Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:35:20 UTC

Tool: THOR

Names	THOR
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Exfiltration
Description	(Palo Alto) While monitoring the Microsoft Exchange Server attacks in March 2021, Unit 42 researchers identified a PlugX variant delivered as a post-exploitation remote access tool (RAT) to one of the compromised servers. The variant observed by Unit 42 is unique in that it contains a change to its core source code: the replacement of its trademark word “PLUG” to “THOR.” The earliest THOR sample uncovered was from August 2019, and it is the earliest known instance of the rebranded code. New features were observed in this variant, including enhanced payload-delivery mechanisms and abuse of trusted binaries.
Information	<https://unit42.paloaltonetworks.com/thor-plugx-variant/>

Last change to this tool card: 09 August 2021

Download this tool card in JSON format

All groups using tool THOR

Changed	Name	Country	Observed	
APT groups				
	Mustang Panda, Bronze President		2012-Jun 2025	

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