



**Presidência da República**  
**Gabinete de Segurança Institucional**  
**Departamento de Segurança da Informação e Comunicações**  
**Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da**  
**Administração Pública Federal**

## **Alerta nº 05/2014 – Fokirtor Trojan.**

### **1. Descrição do Problema**

*Trojan* ou Cavalo de Troia é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. *Trojan Backdoor* é um código malicioso embutido que permite acesso remoto do atacante ao computador, possibilitando a exploração de vulnerabilidades existentes nos programas instalados.

*Extension Mechanisms for DNS* (EDNS) é um mecanismo utilizado para estender as funcionalidades do protocolo DNS e essencial para a implementação do *DNS Security Extensions* (DNSSEC). Originalmente, uma mensagem DNS possui o tamanho máximo de 512 bytes, o que restringe suporte adicional ao protocolo, como o uso do IPv6 ou assinaturas DNSSEC. EDNS permite adicionar informação diretamente na mensagem, por meio de *pseudo-resource-records* (pseudo-RR) na seção “*additional data*”, mantendo a estrutura básica do cabeçalho DNS.

Uma falha de validação de conteúdo permite a exploração do EDNS por meio da execução de consultas maliciosas. Obtendo sucesso, essa ação possibilita escalar privilégios e controlar servidores remotamente para a realização de ações maliciosas, tais como o acesso a informações sensíveis e a execução de comandos.

*Fokirtor Trojan* é um *malware* projetado para atacar sistemas Linux que se utiliza da técnica de exploração de vulnerabilidades apresentadas pelo uso de EDNS. Seu alvo é o servidor *Berkeley Internet Name Domain* (BIND), que é uma implementação do protocolo DNS.

As versões do BIND impactadas por essa vulnerabilidade são:

- 9.10.0; e
- 9.10.0-P1

### **2. Possíveis Riscos**

O comprometimento do servidor permite ao atacante a execução de comandos e a conexão com sistema de comando e controle (C&C).

O trojan coleta dados sensíveis e, utilizando-se de processos SSH, os criptografa para posterior envio ao atacante, dificultando a identificação dos pacotes por meio dos mecanismos de proteção existentes na organização.

### **3. Sugestões para Mitigação do Problema**

Está disponível o relatório de Exposições e Vulnerabilidades Comuns “*CVE-2014-3859: BIND named can crash due to a defect in EDNS printing processing*” em <<https://kb.isc.org>>.

O relatório sugere a atualização do BIND para uma versão com correção (**BIND 9.10.0-P2**).

A realização de requisições, aparentemente normais, via SSH, permite criptografar qualquer informação ou sequência de comandos executados pelo atacante, tornando-as legítimas e dificultando sua detecção.

Para identificar a presença desse *backdoor* na rede, uma possibilidade seria filtrar o tráfego e procurar pela sequência de caracteres “:!;” (dois-pontos, exclamação, ponto-e-vírgula e ponto), utilizada para exprimir o envio de comandos. Outra forma seria realizar o “dump” do processo “SSHD” e procurar pela sequência a seguir (“*VALUE*” pode ser qualquer valor):

- key=[*VALUE*]
- dhost=[*VALUE*]
- hbt=3600
- sp=[*VALUE*]
- sk=[*VALUE*]
- dip=[*VALUE*]

Referências:

- <http://cartilha.cert.br/malware/>
- <http://www.kaspersky.com/internet-security-center/threats/trojans>
- <http://pt.wikipedia.org/wiki/Backdoor>
- <http://tools.ietf.org/html/rfc6891>
- [http://en.wikipedia.org/wiki/Extension\\_mechanisms\\_for\\_DNS](http://en.wikipedia.org/wiki/Extension_mechanisms_for_DNS)
- <http://en.wikipedia.org/wiki/DNSSEC>
- <https://www.isc.org/downloads/bind/>
- <https://kb.isc.org/article/AA-01166/74/CVE-2014-3859%3A-BIND-named-can-crash-due-to-a-defect-in-EDNS-printing-processing.html>

Brasília-DF, 18 de Junho de 2014

Atenciosamente,

Equipe do CTIR Gov