

Basic Security for regional ISP



SEMANA DE CAPACITAÇÃO

Parceria



Realização

ceptro.br nic.br

Introdução Palestrante



Formada em Engenharia da computação pela **FIAP**, Cisco **CMNA**, Cisco Fire Jumper **Elite #144**, LATAM Women in Cybersecurity – **WOMCY**, Consultora de projetos de Segurança da Informação, Instrutora do Treinamento Cisco **Fire Jumper** e pesquisadora na área de Infosec **Red Team**.



www.linkedin.com/in/josianedebarrossilva



Agenda

- ❖ 3 Pilares da Segurança da Informação
- ❖ Erros Comuns
- ❖ BGP Hijacking
- ❖ DNS Hijacking
- ❖ Cryptojacking
- ❖ Command & Control(C2)
- ❖ Distributed Denial of Service (DDoS)
- ❖ Demonstração de como prevenir e bloquear algumas dessas ameaças.



3 Pilares da Segurança da Informação



Confidencialidade

O que é?

Diz respeito á ameaça de **liberação não autorizada de informações**. Este requisito busca garantir o acesso somente **com autorização**, ou seja, para que uma informação seja considerada segura é essencial que haja uma forma de garantir esta seja disponibilizada somente mediante autorização.

Qual a importância?

Por que informações confidenciais **não** se entende apenas os da companhia, mas os de clientes , funcionários e fornecedores. A perda de dados pode gerar **prejuízos financeiros** e até gerar **processos contra a organização** por aqueles que foram afetados.

Como proteger ?

É recomendado a utilização de **criptografia de dados e e-mail, autenticação de múltiplos fatores**, gestão de acesso Mobile, classificação de dados e de Prevenção de Perda de Dados (**DLP/CASB**), garantindo que a pessoa destinada a acessar a informação seja de fato uma pessoa autorizada.



Integridade

O que é?

O aspecto da integridade diz respeito á ameaça da **modificação não autorizada** de informações. Este requisito busca garantir que a informação não sofra **alterações indevidas**. Espera-se que a informação seja disponibilizada de forma completa e sem qualquer tipo de modificação.

Qual a importância?

Instruções, orientações e mensagens trocadas entre departamentos ,organizações e profissionais **precisam chegar aos destinatários da mesma forma que foram enviados** para não comprometer a comunicação interna e externa. Isso pode gerar falhas na execução de atividades, ocasionar desgastes entre equipes e outros problemas graves.

Como proteger ?

É indicada a utilização de **anti-Malware**, dando rastreabilidade principalmente para ataques laterais e alterações de registros e hash, **solução de análise de comportamento** conseguem detectar e alarmar essas ocorrências, **Anti-Spam** evitando que e-mails **propagando informações não-integras** cheguem até os colaboradores, de governança de dados, de segurança no desenvolvimento de aplicações, entre outras.



Disponibilidade

O que é?

É o que garante que dados e sistemas **poderão ser acessados (disponíveis)** por indivíduos, entidades ou processos autorizados quando o acesso a informação for necessário.

Qual a importância?

Aqui, o foco é que as informações permaneçam **sempre acessíveis** para o uso pela empresa. Ou seja, elas precisam estar sempre disponíveis para consultas dos colaboradores, pois qualquer ausência pode dificultar ou mesmo inviabilizar decisões, contratos, vendas, além de prejudicar a relação com o cliente.

Como proteger ?

De forma proativa, evitando incidentes com indisponibilidade, é essencial fazer a devida gestão da infraestrutura de tecnologia, dimensionando corretamente a capacidade do ambiente tecnológico, com a correta definição de **largura de banda, redundância de link** e realizando a **manutenção preventiva**, como a aplicação de **patches** de segurança no sistema operacional dos computadores e servidores. Além disso, é indicado a implementação das ferramentas de **Firewall, proteção Anti DDoS, Proxy, Antivírus, Backup, entre outras**.



Erros Comuns



Cara Crachá



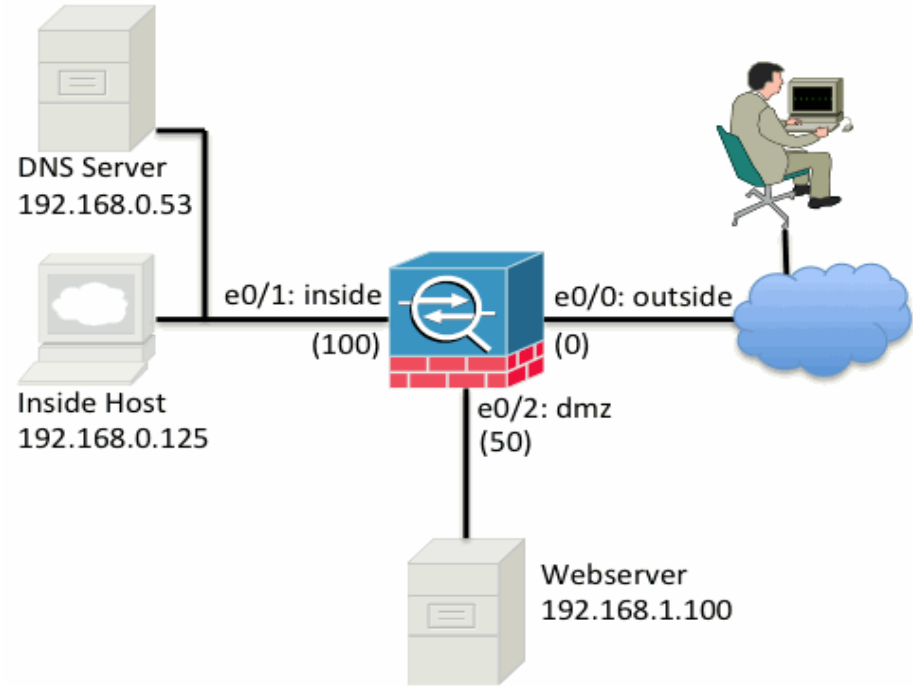
Confiar no Usuário (VPN)

Virtual Private Network, é uma rede de comunicações **privada** construída sobre uma rede de comunicações **pública**.



DMZ (Demilitarized Zone ou Zona Desmilitarizada)

Uma **DMZ** tem como função fornecer serviços aos **usuários externos**, de tal maneira que estes não necessitem **acessar a rede interna**, proporcionando um certo grau de **isolamento** da rede interna (**confiável**) em relação ao tráfego que vem da rede **externa** (**não confiável**).



Default Password

O **Shodan** é o **Google dos Hackers**, é possível encontrar ao redor do globo várias organizações que possuem dispositivos como: IoT, Router, que possuem default password, geolocalização, portas abertas, câmeras de vigilância, web cam entre outras coisas.



Shodan Developers Monitor View All... Show API Key Try out the new beta website! Help Center

SHODAN name:admin password:1234 Explore Downloads Reports Pricing Enterprise Access My Account Upgrade

Exploits Maps Like 22 Download Results Create Report

TOTAL RESULTS
10,864

TOP COUNTRIES

Taiwan	6,570
United States	1,461
Thailand	1,118
South Africa	224
Bangladesh	161

TOP SERVICES

HTTP (8000)	9,264
HTTP	492
Kerberos	218
NAS Web Interfaces	63
9090	59

TOP ORGANIZATIONS

Peicity Digital Cable Television.	6,533
TOT	1,016
Mountain West Technologies Corpor...	794
Natural Wireless, LLC	634
Hinet	197

TOP OPERATING SYSTEMS

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

RELATED TAGS: password default-password hackable

202.58.109.246
Horizon & Associates
Added on 2020-03-09 22:26:58 GMT
Bangladesh

```
HTTP/1.0 401 Unauthorized
Date: Tue, 10 Mar 2020 04:27:07 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm="Default Name:admin Password:1234"
Content-Type: text/html

<HTML><HEAD><TITLE>401 Unauthor...
```

401 Unauthorized
27.142.142.14
Link3 Technologies
Added on 2020-03-09 22:27:27 GMT
Bangladesh, Dhaka

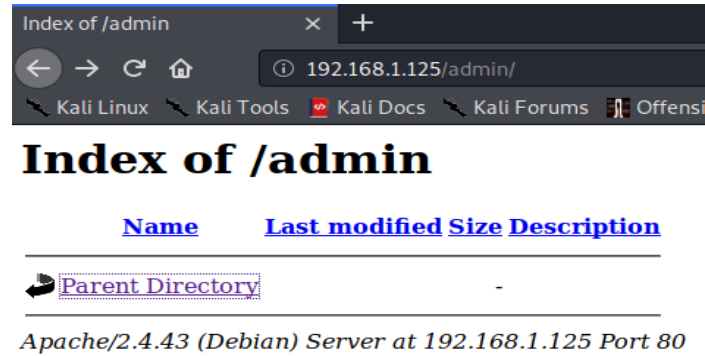
```
HTTP/1.0 401 Unauthorized
Date: Mon, 09 Mar 2020 22:27:36 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm="Default Name:admin Password:1234"
Content-Type: text/html
```

401 Unauthorized
220.130.243.174
220.130.243-174 HINET-IP@hinet.net
HINET
Added on 2020-03-09 22:25:47 GMT
Taiwan, Kaohsiung

```
HTTP/1.0 401 Unauthorized
Date: Mon, 09 Mar 2020 22:25:56 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
```



Servidor Web



Index of /admin

192.168.1.125/admin/

Index of /admin

Name	Last modified	Size	Description
Parent Directory	-	-	-

Apache/2.4.43 (Debian) Server at 192.168.1.125 Port 80

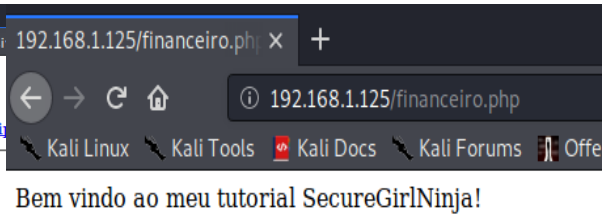


192.168.1.125

Index of /

Name	Last modified	Size	Description
admin/	2020-07-31 15:35	-	-
compras.php	2020-07-31 15:33	45	-
financeiro.php	2020-07-31 15:37	43	-
index.nginx-debian.html	2020-04-18 22:10	612	-
original.html	2020-04-18 22:14	10K	-

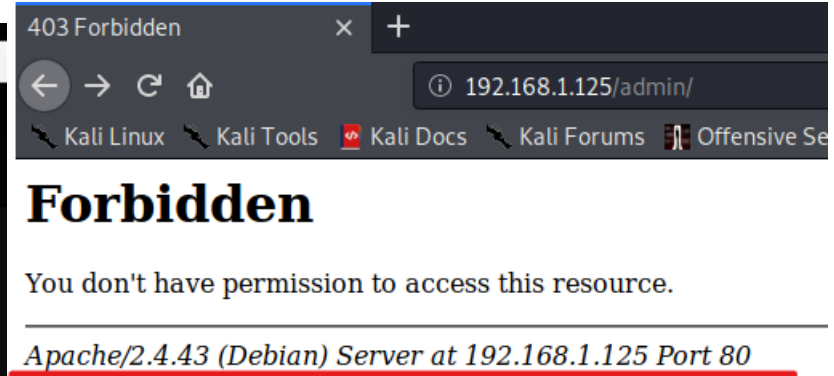
Apache/2.4.43 (Debian) Server at 192.168.1.125 Port 80



192.168.1.125/financeiro.php

Bem vindo ao meu tutorial SecureGirlNinja!

```
GNU nano 4.9.2 /etc/apache2/apache2.conf
</Directory>
<Directory /var/www/>
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
```



403 Forbidden

192.168.1.125/admin/

Forbidden

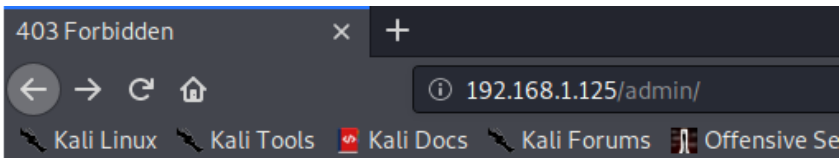
You don't have permission to access this resource.

Apache/2.4.43 (Debian) Server at 192.168.1.125 Port 80



Servidor Web

Versão do serviço que esta rodando



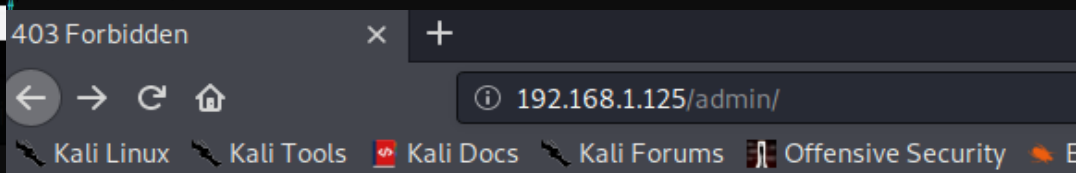
Forbidden

You don't have permission to access this resource.

Apache/2.4.43 (Debian) Server at 192.168.1.125 Port 80

```
GNU nano 4.9.2
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full
```

```
GNU nano 4.9.2 /etc/apache2/conf-enabled/security.conf
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full
```



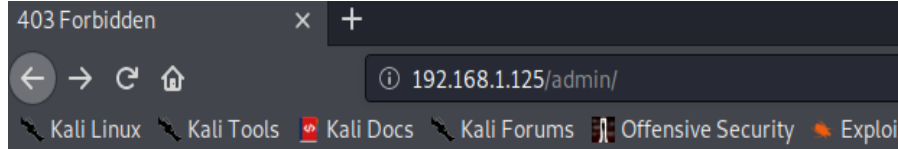
Forbidden

You don't have permission to access this resource.

Apache Server at 192.168.1.125 Port 80

Servidor Web

Ainda aparece como Servidor Apache

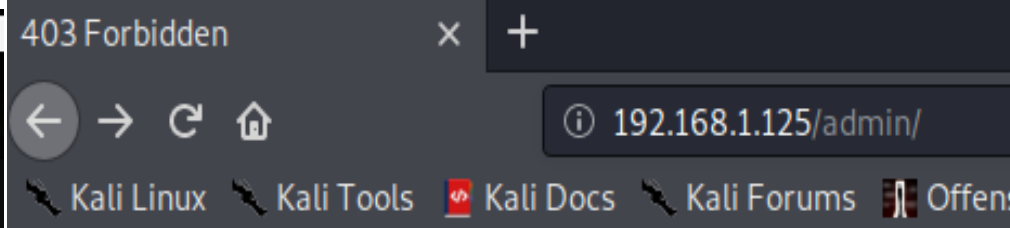


Forbidden

You don't have permission to access this resource.

Apache Server at 192.168.1.125 Port 80

```
GNU nano 4.9.2 /etc/apache2/conf-enabled/security.conf
#ServerTokens Full
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
#ServerSignature Off
ServerSignature On 192.168.1.125 Port 80
```

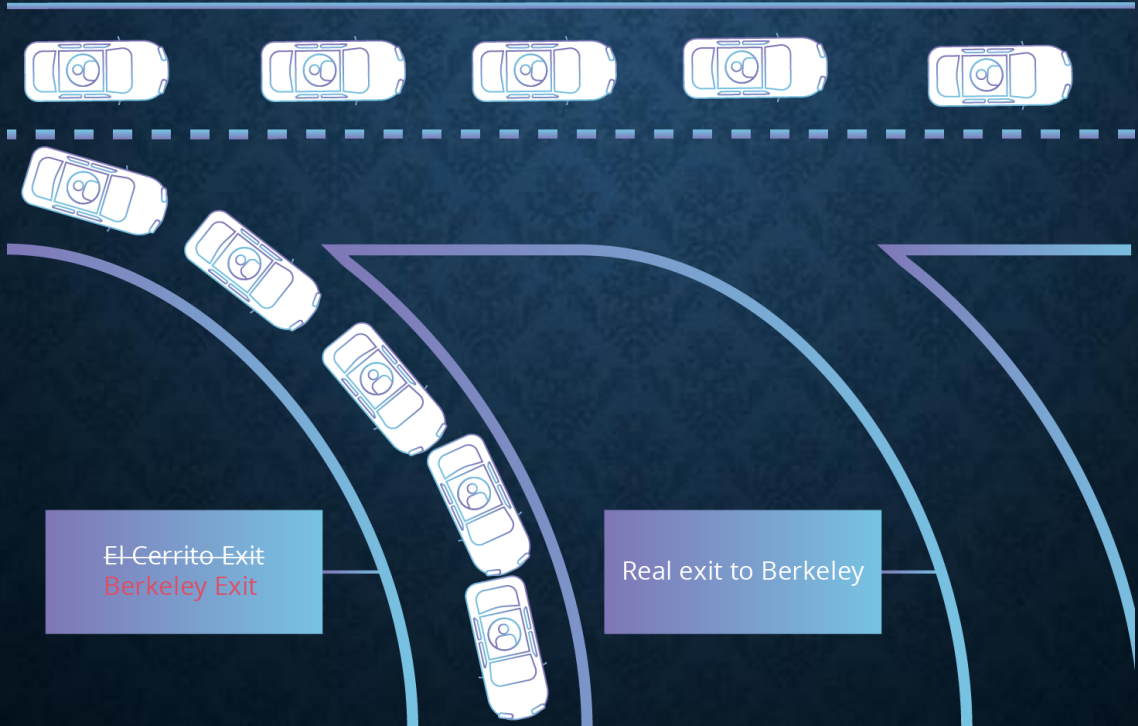


Forbidden

You don't have permission to access this resource.

```
GNU nano 4.9.2 /etc/apache2/conf-enabled/security.conf
#ServerTokens Full
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
#ServerSignature Off
ServerSignature Off 192.168.1.125 Port 80
```

BGP Hijacking



BGP Hijacking

O que é Hijacking?

Tradução = Sequestrar.

Ato de assumir o controle ou usar algo que não lhe pertence para sua própria vantagem.

O que é BGP?

O Border Gateway Protocol (BGP) é usado para **direcionar o tráfego pela internet**, permitindo que as redes troquem “informações de acessibilidade ”para facilitar o acesso a outras redes.



BGP Hijacking

O que é BGP Hijacking?

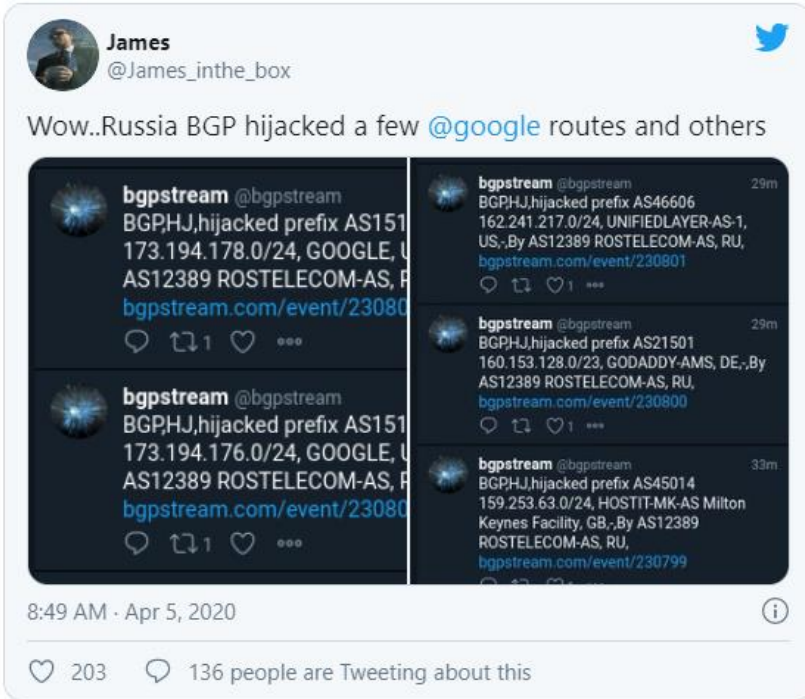
O sequestro BGP é a **aquisição ilegítima de grupos de endereços IP**, corrompendo as tabelas de roteamento da Internet mantidas usando o protocolo Border Gateway.

O que é um Sistema autônomo (AS)?

A Internet é uma rede de redes que é **dividida** em centenas de milhares de **redes menores**, conhecidas como **sistemas autônomos (AS)**. Cada uma dessas redes é essencialmente um grande conjunto de roteadores executados por uma única organização. Os sistemas autônomos geralmente **pertencem** aos ISPs ou outras grandes organizações de alta tecnologia, como empresas de tecnologia, universidades, agências governamentais e instituições científicas. Cada sistema autônomo que deseja trocar informações de roteamento **deve ter um número de sistema autônomo registrado (ASN)**.



BGP Hijacking



Atualmente, os sequestradores de BGP ainda são perigosos, pois permitem que o sequestrador registre o tráfego e tente analisá-lo e descriptografá-lo posteriormente, quando a criptografia usada para protegê-lo se enfraqueceu devido aos avanços nas ciências da criptografia.

Os sequestros de BGP são um problema para o backbone da Internet desde meados dos anos 90, e esforços para reforçar a segurança do protocolo BGP estão em andamento há anos, com projetos como ROV, RPKI e o mais recentemente **MANRS (Mutually Agreed Norms for Routing Security)**.

O último grande sequestro da **Rostelecom** que ganhou as manchetes aconteceu em 2017, quando a empresa de telecomunicações **sequestrou rotas do BGP** para algumas das maiores entidades financeiras **Visa, Mastercard, HSBC e muito mais**

BGP Hijacking

Investigate

SEARCH PATTERN SEARCH

www.company.rt.ru INVESTIGATE

Summary

76
Medium Risk

www.company.rt.ru
The domain is classified as Medium Risk due to a combination of suspect security features.

Security Categories: -
Content Categories: Business Services

SECURITY INDICATORS ▾

Timeline

Current Content Category: Business Services

DNS Queries Domain Events DNS Changes Jun 24th, 2020 - Jul 24th, 2020

DNS Queries Domain Events DNS Changes Apr 9th, 2017 - May 7th, 2017

No further DNS query data available prior to Jun 24th, 2020

Event History

Security Categories DNS Change First Seen: May 18, 2017

< CLOSE

May 18, 2017

1 Events

May 18th

A records:

109.207.14.3

DNS Hijacking

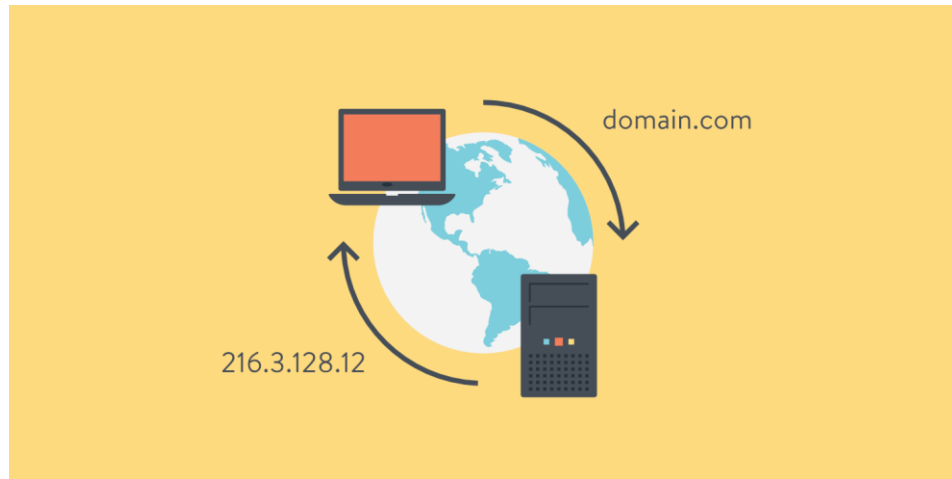


DNS Hijacking

O que significa DNS (**domain name system**)?

Tradução = **Sistema de Nomes de domínio**

O servidor **DNS** resolve **nomes** para os endereços **IP** e de endereços **IP** para os **nomes** respectivos, permitindo a localização de *hosts* num determinado domínio.



DNS Hijacking

Root Name Server (Raiz) - Servidores raiz são servidores de nomes DNS que operam na **zona raiz**. Esses servidores podem responder diretamente às consultas de **registros armazenados** ou **armazenados em cache** na zona raiz e também podem **encaminhar** outras solicitações ao servidor de domínio de nível superior (**TLD**) apropriado.

Top-level-domain (TLD) - Cada domínio é formado por nomes separados por pontos. O nome mais à direita é chamado de domínio de topo. **ccTLD** (country code top-level domain) exemplos :Brasil “**.br**”e Portugal “**.pt**” . **gTLD** (generic top-level domain) exemplos: **.com** “organizações comerciais, mas sem restrições” e **.edu** “estabelecimentos de educação superior”.

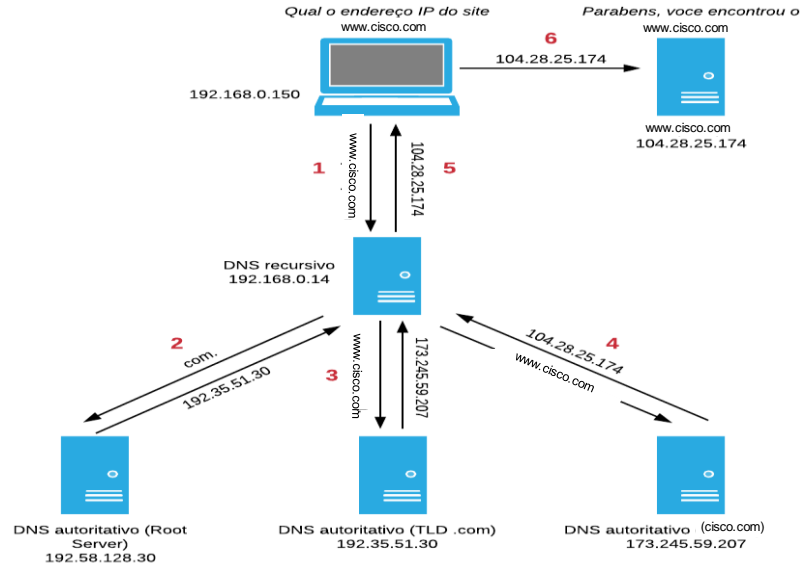
Authoritative name server (Autoritativo) - O servidor com autoridade de um domínio possui os **registros originais** que associam aquele **domínio** a seu endereço de **IP**.

DNS Recursivo - O DNS recursivo é responsável por **procurar** os endereços IPs de servidor que você solicitou acesso. Exemplo o DNS que esta configurado na sua máquina .

Ex: Umbrella (208.67.222.222 / 208.67.220.220)



DNS Hijacking



DNS Hijacking

Qual a importância do DNS?

Se o serviço DNS recursivo for **interrompido** por algum motivo, você não poderá se conectar a sites a menos que digite os **endereços IP diretamente** e quem mantém uma lista de emergência de endereços IP em suas mesas?

Se o serviço DNS recursivo que você usa estiver funcionando, mas tiver sido **desacelerado** por algum motivo (como um **ataque cibernético**), a conexão com os sites também ficará mais lenta.



DNS Hijacking

Principais tipos de ataques DNS Hijacking

Local DNS Hijack- Nesse tipo de invasão de DNS, os invasores **instalam o malware** Trojan no sistema de um usuário, o invasor **altera** as configurações regionais do DNS e **redireciona** o usuário para um site malicioso.

Router DNS Hijack - Esse ataque considera a **invasão de roteadores DNS que possui uma senha padrão**, alterando as configurações DNS afetando todos os usuários conectados a esse roteador.

Rogue DNS Hijack - Depois que um **servidor DNS é invadido**, os registros DNS podem ser alterados para direcionar todo o tráfego do usuário para um **site malicioso**.

Main in the middle DNS Hijack - Aqui, o invasor **intervém na comunicação** entre o usuário e o servidor DNS e exibe um endereço IP falso que redireciona o usuário para um site malicioso.



DNS Hijacking

Motivações

Pharming - O golpe direciona os usuários para um **site falso**, repleto de **anúncios**. Essas páginas da web não cumprem nenhuma função real, mas o operador gera receita cada vez que é visitado. *Host file*.

Phishing - Direciona o acesso para um site “disfarçado/falso” e faz com que o usuário tenha a impressão de que a página é confiável. Nesse processo, são roubadas informações confidenciais, que podem ser **usadas em troca de resgates** ou para que o **cibercriminoso assuma a identidade do usuário** em transações online.



DNS Hijacking



Following

critical: blockchain(.)info now has completely new nameservers (ded91868-1(.)hostwindsdns(.)com,ded91868-2(.)hostwindsdns(.)com)

3:34 AM - 12 Oct 2016

Os endereços IP foram alterados: a

blockchain.info **INVESTIGATE** Visualize

First seen	Last seen	IPs
10/12/16	10/12/16	104.16.54.3 (TTL: 300) 104.16.55.3 (TTL: 300) 192.236.200.26 (TTL: 14400) 198.44.48.226 (TTL: 14400)
7/12/16	10/11/16	104.16.54.3 (TTL: 300) 104.16.55.3 (TTL: 300)

blockchain.com **INVESTIGATE** Visualize Back

First seen	Last seen	IPs
10/12/16	10/12/16	104.16.106.226 (TTL: 300) 104.16.107.226 (TTL: 300) 104.16.108.226 (TTL: 300) 104.16.109.226 (TTL: 300) 104.16.110.226 (TTL: 300) 192.236.200.26 (TTL: 14400) 198.44.48.226 (TTL: 14400)
7/12/16	10/11/16	104.16.106.226 (TTL: 300) 104.16.107.226 (TTL: 300) 104.16.108.226 (TTL: 300) 104.16.109.226 (TTL: 300) 104.16.110.226 (TTL: 300)

It looks like blockchain.info has been DNS hijacked. (self.Bitcoin)
submitted 7 hours ago * by 2348957234 redditor for 7 days

It looks like blockchain.info has just had their domain name hijacked. The whois and DNS records suddenly jumped from CloudFlare to a cheap web host. From the cache, the names used to be

Name Server: BETH.NS.CLOUDFLARE.COM
Name Server: JAY.NS.CLOUDFLARE.COM

and were then **changed to**

Name Server: DEDB8057-1.HOSTWINDSONS.COM
Name Server: DEDB8057-2.HOSTWINDSONS.COM

when queried these are returning

```
;; ANSWER SECTION:  
blockchain.info. 11360 IN A 192.236.200.26
```

OR

```
;; ANSWER SECTION:  
blockchain.info. 14400 IN A 198.44.48.226
```

<https://umbrella.cisco.com/blog/detecting-recent-blockchain-dns-hijack>



DNS Hijacking

SEARCH PATTERN SEARCH

blockchain.info

INVESTIGATE



Summary



blockchain.info

The domain is classified as Low Risk. We found no malicious threats and no suspicious security features.

Security Categories

Content Categories

Software/Technology Online Trading

SECURITY INDICATORS

Timeline

DNS Queries Domain Events DNS Changes

Current Content Category: Software/Technology

CLOSE

Jul 04 - Jul 09, 2014

2 Events

No further DNS query data available prior to Jun 26th.

Jul 4th

MX records:

alt1.aspmx.l.google.com.
alt2.aspmx.l.google.com.
aspmx.l.google.com.
aspmx2.googlemail.com.
aspmx3.googlemail.com.

Jul 9th

NS records:

beth.ns.cloudflare.com.
jay.ns.cloudflare.com.

Event History

Security Categories DNS Changes Query History

2012 2013 2014 2015 2016 2017 2018 2019 2020

WHOIS Record Data

Registrar Name: CloudFlare, Inc. IANAID: 1910

Last retrieved January 15, 2020 GET LATEST

Created: October, 15, 2011

Updated: October, 15, 2019

Expires: October, 15, 2020

Raw data

No email info to display

Nameserver	Associated Domains	Last Observed
jay.ns.cloudflare.com	Greater than 500 Total - At least 1 malicious	Current
beth.ns.cloudflare.com	Greater than 500 Total - At least 2 malicious	Current

Showing 2 of 2 Results

Show more WHOIS data

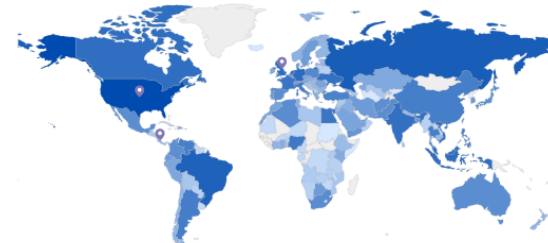
Host

IP Count 3

Registrar Country LU

Requester Distribution

COUNTRY	PERCENTAGE
United States	17.05%
Russian Federation	7.30%
Brazil	5.71%
Singapore	4.53%
Germany	3.94%



Distribution 0 17%

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	e7366052e780be9ef7820023ae723c31f827dc5c757696bc0f9277ca48e77674	
100	2955d081ee9bca7e4f5037728125e7487729025956f93095c58035919d50220b5	Win.Trojan.Sality. (Cloud).Win32.Trojan.Ransom.W32/Ransom.DMWD.Ransom_EMPER.CBQ164J.W32/... (B).0040e7f1.Win.Ransomware.Seven- 6515214.Gen.Variant.Symmi.62481.Backdoor.Win32.Farfli.ahjm.Trojan.Inject2.18859... gen.Riskware.0040e7f1.Trojan.Win32.Generic!BT.Trojan.ServStart.W32.Virut.IqDZ.Tro... FHT152517F410E78.Ransom.Crowti.A6. (.Gen.Variant.Symmi.62481.Gen.Variant.Symmi.62481.Backdoor.Farfli!TOP7Dnw6nw... dLDJ.MZ6r0hC.W32.KuluocAF.Trojan.Ransom_EMPER.CBQ164J.Trojan.Win32.Diplo... UMI.Trojan.Win32.CVRR-eloob3TA/Crypt.ZPACK.oms.Trojan.Diplo.acqj.Win32/Filed... (Trojan.Win32.Boxxx.Gen.Variant.Symmi.62481.Gen.Variant.Symmi.62481.Trojan.W32/...
100	a2e97ef8a0914e1d91a10df523a72e2d514552b82c7bb0947083ea57766d3b7	

Cryptojacking



Cryptojacking

O que é Cryptocurrency?

A palavra crypto vem de **criptografia** e currency significa **moeda**. Logo, cryptocurrency pode ser visto como **moedas criptografadas**.

A principal diferença entre as criptomoedas e o dinheiro real é que **elas são criadas por diversas entidades diferentes**, mas ninguém é proprietário da moeda inteira, apenas da quantidade que possui.

Ao contrário **de sistemas bancários centralizados**, grande parte das criptomoedas usam um sistema de controle descentralizado com base na tecnologia de **blockchain**.



1 Bitcoin igual a

52.232,53 Real brasileiro

27 de jul. 01:00 UTC · Fontes

1

Bitcoin

52232.53

Real brasileiro

1D 5D 1M 1A 5A Máx



Dados de câmbio disponibilizados pela Morningstar e de criptomoeda pela Coinbase

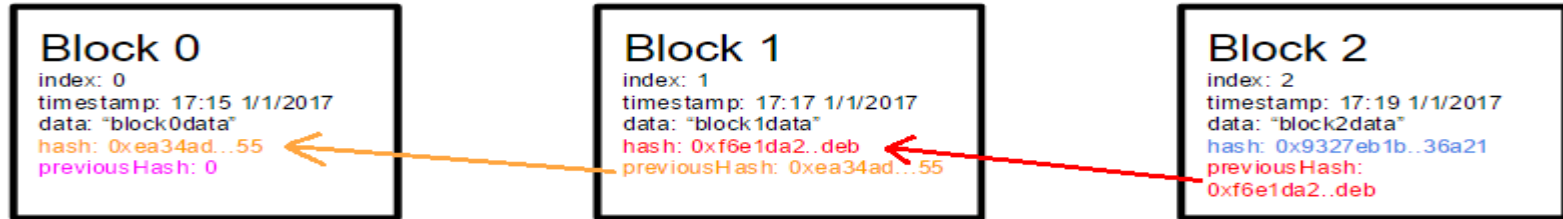
Cryptojacking

O que é Blockchain?

Olhando pelo lado simples o blockchain nada mais é do que um livro razão público (ou livro contábil) que faz o registro de uma transação de moeda virtual **de forma que esse registro seja confiável e imutável.**

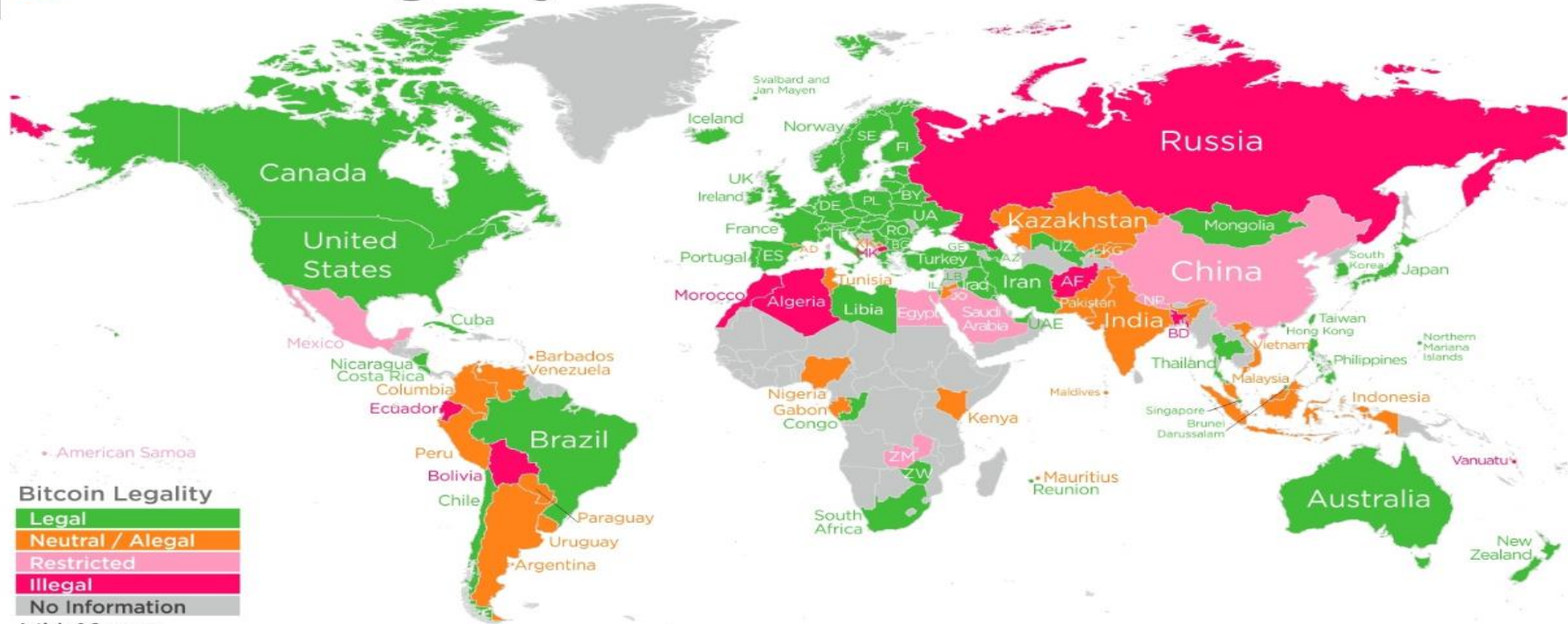
Ele armazena essas informações, esse conjunto de transações, em blocos carimbando cada bloco com um registro de tempo e data. A cada período de tempo (10 minutos no blockchain), é formado um novo bloco de transações, que se liga ao bloco anterior.

A rede do blockchain é formada por **mineradores** que verificam e registram as transações no bloco.





Bitcoin Legality Around the World



Bitcoin Legality

- Legal
- Neutral / Alegal
- Restricted
- Illegal
- No Information

Article & Sources:
<https://howmuch.net/article/bitcoin-legality-around-the-world>
<https://coin.dance/poli>

howmuch.net

<https://howmuch.net/articles/bitcoin-legality-around-the-world>



Cryptojacking

Método antigo/tradicional de Cryptojacking

Nesse modelo, o cibercriminoso precisa desenvolver um **malware**, distribuí-lo e contar com a sorte para que não seja detectado e removido dos computadores atingidos.

Método novo que tem se tornado comum

Nesse modelo, o cibercriminoso esconde um **script** (que contém informações da sua **carteira virtual**) por de trás da página (site) conforme o usuário navega por esse site a mineração acontece.



Cryptojacking

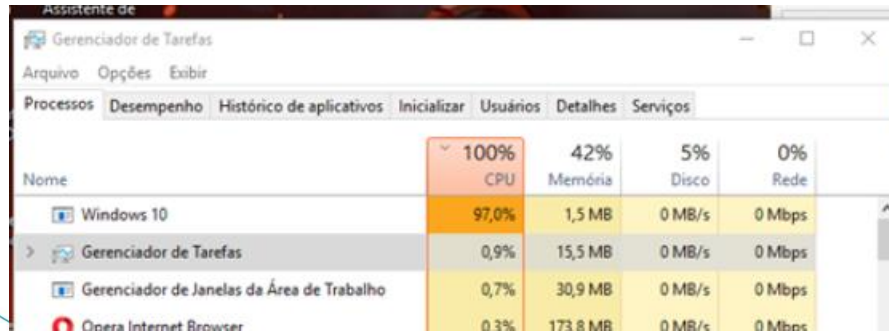
Quais são os sintomas?

Lentidão, travamentos, falta de performance em atividades simples como abrir o navegador e enviar ou ler um e-mail .

Forçar seu hardware para rodar no máximo de suas capacidades faz com que seu computador **consuma maior quantidade de energia**. Em laptops e celulares isso será ainda mais decisivo, já que esses dispositivos **têm baterias menos eficientes**, que duram pouco tempo.

Prejuízos

Desgaste do hardware, consumo elétrico e abrir portas para outros cibercriminosos.



Nome	CPU	Memória	Disco	Rede
Windows 10	97,0%	1,5 MB	0 MB/s	0 Mbps
Gerenciador de Tarefas	0,9%	15,5 MB	0 MB/s	0 Mbps
Gerenciador de Janelas da Área de Trabalho	0,7%	30,9 MB	0 MB/s	0 Mbps
Onea Internet Router	0,3%	173,8 MB	0 MB/s	0 Mbps

Cryptojacking

DEMO

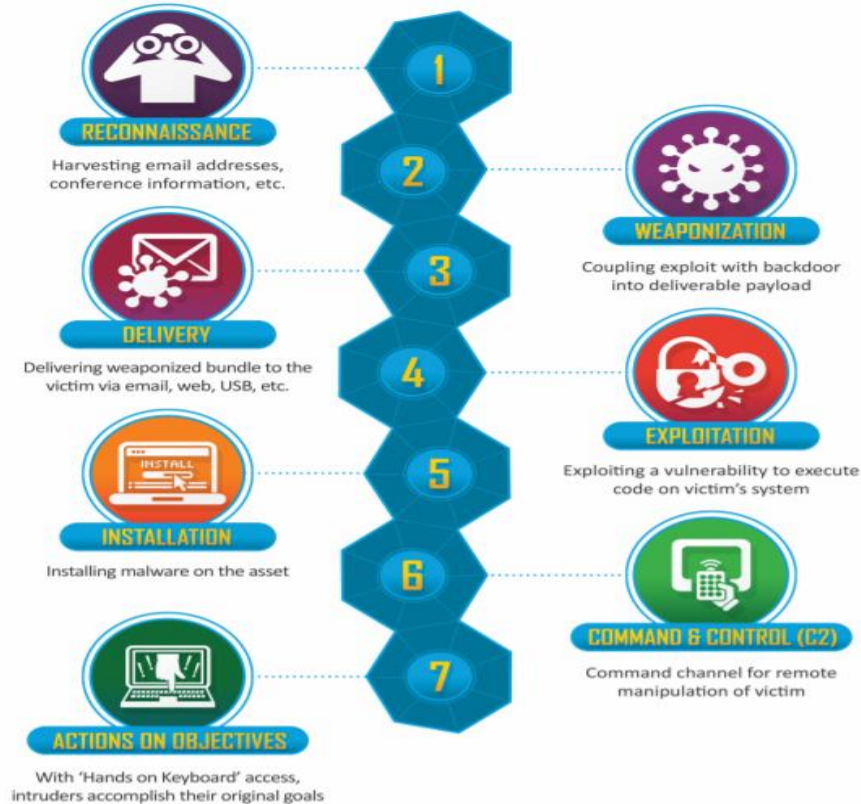


Command & Control (C2)



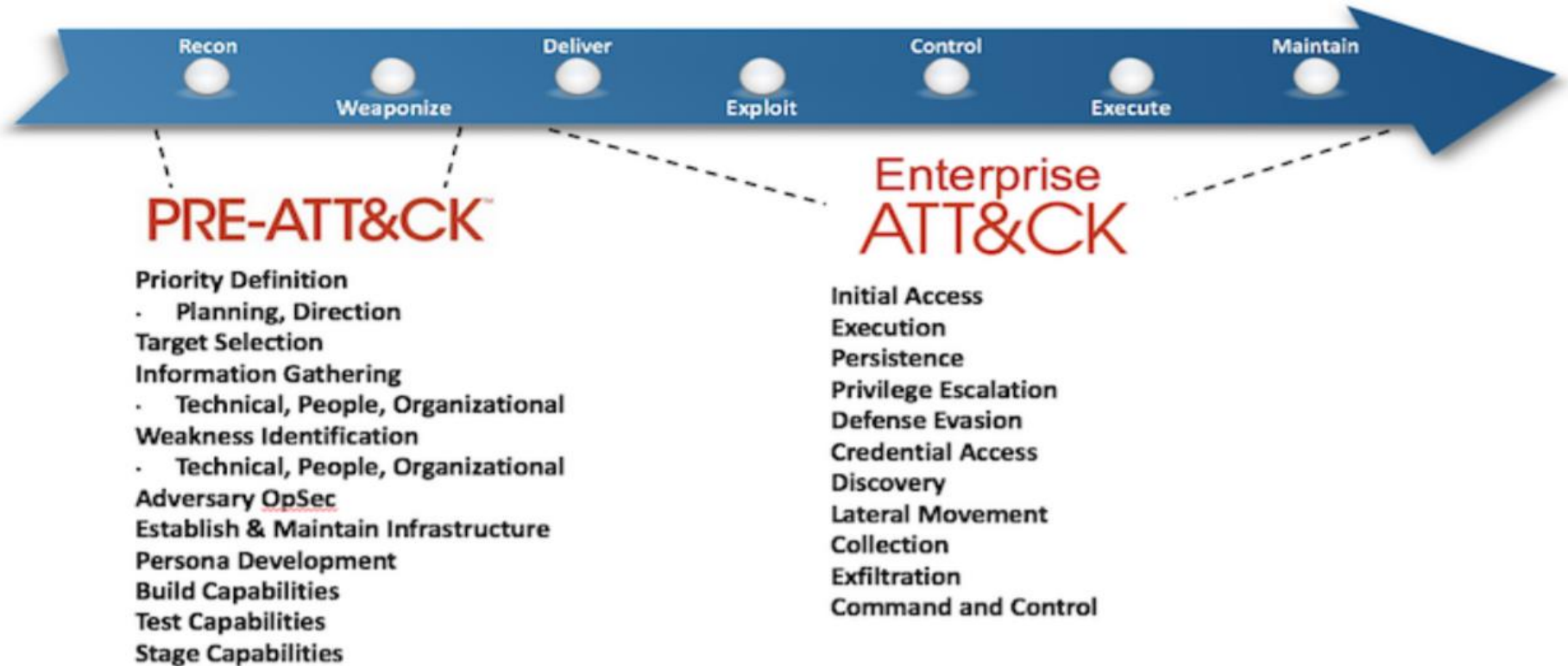
Ciber Kill Chain

As sete etapas da Cyber Kill Chain aumentam a visibilidade de um ataque e enriquecem a compreensão de um analista sobre as **táticas, técnicas e procedimentos** de um adversário.



MITRE

Adversarial Tactics Techniques and Common Knowledge



MITRE ATT&CK

PRE-ATT&CK

ENTERPRISE

Windows.MacOS, Linux,
Cloud

ATT&CK

MOBILE

Android e IOS

ICS

Sistemas de controle
Industrial



Command & Control

- Coleta de Informações do Alvo Comprometido Mapeamento da Rede Interna
- Escalada de Privilégios
- Captura de Credenciais (senha em claro ou o hash)
- Manutenção do Acesso (Persistência/Backdoor)
- Pivoteamento
- Movimento Lateral
- Comprometer outros serviços e sistemas
- Estabelecer um canal de Comando e Controle - C2
- Exfiltração de Dados



Command & Control

Características

- Comunicação Assíncrona
- Linguagem de Programação utilizada no framework
- Canal de Comunicação (protocolos)
- Beacon
- Jitter
- Agentes – quais os Sistemas Operacionais suportados
- Data de validade (kill date)
- Suporte (comunidade ativa)
- Interface de utilização (linha de comando/GUI)



Empire



O Empire é um agente pós-exploração do PowerShell puro, construído em comunicações criptograficamente seguras e uma arquitetura flexível. O Empire implementa a capacidade de executar agentes do PowerShell sem precisar do powershell.exe, módulos de pós-exploração rapidamente implantáveis, que variam de registradores de chaves a Mimikatz, e comunicações adaptáveis para evitar a detecção de rede, tudo envolvido em uma estrutura de foco na usabilidade.

02 Componentes principais

- Servidor de Controle (listener), escrito em Python 3
- Agentes (clientes) escritos em PowerShell
- Assincronismo (Comando/Resposta)

C2 Frameworks

ATACANTE



ALVO



Command & Control

DEMO



Distributed Denial of Service (DDoS)



DDoS

DoS “Denial of Service” = **Negação de Serviço**

Técnica utilizada pelo atacante para tirar de operação um serviço, um computador, um router ou uma rede.

DDoS “Distributed Denial of Service” = **Negação de Serviço Distribuído**

Técnica utilizada pelo atacante, de forma **coordenada e distribuída**, um conjunto de computadores para tirar de operação um serviço, um computador ou uma rede.

Objetivo:

Esgotar/exaurir recursos, aplicações e serviços da rede fazendo com que o tráfego/usuário legítimos não consigam acessá-los.

Muitas pessoas confundem com invasão.



DDoS

Motivação

- **Hacktivismo**
- **Lei de talião**
- **Script Kiddies**
- **Concorrência desleal**

Impactos

- **Serviços e recursos legítimos indisponíveis.**
- **Perda de credibilidade**
- **Backup**
- **Aumento de custos**



DDoS

Tipos de ataques

- **Volumétrico**
- **Na camada de aplicação**
- **Exaustão de Recursos de hardware**

Obs: Podem ser usados isoladamente ou em conjunto.



DDoS

- **Volumétrico**

Tem como intuito **exaurir a banda** disponível enviando ao alvo grande volume de tráfego. Para gerar esse volume os atacantes utilizam meios como botnets, máquinas com bastante banda, máquinas com pouca banda porem em grande quantidade.

DRDoS - *Distributed Reflective Denial of Service*



DDoS

- **Camada de aplicação**

Mais difíceis de serem detectados, pois é facilmente confundido com problemas de implementação da aplicação e não necessitam de muitas máquinas e nem de muito tráfego para ser realizados.

Exploram características de aplicação.

Exemplos: HTTP Flood, VoIP (SIP INVITE Flood) e Slow Read DDoS.



DDoS

- **Exaustão de recursos de hardware**

Os ataques de exaustão de recursos de *hardware* tentam consumir a capacidade de equipamentos e exaurir seus recursos.

Em roteadores: tenta consumir recursos, como CPU e memória, e a capacidade de encaminhamento de pacotes por segundo (pps);

Em *firewalls* e IPSs: tentam consumir a capacidade da tabela de estado de conexões, impedindo que novas conexões sejam estabelecidas.

Exemplos: fragmentação e TCP Syn Flood.



DDoS

- **Detecção**

Validar fluxos de entrada e saída de tráfego: Mudanças de comportamento e padrão e Callbacks.

Instrusion Detection/Protection: IDS/IPS, NGFW, Antivirus e Antimalware.

Utilização de Honeypots: Ferramenta que tem a função de propositalmente de simular falhas de segurança de um sistema e colher informações sobre o invasor. É uma espécie de armadilha para invasores.



OBRIGADO!

Josiane.silva@scansource.com

Parceria



Realização

ceptro.br nic.br