Wicked Spider Adversary | Threat Actor Profile

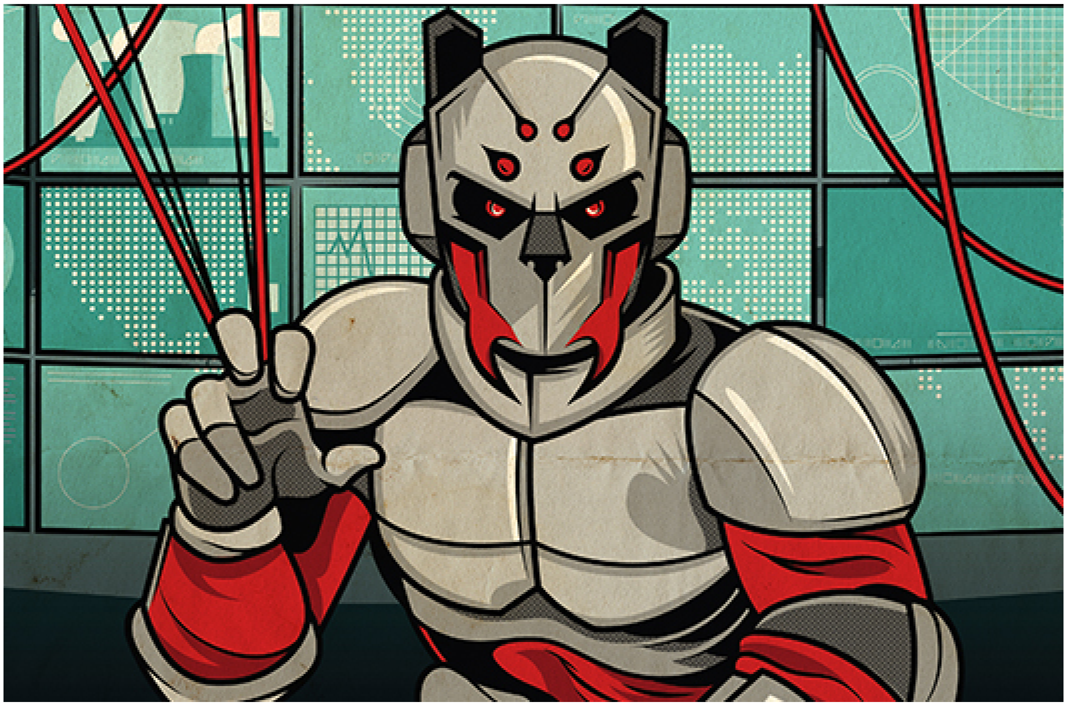
crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/

July 26, 2018

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

July 26, 2018

Adam Meyers Research & Threat Intel



WICKED SPIDER (PANDA) is a suspected China-based adversary that likely operates as an exploitation group for hire. The use of two cryptonyms for this group exemplifies how this adversary has demonstrated two different motivations for conducting malicious cyber operations.

WICKED PANDA refers to the targeted intrusion operations of the actor publicly known as “Winnti,” whereas WICKED SPIDER represents this group’s financially-motivated criminal activity. Originally, WICKED SPIDER was observed exploiting a number of gaming companies and stealing code-signing certificates for use in other operations associated with the malware known as Winnti. Now, Winnti is commonly associated with the interests of the government of the People’s Republic of China (PRC).

The flexibility of the cryptonym system used by CrowdStrike to track adversaries is highlighted by the case of WICKED PANDA/SPIDER. In this instance, one set of activity associated with criminal motivations can be easily separated from a second set of behaviors by the same actor when operating in the interest of a nation-state.

The WICKED PANDA adversary **makes use of a number of open-source and custom tools to infect and move laterally in victim networks**. Analysis of these tools and infrastructure linked to WICKED PANDA operations has traced these operations back to contractors who count multiple Chinese government agencies as clients, including the Ministry of Public Security (MPS). Observed targeting by the WICKED PANDA adversary has focused on high-value entities in the engineering, manufacturing and technology sectors, aligning with the PRC's strategic economic plans. WICKED PANDA has also targeted chemical and think tank sectors around the world.

Most recently, our cyber threat intelligence and proactive threat hunting teams identified ongoing activity by WICKED PANDA targeting organizations in the mining sector, where they attempted to perform lateral movement and credential harvesting before being contained by customer responders and the CrowdStrike Falcon® endpoint protection platform.

As for WICKED SPIDER, earlier this year the Falcon OverWatch team identified malicious activity on the network of a company operating in the technology sector. The incident involved the PlugX malware, as well as a scanning and exploitation tool for the ETERNALBLUE vulnerability with support for DOUBLEPULSAR.

Wicked Spider's Targets

WICKED SPIDER **has been observed targeting technology companies in Germany, Indonesia, the Russian Federation, South Korea, Sweden, Thailand, Turkey, the United States, and elsewhere**. Notably, WICKED SPIDER has often targeted gaming companies for their certificates, which can be used in future PRC-based operations to sign malware. Ongoing analysis is still evaluating how these certificates are used — whether WICKED SPIDER hands the certificates off to other adversaries for use in future campaigns or stockpiles them for its own use.

Other Known Criminal Adversaries

- Cobalt Spider
- Dungeon Spider
- Mummy Spider

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

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