Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:20:43 UTC

APT group: TheWizards

Names	TheWizards *(ESET)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(ESET) In 2022, we discovered the activity of a China-aligned APT group that we have named TheWizards. We analyzed the custom malware and tools developed and used by TheWizards: the IPv6 AitM tool we've named Spellbinder, which allows the attackers to redirect the update protocols of legitimate Chinese software to malicious servers, where the software is tricked into downloading and executing fake updates on victims' machines, and the malicious components that launch the backdoor that we have named WizardNet. ESET continues tracking TheWizards independently of Earth Minotaur. While both threat actors use DarkNights/DarkNimbus, according to ESET telemetry TheWizards has focused on different targets and uses infrastructure and additional tools (for example, Spellbinder and WizardNet) not observed to be used by Earth Minotaur.
Observed	Countries: Cambodia, China, Hong Kong, Philippines, UAE.
Tools used	Spellbinder, WizardNet.
Information	<https://www.welivesecurity.com/en/eset-research/thewizards-apt-group-slaac-spoofing-adversary-in-the-middle-attacks/>

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=81d87955-b54e-425a-8936-111928dc637e