ShadowRay, Campaign C0045 | MITRE ATT&CK®

Archived: 2026-04-05 15:03:11 UTC

ShadowRay was a campaign that began in late 2023 targeting the education, cryptocurrency, biopharma, and other sectors through a vulnerability (CVE-2023-48022) in the Ray AI framework named ShadowRay. According to security researchers ShadowRay was the first known instance of AI workloads being activley exploited in the wild through vulnerabilities in AI infrastructure. CVE-2023-48022, which allows access to compute resources and sensitive data for exposed instances, remains unpatched and has been disputed by the vendor as they maintain that Ray is not intended for use outside of a strictly controlled network environment.[1]

First Seen: September 2023 [1]

Last Seen: March 2024 [1]

Contributors: Shun Miyazaki, NEC Corporation; Sareena Karapoola, NEC Corporation India; Pooja Natarajan, NEC Corporation India

Created: 02 December 2024

Last Modified: 02 December 2024

Domain	ID		Name	Use
Enterprise	T1059	.006	Command and Scripting Interpreter: Python	During ShadowRay, threat actors used the Python `pty` module to open reverse shells. [1]
Enterprise	T1546	.004	Event Triggered Execution: Unix Shell Configuration Modification	During ShadowRay, threat actors executed commands on interactive and reverse shells. [1]
Enterprise	T1190		Exploit Public-Facing Application	During ShadowRay, threat actors exploited CVE-2023-48022 on publicly exposed Ray servers to steal computing power and to expose sensitive data.[1]
Enterprise	T1068		Exploitation for Privilege Escalation	During ShadowRay, threat actors downloaded a privilege escalation payload

Domain	ID		Name	Use
				to gain root access.[1]
Enterprise	T1105		Ingress Tool Transfer	During ShadowRay, threat actors downloaded and executed the XMRig miner on targeted hosts.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	During ShadowRay, threat actors used Base64-encrypted Python code to evade detection.[1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	During ShadowRay, threat actors used tools including the XMRig miner and Interactsh. [1]
Enterprise	T1003	.008	OS Credential Dumping: /etc/passwd and /etc/shadow	During ShadowRay, threat actors used `cat /etc/shadow` to steal password hashes.[1]
Enterprise	T1496	.001	Resource Hijacking: Compute Hijacking	During ShadowRay, threat actors leveraged graphics processing units (GPU) on compromised nodes for cryptocurrency mining.[1]
Enterprise	T1016		System Network Configuration Discovery	During ShadowRay, threat actors invoked DNS queries from targeted machines to identify their IP addresses.[1]