# Informe Técnico Renovación ESET – CORPORACIÓN FINANCIERA NACIONAL

**INFORC ECUADOR**

**17/02/2020**

Contenido

| | |
|---|---|
| **Cliente:** | **CORPORACION FINANCIERA NACIONAL** |
| **Fecha Requerimiento:** | 17/febrero/2020 |
| **Requerido por:** | Ing. Jorge Ortiz |
| **Atendido por:** | Alberto Rivadeneira<br>Technical Support Engineer |
| **Tipo de Requerimiento:** | Informe Renovación de Licenciamiento ESET (ERA)/DESlock |
| **Ciudad:** | Quito / Guayaquil |
| **Software:** | ESET |
| **Producto:** | ESET Endpoint Protection Advanced |

## 1. Detalle de la Protección.

### Informe Técnico de la consola de clientes ESET y DESlock.

Para combatir las nuevas oleadas de malware y ataques de red dirigidos ESET, a inicios del año ha desarrollado en conjunto con los expertos del laboratorio de we live security una tecnología exclusiva incorporada en las nuevas soluciones corporativas Endpoint Solutions, pasando de la versión 5 a la versión 6, dando un salto innovador en el aspecto de manejo de la arquitectura cliente-servidor, administración de políticas y tareas de cliente y servidor, consola de administración web flexible y totalmente funcional, integración de un servidor apache y apache http proxy que reemplaza el antiguo mirror o repositorio local de descarga de la base de firmas, con la integración del proxy a la plataforma de ESET se centraliza la descarga de los clientes a través de este servidor y se puede realizar la replicación de varios sub servidores proxys que replican además de la base de firmas, logs y configuraciones a los equipos regionales. A continuación, se muestran algunas novedades de la versión 6 y las mejoras a nivel de antimalware.

### Bloqueo de exploits

El Bloqueo de exploits se diseñó para reforzar las aplicaciones en los sistemas de los usuarios que sufren ataques de exploits con mayor frecuencia, como los navegadores Web, los lectores de PDF, los clientes de correo electrónico o los componentes de MS Office. Agrega una capa de protección adicional que utiliza una tecnología completamente diferente a las que solo se basan en la detección de archivos maliciosos, y así logra estar un paso más cerca de los atacantes.

Esta tecnología monitorea la conducta de los procesos y busca actividad sospechosa típica de los exploits. Al accionarse, se analiza el comportamiento de los procesos y, si se considera sospechoso, se puede bloquear la amenaza de inmediato en la máquina y enviar metadatos sobre el ataque a nuestro sistema en la nube LiveGrid®. Estos datos se siguen procesando y se correlacionan entre sí, lo que nos permite detectar amenazas desconocidas hasta el momento (llamadas ataques *0-day*) y le proporciona al laboratorio la valiosa inteligencia sobre amenazas.

### Protección contra botnets

La Protección contra botnets suministra otra capa de detección adicional basada en la red para revelar amenazas que se puedan estar ejecutando. Controla las comunicaciones salientes de red en busca de patrones maliciosos conocidos y compara el sitio remoto con una lista negra de sitios maliciosos. Bloquea todas las comunicaciones maliciosas detectadas y se lo informa al usuario.

### Exploración avanzada de memoria

La Exploración avanzada de memoria complementa el Bloqueo de exploits, ya que también se diseñó para fortalecer la protección contra el malware moderno. En un esfuerzo por evadir la detección, los escritores de malware usan ampliamente las técnicas de ofuscación y/o cifrado de archivos. Esto genera problemas en el desempaquetado de archivos y puede suponer un desafío para las técnicas antimalware comunes, como la emulación o la heurística. Para afrontar este problema, la Exploración avanzada de memoria monitorea el comportamiento de los procesos maliciosos y los explora cuando se muestran en memoria. Así se logra una detección efectiva de incluso los tipos más furtivos de malware. A diferencia del Bloqueo de exploits, este método detecta el malware después de su ejecución; es decir, existe el riesgo de que ya se haya llevado a cabo alguna actividad maliciosa. No obstante, constituye un eslabón más en la cadena de protección en caso de que fallen las demás medidas preventivas.

### Protección contra vulnerabilidades

La Protección contra vulnerabilidades es una extensión del Firewall y mejora la detección de las vulnerabilidades conocidas en el nivel de la red. Al detectar las vulnerabilidades comunes en los protocolos de uso más frecuente, como SMB, RPC y RDP, constituye otra importante capa de protección contra el malware en propagación, los ataques que circulan por la red y el aprovechamiento de vulnerabilidades para las cuales aún no se lanzó al público o no se desarrolló la revisión correspondiente.

### ESET LiveGrid®

ESET LiveGrid es un sistema avanzado de alerta temprana compuesta por varias tecnologías basadas en la nube. Ayuda a detectar las amenazas emergentes según la reputación de los archivos y las URL, y utiliza una lista blanca para mejorar el rendimiento de la exploración. Los datos sobre las nuevas amenazas se transmiten a la nube en tiempo real, permitiéndole al Laboratorio de Investigación de Malware de ESET suministrar una respuesta oportuna y una protección consistente en todo momento. Los investigadores de malware en ESET utilizan la información recopilada para crear una instantánea precisa de la naturaleza y el alcance de las amenazas globales, lo que nos ayuda a concentrarnos en los objetivos correctos.

## Anti-Phishing

La tecnología Anti-Phishing te protege de los sitios Web falsos que se hacen pasar por legítimos e intentan extraer contraseñas, información bancaria y otros datos confidenciales. Cuando el equipo del usuario intenta acceder a una URL, el sistema de ESET la corrobora en nuestra base de datos de sitios de phishing conocidos. Si encuentra una correspondencia, se anula la conexión a la URL y se muestra un mensaje de advertencia. Llegado este punto, el usuario cuenta con la opción de correr el riesgo e ingresar de todas formas a la URL o informarnos que la advertencia sobre esta URL probablemente sea un falso positivo.
ESET actualiza la base de datos de Anti-Phishing de manera periódica (los equipos de los usuarios reciben datos sobre nuevas amenazas de Phishing cada 20 minutos).
Aparte de este método sencillo y directo, el Anti-Phishing de ESET también implementa algoritmos proactivos específicos para inspeccionar el diseño visual de los sitios Web y así eliminar aquellos que tratan de imitar sitios legítimos. Por ejemplo, este método sirve para detectar los formularios bancarios falsos.

## Desinfección

Cuando un equipo está infectado con malware, en general alcanza con borrar el archivo o los archivos detectados para desinfectar el sistema. Pero en ciertos casos, por ej., cuando el malware modificó los archivos del sistema operativo, manipuló indebidamente el registro del sistema o cuando un virus parasitario infectó los archivos propios del usuario, la situación se torna mucho más complicada. La mera eliminación del archivo infectado podría causar la pérdida de datos o incluso hacer que el equipo no logre volver a arrancar.
Por lo tanto, se debe tomar un enfoque diferente, como eliminar o desinfectar los archivos infectados. En la mayoría de estos casos, el antivirus instalado directamente lleva a cabo la desinfección. Sin embargo, en algunos casos excepcionales, los pasos para la desinfección son demasiado complejos o simplemente demasiado peligrosos (en lo que respecta a la estabilidad del sistema). Por eso, a veces decidimos lanzar módulos de desinfección auto sostenibles para dicho propósito. Los módulos de desinfección están disponibles en forma gratuita, incluso para quienes no son clientes de ESET.

## Heurística avanzada

La Heurística Avanzada es una de las tecnologías que usa ESET v6 para la detección proactiva. Proporciona la capacidad de detectar malware desconocido mediante el estudio de sus funcionalidades a través de la emulación. La versión más reciente incluye una técnica completamente nueva para la emulación del código, que se basa en la traducción binaria. Este nuevo traductor binario ayuda a evadir las tácticas empleadas por los creadores de malware para sortear la emulación de los programas antimalware. Entre estas mejoras, la exploración basada en ADN también se extendió ampliamente. Permite mejorar las detecciones, que ahora encuentran el malware actual con mayor precisión.

## 2. Objetivos

- Renovación de Licenciamiento ESET Endpoint Protection Advanced.
- Renovación de Licenciamiento DESlock.
- Actualización de versionamiento en productos Endpoint.
- Actualización de versionamiento en Consola de administración ERA.
- Configurar los parámetros de seguridad adecuados para la correcta protección.
- Verificar el estado del servidor proxy de actualización.
- Corrección de posibles problemas que puedan existir.

## 3. Descripción de Actividades:

17 de Febrero de 2020

- Licenciamiento de consola ERA y Equipos con fecha de validez hasta 13/02/2022
- Se revisa el estado actual de la consola ESET Remote Administrator y se ejecuta la actualización a su última versión disponible 7.2 (no se encuentran novedades en hardware y en el performance del servidor.)
- Se realiza una depuración en las políticas existentes, mantenimiento y corrección de configuraciones acorde a las necesidades del cliente.
- Depuración de tareas de cliente y de servidor en estado completo, pendientes y con errores, que encolan a las tareas nuevas.
- En la política principal se realizaron cambios para que se garantice que los equipos actualizan desde el servidor, y no desde el internet para optimizar los recursos de ancho de banda.
- Se Actualizan los paquetes de instalación para endpoints.
- Creación y ejecución de Tareas para la actualización de Endpoints y Servers (reléase actual).
- Instalación/Actualización de protección antivirus en equipos que lo requieren.
- Revisiones y consultas generales

## 4. Versión.

La consola ESET ERA se encuentra actualizada en su última versión, así como la versión de protección en la mayoría de equipos.

## 5. Conclusiones.

- Se actualiza el licenciamiento de ESET tanto en consola de administración como en estaciones de trabajo, la consola se encuentra funcional y se ha realizado todos los correctivos necesarios para brindar la mayor protección a los equipos, y que se pueda adaptar sin inconvenientes a la red de CFN.
- Se han realizado las configuraciones necesarias para el normal funcionamiento de la consola.
- Los equipos se actualizan y reportan con normalidad a la consola ERA a través del agente de red.

## 6. Recomendaciones.

- Realizar backups periódicos de la configuración.
- Escaneos profundos al menos una vez por semana (configurado).
- Verificar que todos los equipos tengan activados sus módulos antimalware y firewall personal.
- Cambiar con periodicidad la contraseña de acceso a la configuración avanzada del antivirus.
- Actualización periódica de protección a los equipos.
- Tener una imagen del servidor principal (opcional).
- Realizar de manera responsable las exclusiones (archivos, ejecutables, unidades de disco) ya que puede ser un repositorio de malware.
- Revisión y depuración de licencias mediante la plataforma ESET License Administrator, https://ela.eset.com/

Hasta aquí el informe.

Alberto Rivadeneira R
**TECHNICAL SUPPORT ENGINEER**
**INFORC ECUADOR**