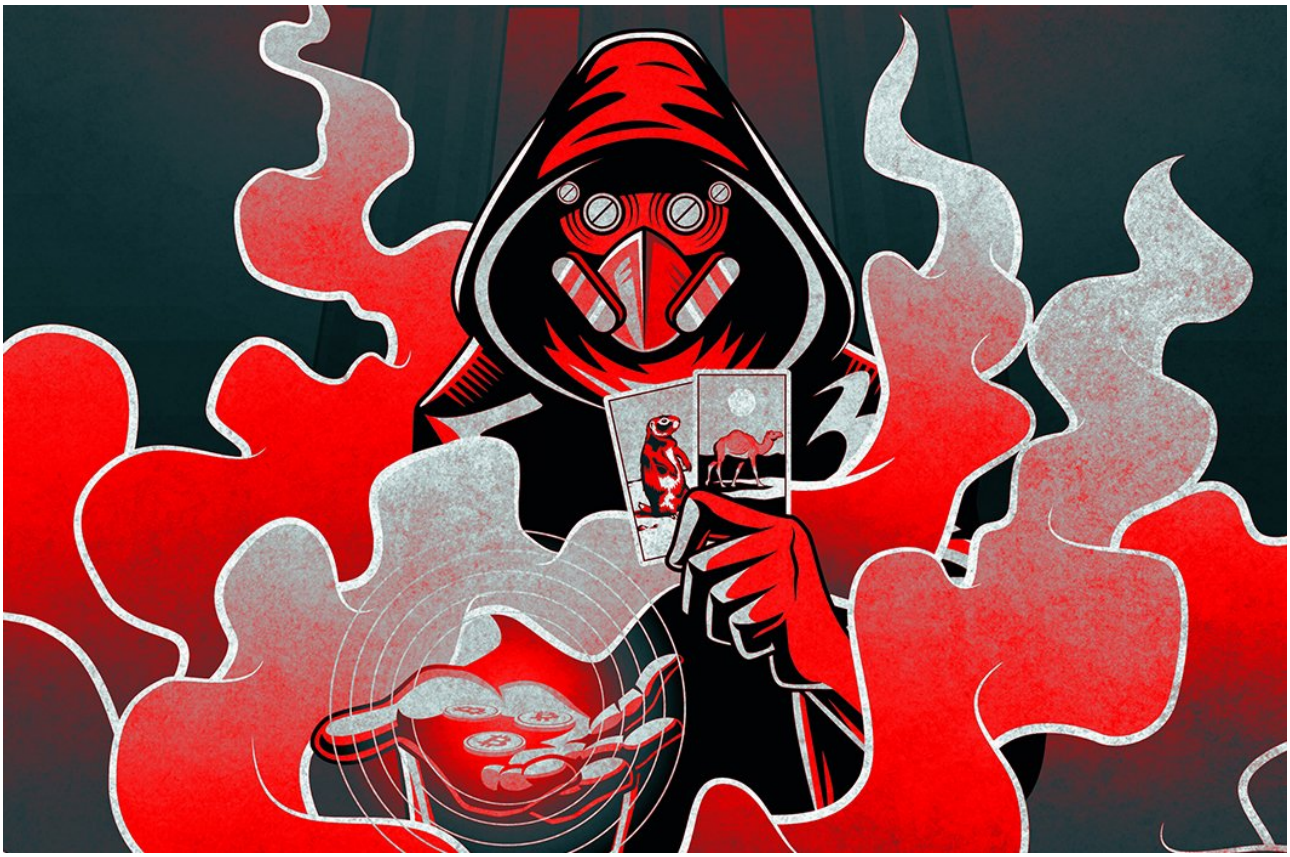
Related Content



Who is EMBER BEAR?



A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router



PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell