É possível interromper os ataques DDoS em zero segundo?

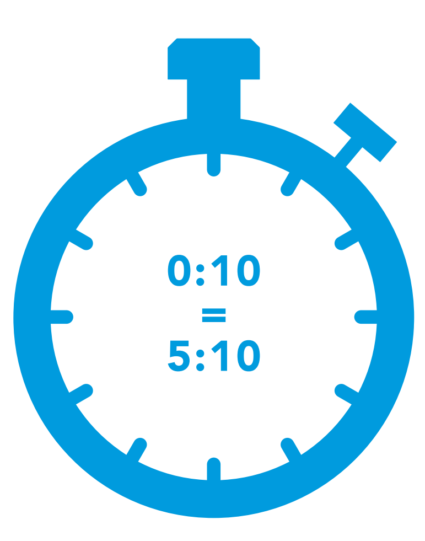
VAMOS DEIXAR CLARO O QUE SIGNIFICA TTM (TIME TO MITIGATE, TEMPO DE MITIGAÇÃO)

O TTM deve ser finito, certo? O tempo entre o momento em que um ataque DDoS inicia e o momento em que seu conteúdo ou suas aplicações são protegidos.

Mas esse não é o real significado dos SLAs (Acordos de Nível de Serviço) dos fornecedores. É necessário entender exatamente quando começa e termina a contagem no relógio.

TENHA CUIDADO COM ESTES CENÁRIOS COMUNS DE FORNECEDORES

FORNECEDOR A



Os controles do Fornecedor A devem analisar um aumento de tráfego por mais de 5 minutos antes de confirmar um ataque DDoS.

O SLA de TTM de 0:10 tem início somente depois da confirmação do ataque.

FORNECEDOR B

Os Termos e condições do Fornecedor B definem TTM como o tempo para implantar um controle de mitigação, uma resposta.

Não há SLA em vigor para interromper o ataque.

FORNECEDOR C

O Fornecedor C compromete-se com a detecção e a mitigação automatizadas em seu SLA de TTM.

Técnicas de defesa manuais e personalizadas para impedir ataques sofisticados não fazem parte desse SLA.

ENTENDA OS TERMOS E CONDIÇÕES

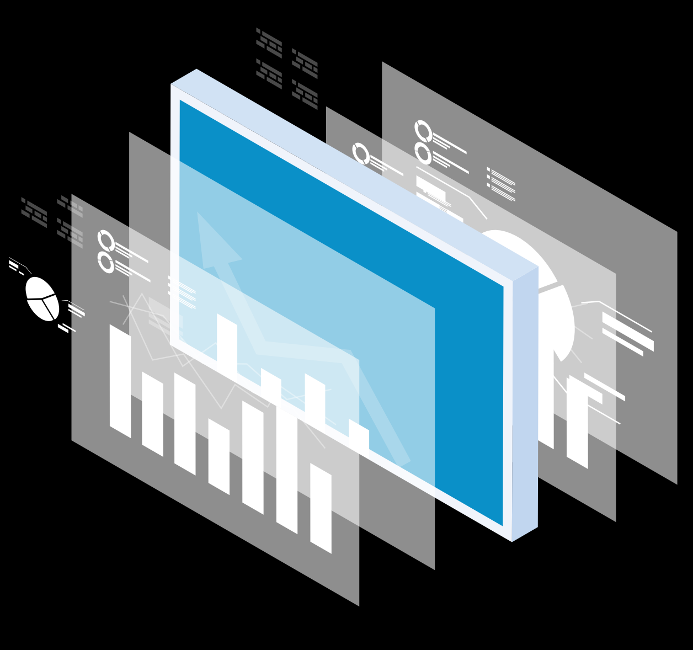
Duvide de expressões, como:

... tempo de resposta ...

No caso de um ataque DDoS contínuo...

... pós-detecção ...

TEMPO DE MITIGAÇÃO DA AKAMAI



Quando **zero significa zero** segundo

Nossos controles proativos de mitigação foram projetados para derrubar ataques DDoS, proporcionando proteção antes mesmo de você perceber que está sob ataque. Esse é o poder da Akamai Intelligent Edge Platform.

TEMPO PARA **detectar ataques** + TEMPO PARA **aplicar controles de mitigação** + TEMPO PARA **bloquear ataques** = **O melhor tempo de mitigação**

OITO ETAPAS PARA A MITIGAÇÃO DE DDOS

A Akamai tem o TTM mais rápido do setor, com uma eficiente combinação de pesquisadores de ameaças, gerentes de incidentes, arquitetos de segurança e tecnologias avançadas de defesa. O SOCC (Security Operations Command Center) da Akamai executa estas etapas:

1. **Detectar** um ataque logo no início com o monitoramento de DDoS sempre ativo.
2. **Alertar** o cliente usando um manual estabelecido.
3. **Gerenciar** o tráfego de clientes com roteamento facilitado sempre ativo.
4. **Analisar** o tráfego e identificar vetores para aplicar a mitigação.
5. **Ajustar** as mitigações aplicadas para otimizar entre falsos positivos e falsos negativos.
6. **Identificar** novos vetores de ataque.
7. **Analisar** o tráfego e identificar os vetores emergentes para aplicar a mitigação continuamente.
8. **Otimizar** as mitigações aplicadas para neutralizar ataques em constante mudança.

OS RISCOS DO ATRASO NO TTM

Quais são as **consequências** do tempo de inatividade?

0:01

Em um segundo, suas aplicações ou seus ativos voltados para a Web ficam indisponíveis.

0:10

Em 10 segundos, as dificuldades para o cliente aumentam, e a produtividade do funcionário diminui.

5:00

Em 5 minutos, a reputação de sua marca é prejudicada, e ocorre perda de receita.

AVALIE SUA POSTURA CONTRA DDOS

Com que rapidez seu fornecedor pode detectar um ataque?

Suas aplicações essenciais estariam disponíveis?

Você sofreria danos colaterais?

Os usuários legítimos seriam afetados?

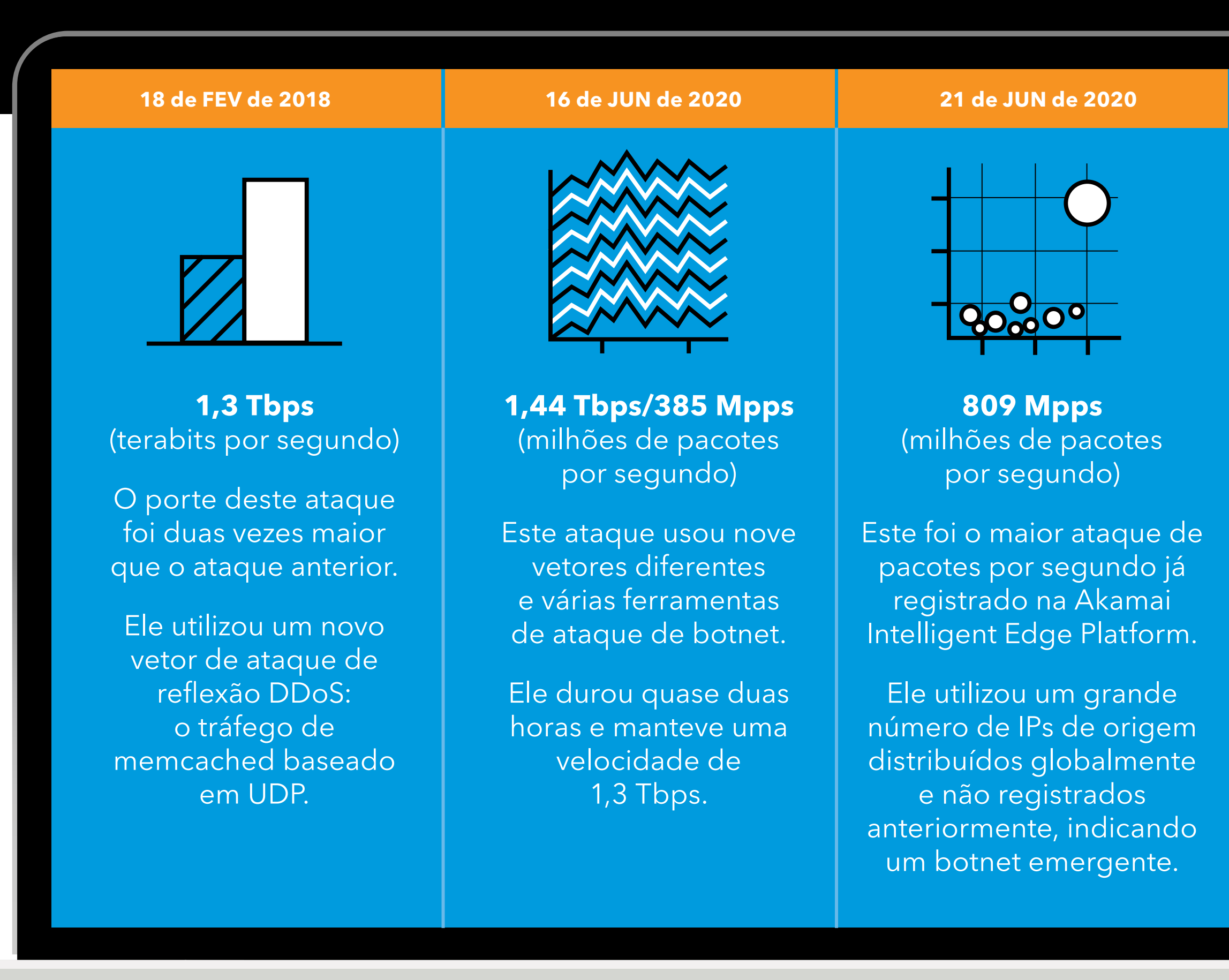
Com que rapidez seu fornecedor pode aplicar contramedidas de mitigação?

Com que rapidez seu fornecedor pode começar a analisar o tráfego?

INSIGHTS DA AKAMAI SOBRE AMEAÇAS

Maiores, mais **complexos** e mais **perigosos**

Os ataques DDoS estão aumentando em tamanhos recorde. Em 2020, observamos atividades de DDoS cada vez maiores e mais complexas; não há precedentes para o número e as combinações de vetores de ataque.



18 de FEV de 2018

1,3 Tbps
(terabits por segundo)

O porte deste ataque foi duas vezes maior que o ataque anterior.

Ele utilizou um novo vetor de ataque de reflexão DDoS: o tráfego de memcached baseado em UDP.

16 de JUN de 2020

1,44 Tbps/385 Mpps
(milhões de pacotes por segundo)

Este ataque usou nove vetores diferentes e várias ferramentas de ataque de botnet.

Ele durou quase duas horas e manteve uma velocidade de 1,3 Tbps.

21 de JUN de 2020

809 Mpps
(milhões de pacotes por segundo)

Este foi o maior ataque de pacotes por segundo já registrado na Akamai Intelligent Edge Platform.

Ele utilizou um grande número de IPs de origem distribuídos globalmente e não registrados anteriormente, indicando um botnet emergente.

A eficácia na defesa exige a combinação de uma plataforma comprovada, de profissionais experientes, além de técnicas e processos refinados.

O **tempo de mitigação** deve estar relacionado à rapidez com que se identifica e bloqueia o tráfego mal-intencionado sem afetar o tráfego e os usuários legítimos.

Por fim, proteger as aplicações essenciais, a infraestrutura e a reputação da marca são a verdadeira medida de sucesso.

FORTALEÇA HOJE MESMO SUA PROTEÇÃO CONTRA DDOS

Saiba como a Akamai pode ajudá-lo a obter uma mitigação de zero segundo.

Saiba mais

Publicado em 11/20