8220 Gang - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:16:04 UTC

Other threat group: 8220 Gang

Names	8220 Gang *(Talos)* 8220 Mining Group *(Talos)* Returned Libra *(Palo Alto)* Water Sigbin *(Trend Micro)*	
Country	China	
Motivation	Financial gain	
First seen	2017	
Description	(Trend Micro) 8220 Gang (also known as “8220 Mining Group,” derived from their use of port 8220 for command and control or C&C communications exchange) has been active since 2017 and continues to scan for vulnerable applications in cloud and container environments. Researchers have documented this group targeting Oracle WebLogic, Apache Log4j, Atlassian Confluence vulnerabilities, and misconfigured Docker containers to deploy cryptocurrency miners in both Linux and Microsoft Windows hosts. The group was documented to have used Tsunami malware, XMRIG cryptominer, masscan, and spirit, among other tools in their campaigns.	
Observed		
Tools used		
Operations performed	May 2021	8220 Gangs Recent use of Custom Miner and Botnet <https://www.lacework.com/blog/8220-gangs-recent-use-of-custom-miner-and-botnet/>
	Jul 2022	8220 Gang Massively Expands Cloud Botnet to 30,000 Infected Hosts <https://www.sentinelone.com/blog/from-the-front-lines-8220-gang-massively-expands-cloud-botnet-to-30000-infected-hosts/>
	Oct 2022	8220 Gang Cloud Botnet Targets Misconfigured Cloud Workloads <https://www.sentinelone.com/blog/8220-gang-cloud-botnet-targets-misconfigured-cloud-workloads/>

	Nov 2022	8220 Gang Continues to Evolve With Each New Campaign <https://sysdig.com/blog/8220-gang-continues-to-evolve/>
	May 2023	8220 Gang Evolves With New Strategies <https://www.trendmicro.com/en_us/research/23/e/8220-gang-evolution-new-strategies-adapted.html>
Information	<https://blog.talosintelligence.com/cryptomining-campaigns-2018/> <https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/the-8220-gang-targeting-cloud-providers/> <https://www.imperva.com/blog/imperva-detects-undocumented-8220-gang-activities/> <https://www.trendmicro.com/en_us/research/24/f/water-sigbin-xmrig.html>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=returnedlibra>	

Last change to this card: 26 August 2024

Download this actor card in PDF or JSON format
