IPs Maliciosos: Como Fazer a Identificação de um?

O número de Ips maliciosos tem crescido muito aqui no Brasil. Mas afinal, o que é um Ip malicioso e compo ele pode ser identificado?

Um IP malicioso é um 'bot' que fica tentando encontrar vulnerabilidades dentro do seu provedor de internet. Esses bots podem invadir roteadores dos seus clientes e distribuir a internet deles, podem invadir câmeras de segurança, usar a sua rede para minerar criptomoedas como o bitcoin e etc. Enfim, esses bots são utilizados para a prática de crimes cybernéticos.

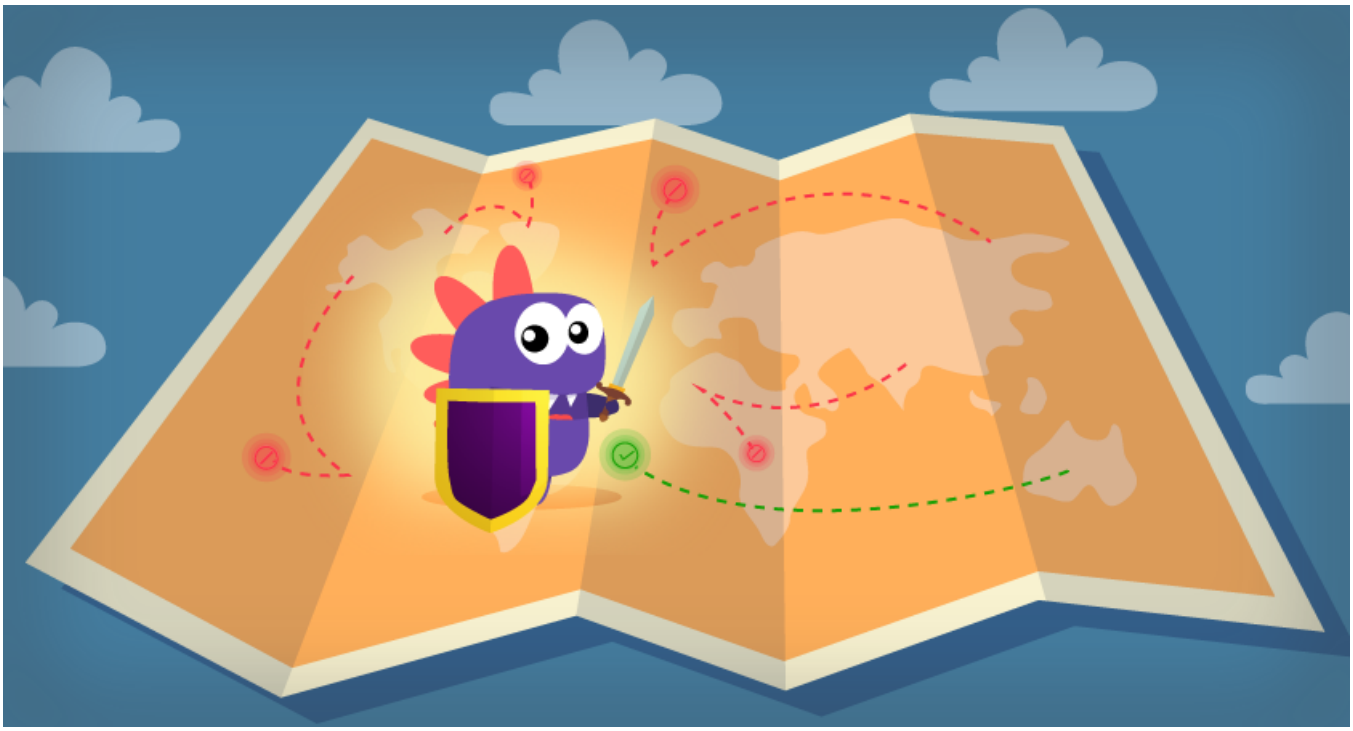
Como os servidores de proteção identificam quais os IPs são ou não maliciosos?

O que você dono de um provedor de internet vai fazer para descobrir se um IP é ou não malicioso é procurar ele no sistema Black Hole (em português, buraco negro). E o bom do sistema Black Hole é que, ao invés de você aplicar algo aos seus equipamentos (o que poderia consumir memória deles, por exemplo) para detectar ips maliciosos, você vai simplesmente mandar esse IP para um sistema armazenado em nuvem e isso vai fazer o mesmo trabalho que um aparelho de identificação de ips maliciosos faria sem custar o processamento das suas máquinas.

O jeito que o sistema Black Hole utiliza para identificar ips maliciosos é analisando o número de vezes que um determinado IP tenta acessar uma rede de modo indevido. Geralmente, esse é o modo que os bots utilizam para invadir redes, tentando vários tipos de senhas para encontrar a vulnerabilidade da rede. Quando esse bot finalmente consegue "acertar" a senha, ele ganha acesso total àquela rede e aos dispositivos que estão conectados a ela.

Isso quer dizer que quando um IP age de forma estranha (ou seja, tentando acessar uma rede diversas vezes e falhando na maioria delas) ele passa a ser considerado um ip malicioso e passa a fazer parte do sistema global do Black Hole.

O Black Hole nada mais é, então, do que uma lista que identifica IPs maliciosos ao redor do mundo.



O Black Hole possui um algorítmo que avalia os IPs; Em outras palavras, um IP que falha ao entrar em uma rede por algumas vezes não é considerado como um ip malicioso. Só são considerados como ips maliciosos aqueles que tentam entrar várias vezes seguidas. Nesse sentido, o algorítmo é muito eficiente.

Você pode assistir ao vídeo que deu origem a este artigo Clicando Neste Link.

Neste meu outro artigo eu falo sobre Provedores de Internet e a Tecnologia da Informação.

Allan Caldas é Digital Influencer a 10 anos, programador, Profissional de TI, Eletrônica e Eletrotécnica.

Proprietário de provedor de provedor internet grande numa empresa especializada em links dedicados corporativos e telefonia.

Trabalha no setor de Telecom a 14 anos.

Autor do treinamento Milionários da Telecom (Curso que ensina a montar um provedor de Internet do Zero).