gocache

Contextualização

Ataques de negação de serviço (Denial of Service) são uma das principais ameaças a empresas que expõem aplicações na internet. O objetivo deste ataque é tirar uma aplicação do ar. Sua forma mais comum é pela exaustão dos recursos que mantém tal serviço no ar, na maioria das vezes, por meio de um volume muito alto de solicitações.

O cenário é ainda mais desafiador quando esse alto volume de solicitações vêm de muitos dispositivos, o que se chama de DDoS (Distributed Denial of Service), porque por mais que o volume total de solicitações seja claramente alto, este volume é distribuído em muitos dispositivos, deixando-os menos evidentes comparados a dispositivos que acessam a aplicação com propósitos legítimos.

Para a pessoa que mitiga um ataque, isso é um problema, pois está sujeita tanto a não conseguir mitigar todos os dispositivos que participam do ataque, deixando um volume ainda muito alto atingir o servidor (falsos negativos), quanto a bloquear usuários legítimos, gerando problemas de experiência aos clientes (falsos positivos).

Para este teste, focaremos na variante que atinge a camada de aplicação (camada 7). Não entraremos em detalhes sobre essa camada, mas o que é importante saber é que as solicitações se resumem a requisições HTTP, cujas características são registradas em logs de servidor. Logo, os dados em que você irá trabalhar são logs de servidor.

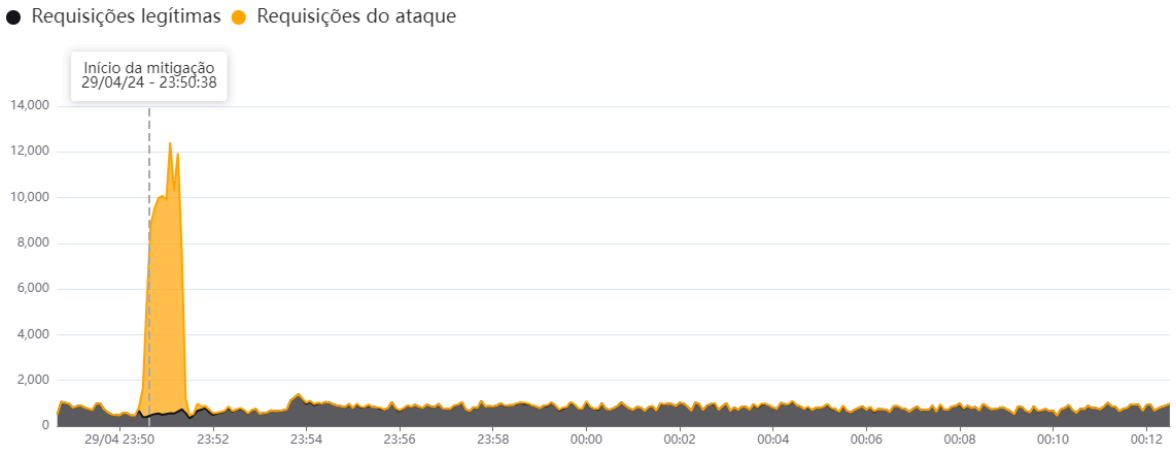
Uma característica interessante deste ataque, é que por mais que o adversário tente se esconder, os comportamentos derivados de seus objetivos e das próprias estratégias de evasão, os entregam. Por exemplo, por mais que um adversário utilize muitos dispositivos para dividir o tráfego, os custos limitam a quantidade de dispositivos que são utilizados, o que faz com que na média eles ainda tenham um tráfego relevante.

Algumas características de dispositivos são difíceis de simular, o que faz com que o tráfego do ataque exiba algumas dessas características em comum. E mesmo que haja características fáceis de simular, pode ficar óbvio que um dispositivo está variando excessivamente suas características ou que elas destoam do padrão normal esperado para o tráfego.

gocache

Problema

O exemplo abaixo mostra o momento que um de nossos clientes recebeu um ataque DDoS. A métrica do eixo Y é a quantidade de requisições em um intervalo de 5s. Nosso objetivo é detectar essa elevação de tráfego repentina o mais rápido possível, entender se trata-se mesmo de um ataque DDoS, e bloquear exatamente as requisições HTTP que fazem parte do ataque, sem prejudicar a audiência verdadeira da aplicação.



Enviaremos para você dois conjuntos de dados, que não tem relação com os dados que geraram o gráfico ilustrado acima. Sua missão será, utilizando linguagem de programação Python e as bibliotecas tradicionais de ciência de dados:

1) Realizar uma análise exploratória dos dados, levantando estatísticas e identificando suas características, com a finalidade de apontar quais atributos são relevantes para a análise.
2) O primeiro arquivo `arquivo_sem_ataque.csv` apresenta um período com tráfego normal, enquanto que o `arquivo_com_ataque.csv` apresenta um período de tráfego normal, seguido de um período com ataque e por fim retorno ao tráfego normal. A partir da sua análise exploratória, explique porque podemos identificar um ataque no segundo arquivo, ou seja, mostrar qual lógica usou para identificar o aumento de tráfego.

3) Utilizando os dados do arquivo `arquivo_com_ataque.csv` desenvolva um modelo para diferenciar quais requisições foram do ataque e quais não foram

gocache

Extra

- Esclareça as premissas utilizadas e o porquê você optou por elas.
- Utilização de controle de versão com git.
- Utilização de ambiente virtual (poetry, pipenv, anaconda, etc.)
- Aplicação de boas práticas de programação.

O uso de LLMs (Large Laguage Models) como ChatGPT, GitHub Copilot, etc. **está autorizado - mas não é incentivado -** caso opte por utilizar, pedimos que aponte, de maneira clara, onde e como você utilizou, preferencialmente, nos enviando uma cópia do log dos prompts utilizados.