Inferring BGP Blackholing Activity in the Internet

Grupo 1
Francisco Caeiro, **47823**
Bruno Andrade, **47829**
António Estriga, **47839**

Qual é o problema que os autores tentam resolver?

Há décadas que é usado o mesmo protocolo para trocar informação de acessibilidade entre as redes da Internet, Border Gateway Protocol (BGP). Apesar disso, pouco foi estudado em relação à maneira como o mesmo protocolo pode restringir essa acessibilidade, através da sua técnica de *blackholing*, onde o tráfego para um certo destino (vítima de DoS) é *dropped*. É uma técnica de mitigação agressiva mas eficaz, rápida e barata comparando com outras alternativas disponíveis.

Neste artigo, os autores desenvolveram e avaliaram uma metodologia para detetar atividade de BGP blackholing automaticamente. Com a ajuda de artigos anteriores e dessa metodologia aplicada em *BGP datasets*, realizaram um estudo aprofundado sobre (i) a adoção da técnica de blackholing por vários tipos de operadores de rede durante os últimos anos (2014-2017), (ii) as práticas atuais, (iii) a eficácia e (iv) o perfil dos destinos "atingidos" por blackholing.

Este problema é relevante?

Tendo em conta que a solução de blackholing é de baixo custo e, pelo que mostram neste artigo, eficaz, o problema de pouco uso desta restrição de acessibilidade é relevante. Esta restrição pode facilitar (e facilita) a mitigação de ataques de negação de serviço (DoS), onde ocorre um grande envio de dados em pouco tempo.

Qual é a sua solução?

Com a explicação do *background* e do funcionamento do blackholing, os autores deste artigo mostram que o BGP possibilita o blackholing usando o *BGP communities attribute*, que pode ser visto como uma *flag* que marca um conjunto de routes. As redes vítimas solicitam blackholing enviando *BGP announcements* aos seus vizinhos BGP, com prefixos de destinatário específicos juntamente com a *blackhole community* apropriada.

Apesar do blackholing "desligar" a vítima da rede, concretizando o objetivo de um DoS, previne dano colateral e saturação pelo caminho do ataque. Para restringir este impacto, os *blackholing providers* aceitam *routes* mais específicas que /24, se forem *tagged* com uma blackholing community.

Em suma, a sua metodologia consistiu em construir um dicionário de communities, tendo em conta que não existe nenhuma convenção universal. Usando este dicionário, conseguiram estudar vários *BGP datasets* públicos e privados para inferir os seus resultados:

- Sendo identificados mais de 250 redes, sendo cerca de 50 IXPs, que oferecem blackholing, o uso do mesmo está a aumentar. Entre 2014 e 2017, estes providers duplicaram, a quantidade de *users* quadruplicou e o número de *prefixes* aumentou num factor de 6. Este aumento pode ter acontecido devido ao aumento de

documentação pública de ataques de DoS e, por conseguinte, de sensibilização de soluções de mitigação de ataques deste tipo.

- Com o estudo dos blackholing users, descobriram que 2% dos prefixes contém addresses marcados por atividade suspeita, em vez de serem vítimas (tal como normalmente é usado).
- Para estudar o seu impacto, foram realizadas medições ativas (com uma *BGP stream*) e passivas (com *IPFIX traffic traces*) durante e depois dos eventos de blackholing. Conseguiram comprovar que este serviço é eficaz a dar drop do tráfego antes de chegar ao destino, sendo que, em quase 50% dos casos, o provider nem aparece no *path* (sabemos da atividade de blackholing através de *bundling* de communities).

Terminam os resultados apontando que é necessário uma standartização das BGP blackhole communities e a documentação de melhores práticas comuns e de *guidelines* relacionadas com o tamanho do blackhole prefix, de modo a reduzir o uso indevido e má configuração não intencional de BGP blackholing (que ainda são origens de grandes problemas de *reachability* atualmente).

Quais são os pontos mais fortes deste artigo? E os seus pontos fracos?

É o primeiro estudo relacionado com o estado e a adoção da técnica de BGP blackholing e, sem dúvida, muito detalhado. É mostrado quantas redes, enumerando-as por tipo, oferecem esta técnica; a quantidade e qualidade de dados de BGP que já existem; onde e como, pelo mundo, é usada (tendo em conta os providers e os users); como é que os DoS estão relacionados com a sua adoção; qual a sua eficácia e como poderia ser melhorada. É uma leitura extensa, cheia de detalhes, mas bem escrita e uma base incontestável para os operadores que usam ou querem usar BGP blackholing ou para outros estudos relacionados com mitigação de ataques DoS.

Porém, é explicado com pouco detalhe como evitar ou conter o envio de blackholing communities falsas. É apenas mencionado num parágrafo (no background) que uma prática comum é os providers requererem algum tipo de autenticação e ainda (nas implicações para a reputação) que blackholing pode ser causado por uma third-party; no caso de esta não ser autorizada, pode ser investigada, determinando o blackholing provider.

Como seria uma extensão deste trabalho?

É referido pelo artigo algumas possíveis extensões, tendo em conta os resultados deste estudo. Em destaque, mencionam que gostariam de estudar a fundo a relação entre a causalidade de eventos de blackholing e ataques DoS.