

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:44:22 UTC

Tool: HELLOKITTY

Names	HELLOKITTY HelloKitty KittyCrypt
Category	Malware
Type	Ransomware , Big Game Hunting
Description	(FireEye) HELLOKITTY ransomware—used to target Polish video game developer CD Projekt Red—is reportedly built from DEATHRANSOM. HELLOKITTY is named after a mutex named ‘HELLOKITTYMutex,’ used when the malware executable is launched
Information	< https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html > < https://www.bleepingcomputer.com/news/security/HELLOKITTY-ransomware-behind-cd-projekt-red-cyberattack-data-theft/ > < https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/ > < https://www.ic3.gov/Media/News/2021/211029.pdf > < https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/ > < https://blog.barracuda.com/2024/04/24/hellokitty--hellogookie--hello--lockbit >
MITRE ATT&CK	< https://attack.mitre.org/software/S0617/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.hellokitty > < https://malpedia.caad.fkie.fraunhofer.de/details/elf.hellokitty >
Playbook	< https://pan-unit42.github.io/playbook_viewer/?pb=hellokitty-ransomware >

Last change to this tool card: 18 June 2024

Download this tool card in [JSON](#) format

All groups using tool HELLOKITTY

Changed	Name	Country	Observed
---------	------	---------	----------

APT groups

	UNC2447	[Unknown]	2020	
--	-------------------------	-----------	------	--

1 group listed (1 APT, 0 other, 0 unknown)



Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fed08e25-fd63-4def93d4-0fa8555fc680>