Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:19:45 UTC

APT group: Worok

Names	Worok *(ESET)*
Country	China
Motivation	Information theft and espionage
First seen	2020
Description	(ESET) ESET researchers recently found targeted attacks that used undocumented tools against various high-profile companies and local governments mostly in Asia. These attacks were conducted by a previously unknown espionage group that we have named Worok and that has been active since at least 2020. Worok's toolset includes a C++ loader CLRLoad, a PowerShell backdoor PowHeartBeat, and a C# loader PNGLoad that uses steganography to extract hidden malicious payloads from PNG files. Activity times and toolset indicate possible ties with TA428, but we make this assessment with low confidence.
Observed	Sectors: Energy, Financial, Government, Telecommunications. Countries: Botswana, Cambodia, China, Indonesia, Iran, Iraq, Japan, Kazakhstan, Kyrgyzstan, Laos, Lebanon, Malaysia, Mongolia, Myanmar, Namibia, North Korea, Oman, Philippines, Saudi Arabia, Singapore, South Africa, South Korea, Syria, Tajikistan, Thailand, Turkey, Turkmenistan, UAE, Uzbekistan, Vietnam, Yemen.
Tools used	CLRLoad, EarthWorm, Mimikatz, nbtscan, PNGLoad, PowHeartBeat, reGeorg.
Information	<https://www.welivesecurity.com/2022/09/06/worok-big-picture/>

Last change to this card: 13 September 2022

Download this actor card in PDF or JSON format