Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Recomendação de Segurança 001/2016 - CGTI/VPGDI

Em 23 de maio de 2016

Para: Gestores de TI das unidades da Fiocruz

Assunto: Recomendação para minimizar ataques DDoS

Prezados Gestores,

Negação de serviço – ou DoS (*Denial of Service*) – é uma técnica pela qual um atacante utiliza um equipamento conectado à rede para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de **Ataque Distribuído de Negação de Serviço** (DDoS -*Distributed Denial of Service*).

Não existe um tipo único de ataque DDoS e, infelizmente, não há uma solução única para tratamento desse problema. Por isso, conhecer e entender os diferentes tipos de ataques é essencial para que se possa planejar adequadamente as ações a serem tomadas.

Basicamente existem três tipos de ataques DDoS: ataques à camada de aplicação, ataques de exaustão de recursos de *hardware* e os ataques volumétricos. Eles podem ser realizados de forma isolada ou em conjunto.

Segue abaixo algumas das orientações publicadas pelo Cert.br para mitigar esse problema:

Para usuários finais

- Proteger os equipamentos de rede, mantendo atualizado o *firmware* e alterando a senha de administração;
- Proteger os computadores e dispositivos móveis, mantendo os programas instalados com as versões mais recentes e com todas as atualizações aplicadas;
- Usar senhas bem elaboradas, com grande quantidade de caracteres e que não contenham dados pessoais, palavras conhecidas e sequências de teclado;
- Instalar e manter atualizados mecanismos de segurança, como antivírus e *firewall* pessoal.

A postura preventiva deve incluir cuidados como:

- Ficar atento ao clicar em *links*, independente de como foram recebidos e de quem os enviou. Ao acessar *links* curtos usar complementos que possibilitem que o *link* de destino seja visualizado;
- Não considerar que mensagens vindas de conhecidos são sempre confiáveis, pois o campo de remetente pode ter sido falsificado ou elas podem ter sido enviadas de contas falsas ou invadidas;
- Não abrir ou executar arquivos sem antes verificá-los com o antivírus.

Para desenvolvedores Web

- Incorporar práticas de desenvolvimento seguro de *software* logo nas primeiras fases de projeto;
- Seguir boas práticas de programação segura. No site do projeto Top 10 da OWASP (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013) é possível verificar recomendações de como evitar os riscos de segurança mais críticos, como *Cross-Site Scripting* (XSS), referência insegura e direta a objetos e, principalmente, a configuração incorreta de segurança;
- Implementar os recursos de segurança, como por exemplo a validação de dados de entrada, sempre no servidor Web pois, quando implementados apenas no cliente, podem ser burlados tanto pelos usuários, ao desabilitarem o *JavaScript*, como por atacantes, ao usarem ferramentas específicas para interagir com o servidor sem passar pela interface cliente;
- Assegurar que as aplicações gerem *logs* que facilitem o monitoramento, a detecção de erros e a identificação de tentativas de ataque e de acesso indevido;
- Usar sistemas de controle de versão de código, pois caso uma falha seja encontrada será mais fácil identificar quando ela foi inserida e quais as versões que precisam ser modificadas;
- Manter seguros os computadores usados para o desenvolvimento da aplicação, pois se forem invadidos ou infectados podem comprometer também o ambiente de produção;
- Considerar que as aplicações serão executadas em um ambiente hostil e, por isso, devem ser testadas não apenas para os casos de uso, mas também, para os de abuso;

- Usar ferramentas de teste, como a do projeto OWASP Zed Attack Proxy (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project) que analisa o comportamento da aplicação e aponta possíveis vulnerabilidades;

Administradores de Rede

- Manter os equipamentos atualizados, não apenas o sistema operacional, mas também todos os serviços nele executados;
- Excluir os serviços desnecessários (*hardening*), pois quanto menos serviços estiverem sendo executados menores serão as chances de vulnerabilidades neles existentes serem exploradas;
- Configurar adequadamente os serviços, principalmente os que podem ser abusados para amplificação do tráfego;
- Ser cuidadoso ao usar e elaborar senhas e, se disponível, usar verificação em duas etapas;
- Criar usuários distintos para diferentes serviços e funções;
- Monitorar os *logs*, a procura de erros e de tentativas de exploração de vulnerabilidades;
- Verificar o tráfego de entrada na rede à procura de tentativas de acesso não autorizado;
- Verificar o tráfego de saída da rede, a procura de indícios de vazamento de dados, varreduras (*scan*) e acessos indevidos partindo da rede;
- Habilitar filtro *antispoofing*, implementando mecanismos de *egress filtering* que impedem a saída da rede de pacotes com endereço de origem pertencente a uma rede reservada e que não faça parte de um dos blocos de endereços da rede interna;
- Estar atento a *sites* e *blogs* de segurança para ficar ciente de tendências de ataques e novas vulnerabilidades.

Informações adicionais podem ser obtidas no site http://www.cert.br/docs/whitepapers/ddos

Atenciosamente,

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações