Manual de Treinamento

Proteção DDoS
Versão 1.0

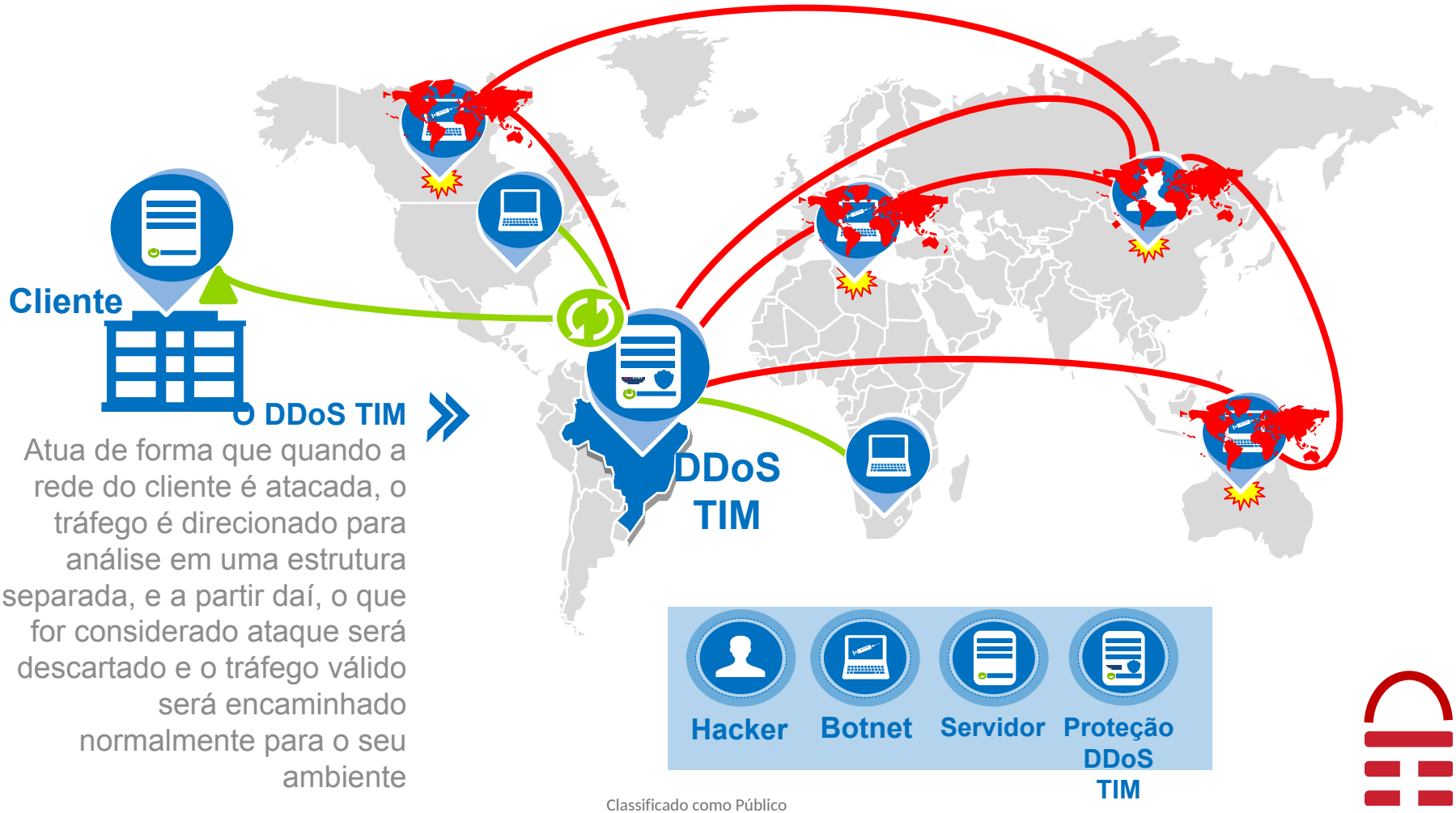
Autor:
Technological Security – SOC

Introdução

Perímetro de Trabalho

INTRODUÇÃO

O serviço Proteção DDoS da TIM monitora o fluxo de informações enviadas ao cliente, e quando é detectada uma alteração do perfil padrão, todo o tráfego é desviado para uma plataforma de limpeza, bloqueando todo ataque e liberando o acesso legítimo.



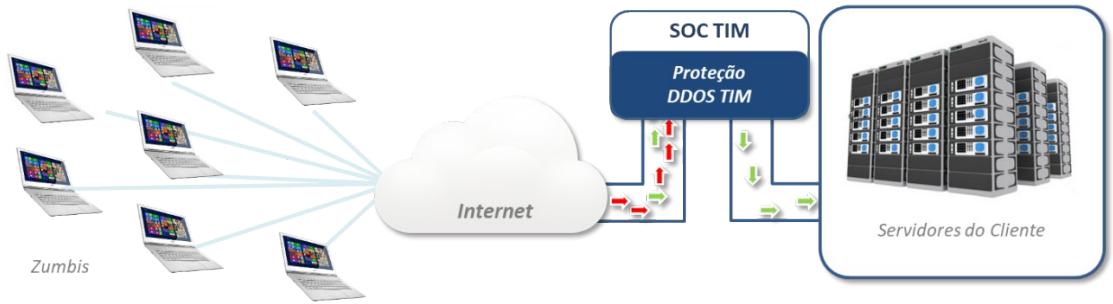
O DDoS TIM

Atua de forma que quando a rede do cliente é atacada, o tráfego é direcionado para análise em uma estrutura separada, e a partir daí, o que for considerado ataque será descartado e o tráfego válido será encaminhado normalmente para o seu ambiente

Modalidade Automática

Na modalidade automática a TIM elenca assinaturas de ataques para mitigação automática. Contratando esta modalidade o CLIENTE aceita previamente que as assinaturas descritas abaixo serão mitigadas automaticamente pela TIM assim que identificadas no tráfego cursado.

Nesta modalidade a atuação da TIM fica restrita aos ataques mitigados automaticamente, outros tipos de ataques que não estão descritos nesta modalidade não terão atuação da TIM

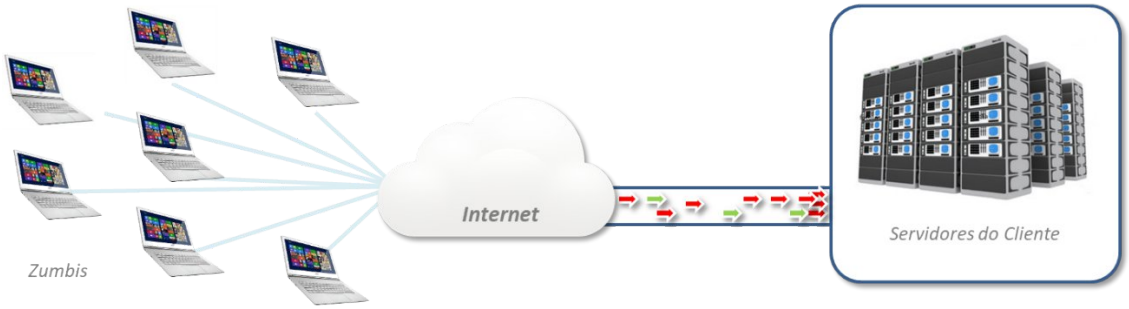


MODALIDADES

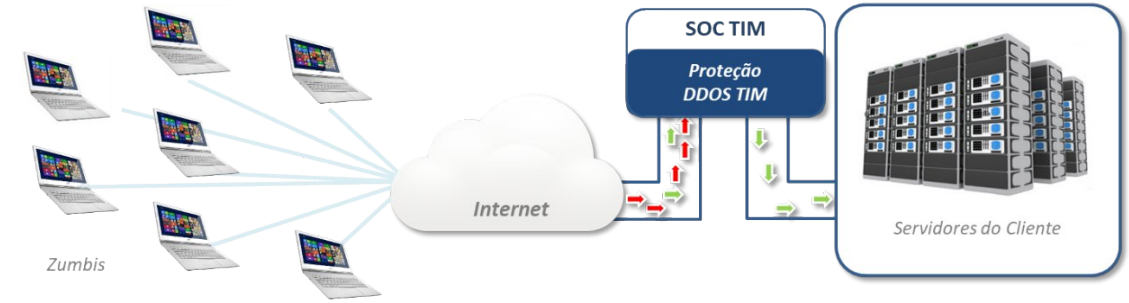
Modalidade Reativa

Na modalidade reativa a TIM não realiza um monitoramento continuo da rede do cliente. Quando da ocorrência de um ataque este deve ser identificado pelo CLIENTE que aciona a TIM através de chamado técnico. Após a abertura de chamado a TIM ativa a plataforma para mitigação do ataque identificado pelo CLIENTE com base no SLA descrito em contrato.

Antes do chamado do cliente



Depois do chamado do cliente

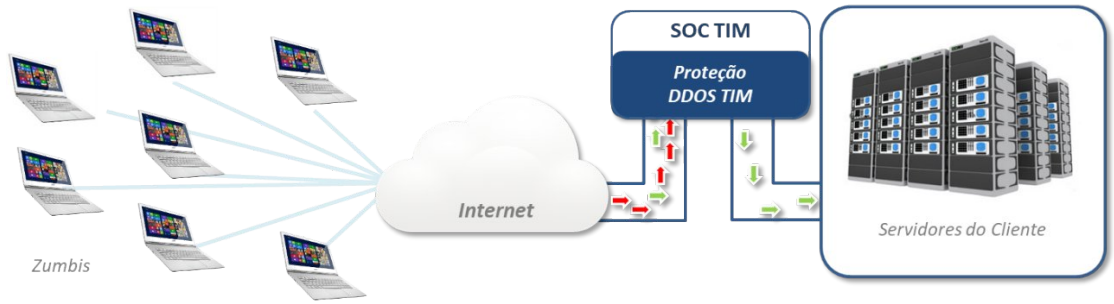


MODALIDADES

Modalidade Proativa

A modalidade proativa monitora todo o tráfego destinado a rede dos clientes e cria um perfil deste tráfego. Quando é detectada uma alteração neste perfil, o tráfego é desviado para uma estação de mitigação e analisado completamente, o tráfego malicioso é descartado e o tráfego legítimo é re-injetado no circuito do CLIENTE.

Para se realizar uma mitigação na modalidade proativa é necessário o tráfego ou assinatura de ataque seja previamente aprovada (para mitigação) pelo CLIENTE. Outros tráfegos e ataques não aprovados previamente pelo CLIENTE serão objeto de questionamento da TIM ao CLIENTE quando da ocorrência de um alarme na plataforma do produto.




DÚVIDAS?
TIM

Obrigado