

INFRAESTRUTURA DE ATAQUE & DISPONIBILIDADE

Ataques de Negação e Redes Zumbis

Um estudo aprofundado sobre como **Botnets (redes de dispositivos infectados)** operam silenciosamente em escala global e atuam como a principal infraestrutura para orquestrar ataques massivos de **DoS e DDoS**.

TEMA 01

Botnets & Redes Zumbis

Recrutamento, C&C, P2P, BaaS e impacto invisível

TEMA 02

Ataques DoS e DDoS

Tríade CIA, camadas OSI, SYN Flood e Amplificação

CONEXÃO TÉCNICA

O Motor do Colapso

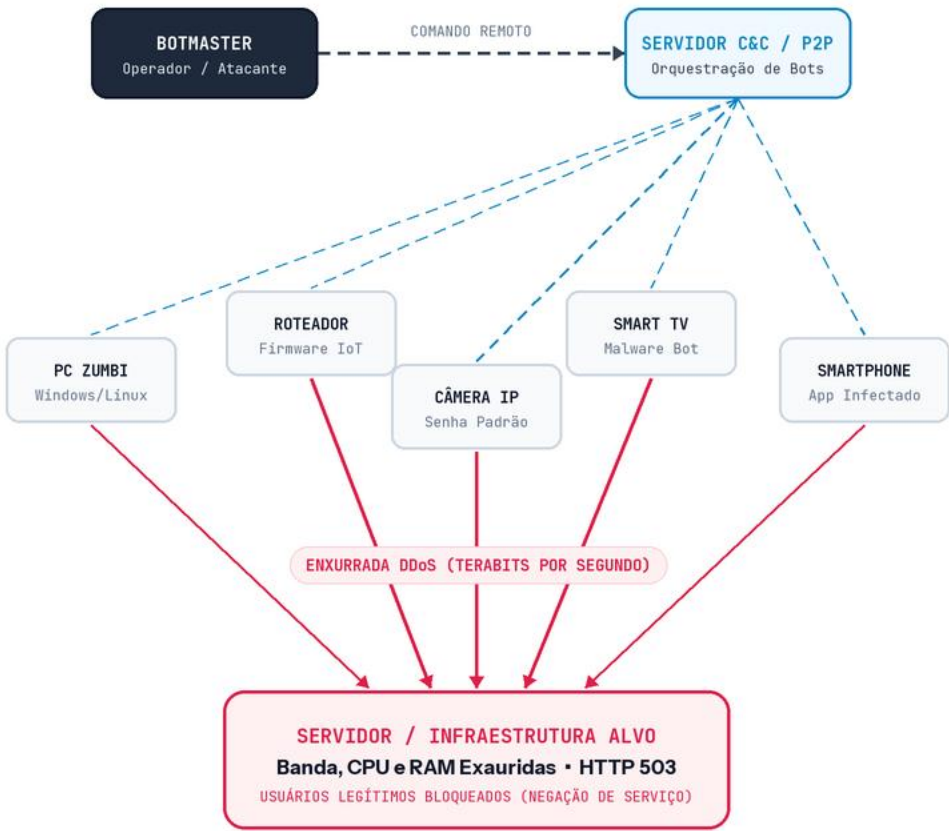
Como a Botnet viabiliza ataques na casa dos Terabits/s

INTEGRANTES DA DUPLA // APRESENTADORES

Felipe Augusto & Lucas Arantes

DURAÇÃO: 15-18 MIN

TOPOLOGIA CONCEITUAL // DA REDE ZUMBI AO COLAPSO DO ALVO



VETOR PRIMÁRIO: Botnet IoT & Estações

IMPACTO: Indisponibilidade Total (DDoS)

Estrutura da Apresentação e Conexão Técnica

Sequência lógica dividida em 4 blocos para compreender a ameaça das Botnets, a mecânica do DoS/DDoS e as estratégias de defesa.

BLOCO 01

Tema 1: Botnets

Apresentador: Felipe Augusto

- 01 **Conceito & Etimologia:** O exército de 'zumbis' (Robot + Network) e sua ação invisível.
- 02 **Recrutamento:** Engenharia social vs. exploração automatizada de IoT.
- 03 **Arquitetura C&C vs. P2P:** Do servidor único centralizado às redes em malha resilientes.
- 04 **Economia & BaaS:** Os 4 fins lucrativos e o aluguel de botnets na Dark Web.

BLOCO 02

Tema 2: DoS e DDoS

Apresentador: Lucas Arantes

- 01 **Negação de Serviço:** Ataque direto ao pilar da Disponibilidade na Tríade CIA.
- 02 **DoS vs. DDoS:** Diferença crítica entre origem única e ataque distribuído.
- 03 **3 Categorias (OSI):** Ataques Volumétricos, de Protocolo e de Aplicação (L7).
- 04 **Amplificação:** Como IP Spoofing e servidores DNS/Memcached multiplicam o ataque.

BLOCO 03

A Conexão Técnica

Apresentador: Felipe & Lucas

- 01 **Sinergia Técnica:** Por que a Botnet é o motor indispensável do DDoS massivo.
- 02 **Ciclo em 5 Fases:** Da infecção inicial ao disparo sincronizado e extorsão.
- 03 **Estudo de Caso Mirai:** Como 600 mil câmeras e roteadores derrubaram metade da internet.
- 04 **Escala Atual:** A evolução dos ataques de Gbps para múltiplos Terabits/s.

BLOCO 04

Impacto e Defesa

Apresentador: Felipe & Lucas

- 01 **Impactos Reais:** Prejuízo financeiro, hospitais, governos e 'Smoke Screen'.
- 02 **Mitigação Corporativa:** Redes Anycast, CDN, WAF e Scrubbing Centers (lavagem de tráfego).
- 03 **Higiene Digital:** Boas práticas para impedir que seus aparelhos virem zumbis.
- 04 **Síntese Final:** Responsabilidade coletiva na segurança da internet.

TESE CENTRAL // CONEXÃO TÉCNICA ENTRE OS TEMAS

Uma **Botnet (rede de máquinas infectadas)** é a principal infraestrutura usada para orquestrar ataques massivos de **DDoS**. Sem um exército distribuído de dispositivos zumbis somando largura de banda e IPs reais pelo mundo, os ataques volumétricos modernos seriam física e tecnicamente impossíveis.

OBJETIVOS DE APRENDIZAGEM

- Identificar as ideias principais de Botnet e DoS/DDoS
- Explicar a arquitetura técnica com clareza e profundidade
- Demonstrar a conexão prática entre rede zumbi e negação
- Analisar casos reais (Mirai) e métodos de mitigação

O que é uma Botnet? O Exército de 'Zumbis' Virtuais

Uma das ameaças mais invisíveis, silenciosas e destrutivas do ciberespaço contemporâneo.

ORIGEM DO TERMO & DEFINIÇÃO

ROBOT (Robô)

Executa tarefas automáticas

+

NETWORK (Rede)

Malha de nós interligados

=

BOTNET

- 01 O Conceito de 'Zumbi Virtual':** trata-se de uma rede de dispositivos conectados à internet — PCs, smartphones, Smart TVs e aparelhos IoT — infectados por malware e controlados remotamente sem que o dono saiba.
- 02 Transformação em Bot:** após a infecção, cada aparelho vira um 'bot' programado para obedecer silenciosamente a um servidor de Comando e Controle (C&C) operado pelo cibercriminoso (Botmaster).
- 03 O Perigo está na Escala:** uma única botnet reúne frequentemente dezenas de milhares ou milhões de máquinas atuando em perfeita sincronia.

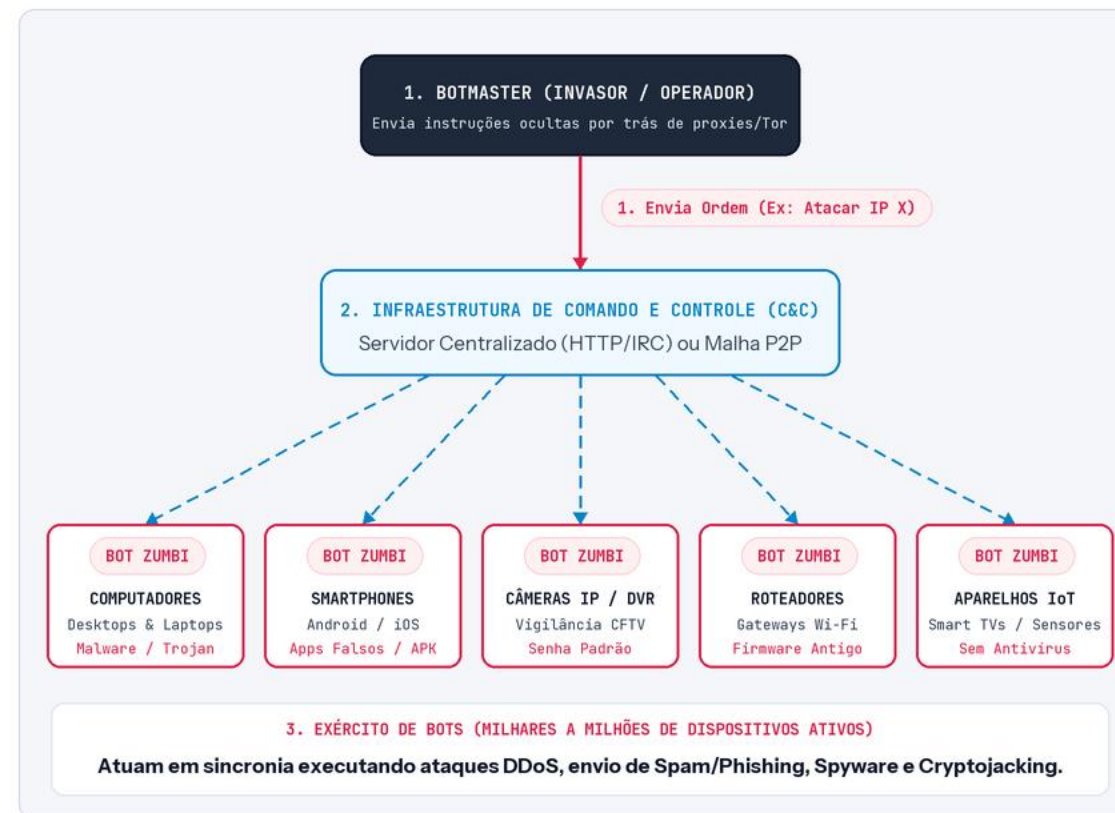
POR QUE O USUÁRIO COMUM RARAMENTE PERCEBE?

O malware é projetado para **não inutilizar o aparelho** (o que levaria a vítima a formatá-lo). Os sinais de infecção são extremamente sutis:

- Ligeira lentidão no sistema operacional ou aquecimento sem uso aparente
- Aumento inexplicável no consumo de dados de internet (upload alto)
- Pequenos picos de uso de CPU/GPU e energia elétrica em segundo plano

ANATOMIA OPERACIONAL DE UMA BOTNET

CADEIA DE COMANDO EM 3 NÍVEIS



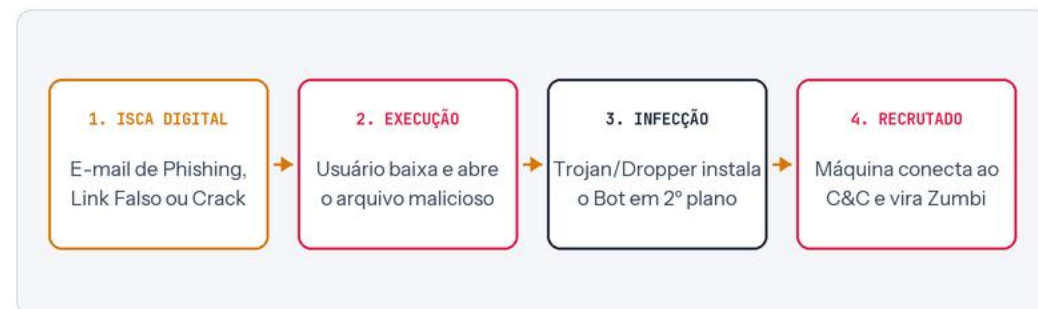
Como Nascem os Zumbis: Os 2 Vetores de Recrutamento

Nenhum usuário escolhe integrar uma rede criminosa. O recrutamento ocorre por manipulação humana ou varredura automatizada.

VETOR 01 // PCs, NOTEBOOKS E SMARTPHONES

Engenharia Social

EXIGE AÇÃO DO USUÁRIO



- 01 **Campanhas de Phishing e Anexos:** e-mails e mensagens falsas simulando bancos, notas fiscais ou entregas que induzem o clique em links ou anexos executáveis.
- 02 **Softwares Piratas e 'Cracks':** uma das maiores portas de entrada em computadores domésticos; ativadores e jogos piratas frequentemente embutem Cavalos de Troia (Trojans).
- 03 **Fontes Não Oficiais:** download de aplicativos fora das lojas oficiais (APKs modificados) ou extensões maliciosas de navegador.

FATOR CHAVE: Explora a confiança, curiosidade ou descuido humano para burlar barreiras.

VETOR 02 // DISPOSITIVOS IoT, CÂMERAS IP E ROTEADORES

Exploração de Vulnerabilidades

ZERO INTERAÇÃO HUMANA



- 01 **Varredura Automatizada Global:** scripts varrem toda a faixa de IPs da internet 24/7 procurando portas abertas (Telnet, SSH, HTTP) em câmeras de vigilância, DVRs e roteadores.
- 02 **Credenciais Padrão de Fábrica:** milhões de aparelhos IoT são instalados sem nunca terem a senha de fábrica alterada, permitindo invasão instantânea por dicionário.
- 03 **Abandono de Firmware:** diferente de PCs e celulares, aparelhos IoT raramente recebem atualizações automáticas de segurança, mantendo brechas abertas por anos.

FATOR CHAVE: Um aparelho IoT vulnerável na internet pode ser infectado em menos de 5 minutos.

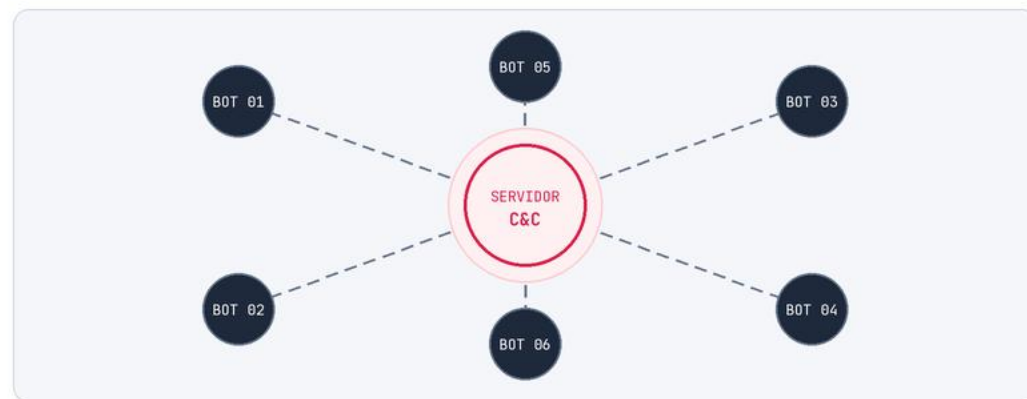
Evolução da Arquitetura: C&C Centralizado vs. P2P

Como o invasor controla milhares de máquinas infectadas — e por que o modelo descentralizado resiste a operações policiais.

MODELO TRADICIONAL (CLIENTE-SERVIDOR)

Comando Centralizado (C&C)

PONTO ÚNICO DE FALHA

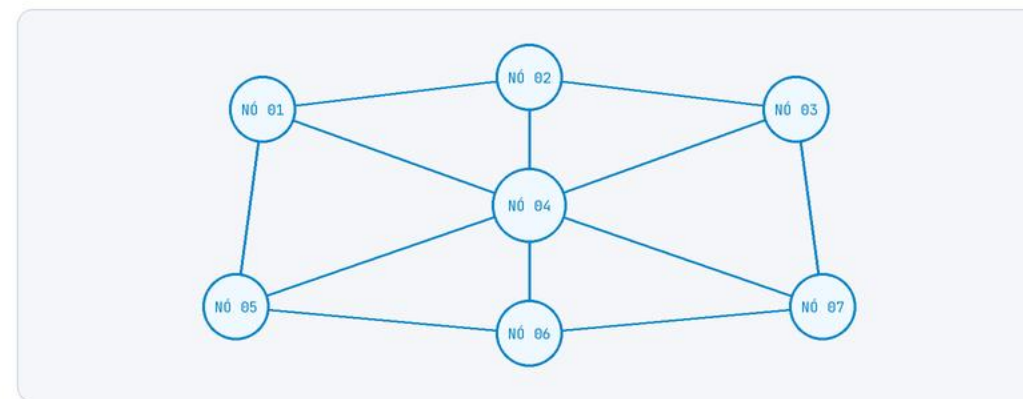


- 01 Hierarquia Estrela:** todos os dispositivos infectados conectam-se diretamente a um único servidor central (via protocolos HTTP ou IRC) para buscar ordens.
- 02 Vantagem para o Criminoso:** arquitetura simples de programar e com repasse imediato de comandos para toda a rede.
- 03 Ponto Único de Falha (SPOF):** se autoridades policiais ou especialistas derrubarem ou bloquearem o servidor central, a botnet inteira fica inoperante de imediato.

MODELO DESCENTRALIZADO EM MALHA

Arquitetura Peer-to-Peer (P2P)

ALTA RESILIÊNCIA



- 01 Comunicação Descentralizada:** não há servidor central; as máquinas infectadas comunicam-se diretamente umas com as outras, atuando como cliente e servidor.
- 02 Reorganização Automática:** se um ou centenas de nós da rede forem descobertos e destruídos, a malha P2P recalcula as rotas e continua operando normalmente.
- 03 Resistência a Takedowns:** desativar uma botnet P2P é extremamente complexo, exigindo infectar a própria malha (sinkholing) ou tomar a chave privada do invasor.

A Economia das Botnets: 4 Funções Principais e BaaS

A criação de uma botnet visa o lucro financeiro, capitalizando o poder computacional e a rede combinada das vítimas.

01 // FUNÇÃO PRIMÁRIA

Ataques de DDoS (Negação de Serviço)

Sabotagem e Queda: os criminosos ordenam que toda a rede acesse um site ou servidor em simultâneo, sobrecarregando o alvo até deixá-lo offline. • **Foco Financeiro:** muito utilizado para extorsão (Ransom DDoS) ou para derrubar concorrentes comerciais.

02 // EVASÃO DE FILTROS

Envio Massivo de Spam e Phishing

Contorno de Bloqueios: disparar milhões de e-mails fraudulentos de um único servidor causaria bloqueio imediato. • **Camuflagem Residencial:** ao distribuir o envio por milhares de computadores domésticos legítimos, os atacantes mascaram a origem e furam filtros anti-spam.

03 // ESPIONAGEM SILENCIOSA

Roubo de Dados e Credenciais (Spyware)

Captura em Segundo Plano: o malware instalado nos zumbis atua como spyware/keylogger, coletando senhas, logins corporativos e dados bancários. • **Comércio Illegal:** os pacotes de credenciais roubadas (logs) são vendidos em lotes no mercado negro.

04 // SEQUESTRO DE HARDWARE

Mineração de Criptomoedas (Cryptojacking)

Processamento Gratuito: minerar criptomoedas exige altíssimo poder de CPU/GPU e consome muita energia elétrica. • **Custo Repassado à Vítima:** ao dividir esse esforço entre milhares de máquinas infectadas, o invasor lucra sem pagar nada por hardware ou eletricidade.

MODELO DE NEGÓCIO DO CRIME // BOTNET-AS-A-SERVICE (BaaS)

O Aluguel de Exércitos Zumbis na Dark Web

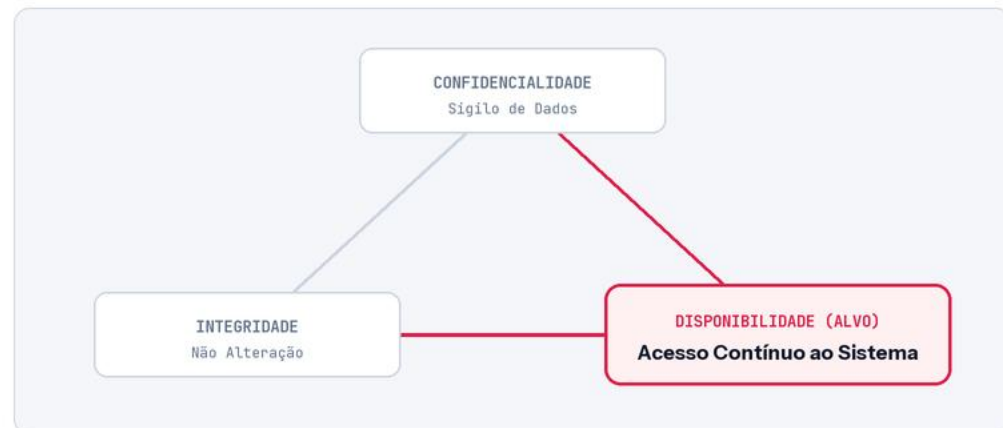
No modelo **Botnet-as-a-Service**, os criadores da botnet não precisam realizar os ataques por conta própria: eles **alugam o poder computacional do seu exército de zumbis** (frequentemente vendidos como 'Stressers' ou 'Booters') para outros criminosos por valores acessíveis por hora ou assinatura.



O que é um Ataque de Negação de Serviço (DoS)?

Diferente de invasões que buscam roubar senhas, o objetivo do DoS é paralisar a operação e impedir o acesso legítimo.

IMPACTO NA TRIÁDE DA SEGURANÇA DA INFORMAÇÃO (CID / CIA)



- 01 Conceito de DoS (Denial of Service):** ataque projetado para tornar uma máquina, servidor ou rede indisponível para seus usuários reais.
- 02 Princípio da Exaustão:** todo servidor possui recursos finitos. O atacante envia mais tarefas ou pacotes do que o sistema consegue processar simultaneamente.
- 03 Resultado Prático:** lentidão extrema, queda de conexões (Time-out) ou erro HTTP 503 (Service Unavailable).

OS 4 GARGALOS TÉCNICOS EXPLORADOS NA NEGAÇÃO DE SERVIÇO

1. LARGURA DE BANDA (LINK)

O 'cano' de rede que liga o servidor à internet fica completamente entupido de pacotes inúteis.

2. TABELA DE CONEXÕES (STATE)

Firewalls e sistemas operacionais têm limite de sessões TCP abertas; novas conexões são recusadas.

3. PROCESSAMENTO (CPU)

Requisições complexas (ex: buscas no banco, criptografia TLS) travam os núcleos do processador.

4. MEMÓRIA RAM / DISCO

Alocação contínua de buffers por requisições incompletas leva à exaustão de memória e reinício.

VISUALIZAÇÃO DO EFEITO DE FILA SATURADA NO SERVIDOR



DoS vs. DDoS: A Diferença de Escala e Complexidade

Por que a evolução do ataque individual (DoS) para o distribuído (DDoS) mudou completamente a defesa cibernética.

ATAQUE CLÁSSICO // ORIGEM ÚNICA

1 ORIGEM → 1 ALVO

DoS (Denial of Service)

```
graph LR; M1[1 MÁQUINA  
IP: 203.0.113.5] --> F1[FIREWALL  
Bloqueia IP  
facilmente]; F1 -.-> S1[SERVIDOR  
Protegido / Online];
```

- **Limitação Física:** a força do ataque está limitada à placa de rede e internet de um único computador.
- **Fácil Mitigação:** basta identificar o IP que está disparando as requisições e bloqueá-lo no Firewall.

ATAQUE MODERNO // ORQUESTRAÇÃO POR BOTNET

MILHÕES DE ORIGENS → 1 ALVO

DDoS (Distributed Denial of Service)

```
graph LR; B1[BOTs ÁSIA (IPs Reais)] --> F2[FIREWALL  
Sobrecarga  
de Tabela]; B2[BOTs EUROPA (IoT)] --> F2; B3[BOTs AMÉRICAS (PCs)] --> F2; B4[SERVIDORES DNS/NTP] --> F2; F2 --> S2[SERVIDOR  
OFFLINE (503)];
```

- **Poder Multiplicado:** soma a banda de milhares de conexões residenciais e comerciais infectadas.
- **Bloqueio Complexo:** como os pacotes vêm de milhares de IPs legítimos espalhados pelo mundo, não há um único IP para bloquear.

CRITÉRIO TÉCNICO	ATAQUE DoS (INDIVIDUAL)	ATAQUE DDoS (DISTRIBUÍDO VIA BOTNET)
Origem do Tráfego	Um único computador ou servidor controlado pelo atacante	Milhares a milhões de dispositivos zumbis (Botnet) globalmente
Volume de Tráfego	Baixo a Moderado (Megabits a poucos Gigabits por segundo)	Extremo / Hiper-Volumétrico (Centenas de Gbps a múltiplos Terabits/s)
Rastreamento e Bloqueio	Simples (regra de bloqueio de IP único na borda da rede)	Altamente complexo (exige Scrubbing Centers, Anycast e IA)
Infraestrutura Usada	Script local ou máquina virtual alugada	Botnet C&C ou P2P + Servidores Refletores (DNS, NTP, Memcached)

Anatomia Técnica: As 3 Categorias de Ataques DDoS

Os ataques distribuídos são classificados de acordo com a camada da rede (Modelo OSI) e o recurso que buscam esgotar.

CATEGORIA 01 // CAMADAS 3 & 4

Ataques Volumétricos

UNIDADE: Gbps / Tbps

Saturação Total da Largura de Banda

Consomem toda a capacidade do link de internet entre o alvo e o provedor, impedindo que qualquer pacote legítimo passe.

PRINCIPAIS TÉCNICAS UTILIZADAS:

- 01 UDP Flood:** disparo massivo de pacotes UDP para portas aleatórias do servidor alvo.
- 02 ICMP (Ping) Flood:** sobrecarga com milhões de requisições de eco (Echo Request).
- 03 Amplificação DNS / NTP:** usa servidores públicos para multiplicar o tamanho do tráfego em até 50.000x.

Representam mais de 65% dos ataques massivos gerados por botnets IoT.

CATEGORIA 02 // CAMADAS 3 & 4

Ataques de Protocolo

UNIDADE: Pacotes/s (Mpps)

Exaustão de Tabelas de Estado (State)

Exploram falhas no funcionamento dos protocolos de rede (TCP/IP) para esgotar a memória de Firewalls e Balanceadores.

PRINCIPAIS TÉCNICAS UTILIZADAS:

- 01 TCP SYN Flood:** inicia milhares de conexões TCP sem nunca enviar a confirmação final (ACK), travando a fila.
- 02 Ping of Death / Fragmentação:** envio de pacotes IP malformados ou fragmentados que travam a remontagem.
- 03 Smurf Attack:** abuso de endereços de broadcast para inundar a rede local do alvo.

Podem derrubar um datacenter mesmo sem saturar 100% do link de internet.

CATEGORIA 03 // CAMADA 7 (APLICAÇÃO)

Camada de Aplicação

UNIDADE: Requisições/s (RPS)

Colapso do Servidor Web e Banco de Dados

Simulam o comportamento de usuários reais fazendo cliques, buscas ou logins pesados via HTTP/HTTPS.

PRINCIPAIS TÉCNICAS UTILIZADAS:

- 01 HTTP GET / POST Flood:** bots solicitam páginas dinâmicas pesadas ou enviam formulários continuamente.
- 02 Ataque Slowloris:** abre conexões HTTP e envia cabeçalhos extremamente devagar para prender os processos.
- 03 Ataques a APIs e Login:** disparam consultas que forçam o banco de dados SQL a trabalhar em 100% de CPU.

São os mais furtivos: usam pouco tráfego de rede, mas exigem alto processamento do servidor.

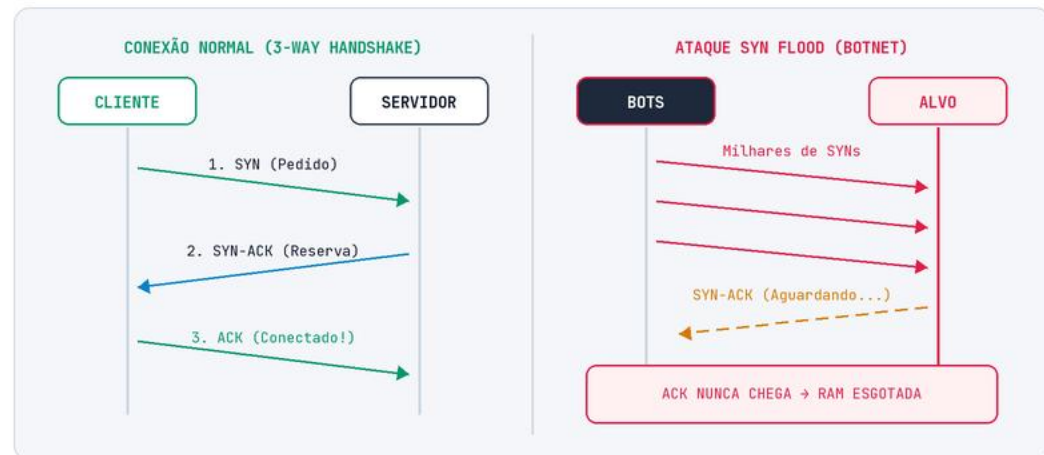
Como o Ataque Funciona por Dentro: SYN Flood e Amplificação

Duas das técnicas mais exploradas por Botnets para derrubar servidores e multiplicar o volume de tráfego.

EXAUSTÃO DE PROTOCOLO // CAMADA 4 (TRANSPORTE)

Ataque TCP SYN Flood

HANDSHAKE INCOMPLETO

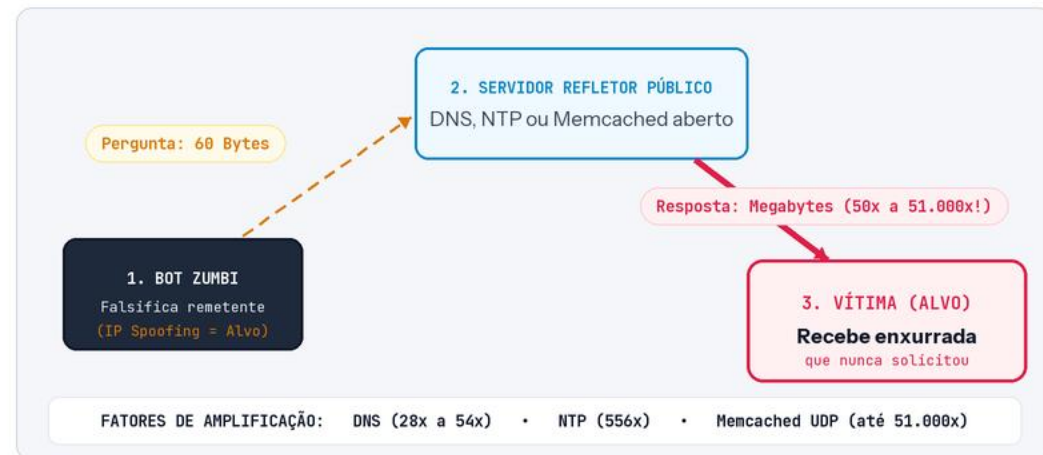


- 01 Exploração do Handshake TCP:** para abrir uma conexão na internet, o protocolo TCP exige 3 passos (SYN → SYN-ACK → ACK).
- 02 Conexões Semiabertas (Half-Open):** os bots enviam milhares de pacotes SYN (muitas vezes com IP falso) e ignoram a resposta SYN-ACK do servidor.
- 03 Colapso da Tabela:** o servidor reserva memória esperando o ACK final de cada pedido até a fila de conexões travar completamente.

MULTIPLICAÇÃO DE FORÇA // IP SPOOFING + REFLEXÃO

Reflexão e Amplificação DDoS

ATÉ 51.000x DE AMPLIFICAÇÃO

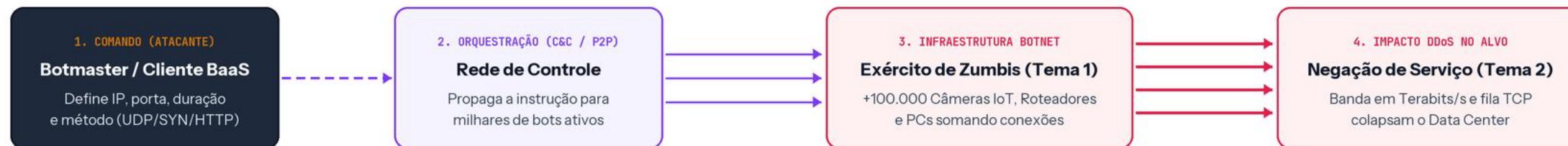


- 01 IP Spoofing (Falsificação de Origem):** o bot envia um pacote UDP para um servidor público (como DNS), mas escreve o endereço IP da vítima no campo de 'remetente'.
- 02 Reflexão Assimétrica:** o bot pede a maior resposta possível com uma pergunta minúscula (ex: pedir todos os registros DNS de uma zona).
- 03 Efeito Megafone:** milhares de servidores públicos respondem pacotes gigantes diretamente para o IP da vítima, multiplicando o poder da botnet.

A Conexão Técnica: Por que a Botnet é o Motor do DDoS?

Uma Botnet (rede de máquinas infectadas) é a principal infraestrutura usada para orquestrar ataques massivos de DDoS.

FLUXO DE ARQUITETURA INTEGRADA // DO RECRUTAMENTO ZUMBI À QUEDA DO ALVO



EQUAÇÃO DA ESCALA: 200.000 Dispositivos Zumbis × 10 Mbps de Upload cada (conexão doméstica comum) = 2,0 Terabits/s de DDoS!

Nenhum computador isolado possui essa banda — somente uma Botnet transforma aparelhos comuns em uma superarma de rede.

PILAR 01 // FORÇA BRUTA

Soma de Largura de Banda

Data centers corporativos contam com links de dezenas ou centenas de Gigabits por segundo. Para saturar essa infraestrutura, o atacante precisa somar a taxa de upload de centenas de milhares de roteadores, câmeras e PCs domésticos simultaneamente.

PILAR 02 // CAMUFLAGEM DE TRÁFEGO

IPs Residenciais Legítimos

Como os bots estão instalados em casas, empresas e celulares reais espalhados por dezenas de países, os pacotes de ataque vêm de endereços IP legítimos. Isso dificulta imensamente para os firewalls separarem quem é cliente real e quem é zumbi.

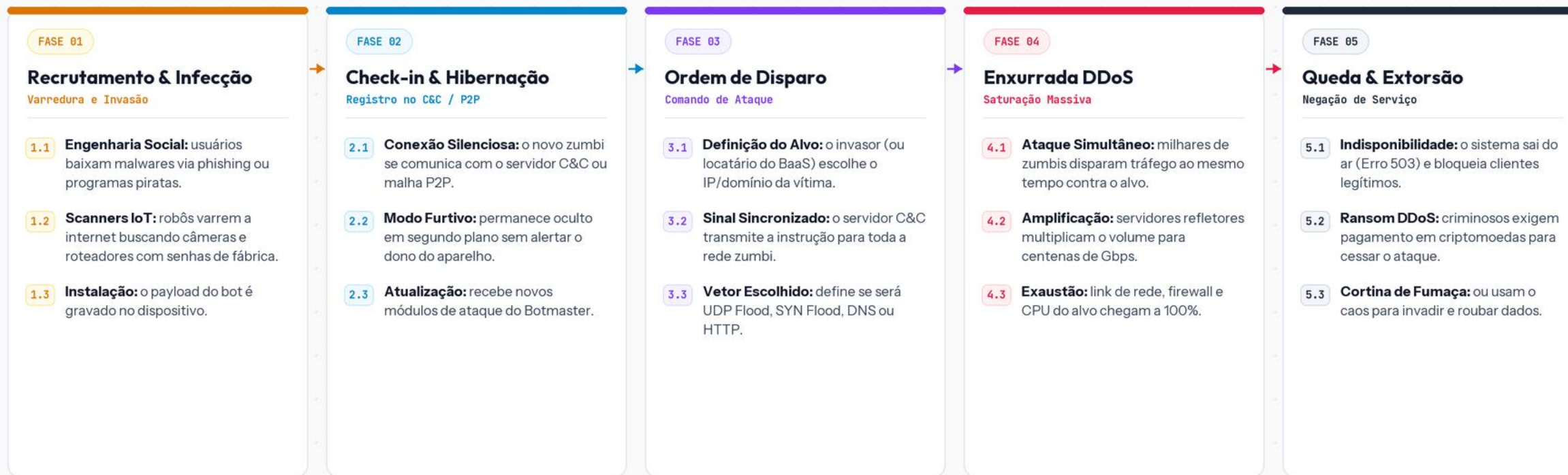
PILAR 03 // BLINDAGEM DO ATACANTE

Anonimato e Custo Zero

O criminoso não gasta com servidores caros nem expõe seu próprio endereço IP no ataque. Quem consome banda, processamento e energia elétrica — e quem aparece nos logs iniciais do servidor atacado — são as vítimas donas dos aparelhos infectados.

Linha do Tempo: As 5 Fases de um Ataque DDoS por Botnet

Passo a passo cronológico desde a infecção silenciosa dos dispositivos até a queda do serviço alvo.



OBSERVAÇÃO OPERACIONAL // ATAQUES EM ONDAS (PULSE WAVE & MULTI-VECTOR)

Nas botnets modernas, as Fases 03 e 04 raramente usam um único método: os atacantes combinam **Ataques Multi-Vetor** (ex: inundação volumétrica UDP para saturar o link + SYN Flood contra o firewall + HTTP Flood na camada 7). Se a equipe de defesa bloqueia um vetor, o Botmaster alterna instantaneamente o comando no C&C para manter o alvo offline.

Estudo de Caso: Botnet Mirai (2016) e Recordes de DDoS

O ataque histórico que provou ao mundo como câmeras e roteadores domésticos podem derrubar gigantes da internet.

OUTUBRO DE 2016 // O MARCO DAS BOTNETS DE IoT

A Botnet Mirai e o Colapso da Dyn DNS

600 mil+

Dispositivos IoT Zumbis

60 senhas

Lista de fábrica usada

1,2 Tbps

Pico de tráfego DDoS

- 01

Como o Mirai Infectou a Rede: o malware varria a internet procurando aparelhos IoT rodando Linux (câmeras IP, DVRs de vigilância e roteadores) com porta Telnet aberta, testando apenas 60 combinações de usuário/senha padrão de fábrica (como admin/admin, root/vizxv).
- 02

O Alvo Estratégico (Provedora Dyn): em 21 de outubro de 2016, a botnet Mirai disparou uma enxurrada massiva de DDoS contra os servidores da Dyn, uma das maiores operadoras de DNS do planeta.
- 03

Efeito Dominó Global: ao derrubar o DNS que traduzia os nomes dos sites, o ataque tirou do ar simultaneamente nos EUA e na Europa dezenas de serviços gigantesco.

SERVIÇOS AFETADOS SIMULTANEAMENTE PELO ATAQUE DA BOTNET MIRAI:

Twitter / X

Netflix

Spotify

GitHub

Reddit

PlayStation Network

PayPal

Airbnb

ESCALADA DE POTÊNCIA // EVOLUÇÃO HISTÓRICA DOS PICOS DE DDoS

A Era dos Ataques em Terabits por Segundo



POR QUE OS ATAQUES CONTINUAM CRESCENDO?

1) Expansão da fibra óptica doméstica:

bots agora têm conexões de 300 a 1000 Mbps em casa; e

2) Explosão de aparelhos IoT:

bilhões de dispositivos conectados sem padrões rígidos de segurança.

Impactos no Mundo Real: Muito Além de um 'Site Fora do Ar'

Quando uma Botnet derruba um serviço via DDoS, os danos atingem finanças, serviços essenciais e a segurança de dados.

IMPACTO 01 // PERDA DIRETA & EXTORSÃO

Prejuízo Financeiro e Ransom DDoS

CUSTO MÉDIO: US\$ 20.000 A US\$ 100.000 / HORA

- 01 Paralisação de Vendas e Transações:** em e-commerces, fintechs e bancos digitais, cada minuto fora do ar representa milhares de transações perdidas.
- 02 Extorsão Cibernética (RDoS):** grupos criminosos lançam um ataque de demonstração de 15 minutos e exigem pagamento em Bitcoin para não manter a empresa offline na Black Friday ou datas críticas.

IMPACTO 02 // RISCO À VIDA E CIDADANIA

Sabotagem de Infraestruturas Críticas

HOSPITAIS, GOVERNOS & TELECOM

- 01 Sistemas de Saúde e Emergência:** ataques DDoS contra hospitais e prontuários eletrônicos atrasam cirurgias, exames e atendimento de urgência.
- 02 Guerra Cibernética e Geopolítica:** botnets são amplamente usadas em conflitos entre nações para derrubar portais governamentais, redes elétricas, transporte público e sistemas bancários nacionais.

IMPACTO 03 // TÁTICA DE DISTRAÇÃO

DDoS como 'Cortina de Fumaça' (Smoke Screen)

ATAQUE COMBINADO

- 01 Distração da Equipe de Segurança (SOC):** enquanto todos os engenheiros correm para conter o ataque DDoS e restaurar o site, os invasores executam uma intrusão silenciosa em paralelo.
- 02 Cegueira de Logs:** o volume massivo de pacotes satura os sistemas de monitoramento (SIEM/IDS), escondendo o roubo de bancos de dados ou a instalação de Ransomware.

IMPACTO 04 // EFEITO DE LONGO PRAZO

Danos de Reputação, SLA e Efeito Colateral

CONFIANÇA & INFRAESTRUTURA

- 01 Perda de Confiança e Multas de SLA:** clientes migram para concorrentes quando um serviço falha repetidamente; provedores B2B pagam multas contratuais por indisponibilidade.
- 02 Prejuízo aos Donos dos Dispositivos Zumbis:** aumento na conta de energia elétrica, desgaste prematuro de hardware, internet lenta e inclusão do IP doméstico em listas globais de bloqueio (Blacklists).

Defesa e Mitigação: Como Deter DDoS e Evitar Virar um Zumbi

O combate exige infraestrutura de mitigação nas empresas e boas práticas de higiene digital nos dispositivos domésticos.

FRENTE 01 // PROTEÇÃO DE SERVIDORES E EMPRESAS

Como Mitigar Ataques DDoS Massivos?

ARQUITETURA DE UM SCRUBBING CENTER (CENTRO DE LIMPEZA DE TRÁFEGO)



- 01 Redes Anycast e CDN (Cloudflare, Akamai, AWS Shield):** distribuem e absorvem o tráfego de ataque em centenas de data centers pelo mundo antes que chegue ao servidor original.
- 02 Scrubbing Centers (Centros de Lavagem):** quando um ataque é detectado, o tráfego é desviado (via BGP) para túneis de limpeza que filtram anomalias e entregam só requisições válidas.
- 03 WAF, Rate Limiting e SYN Cookies:** bloqueiam IPs que fazem requisições excessivas por segundo e evitam que a fila TCP estoure em ataques SYN Flood.

FRENTE 02 // HIGIENE DIGITAL (PREVENÇÃO DE BOTNETS)

Como Impedir que Seus Aparelhos Virem Zumbis

01 // ROTEADORES E APARELHOS IoT

Alterar Credenciais de Fábrica e Ativar 2FA

Trocar imediatamente senhas padrão (admin/admin) de roteadores Wi-Fi, câmeras IP e Smart TVs por combinações complexas e ativar a Autenticação de Dois Fatores (2FA), impedindo invasões automatizadas.

02 // CORREÇÃO DE VULNERABILIDADES

Manter Sistema, Apps e Firmware Atualizados

Instalar sempre as versões mais recentes do sistema operacional, navegadores e firmware de roteadores. As atualizações fecham as brechas de segurança conhecidas antes que scanners as explorem.

03 // BARREIRA CONTRA ENGENHARIA SOCIAL

Evitar Links Duvidosos e Softwares Piratas

Desconfiar de links e anexos em e-mails/mensagens (anti-phishing) e jamais instalar programas piratas, cracks ou aplicativos fora das lojas oficiais — principal vetor de Trojans em PCs.

04 // MONITORAMENTO PROATIVO

Utilizar Antivírus Robusto e Firewall Ativo

Manter um antivírus/EDR atualizado para interceptar e bloquear malwares antes da instalação, além de desativar o acesso remoto (portas Telnet/SSH/UPnP na WAN) no roteador doméstico.

Conclusão: A Segurança da Rede é Coletiva

Síntese das ideias principais conectando Botnets, Ataques de Negação de Serviço (DoS/DDoS) e defesa cibernética.

SÍNTESE 01 // TEMA 1: BOTNET

O Exército Invisível

As Botnets recrutam silenciosamente milhões de PCs, celulares e aparelhos IoT via engenharia social e senhas padrão. Com arquiteturas P2P resilientes e o modelo Botnet-as-a-Service na Dark Web, tornaram-se uma indústria altamente lucrativa.

SÍNTESE 02 // TEMA 2: DoS / DDoS

Ataque à Disponibilidade

Diferente de ataques que roubam dados, o DoS/DDoS mira destruir a Disponibilidade do sistema. Explorando volume de banda, exaustão de protocolo (SYN Flood) ou camada de aplicação (HTTP), impede que usuários legítimos sejam atendidos.

SÍNTESE 03 // CONEXÃO TÉCNICA

Responsabilidade Coletiva

A Botnet é o motor que viabiliza os ataques DDoS massivos. Na internet interconectada, uma câmera ou roteador desprotegido na sua casa deixa de ser apenas um risco individual e pode se tornar a arma usada para derrubar um hospital ou banco.

RECURSOS VISUAIS & DEMONSTRAÇÕES EM TEMPO REAL PARA A TURMA

Mapas de Ataques DDoS Ao Vivo e Animações Curtas

- 01 **Cloudflare Radar & Digital Attack Map (Ao Vivo):** <https://radar.cloudflare.com> | <https://www.digitalattackmap.com> — visualização global de fluxos volumétricos de DDoS e botnets em tempo real.
- 02 **Kaspersky & Radware Live Cyberthreat Map:** <https://cybermap.kaspersky.com> — exibe varreduras de botnets e ataques de negação ocorrendo segundo a segundo entre países.
- 03 **Vídeo Curto (Cloudflare — O que é uma Botnet e DDoS):** explicação visual rápida de 2 minutos ideal para exibir na transição entre os Blocos 02 e 03.

OBRIGADO PELA ATENÇÃO!

Perguntas & Debate

Eixo Temático: Ataques de Negação e Redes Zumbis

APRESENTADORES (DUPLA):

Felipe Augusto
Lucas Arantes