UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Titulo: Análisis e implementación de DNS RPZ en la Universidad Nacional de La Plata
Autor: Matías Emanuel Ferrigno
Director: Lic. Paula Venosa
Codirector: Lic. Einar Felipe Lanfranco
Carrera: Licenciatura en Sistemas

Resumen

Resultados de análisis alertan que el 91,3% del malware que hoy en día circula en Internet se apoyan en el funcionamiento del servicio de resolución de nombres para su funcionamiento. A partir de esto, se aborda un análisis de DNS RPZ (Response Policy Zones), más genéricamente conocido como DNS Firewall. Un mecanismo que permite restringir o alterar respuestas a recursos de DNS de acuerdo a reglas predefinidas. Como toda regla de firewall, posee una condición a evaluar que actúa de disparador de una acción a tomar. Se brinda un recorrido por los diferentes disparadores y acciones que especifica el borrador de RPZ de la IETF. De esta manera, las Response Policy Zones permiten fortalecer las medidas de seguridad que a través del servicio de DNS pueden implementarse en una red de datos. También se evalúan diferentes opciones que existen para utilizar como fuentes para nuestro DNS RPZ.
Además, se presentan las diferentes tecnologías que se integraron para componer una solución que conste de recolectar los registros arrojados por el módulo RPZ, recolectar los datos que se poseen acerca del host posiblemente infectado, generar un incidente y reportarlo al Sistema de Incidentes de CERTUNLP.

Palabras Claves

Sistema de Resolución de Nombres de Dominio, DNS, Response Policy Zones, RPZ, Seguridad en Redes de Datos, Malware

Conclusiones

Una solución simple como aplicar el concepto de Firewall en el sistema de nombres resultó ser una contramedida satisfactoria para evitar la efectividad del malware que utiliza al DNS como pilar para su funcionamiento. Sin embargo, no deja de ser una pieza de seguridad más, por lo cual hay que abordar la problemática con otros recursos y contramedidas que dispone el administrador como por ejemplo, una política de seguridad y buen uso de la red.

Trabajos Realizados

Para el presente trabajo se llevaron a cabo la siguientes tareas:
- Evaluación y análisis de Response Policy Zones (RPZ)
- Configuración del principal sistema de DNS de la UNLP para que adopte RPZ.
- Integración de diversas herramientas para la realización de un desarrollo que permite la automatización del análisis de los registros de logs arrojados por el módulo RPZ y la generación y reporte de incidentes al CERTUNLP.

Trabajos Futuros

Los trabajos futuros que se proponen son:
- Fomentar el uso de DNS RPZ a los administradores de red de la UNLP.
- Lograr una mayor cobertura de la red que esté bajo el espectro de red analizado por la solución implementada.
- Buscar alguna metodología que permita generar heurísticas basadas en DNS pasivos y/o análisis de tráfico de red para automatizar la incorporación de entradas en una zona RPZ propia.

Fecha de la presentación: AGOSTO 2017