8220 Gang Cloud Botnet Targets Misconfigured Cloud Workloads

By Tom Hegel

Published: 2022-10-13 · Archived: 2026-04-05 19:41:53 UTC

In July of 2022 we reported on 8220 Gang, one of the many low-skill crimeware gangs we observe infecting cloud hosts through known vulnerabilities and remote access brute forcing infection vectors. We noted that 8220 Gang had expanded its cloud service botnet to an estimated 30,000 hosts globally.

In recent weeks, the group has rotated its attack infrastructure and continued to absorb compromised hosts into its botnet and to distribute cryptocurrency mining malware.

Misconfiguration Key to Infection Attempts

Exploit attempts from 8220 Gang continue at a pace consistent with our previous reporting. The majority of active victims are still operating outdated or misconfigured versions of Docker, Apache, WebLogic, and various Log4J vulnerable services.

8220 Gang identifies targets via scanning for misconfigured or vulnerable hosts on the public internet. Victims are typically using cloud infrastructure such as AWS, Azure and similar with misconfigured instances that allow remote attackers to gain access. Publicly-accessible hosts running Docker, Confluence, Apache WebLogic, and Redis can easily be discovered and attacked with little technical know-how. 8220 Gang is known to make use of SSH brute force attacks post-infection for the purposes of lateral movement inside a compromised network.

The top victims recently communicating as miner bots are exposed Ubiquiti Unifi Cloud Keys running outdated Network Controller software or Prometheus container monitoring systems. The vulnerabilities exploited are

usually far from fresh – such as with CVE-2019-2725 – the Oracle Weblogic vulnerability being exploited to download the installer script, e.g., 871f38fd4299b4d94731745d8b33ae303dcb9eaa. The objective of the infection attempts continues to be growing the botnet and expanding cryptocurrency hosts mining when possible.

8220 Gang Leverages PureCrypter

We have observed 8220 Gang using the PureCrypter Malware-as-a-service. PureCrypter is a loader service available for a low cost since 2021 and has been observed distributing a large variety of commodity malware. Windows systems targeted by 8220 Gang have been served by the PureCrypter downloader through the group's traditional C2 infrastructure, most commonly `89.34.27[.]167`. The downloader then beacons back following the injectors image extension URLs. The use of Discord URLs can also be observed for the download of illicit minors.

One clear example is the miner `ee6787636ea66f0ecea9fa2a88f800da806c3ea6` being delivered post-compromise. This loader beacons to Discord:

```
https://cdn.discordapp[.]com/attachments/994652587494232125/1004395450058678432/miner_Nyrpcmbw[.]png
```

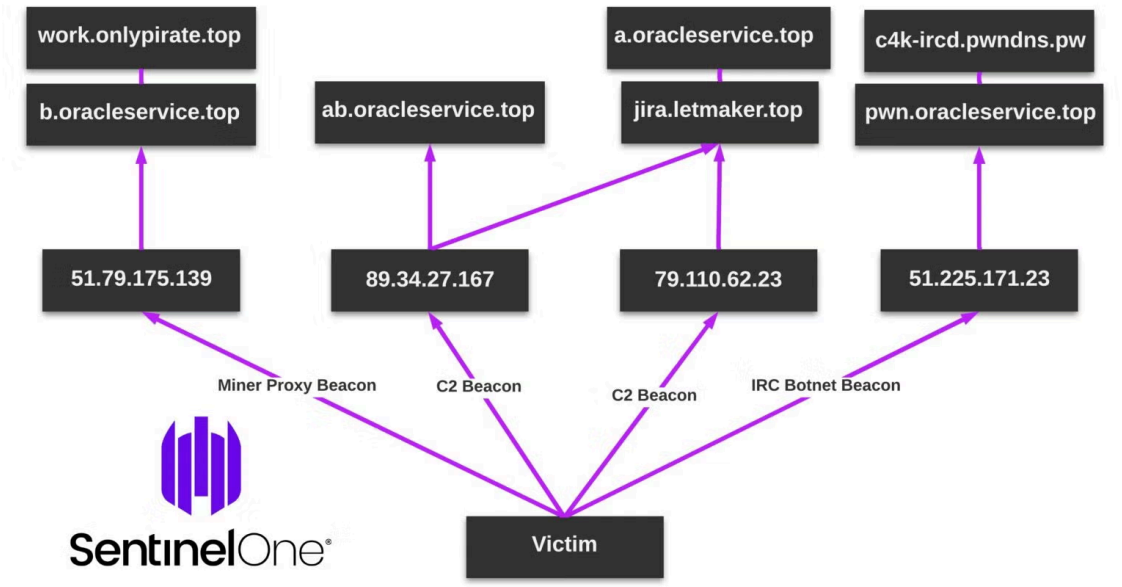
and downloads `833cbeb0e748860f41b4f0192502b817a09eff6a`, ultimately beginning cryptomining on the victim host.

It is unsurprising to discover 8220 Gang experimenting with new loaders and miners alongside their traditional exploitation attempts against publicly exposed services. As the threat landscape evolves, we can expect threat actors to seek new methods to thwart defenses, hide their campaigns, and generally attempt to increase attack success. This is simply a new iteration of 8220 Gang attempting to do so.

Shifting Infrastructure

Since July, 8220 Gang shifted to using `89.34.27[.]167`, and then in early September 2022 rotated its infrastructure to `79.110.62[.]23`, primarily relying on two previously reported domains `letmaker[.]top` and `oracleservice[.]top`.

8220 Gang also makes use of a miner proxy at 51.79.175[.]139. Hosts infected with illicit miners will communicate with the proxy as it acts as a pool to combine resources and avoid analysis of their cumulative mining metrics.



Visual Context of 8220 Gang Infrastructure Roles

Thriving Abuse of Amateur Tooling

As we've reported in the past, the scripts, miners, and infrastructure surrounding the campaigns of 8220 Gang stem from the general reuse of known tools. "Script Kiddies" may be a more industry appropriate name. Analysis of the tools and vulnerabilities at a high level reveals a much wider set of illicit activity.

For example, through GreyNoise data we can see how common CVE-2019-2725 crawlers are over the last 30 days. 8220 Gang and other attackers make use of scanning for and exploiting similar n-day vulnerabilities with success. One theory may be that these types of attackers seek out easy to compromise systems like this as they are unlikely to be remediated quickly since they are not even meeting common updating practices. These attackers are operating with success, regardless of the state of vulnerability management. One could consider such attacks to be bottom feeders of targeting perhaps.

GreyNoise Trend of CVE-2019-2725 Crawlers

The loader script is also incredibly common to observe through publicly accessible hosts and honeypots running common cloud services. The script has evolved greatly even in a single year, with many variants, and it is no longer useful tracking as a single name (e.g., Carbine Loader). For example, searching VirusTotal for any shell scripts containing the go-to uninstall commands for common cloud security tools, plus unique variable names, leads to hundreds of recent results. 8220 Gang is only one of many abusing the same scripts to keep their botnets alive.

Conclusion

8220 Gang continues their botnet proliferation efforts, rotating to new infrastructure. The group continues to make use of the same mining proxy server, and defenders should investigate any continual traffic to that destination. Additionally, with the experimentation with PureCrypter MaaS, the group has clearly attempted to evolve their attack efforts. As cloud infrastructure and common publicly accessible services remain vulnerable, we expect 8220 Gang to continue growing into the future.

Indicators of Compromise

Communications
89.34.27.167 (From July into September 2022)
79.110.62.23 (Primary since September 2022)
51.79.175.139 (Miner Proxy)
198.23.214.117 (Miner Proxy)
work.onlypirate[.]top
a.oracleservice[.]top
b.oracleservice[.]top
pwn.oracleservice[.]top

c4k-ircd.pwndns[.]pw
jira.letmaker[.]top
https://cdn.discordapp[.]com/attachments/994652587494232125/1004395450058678432/miner_Nyrpcmbw[.]png

File Hashes SHA1

165f188b915b270d17f0c8b5614e8b289d2a36e2
528477d0a2cf55f6e4899f99151a39883721b722
557d729f8a7ba712a48885304280b564194406d3
58af7af0dbf079bafd8fae1a7b3a2230b2bcba31
740a1cdee7b7f4350eec53c1ca3022562ea83903
7477812278038e8d3606c433f1c4389b897012e2
75ea4b0b76a0b61bd0f8f4a491e5db918bc1df1c
7b128cd6cf092409fc9c71ddd27c66dd98002b1a
871f38fd4299b4d94731745d8b33ae303dcb9eaa (CVE-2019-2725 example)
9bc4db76ae77ea98fdcaa9000829840d33faba97
be53175a3b3e11c1e3ca7b87abb6851479453272
c1630af40f38f01e94eec2981c5f4f11481ba700
c22f9ae02601a52c9dca91c3b4cb3d2221f54b50
c537cf320e90a39e7f5e9846e118502802752780
c86349460658a994e517fede6773e650f8f3ac9b
d5138d1708d5d77ea86920a217c2033a2e94ad7e
ee6787636ea66f0ecea9fa2a88f800da806c3ea6
