

Antecedentes:

Hoy en día, el DNS es una fuente de información valiosa para detectar un ciberataque. Los artefactos maliciosos utilizados en un ataque por lo general requieren conectarse a un dominio, ya sea para descargarse o para recibir las instrucciones (C&C).

Detectando una petición DNS a un dominio malicioso e interrumpiendo la respuesta, se podría interrumpir un ciberataque en sus etapas tempranas.

Objetivo del proyecto:

Contar con una solución que permita obtener visibilidad sobre las peticiones DNS de otras organizaciones, de tal manera a poder contrastarla contra listas de dominios maliciosos conocidos y poder bloquearlas, así como también poder utilizar dichas detecciones como información accionable para la gestión de incidentes.

De esta manera, la solución permitirá al MITIC ofrecer un **servicio de DNS seguro** a las demás instituciones públicas del Estado Paraguayo.

Funcionalidades mínimas esperadas:

- **Monitorear las peticiones DNS** realizadas por las instituciones y detectar aquellas peticiones sospechosas desde el punto de vista de ciberseguridad (peticiones a C&C maliciosos, principalmente)
- **Bloquear las respuestas DNS** a peticiones maliciosas. La solución debe incluir una lista o base de datos de IPs maliciosas integrada, y poder alimentarse de manera dinámica a partir de fuentes propias de la solución y otras diversas customizadas, incluidas las que el CERT-PY puede conseguir por otras vías (ej.: Talos, Shadowserver, Kaspersky, ESET, Microsoft, otros CSIRTs, etc.).
- Las **alertas de peticiones DNS** sospechosas que hayan sido detectadas y/o bloqueadas deben poder volcarse a algún sistema de correlación de eventos (SIEM o similar).
- La solución debe poder **enviar notificaciones de alertas** sobre peticiones DNS sospechosas que hayan sido detectadas por correo electrónico
- Debe poder identificarse **el origen de la petición** sospechosa. Como mínimo, se debe poder identificar la institución que está realizando la petición. Idealmente, quisiéramos también considerar una opción en la que se pueda llegar al nivel de detalle de qué máquina interna a dicha institución está realizando la petición.
- **Registro de peticiones de DNS**, aún aquellas que no hayan sido detectadas al momento de la petición, tal que si en un futuro se encuentra un dominio sospechoso, se pueda ver en los registros, qué organizaciones y/o equipos se han conectado a él.
- Preferentemente, quisiéramos tener un **dashboard gráfico** en el que se pueda visualizar las alertas e incluso aplicar acciones que fueran necesarias.

Modelos aceptables:

Cualquier tipo de modelo de solución es aceptable, incluido, pero no limitado a:

- ☐ Solución SaaS (software-as-a-service), 100% basado en cloud
- ☐ Appliance / Hardware
- ☐ Software / Virtual appliance

- ☐ Modelos híbridos que combinan hardware, software y/o cloud/SaaS
- ☐ Solución comercial
- ☐ Solución a medida basada en open source ("from scratch")

Características valoradas:

Nos gustaría conocer todas las posibles opciones para resolver estas cuestiones. En esta fase exploratoria de soluciones, valoraremos las siguientes características:

- Mayor **costo-beneficio**: mayor nivel de visibilidad a menor costo (ya sea económico, de esfuerzo o ambos)
- **Sostenibilidad en el tiempo**: una solución cuyo costo de mantenimiento sea el menor posible y cuyo funcionamiento a futuro no estuviera a grandes inversiones monetarias para seguir operando. Por ejemplo: una solución que implique un costo de implementación de 100.000usd y un costo anual de mantenimiento de 5.000usd, por lo general, será preferido a una solución que implique un costo mensual de 5.000usd, ya que en apenas 2 años se estará superando a la primera opción (y ese crecimiento es lineal). Para el análisis de sostenibilidad deberá considerarse por lo menos 5 años.
- **Escalabilidad**: la propuesta debe permitir escalar de una implementación que contemple un número relativamente pequeño de instituciones o cantidad de peticiones, a un volumen mayor, considerando que en un futuro el MITIC pudiera obligar a que todo el Estado utilice este servicio de DNS seguro. La escalación debería requerir el menor costo posible y minimizar la repetición de inversión. Las fases y sus costos deben ser incluidas en las diferentes propuestas que hubiera, de modo a poder tomar la decisión de hasta qué fase puede llegarse, de acuerdo a nuestra disponibilidad financiera.
 - *Obs.: como sería un servicio a demanda que dependerá del interés de los demás OEE, no se puede saber con exactitud la cantidad de usuarios ni el ratio de crecimiento*
- **Arquitectura flexible y multi-tenant**: podría haber instituciones que deseen que MITIC detecte qué máquina interna está haciendo la petición sospechosa, (les es suficiente que le indiquemos la petición y el timestamp). Podría haber instituciones que desean visualizar también ellos las peticiones DNS que realizan sus usuarios y las alertas asociadas a través de un dashboard.
- Son igualmente válidas las soluciones en las que la institución "cliente" debe poner **algo de su parte** (una PC en la que instalar algo virtual, una configuración, etc.), siempre y cuando la inversión y/o el esfuerzo requerido como contraparte no sea excesivo. La estimación de esa contraparte (en términos de costo monetario aproximado) debe incluirse igualmente en la propuesta, aunque no vaya a ser financiado por MITIC, para poder tomar la decisión conociendo ese dato.

Estructura y presentación de propuestas:

Las propuestas deben incluir, como mínimo la siguiente información:

- Descripción técnica de la solución:
 - o Diagramas / Arquitectura propuesta
 - o Explicación de la solución
 - o Funcionalidades incluidas (las deseadas conforme esta solicitud y otras que pudieran ser de interés conforme a la misión y rol del MITIC)

- Propuesta y/o modelo financiero
 - Costo inicial de la solución (hardware/software) – *si lo hubiera*
 - Costos asociados al mantenimiento (licencias anuales, derecho a actualizaciones, etc) – *si lo hubiera*
 - Costos asociados a la implementación, configuración, capacitación, etc. – *si lo hubiera*
 - Planes y/o opciones de crecimiento (año 1: X usuario, año 2: Y usuarios, ...)
 - Obs.: el oferente podrá incluir la cantidad de opciones que desea, bajo los supuestos que desea. Como información adicional, puede considerar que existe un total de aprox. 300.000 funcionarios públicos, incluido docentes, personal de blanco, etc.
- Requerimientos o supuestos previos o necesarios para la implementación:
 - Equipamiento (físico o virtual) que el MITIC y/o las instituciones cliente deberán contar antes de la implementación
 - Costo de feeds de terceros – *si fuera necesario y/o no estuviera incluido*
 - Otros

Se solicita que toda propuesta además incluya la plantilla de funcionalidades completada, como anexo a la propuesta. Las propuestas deben ser enviadas a audiencias_ciber@mitic.gov.py.

Las consultas deben ser enviadas a: ciberseguridad@mitic.gov.py.

audiencias_ciber@mitic.gov.py

Fecha límite: viernes 30 de julio

ANEXO - Plantilla de Funcionalidades de la propuesta presentada

Funcionalidades	Nombre de la Solución:	
	Si	No
Bloqueo de un dominio identificado como malicioso		
Bloqueo de dominios potencialmente maliciosos / sospechosos		
Almacena registro de todas las peticiones DNS detectadas (maliciosas, sospechosas y legítimas)		
Almacena registro de todas las peticiones DNS maliciosas detectadas		
Generación de alertas o algún indicador visual de un potencial incidente / detección de petición DNS para los analistas		
Configuración personalizable de alertas o indicador visual ante la detección de una determinada petición DNS a un determinado dominio.		
Envío de alertas o notificaciones a través mensajes de correo electrónico		
Almacena registros de peticiones durante _____ días o _____ MB (dejar en blanco si no lo hace)		
Manejar múltiples Organizaciones (Multi-tenant)		
Administrar redes, segmentos y políticas de otras organizaciones de manera centralizada		
Filtrar registros de petición de DNS por IP		
Filtrar registros de DNS por organización		
Elaborar zonas DNS personalizables		
Exportación de logs o registros de peticiones DNS		
Se integra o incluye al menos una fuente de listas de dominios maliciosos conocidos, mantenida por una organización o comunidad de inteligencia de amenazas		
Integración con fuentes externas existentes de Listas de dominios maliciosos conocidos (URL Haus, Talos, etc.)		
Integración con fuentes personalizadas a través de APIs		
Integración con herramientas tipo SIEM (Elastic, Splunk, etc)		
Dashboard de Visualización General y global para todas las organizaciones		
Dashboard segmentado por organización, con accesos/roles por organización		