Prezados Senhores integrantes de Equipes de Tratamento de Incidentes e Profissionais de Segurança da Administração Pública Federal e Estados,

Segue alerta versando sobre "Ataques de negação de serviço (Denial of Service) em Servidores Web da APF usando Slowloris".

1. Descrição do Problema

O grupo "*Hackativismo"* está organizando a campanha denominada "Operação *Hacking World Cup DoS (Denial of Service)*", por meio de Redes Sociais, com o objetivo de incitar a realização de ataques de negação de serviço a sítios governamentais durante a Copa do Mundo Fifa 2014. A campanha divulga um vídeo que ensina todos os procedimentos para execução do ataque, bem como os links para download das ferramentas necessárias.

A divulgação da operação pode ser encontrada em:

- https://www.youtube.com/watch?v=b1JlalfqaKs
- https://www.facebook.com/events/270074546493671/
- https://www.facebook.com/hackativismo

O ataque explora vulnerabilidades nos servidores web Apache 1.x, Apache 2.x, dhttpd, *GoAhead WebServer, WebSense e outros*, utilizando o programa "*Slowloris*" (http://en.wikipedia.org/wiki/Slowloris).

2. Possíveis Riscos

- Negação de Serviço (*Denial of Service – DoS*):

O ataque executado pelo programa "*Slowloris*" consiste em estabelecer diversas conexões com um servidor web, mantendo-as abertas durante um grande espaço de tempo, causando lentidão e sobrecarga do serviço.

Importante destacar que vários equipamentos realizando ataques de *DoS* simultaneamente a um mesmo host resultam em um ataque de *DDoS (Distributed Denial of Service)*.

3. Sugestões para Mitigação do Problema

Recomendações específicas:

- Limitar o número de conexões permitidas para um endereço IP;
- Impor restrições à taxa mínima permitida de transferência em uma conexão; e
- Restringir o tempo máximo de conexão de um cliente.

Recomendações gerais:

- Revisar a configuração de roteadores, *firewalls e demais equipamentos de rede,* para deter IPs inválidos e filtrar protocolos e portas desnecessários;
- Configurar *os equipamentos de rede* para prevenir inundações (*floods*) nos protocolos TCP/UDP;

- Habilitar a opção de *logging* (logs) nos equipamentos para obter conhecimento e controle adequado acerca das conexões;
- Possuir estreito relacionamento com o Provedor de Serviços da Internet (ISP), com vistas a ajudar no bloqueio de tráfego malicioso destinado à organização;
- Utilizar sistemas de prevenção e detecção de intrusão (IDS/IPS) para detectar o mal uso de protocolos válidos como possíveis vetores de ataque;
- Limitar a taxa do tráfego proveniente de um único host;
- Limitar o número de conexões simultâneas ao servidor;
- Restringir o uso da largura de banda pelos *hosts* que cometam violações; e
- Realizar um monitoramento das conexões TCP/UDP feitas no servidor para identificar padrões de ataque.

Mais informações de como evitar um ataque DoS podem ser encontradas em:

- http://cartilha.cert.br/ataques/ [item 3.7. Negação de serviço (DoS e DDoS)]
- http://www.cert.org/blogs/certcc/post.cfm?EntryID=42
- https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf
- http://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.html
- http://blogs.eset.com.br/laboratorio/2012/03/30/conselhos-para-evitar-um-ataque-de-negacao-de-servico/
- http://www.techrepublic.com/blog/it-security/ddos-attack-methods-and-how-to-prevent-or-mitigate-them/
- http://technet.microsoft.com/en-us/library/cc750213.aspx

Atenciosamente,

Equipe do ***CTIR Gov***