Wicked Spider, APT 22 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:24:04 UTC

APT group: Wicked Spider, APT 22

Names	Wicked Spider *(CrowdStrike)* APT 22 *(Mandiant)* Bronze Export *(SecureWorks)* Bronze Olive *(SecureWorks)*
Country	China
Motivation	Financial crime
First seen	2018
Description	(CrowdStrike) Winnti Group, 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). 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.
Observed	Sectors: Technology. Countries: Germany, Indonesia, Russia, South Korea, Sweden, Thailand, Turkey, USA and elsewhere.
Tools used	DoublePulsar, EternalBlue, Gh0st RAT, PlugX.
Information	<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/>

Last change to this card: 13 March 2024

Download this actor card in PDF or JSON format
