Presidência da República
Casa Militar
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 01/2016 – Comprometimento de servidores de páginas com *Web Shell*

1. Descrição do Problema

Este alerta relata o frequente uso de *Web Shells* como vetor de exploração de servidores de páginas.

1.1 O que é um *Web Shell*

Web Shell é um código que pode ser carregado em um servidor de página para proporcionar administração remota do servidor. Ele é acessado via navegador como se fosse um acesso legítimo ao sítio, iludindo as regras de segurança. Uma vez que o *Web Shell* está carregado no servidor, o atacante utiliza técnicas de exploração para escalar privilégios, executar comandos e scripts, acessar e extrair arquivos do servidor, além de explorar a rede da organização.

Exemplos de *Web Shells*:

- ***China Chopper*** – um programa pequeno e repleto de recursos, tais como de comando e controle e capacidade de força bruta em senhas;
- ***WSO*** – mascara-se como uma página de erro e contém um formulário de login escondido;
- ***C99*** – versão do WSO com funcionalidades adicionais;
- ***B374K*** - baseado em PHP com funcionalidades comuns, tais como, visualização de processos e execução de comandos.

2. Possíveis Riscos

- Controle total do servidor;
- Obtenção de dados sensíveis e credencias de acesso;
- Execução de programas maliciosos;
- Roubo de informações da organização;
- Porta de entrada para ataques mais sofisticados;
- Utilização da infraestrutura da organização para ataques a outras organizações e cidadãos.

3. Ameaças

Os *Web Shells* são carregados nos servidores de página através de exploração de vulnerabilidades ou falhas de configuração tanto das aplicações quanto dos servidores, incluindo:

- *Cross-Site Scripting*;
- *SQL Injection*;
- Aplicações e serviços com vulnerabilidades, por exemplo: WordPress, Joomla, Moodle;
- Vulnerabilidades no processamento de arquivos, como por exemplo: permissão para uploads de arquivos sem filtros e controle de privilégio;
- Vulnerabilidades de *Remote File Include* (RFI) e *Local File Include* (LFI);
- Interfaces de administração expostas.

4. Sugestões para Mitigação do Problema

a. Antes da inserção do *Web Shell* no servidor, normalmente ocorrem ataques que exploram as vulnerabilidades ou falhas de configuração das aplicações e dos servidores. Portanto, é importante identificar e corrigir as vulnerabilidades para evitar possíveis comprometimentos. Deste modo, recomenda-se:

- Manter as aplicações, serviços e sistema operacional atualizados, para proteger de vulnerabilidades conhecidas, que possuem *exploits* de fácil utilização e alta efetividade;
- Aplicar uma política de privilégios mínimos no servidor de página para:
  - Reduzir a capacidade do atacante de escalar privilégio ou explorar outros usuários no mesmo nível;
  - Controlar a criação e execução de arquivos em diretórios.
- Subdividir a rede da organização, dificultando o acesso do atacante a redes com informações sensíveis;
- Certificar-se da configuração segura dos servidores;
- Utilizar sistemas de filtragem de conteúdo, como *firewalls* de aplicação;
- Utilizar sistemas de identificação de alteração de arquivos, em momentos não autorizados ou informados; e
- Definir e executar protocolos de busca e correção de vulnerabilidades nas aplicações.

b. Devido a simplicidade e dinamicidade na utilização dos *Web Shells*, eles podem ser de difícil detecção. Os indicadores a seguir podem indicar que seu sistema tenha sido infectado por um *web shell*:

- Períodos anormais de alto uso do sítio (devido às atividades upload e download);
- Os arquivos com timestamp incomum (por exemplo, mais recente que a última atualização das aplicações web instaladas);
- Arquivos com referências a palavras-chave suspeitas, tais como: cmd.exe, eval, base64_decode;
- Conexões inesperadas nos logs. Por exemplo:
  - Um tipo de arquivo gerando tráfego de rede inesperado ou anormal (por exemplo, conexões POST a arquivo JPG);
  - Logins suspeitos provenientes de subredes internas para servidores DMZ e vice-versa; e
- Quaisquer evidências de execução de comandos, como mudança de diretório, listagem de arquivos, no corpo das URLs requisitadas aos servidores de página.

5. Referências:

https://www.us-cert.gov/ncas/alerts/TA15-314A
http://asd.gov.au/publications/protect/securing-cms.htm
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-china-chopper.pdf
https://www.owasp.org/images/c/c3/ASDC12-Old_Webshells_New_Tricks_How_Persistent_Threats_haverevived_an_old_idea_and_how_you_can_detect_them.pdf
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html
http://www.stratigery.com/phparasites/wso.html
http://resources.infosecinstitute.com/web-shell-detection/

Brasília-DF, 22 de fevereiro de 2016.

Equipe do CTIR Gov