Ataques SYN+ACK

Da Semelhança com HTTPS às Barreiras da Mitigação

Telic TECHNOLOGIES

We know about **network**

Portfólio de **Soluções**

Inteligência em
Redes

Inteligência em
Infraestrutura

Inteligência
Anti-DDoS

Inteligência em
Monitoramento

Atendimento
N1

Números Telic

Conectamos mais de **6 milhões de residências e empresas** na internet.

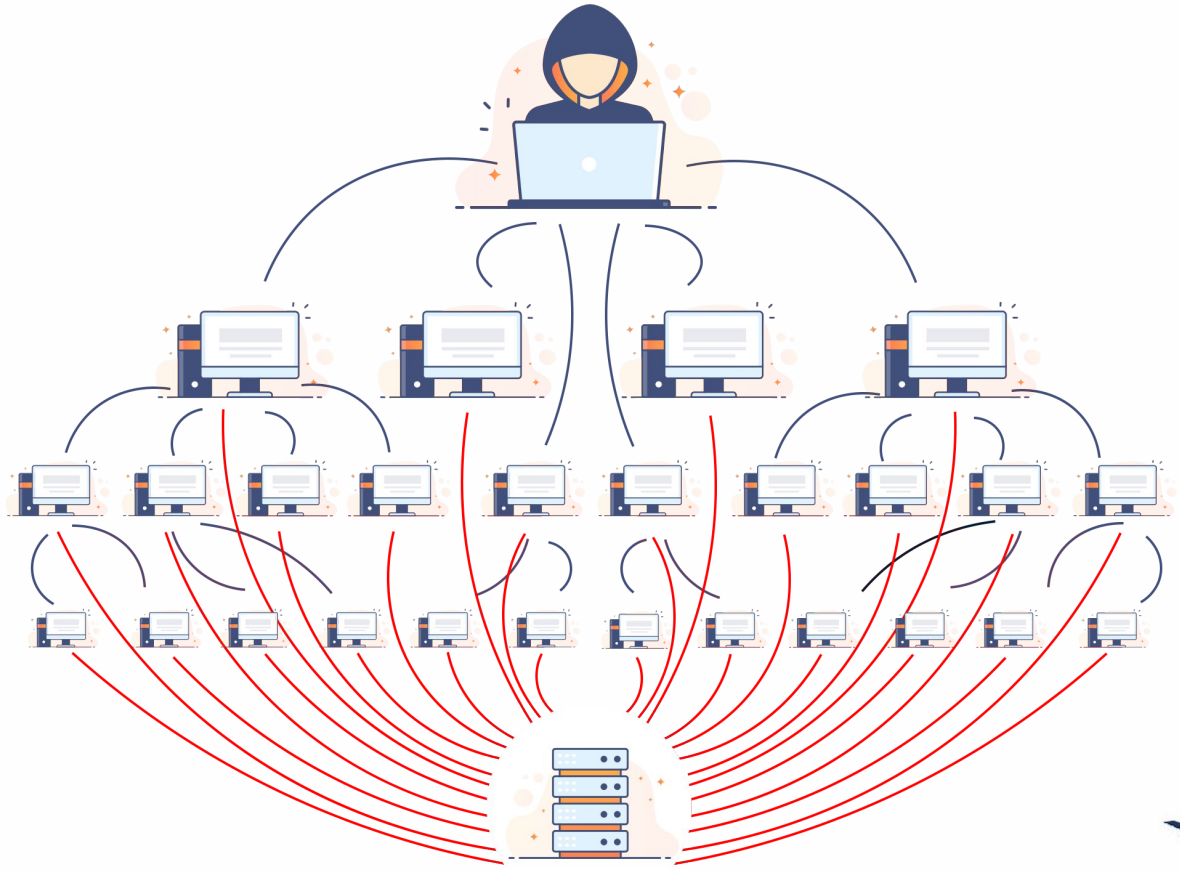
Nossos clientes somam mais de **7.5 Tb/s de tráfego** agregado.

O maior ataque de **DDoS** que mitigamos alcançou o patamar de **850Gb/s**.

Como funciona um ataque DDoS

O atacante não envia o tráfego de sua própria máquina ou de poucas máquinas que estão ao seu redor. Ele usa um exercito de bot's (botnet) para atacar.

1. Origem sempre será aleatória, com origem no mundo todo.
2. Como a origem é aleatória, descobrir quem é o atacante fica quase impossível.
3. O atacante envia o comando para alguns bot e esses além de gerar tráfego, também solicitam que mais bot enviem tráfego anômalo.
4. Com apenas um comando o atacante é capaz de gerar centenas de gb/s e pps de ataque.



Cenário de DDoS no Brasil e no mundo.

O Brasil é um país bem diferente do restante do mundo quando o assunto é ataques DDoS.
Citarei alguns dos motivos principais:

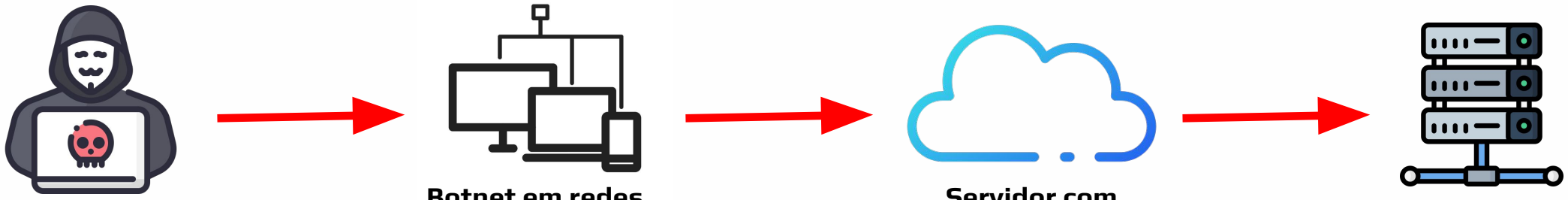
1. Na Europa e nos Estados Unidos as maiores vítimas de ataques DDoS são Datacenters e não ISP's.
2. Apenas 10% dos ataques ao maior provedor residencial dos EUA é do tipo carped-bomb.
3. No Brasil, 95% do ataques são do tipo carped-bomb
4. Somos o segundo maior país do mundo em numero de ASN's, grande maioria ISP's.
5. Somos o maior país do mundo em número de ISP's, ou seja, grande concorrencia.
6. Brasil é o segundo maior país em ataques DDoS do mundo, perde apenas para os EUA.
7. Brasil é o país onde mais se origina spoof e consequentemente ataques do mundo (extra oficial).

O que é IP Spoofing e Reflexão?

Basicamente IP Spoof é o ato de gerar um pacote alterando o IP de origem para qualquer outro IP que não seja o IP configurado naquele equipamento.

1. Nada tem a ver com RPKI ou IRR, ou seja, voce estar com IRR e RPKI tudo certo e ainda sofrer ataques com IP Spoofig
2. Pouco ou nada pode ser feito pela vítima de ataque com ip's spoofados
3. Facilmente resolvido com filtros anti-spoof ou uRPF
4. Facilmente detectável na rede que faz ataque.

Reflexão acontece quando um servidor aberto na internet recebe o tráfego de um IP com orgiem falsa (ip spoofig) e devolve as respostas a rede vítima, ou seja, funciona como um espelho, refletindo o tráfego.



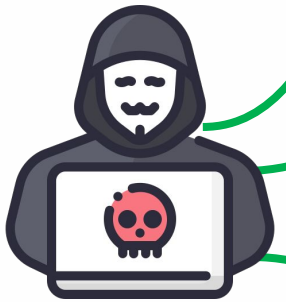
Como esse ataque funciona?

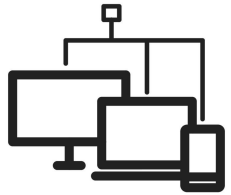
Vítima 1

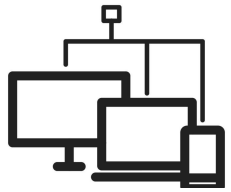
Vítima 2

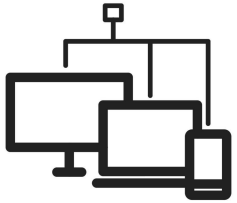
Vítima 3

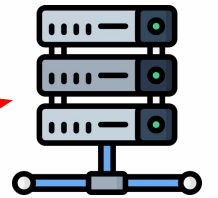
Atacante envia o comando para que os zumbis iniciem o ataque.

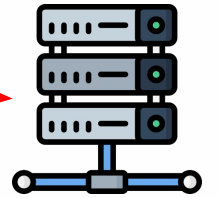


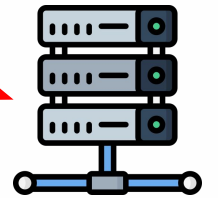












Zumbis enviam um pacote TCP na porta de destino 443 com a flag SYN para qualquer servidor da internet com porta TCP 443 aberta, forjando o IP de origem e colocando como sendo o da Vitima 3

A Vitima 2, recebe o pacote SYN e “devolve” o SYN+ACK para o IP da vítima 3 que foi forjado pela vitima 1.

Como a Vitima 3 não responde o 3way hand-shake com ACK, a vítima 2 ainda envia um pacote TCP com a flag RST.

O tráfego indesejado chega na Vítima 3, efetivando o ataque a vítima.

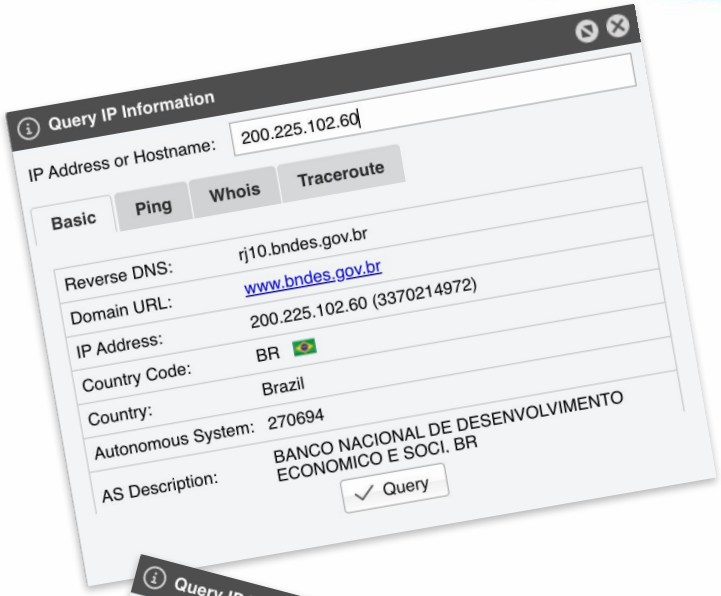
Estratégia do atacante

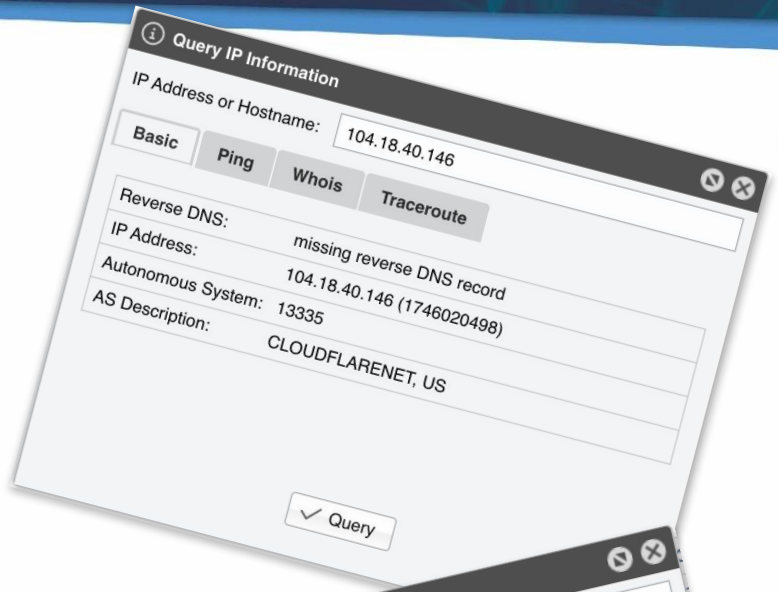
A estratégia do atacante basicamente é:

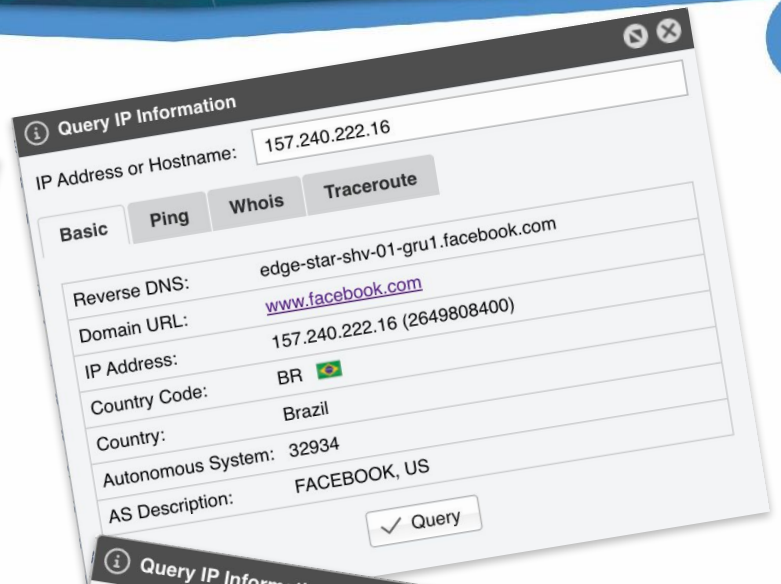
- Enviar uma quantidade de pacotes SYN para o maximo de servidores com porta 443 aberta na internet
- Essa quantidade não pode ser grande a ponto da Vítima 2 entender como se fosse um syn-flood
- Essa quantidade não pode ser pequena a ponto de não impactar a vítima 3 (que é o alvo final do ataque)
- Por isso usa-se o maximo de servidores com portas 443 abertas refletindo para o máximo de IP's possível da vítima 3
- Efeito do RST que vem para efetivar ainda mais o ataque
- Com isso é possível gerar o máximo de pps possível com baixo tráfego e alto impacto

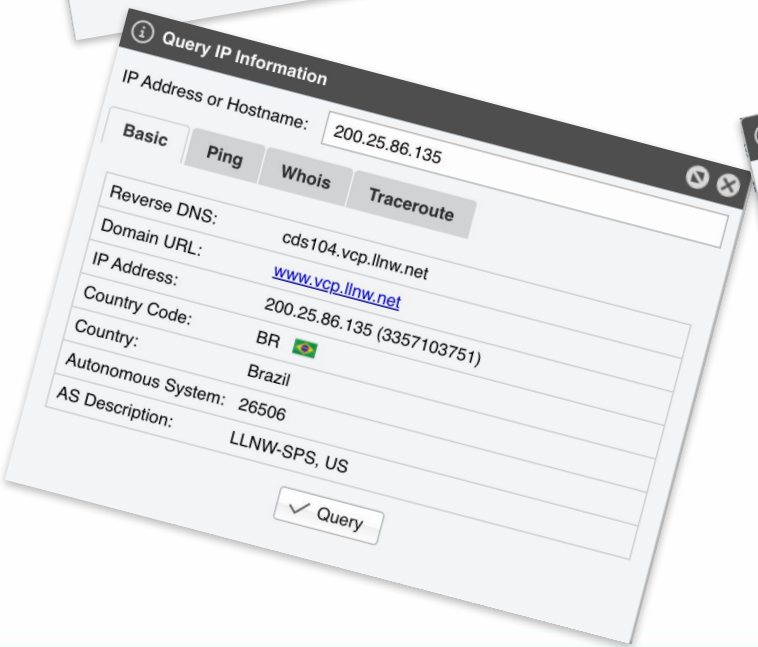
Temos aqui um dos mais poderosos ataques contra ISP

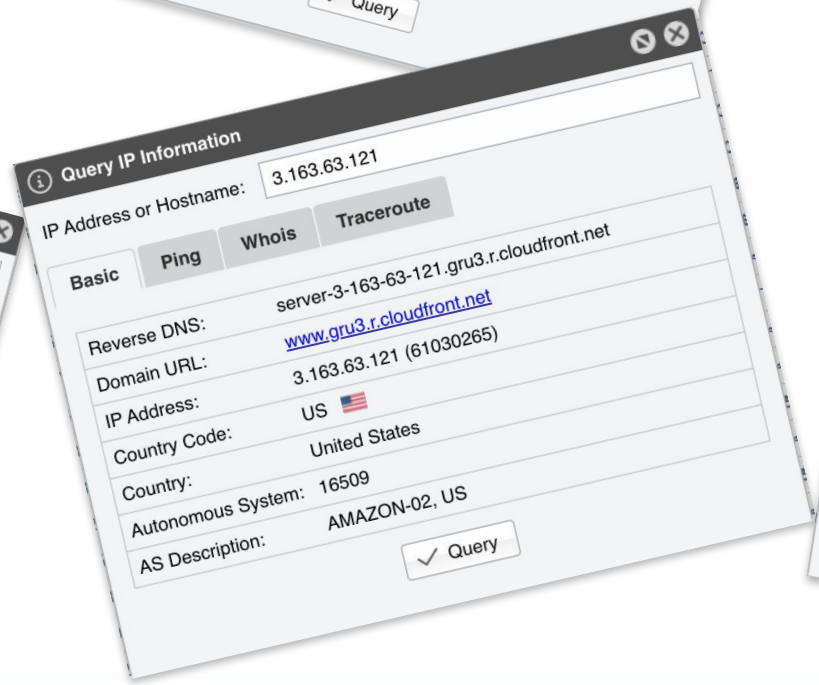
De onde esse tipo de ataque vem?

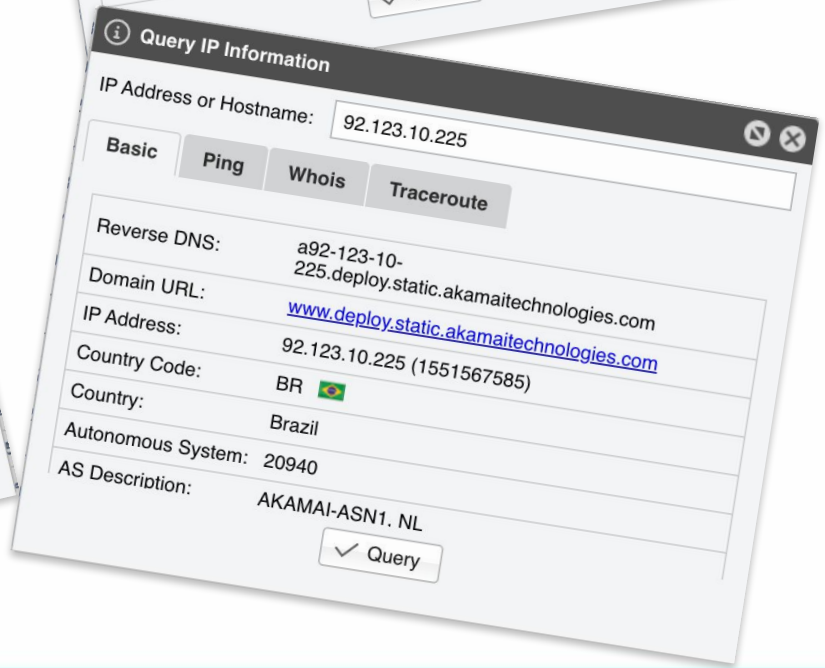




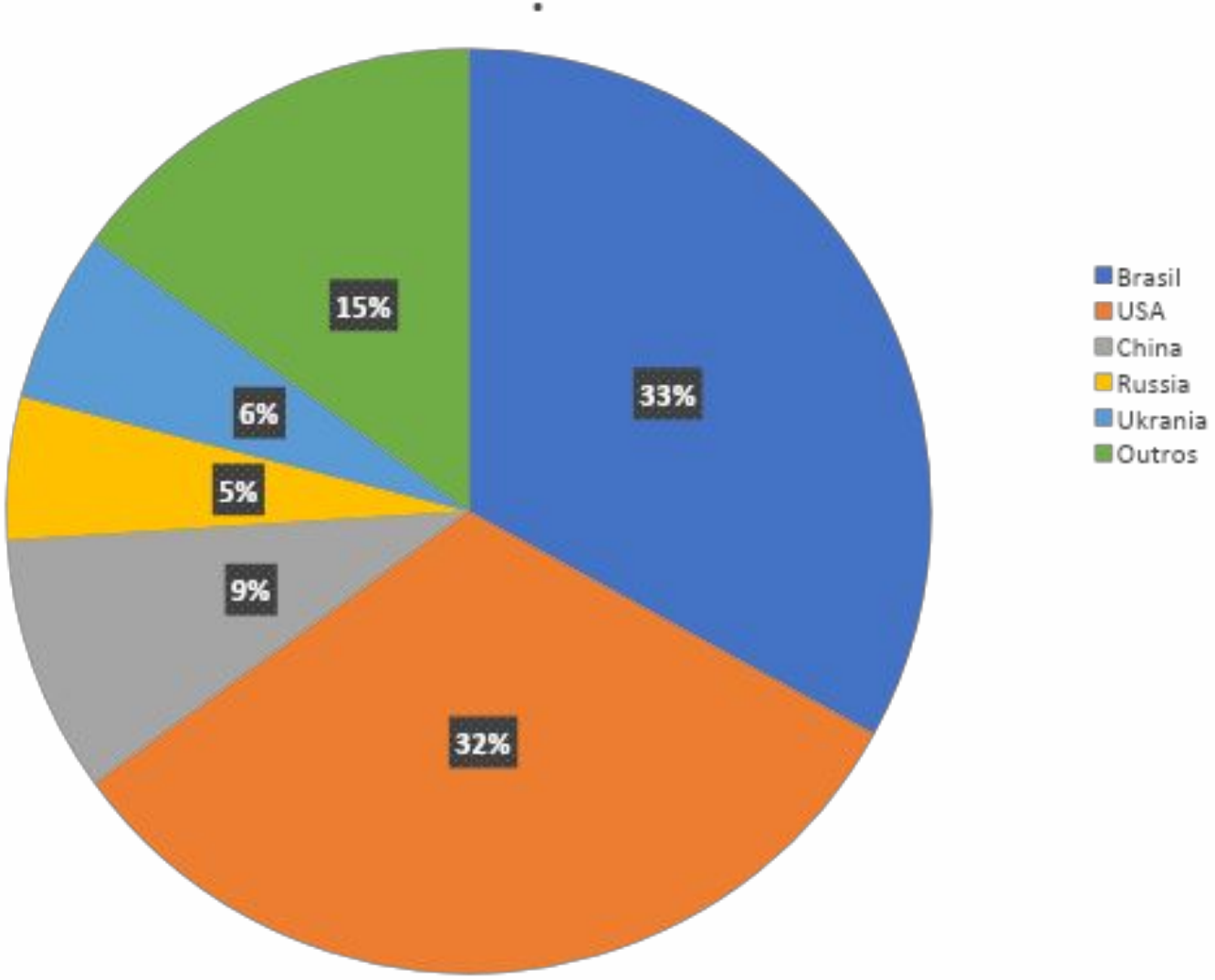








De onde esse tipo de ataque vem?



Efeito do Ataque

Além de todos efeitos negativos que qualquer ataque causa a uma rede, nesse caso ainda temos:

Prezados,

Nós somos a equipe de resposta a incidentes de segurança da Locaweb.

Você está recebendo esta mensagem porque é o contato WHOIS da rede mencionada abaixo. Esta comunicação é destinada à pessoa responsável pela segurança da informação. Caso este não seja o endereço correto, solicitamos que encaminhe esta mensagem ao responsável apropriado.

Identificamos um ataque direcionado proveniente do AS [redacted] contra nossa infraestrutura. Assim, foi necessário realizar o bloqueio do referido bloco.

Evidências:

2024-10-28 16:05:25,206519 [redacted].57 xxxxxxxxx.71 TCP 70 37221 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,198582 [redacted].144 xxxxxxxxx.243 TCP 70 42116 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,211430 [redacted].59 xxxxxxxxx.208 TCP 70 36249 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,216353 [redacted].182 xxxxxxxxx.4 TCP 70 55947 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,218042 [redacted].16 xxxxxxxxx.144 TCP 70 4283 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,222822 [redacted].189 xxxxxxxxx.250 TCP 70 61763 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,210255 [redacted].64 xxxxxxxxx.9 TCP 70 41030 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,211588 [redacted].59 xxxxxxxxx.191 TCP 70 45286 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,213074 [redacted].247 xxxxxxxxx.59 TCP 70 17526 → 443 [SYN] Seq=0 Win=64240
2024-10-28 16:05:25,199268 [redacted].91 xxxxxxxxx.247 TCP 70 44245 → 443 [SYN] Seq=0 Win=64240

Poderiam nos informar quais medidas foram tomadas para neutralizar essa situação?

========== X-ARF Style Summary ==========
Date: 2024-11-08T13:28:24+01:00
Source: [redacted].27.219
Type of Abuse: Portscan/Malware/Intrusion Attempts
Logs: 13:28:14.465667 rule 0/0(match): block in on vmx0: [redacted]7.219.64279 > 91.190.98.11.445: Flags [S], seq 3067376686, win 0, options [mss 1412], length 0

To whom it may concern,

[redacted].27.219 is reported to you for performing unwanted activities toward our server(s).

==========

Current records of unwanted activities toward our server(s) on file;
the second field designates our server that received the unwanted connection;
if this is a webserver log, the [VirtualHost] designates the visited website.

Source IP / Targeted host / Issue processed @ / Log entry

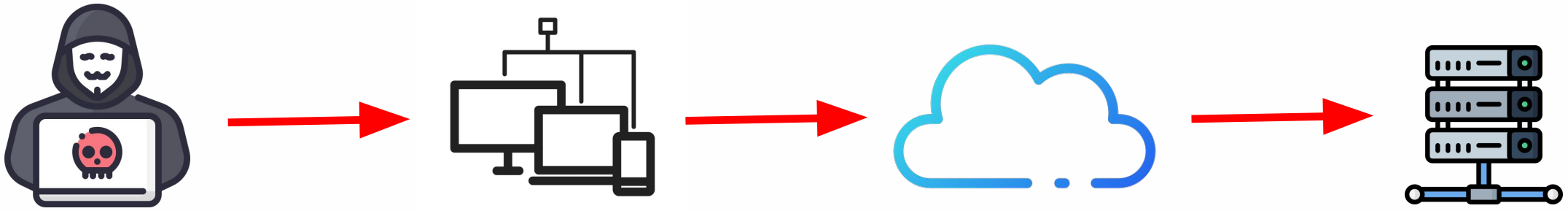
[redacted]27.219 tpc-022.mach3builders.nl 2024-11-08T13:28:24+01:00 13:28:14.465667 rule 0/0(match): block in on vmx0: [redacted].219.64279 > 91.190.98.11.445: Flags [S], seq 3067376686, win 0, options [mss 1412], length 0
[redacted]27.219 tpc-046.mach3builders.nl 2024-11-08T13:27:33+01:00 13:27:20.669969 rule 0/0(match): block in on vmx0: [redacted].219.63839 > 91.190.98.10.445: Flags [S], seq 2775040216, win 0, options [mss 1412], length 0
[redacted]27.219 tpc-035.mach3builders.nl 2024-11-08T13:25:38+01:00 13:25:33.257586 rule 0/0(match): block in on vmx0: [redacted].219.63922 > 91.190.98.8.445: Flags [S], seq 1869109142, win 0, options [mss 1412], length 0
[redacted]27.219 tpc-035.mach3builders.nl 2024-11-08T13:25:37+01:00 13:25:33.003344 rule 0/0(match): block in on vmx0: [redacted].219.64360 > 91.190.98.8.445: Flags [S], seq 2679933608, win 0, options [mss 1412], length 0
[redacted]27.219 tpc-033.mach3builders.nl 2024-11-08T13:21:05+01:00 13:20:56.615823 rule 0/0(match): block in on vmx0: [redacted].219.64089 > 91.190.98.93.445: Flags [S], seq 4274731469, win 0, options [mss 1412], length 0

Como resolver esse ataque?

Nesse ataque temos 3 vitimas, porém se a vitima 1 fizesse filtros anti spoofing esse ataque (e outros) simplesmente não existiria.

1. Podemos chamar a vitima 1 de vitima?
2. Simples de ser feito em roteadores Huawei, Juniper, Cisco e Mikrotik.
3. Custa muito pouco ao roteador.
4. NÃO RESOLVE ATAQUES DESTINADOS A SUA REDE.
5. Resolve ataques originados da sua rede.
6. 8 dos 10 maiores ISP de banda larga do país aceitam spoofing

ANTI SPOOFING!!!!



Quais equipamentos sofrem com esse tipo de ataque?

1. Todos os soft-routers.
2. Qualquer CGNAT que não tenha aceleraçao por hardware.
3. Roteadores mais antigos como MX(8 a 104), NE20, Ciscos ASR1001, 1002, etc.
4. Switchs menores atuando em L3
5. Caixas de mitigação mais antigas.

Como sofrer menos com esses ataques?

Esse ataque não tem como característica uma banda muito alta, dificilmente passa-se dos 200gb/s de trafico ilicito, a maior característica desse ataque é a quantidade de pps gerado na reflexão, então por isso recomendamos:

1. Evitar o uso de equipamentos de rede defasados.
2. Evitar o uso de IP público desnecessários em interfaces de roteadores
3. Evitar o uso de Mikrotik
4. Contratar uma mitigação de ataques DDoS

Desafios para mitigar esse ataque

Esse tipo de ataque sempre existiu, mas (quase) nunca com destino a ISP's. Temos uma política interna de não terceirizar mitigação, ou seja, todas as mitigações são pensadas, construídas e executadas pelo nosso time e isso fez demorar um pouco para finalizar:

1. Se origina de paises que são importantes para o nosso tráfego de internet.
2. Vem com porta de origem 443 que também é bem importantes para o tráfego de um ISP.
3. Quantidade de pacotes superiores a 120mpps por ataque.
4. Nossas ferramentas estavam prontas, mas não para essa quantidade de tráfego.
5. A origem sempre é um IP que são realmente um servidor HTTPS, então proxies não fariam sentido.
6. A origem sempre é um servidor HTTPs conhecido e muito utilizado (Google, facebook, Akamai, etc)
7. O pacote ilícito é idêntico a um pacote lícito de início de conexão HTTPs

[GTER] Contato do AS28220

Bruno Vane broonu at gmail.com
Thu Nov 14 10:34:11 -03 2024

- Previous message (by thread): [GTER] Contato Locaweb
- Next message (by thread): [GTER] Contato do AS28220
- **Messages sorted by:** [date] [thread] [subject] [author]

Bom dia senhores,

Por acaso há um representante do AS28220 no grupo?
Temos recebidos ataques constantes deste ASN, do tipo SYN+ACK com SRC PORT 443.
Já tentei entrar em contato com eles pelo e-mail noc at alaresinternet.com.br mas sem resposta.

AS28220 SYN+ACK Attack <https://imgur.com/a/XXsWeGK>

- Previous message (by thread): [GTER] Contato Locaweb
- Next message (by thread): [GTER] Contato do AS28220
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the gter mailing list

[GTER] Contato do AS28220

Gustavo Santos gustkiller at gmail.com
Thu Nov 14 12:14:24 -03 2024

- Previous message (by thread): [GTER] Contato do AS28220
- Next message (by thread): [GTER] Contato do AS28220
- **Messages sorted by:** [date] [thread] [subject] [author]

Já cheguei a entrar em conato, mas até então continuam usando eles como refletores..

Como não teve nenhuma ação por parte deles até o momento, o que origina estes syn/ack floods partindo deste ASN
são CPEs da Nokia com a porta 443 aberta (Gerência) aberta para o mundo.
Coisa que uma ACL simples
na gestão da rede xPON deles resolveria.

É só verificar no log do ataque, e acessar os hosts na porta 443...

https://eng.registro.br/pipermail/gter/2024-November/080727.html

Desafios para mitigar esses tipos de ataque

Pacote **ilícito**

```
Internet Protocol Version 4, Src: 31.13.91.21, Dst: 100.124.3.63
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 55
    Protocol: TCP (6)
    Header Checksum: 0x61df [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 31.13.91.21
    Destination Address: 100.124.3.63
Transmission Control Protocol, Src Port: 443, Dst Port: 39242, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 39242
    [Stream index: 61]
  > [Conversation completeness: Incomplete (2)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3065608183
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3864787792
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xeedf [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  > [Timestamps]
```

Pacote **ilícito**

```
Internet Protocol Version 4, Src: 45.161.84.78, Dst: 193.8.112.203
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x8701 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 45.161.84.78
    Destination Address: 193.8.112.203
Transmission Control Protocol, Src Port: 443, Dst Port: 57794, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 57794
    [Stream index: 8]
  > [Conversation completeness: Incomplete (2)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1443854274
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2835958702
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x1a46 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  > [Timestamps]
```

Como fizemos para mitigar esses ataques

1. Mesmo todas as técnicas e ferramentas de mitigação sendo criado e mantidas por nós, fomos atrás de ajuda
2. Conversamos e fizemos POC com as três dos mais conhecidos vendors de mitigação.
3. Conversamos e fizemos POC com dois operadores Tier1 utilizando a ferramenta de mitigação deles.
4. Em paralelo a isso, uma parte do time focou em reconstruir nossa ferramenta para mitigação desse tipo de ataque
5. Flowspec ajuda em muito pouco, nada efetivo para mitigar esse ataque, apenas para direcionar o trafego para nosso serviço
6. Monitoramento de 3way hand-shake.
7. Upload é importante.

Junior Corazza
coraza@telic.com.br
https://www.linkedin.com/in/jrcorazza/

Telic TECHNOLOGIES

Dúvidas?

We know about **network**