The 8220 Gang: Targeting Cloud Providers and Vulnerable Applications

By Radware

Archived: 2026-04-09 02:18:34 UTC

January 19, 2023 11:46 AM

The 8220 Gang, also known as 8220 Mining Group, is a for-profit threat group from China that mainly targets cloud providers and poorly secured applications with a custom-built crypto miner and IRC bot.

Read the Complete Alert

Overview

As initially reported by Cisco Talos, the 8220 Gang has been active since 2017. While the threat group may be considered low-level, they have continued to advance and update their campaign over the years, proving how impactful a persistent low-level threat group can be. For example, in 2022, Lacework reported on how this highly active group continued evolving tactics and techniques to evade detection. Later in the year, Aqua reported on the group's exploitation of CVE-2022-26134, a vulnerability in the Atlassian Confluence software; SentinelOne also said that they had recently observed the 8220 Gang Botnet proliferate after successfully infecting over 30,000 hosts.

The threat group typically leverages publicly available exploits and brute-force attacks to spread its malware. But the group also leveraged Pastebin, Git repositories, and malicious Docker images to spread their malicious code. The 8220 Gang is known to use a variety of tactics and techniques to hide their activities and evade detection, including the use of a blocklist to avoid tripping over honeypots. Yet, the group is not perfect and was caught attempting to infect one of Radware's Redis honeypots at the beginning of this year.

Tactics, Techniques, and Procedures

By profiling and documenting the tactics, techniques, and procedures (TTPs) used by threat groups like the 8220 Gang, network defenders can better understand their behavior and how specific attacks are orchestrated, allowing organizations the ability to prepare, respond and mitigate current and future threats posed by the group.

In cybersecurity, tactics refer to the high-level description of the behavior the threat actors are trying to accomplish. For example, initial access is a tactic a threat actor leverages to gain a foothold in your network. Techniques are detailed descriptions of the behavior or actions that lead up to the tactic. For example, a technique to gain initial access includes exploiting public-facing applications. Procedures are technical details or directions about how a threat actor will leverage the technique to accomplish an objective. For example, procedures for exploiting a public-facing application can include information on a weakness in a targeted application.

INITIAL ACCESS

The source IP address in this attack originated from a compromised Apache server hosted on a major cloud provider. The IP address originally sent several requests to our Redis honeypot via '/api/login' and port 8443. Following this event, a few days later, the same IP address began sending a series of scripted commands to our Redis honeypot via port tcp/6379, the default port used by Redis. These commands were cron jobs intended to download, install and execute a shell script named 'xms?redis', a python script named d.py, a crypto miner called PwnRig, and the Tsunami IRC bot on the system where Redis is running.

Figure 1: Redis commands executed through initial access shell script

REDIS

Redis is an open-source (BSD licensed), in-memory data structure store used as a database, cache, and message broker. It is not the first time Redis has been subject to exploit activities by malicious gangs. In March of 2022, after a proof-of-concept exploit was released for CVE-2022-0543, Juniper Threat Labs reported that the Muhstik malware gang was actively targeting and exploiting the Lua sandbox escape vulnerability. In December, Aqua discovered a previously undocumented Golang based backdoor they dubbed Redigo and targeted their Redis honeypots vulnerable to CVE-2022-0543. The malware aimed to take control of systems to likely build a botnet network. The dropped malware mimicked the Redis protocol to communicate with its C2 infrastructure. The objective of the botnet and the attackers remains unknown.

According to the 2022 Radware Threat Report, Redis was the fourth most scanned and exploited TCP port in Radwares Global Deception Network in 2022, up from 10th position in 2021. Redis has gained a lot of popularity with the criminal community in 2022 and is one of the services that should be monitored, and not be exposed to the internet if not required

---

Source: https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/the-8220-gang-targeting-cloud-providers/