"¿Cómo detectar Ransomware con FileAudit?"

Nombre del Partner	IS Decisions
Nombre de la Solución	FileAudit
Fecha	30 de julio de 2018

Desarrollado por el Departamento IT
de Macroseguridad y el Equipo de Integraciones

Revisiones:

Versión	Autor	Fecha	Comentarios
1.0	Pablo Lloveras	24/07/18	Release Inicial

Tabla de Contenidos

A Acerca de Macroseguridad

Macroseguridad.org es un Mayorista exclusivo de Soluciones de Seguridad Informática, Líder en seguridad digital y proveedores de seguridad para comercio electrónico e Internet. La compañía atiende a clientes en toda Latino América, México y Brasil.

Macroseguridad.org cuenta con una experiencia de más de 10 años en el área de seguridad y más de 20 años en el conocimiento y manejo de canales de distribución. Sus consultores y profesionales (Partners, Resellers, Integradores y Partners HI-TECH) demuestran un sólido expertise en los servicios y productos que ofrecen, gracias a un sistema orgánico de capacitación continua tanto en el país como en el exterior, con un amplio conocimiento en diferentes industrias para lograr la diversificación que nuestros clientes necesitan.

Los productos que Macroseguridad.org distribuye incluyen: Los Tokens USB y las Smartcards que brindan autenticación robusta, portabilidad y transporte seguro de certificados digitales para Firma Digital. A su vez son un mecanismo de doble factor de autenticación de usuarios en los accesos a la red y garantizar su identidad (VPN, SSLVPN, Web Portal).

También ofrecemos Lectoras de Smartcards (con o sin biometría, de contacto y contactless -NFC-, etc). Dentro del portfolio se ofrece soluciones de Time Stamping, Timbre Digital, HSM (hardware security module), equipos utilizados para el resguardo, generación de claves privadas y Firma Digital Cloud. También se ofrecen soluciones para Medios de pago que cumplen los requerimientos y estándares de Payment Cards y EMV (PCI DSS).

Macroseguridad.org incluye en su portfolio las lectoras biométricas con estándares de seguridad mundial que poseen certificaciones del FBI IAFIS Appendix F, FBI PIV/FIPS 201 y FBI Mobile ID FAP 10 así como también cumplen con los estándares ANSI-378 y ISO19794-2/4.

La empresa también comercializa Tokens OTP (One-Time-Password), dispositivos generadores de números aleatorios para autenticación robusta de usuarios, software para single-sign-on y autenticación.

Macroseguridad.org ofrece Certificados Digitales SSL para validación de dominios web y protección de datos sensibles en la red, con licencia para ilimitados servidores y compatibles con todos los webservers. Contamos con Certificados SSL para dominio único, certificados Wildcard, multi-dominios y certificados que cumplen con el estándar EV SSL (simple y multi-dominio). También certificados para encripción y firma digital de correos corporativos y certificados Code Signing (Firma de Código) que jerarquizan la venta de software vía Internet y evitan los mensajes de error en la descarga y ejecución de software.

Macroseguridad.org ofrece soluciones orientadas a los administradores de servidores como UserLock (orientada a robustecer las políticas de seguridad dentro de un Active Directory) y FileAudit (orientada a la auditoría de carpetas y archivos dentro de un File Server).

Por último, MacroSeguridad.org también distribuye soluciones para la Administración de Derechos Digitales, por ejemplo Dongles - sistemas de protección de software basados en hardware (llaves USB) – para la protección de la propiedad intelectual de los desarrolladores.

Macroseguridad Latino América logra el equilibrio entre las necesidades de las empresas y sus soluciones.

Para más información puede visitar www.macroseguridad.net

B Información de Contacto

Por cualquier consulta, sugerencia o comentario sobre la utilización de la solución o de esta guía, por favor contacte al soporte técnico de MacroSeguridad Latino América:

Mail: soporte@macroseguridad.net

Portal de soporte: https://soporte.macroseguridad.la

Web: www.macroseguridad.net

C Copyright y Marcas Registradas

D Acuerdo de Licencia

MacroSeguridad Latino América

LEA ATENTAMENTE ANTES DE CONTINUAR CON LA INSTALACIÓN DE SOFTWARE Y/O HARDWARE.

Todos los Productos de Software y/o Hardware que en Latinoamérica son distribuidos por Macroseguridad Latino América (MS Argentina SRL) incluyendo, pero no limitados a, copias de evaluación, diskettes, CD ROMs, hardware y documentación, y todas las órdenes futuras, están sujetas a los términos de este Acuerdo de Licencia y Uso. Si Ud. no está de conforme con los términos aquí incluidos, por favor devuélvanos el paquete de evaluación, empaque y contenido prepago, dentro de los diez (10) días de su recepción, y le reembolsaremos el precio del producto, menos los gastos de envío y cargos incurridos.

1. **Uso Permitido** – Respecto del Software el presente es un acuerdo de Licencia de Uso. Usted no adquiere la propiedad sobre el Software objeto de este Acuerdo sino un Permiso (Licencia) para utilizarlo de conformidad a las siguientes especificaciones. TODOS LOS DERECHOS DE PROPIEDAD INTELECTUAL (incluyendo pero no limitando derechos de autor, secretos comerciales, marcas y patentes) relacionados con el Software, Hardware, sus códigos fuentes, guías de usuario y toda otra documentación comprensiva del mismo son de propiedad exclusiva de Macroseguridad Latino América (MS Argentina SRL) o de las compañías que ésta representa. Ud. puede utilizar este Software únicamente en modo ejecutable, utilizándolo sólo en las computadoras de su empresa u organización, y pudiendo hacer sólo las copias adquiridas en el proceso de compra. En relación al Hardware comercializado por Macroseguridad, usted deberá utilizarlo conforme todas las especificaciones y recomendaciones técnicas informadas. En caso de duda, comunicarlas en el portal de soporte **https://soporte.macroseguridad.la**:

   IMPORTANTE PARA DISPOSITIVOS CRIPTOGRÁFICOS: Si el dispositivo criptográfico provisto por MACROSEGURIDAD es utilizado apropiadamente y conforme su destino, en el entorno recomendado (Sistema operativo Windows) y con las PASSWORDS correctas, el mismo no bloquea en ningún caso el acceso a la información.

   Si esto ocurre, no es por un defecto del producto, sino que, se produce para el resguardo de la información contenida en el dispositivo ante intentos no autorizados o erróneos (por impericia o negligencia del usuario), cumpliendo de esta manera su finalidad.

   Se debe tener especial cuidado y precaución en el manejo del dispositivo en el entorno recomendado, así como en el resguardo y respaldo de PASSWORDS de USUARIO y/o ADMINISTRADOR. Al adquirir el producto, el Usuario se compromete a seguir TODAS las recomendaciones técnicas provistas por MACROSEGURIDAD y ante cualquier duda, consultar al equipo de soporte técnico en **https://soporte.macroseguridad.la**

2. **Uso Prohibido** – No puede utilizarse el Software ni el Hardware con otro propósito que el descripto en el apartado 1. El Software o el Hardware o cualquier otra parte del producto no puede ser copiado, realizarse reingeniería, desensamblarse, descompilarse, revisarse, ser mejorado y/o modificado de ninguna otra manera, excepto como específicamente se encuentra admitido en el item 1. Ud. no pude utilizar ingeniería inversa en el Software ni en ninguna otra parte del mismo ni intentar descubrir su código fuente. No está permitido tampoco: (1) usar, modificar, fusionar o sublicenciar el Software, salvo lo expresamente autorizado en este contrato; (2) vender, licenciar o sub-licenciar, arrendar, asignar, transferir, comprometerse o compartir sus derechos bajo esta licencia con terceros ;(3) modificar, desensamblar, descompilar, realizar ingeniería inversa, revisar o mejorar el Software o el intento de descubrir el código de fuente del Software; (4) Colocar el Software en un servidor para que sea accesible a través de una red pública; o (5) utilizar cualquier copia de respaldo o archivo del Software (o permitir a otra persona a usar dichas copias) para cualquier propósito distinto del establecido en la presente Licencia.

3. **Garantía** – Se garantiza el Software y el Hardware está sustancialmente libre de defectos significativos en su manufactura o en sus materiales, por el período legal que corresponda contado desde la fecha de entrega del producto conforme factura. La presente garantía no regirá cuando se trate de errores que pueden ser subsanados fácilmente y no implican afectación del rendimiento, cuando los defectos descubiertos hayan sido modificados o alterados sin consentimiento previo del fabricante o cuando el error provenga del mal uso o negligencia o defectos en la instalación. El reclamo deberá realizarse por escrito durante el período de garantía y dentro de los 7 siete días de la observación del defecto acompañado de prueba de los errores detallados. Cualquier producto que Ud. devuelva al fabricante o a un distribuidor autorizado de Macroseguridad deberá ser remitido con el envío y el seguro prepago.
4. **Incumplimiento de la Garantía** – Para el caso de incumplimiento de esta garantía, Macroseguridad Latino América podrá reemplazar o reparar, a discreción del fabricante y con cargo al adquirente /usuario, cualquiera de los productos involucrados.

CON EXCEPCION DE LO DISPUESTO EXPRESAMENTE EN EL PRESENTE, NO EXISTE NINGUNA OTRA GARANTIA O REPRESENTACIÓN DEL PRODUCTO, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADA A, CUALQUIER GARANTIA IMPLICITAS DE COMERCIALIZACIÓN Y/O ADAPTABILIDAD PARA UN PROPÓSITO PARTICULAR.

5. **Limitación de la Garantía del fabricante y/o Macroseguridad** – La responsabilidad total del fabricante frente a cualquier persona o causa, sea contractual como extracontractualmente, incluyendo negligencia o dolo, no podrá exceder el precio de la unidad de producto por Ud. pagado que ha causado el daño o resulta ser el objeto que directa o indirectamente se encuentra relacionado con el hecho dañoso. En ningún caso Macroseguridad Latino América o el fabricante serán responsabilizados por cualquier daño causado por un acto ajeno, impropio, o negligente en el uso del producto, o el incumplimiento de las obligaciones en el presente asumidas, así como tampoco, por la pérdida de cualquier información, dato, ganancia o ahorro, o cualquier otro daño consecuente o incidental, incluso si el fabricante y/o Macroseguridad Latino América hubiese sido advertido de la posibilidad de daño.
6. **TERMINACIÓN DEL ACUERDO DE LICENCIA**. El Acuerdo se considerará terminado frente al incumplimiento de los términos a su cargo. Al término de este contrato expirará la Licencia otorgada y deberá suspender todo uso posterior del Software, y borrar o eliminar cualquier información vinculada al mismo y de propiedad del fabricante. Los items 2, 3, 4 y 5 se mantendrán a pesar de la finalización del acuerdo.

1 Antes de Comenzar

1.1 Sistemas operativos soportados

Actualmente **FileAudit** soporta las siguientes plataformas:

- Windows 10
- Windows 8
- Windows Server 2012 R2
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP

1.2 Requisitos mínimos de instalación

Antes de comenzar con la instalación deberá verificar que los siguientes requisitos se cumplan:

- El sistema operativo es alguno de los mencionados anteriormente.
- Poseer al menos 60 MB de espacio libre para la instalación. Cada evento registrado por FileAudit consume 0.5 KB de espacio.
- Una de las siguientes bases de datos:
  - ***1.-*** Microsoft Access archivo de base de datos (mdb)
  - ***2.-*** Microsoft SQL Server Express 2008/2008 R2/2012/2014/2016
  - ***3.-*** Microsoft SQL Server 2008/2008 R2/2012/2014/2016
  - ***4.-*** MySQL 5.6 y superior
- FileAudit requiere que los siguientes dos protocolos se encuentren autorizados en los sistemas auditados:
  - ***1.-*** File and Printer Sharing for Microsoft Networks - SMB TCP 445
  - ***2.-*** ICMP - Ping

2 ¿Cómo detectar Ransomware con FileAudit?

De acuerdo a agencias de seguridad como por ej. el FBI, el Ransomware – malware que encripta archivos y carpetas hasta se pague un rescate para la liberación de la información - Hoy en día, se ha convertido en unos de los mayores problemas. FileAudit permite detectar estos ataques de manera temprana permitiendo que el impacto sea mínimo o nulo.

FileAudit juega un rol importante en la protección de los activos de una red contra este tipo de ataques, por lo que a continuación se proveerá una visión de las mejores prácticas de usabilidad así como también un test de encripción práctico, incluyendo los resultados.

2.1 ¿Cómo funcionan los ransomware?

Primero expliquemos cómo funciona un ataque de ransomware.

El ransomware típicamente llega como un adjunto de correo electrónico, el cual es abierto por la víctima, por lo general un empleado desprevenido de la empresa. A través de un exploit o vulnerabilidad, el código malicioso se ejecuta permitiendo descargar e instalar un programa en el equipo de la víctima.

El programa contactará un servidor remoto perteneciente al atacante donde un par de llaves asimétricas son generadas. La llave privada se almacena en el servidor del atacante mientras que las llaves públicas se almacenan en el equipo de la víctima. Una vez creadas las claves, el ransomware empieza a encriptar los documentos a los cuales el usuario tiene acceso utilizando una llave simétrica particular para cada archivo, encriptando cada archivo con su clave particular y agregando al final de cada archivo la llave asimétrica encriptada con la llave pública.

El ransomware lo hace de esta manera ya que encriptar datos directamente con una llave asimétrica es mil veces más lento que con una llave simétrica, aunque en ambos casos el resultado es el mismo. Sin la llave privada, no se puede acceder a la información.

Esto significa que si la víctima no posee un backup de toda la información encriptada, el atacante podrá forzar el pago de un rescate, para obtener la llave privada.

2.2 Defensa en profundidad

Entonces, ¿Cómo podemos protegernos ante un ataque de este tipo? Hay varias medidas preventivas que se pueden tomar:

- Fundamental: Educar a los usuarios para que no abran adjuntos extraños de correo
- Se pueden bloquear archivos con ciertas extensiones de los adjuntos. (por ejemplo ejecutables, archivos no necesarios para los usuarios).
- Se debe garantizar que los programas con permisos para abrir los adjuntos se encuentran actualizados. Por ejemplo, tener la última versión de Microsoft Word o Acrobat Reader.
- Normal users should be disallowed from being able to execute programs from locations they are allowed to write to (e.g. their document folders). They should only be able to launch programs approved by the administrator. In Windows, this can be implemented with AppLocker.
- No se debe permitir, a los usuarios, ejecutar aplicaciones en carpetas donde posean permisos de escritura (por ejemplo su carpeta de documentos). Únicamente se debe ejecutar software pre aprobados por el administrador. En Windows se puede lograr esto utilizando la herramienta AppLocker.
- Las cuentas de administrador no deben ser utilizadas para hacer tareas básicas tales como leer correo, navegar por internet o tareas de oficina normales.
- Los usuarios solo deben poder modificar los archivos necesarios para realizar su trabajo. Archivos para los cuales no existe razón que sean modificados por dichos usuarios, deben restringirse a “solo lectura”.

- Se debe tener el antivirus actualizado en el servidor de correo y en los equipos de trabajo para detectar ataques y protegerse ante ellos.
- Debe existir una forma de detectar la encripción masiva de archivos en servidores. Cuanto antes se detecte un ataque, más temprano podrá detenerlo, lo que significa menor perdida de datos y menor trabajo de reparación. En este paso es donde FileAudit puede ayudarle para alertar estos ataques.
- Se debe tener un backup de todos los archivos en un lugar seguro.

Estas son algunas medidas pero no son todas. Se recomienda siempre crear una política robusta y unificada a fin de evitar pérdida de información.

AppLocker es una excelente línea de defensa, debido a que la mayoría del malware no podrá infectar un equipo si al usuario solo se le permite ejecutar programas, y no escribir desde las carpetas establecidas como “c:\Program files” y “c:\Windows”

Sin embargo, la dificultad se encuentra en que cada vez más aplicaciones basadas en la nube se ejecutan desde el perfil del usuario para poder actualizar automáticamente. Los administradores pueden necesitar controlar muchas excepciones en las reglas de AppLocker, dependiendo en el tipo de aplicaciones que puede ejecutar un usuario. La segunda dificultad es que AppLocker solo se encuentra disponible en las versiones Enterprise y Ultimate de Windows.

2.3 Cómo detectar una encripción masiva de archivos

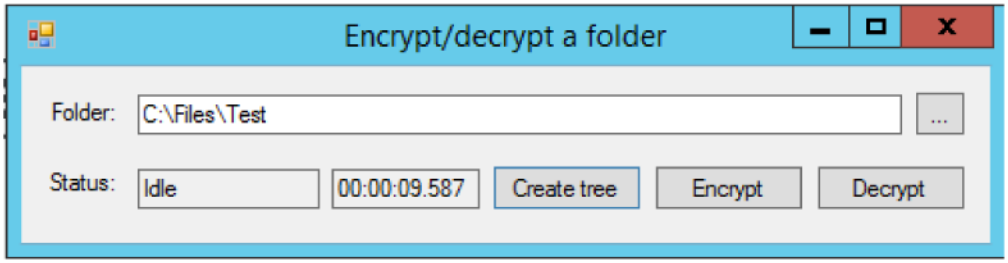
Ahora sabemos qué papel puede tener FileAudit en nuestra defensa, entonces ¿Cómo se configura?

Si el ransomware se encuentra encriptando archivos en una carpeta o unidad auditada por FileAudit, varias alarmas se dispararán en FileAudit por lo que podemos detectarlo rápidamente.

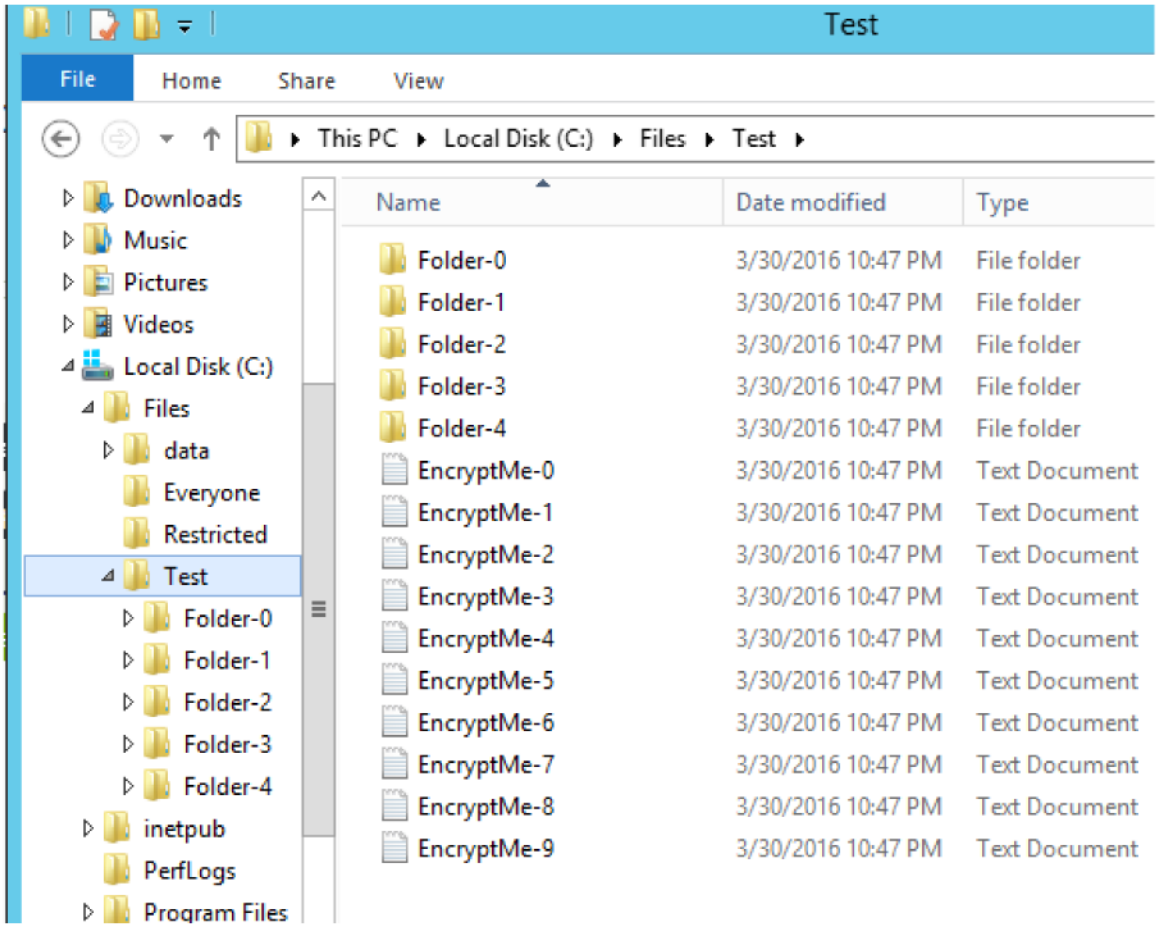
Pero, ¿Qué tipo de registros se generan al encriptar un archivo? Primero, el contenido del archivo debe ser leído para poder ser cargado en la memoria. Luego, la información es encriptada en la memoria, la información encriptada se escribe en un nuevo archivo y por último el archivo original es eliminado.

En consecuencia se deben ver tres operaciones consecutivas sobre archivos en Fileaudit: una lectura, una escritura y un borrado. Para poder detectar un ataque masivo de encripción en un servidor de archivos debemos establecer tres alertas masivas (una por cada acción). Si ocurren las tres alertas simultáneamente probablemente estemos ante un ataque masivo de encripción.

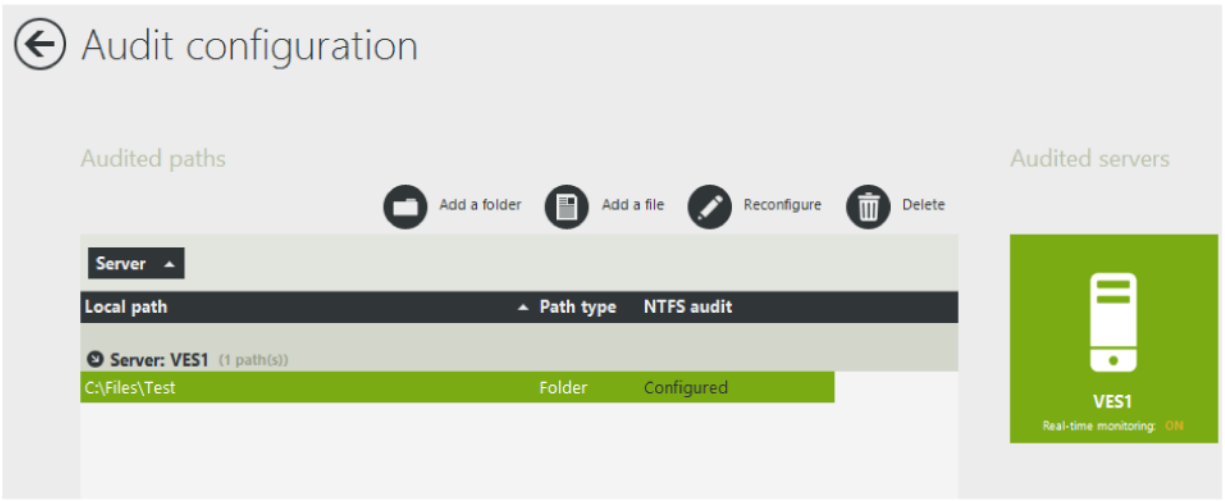
Para probar esto utilizamos una herramienta de encripción creada para este caso para encriptar los archivos de una carpeta específica.



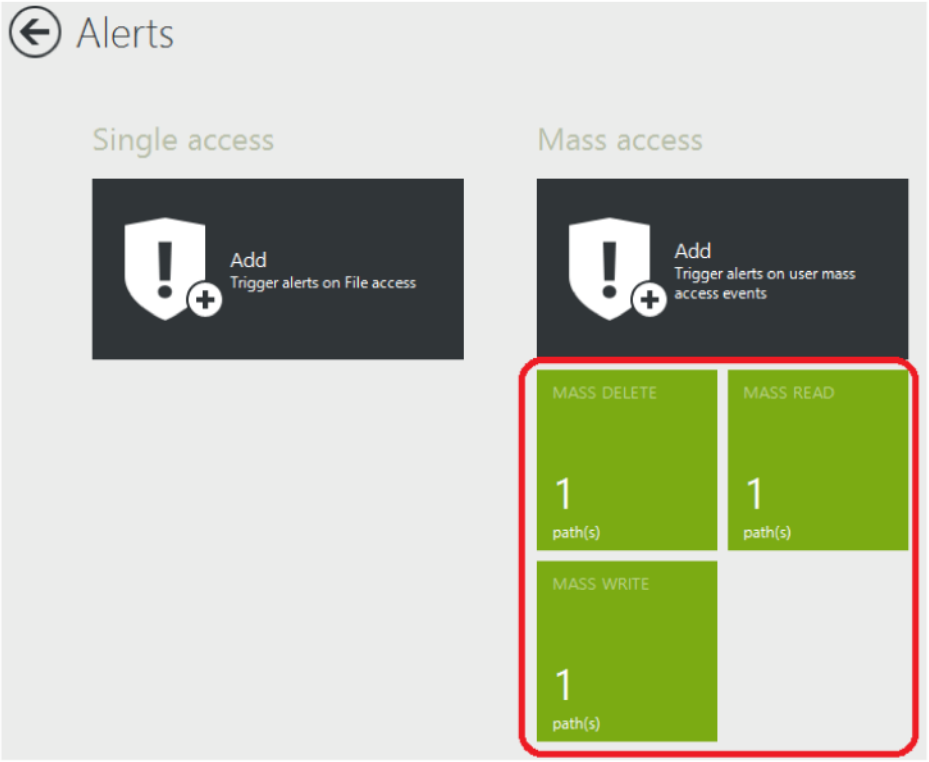
La herramienta permite la generación de un árbol de carpetas con muchos archivos dentro. El nombre de los archivos coincidirán con el patrón “EncrypteMe*.*” para evitar cualquier error luego cuando realicemos la encripción. Los archivos que no coincidan con este patrón no serán encriptados. En este ejemplo habrá 8000 archivos dentro de la carpeta.



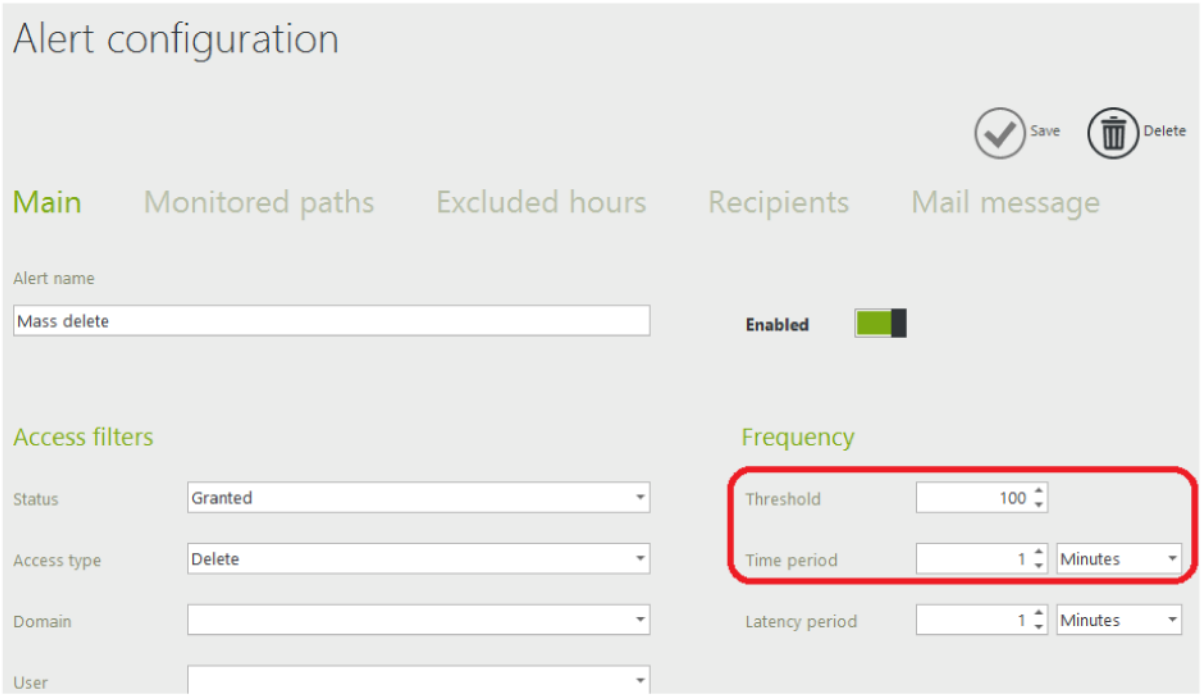
Una vez generado el árbol de carpetas debemos configurar la carpeta para que sea auditada por FileAudit.



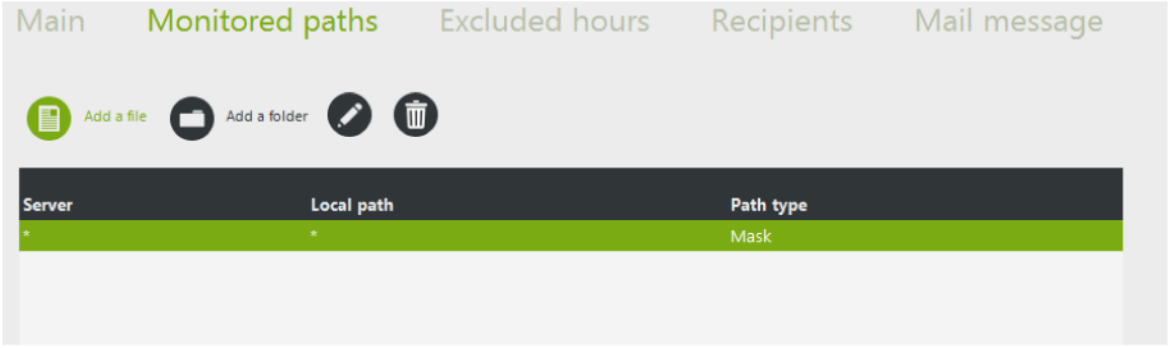
Luego podemos crear tres alertas masivas en FileAudit filtradas por “Access Type” respectivamente: “Read”, “Write” y “Delete”.



Por el momento, dejamos los intervalos por defecto después veremos si debemos ajustarlos o no.



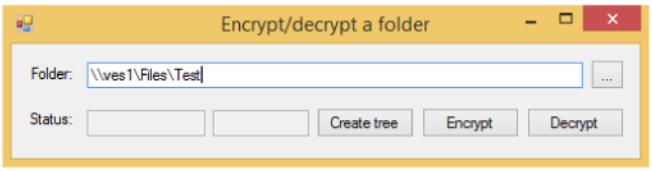
En las alertas agregadas a los monitores auditados por FileAudit especificamos el asterisco (*) para monitorear todos las carpetas auditadas.



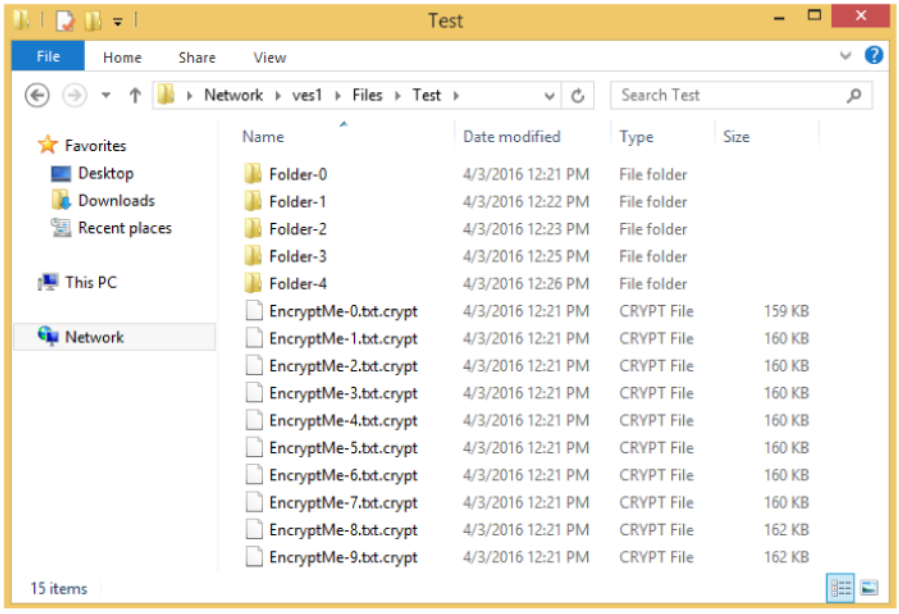
Cuando terminemos, guardamos el alerta y nos aseguramos de que las configuraciones de SMTP sean correctas.

2.4 Ejecutando la simulación de ransomware

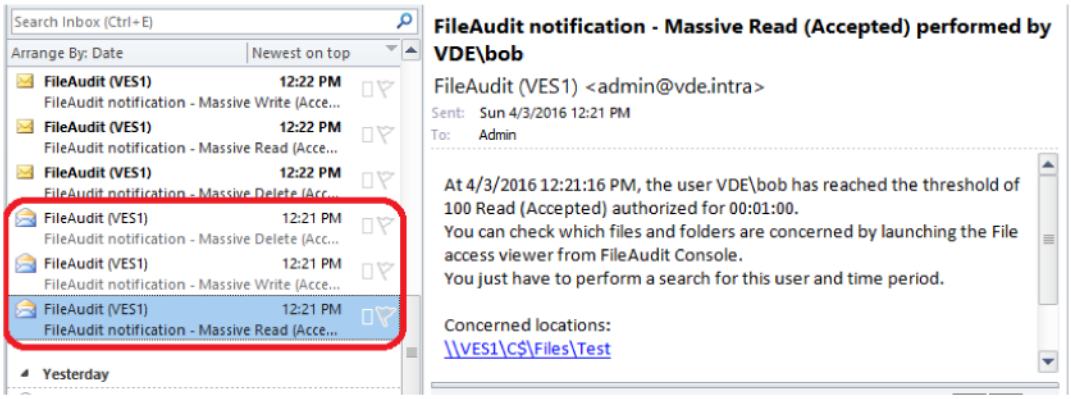
Ahora que FileAudit se encuentra configurado, iniciamos sesión en un equipo de trabajo con una cuenta de usuario, iniciamos la herramienta de encripción y especificamos la carpeta. Luego hacemos click en “Encrypt”.



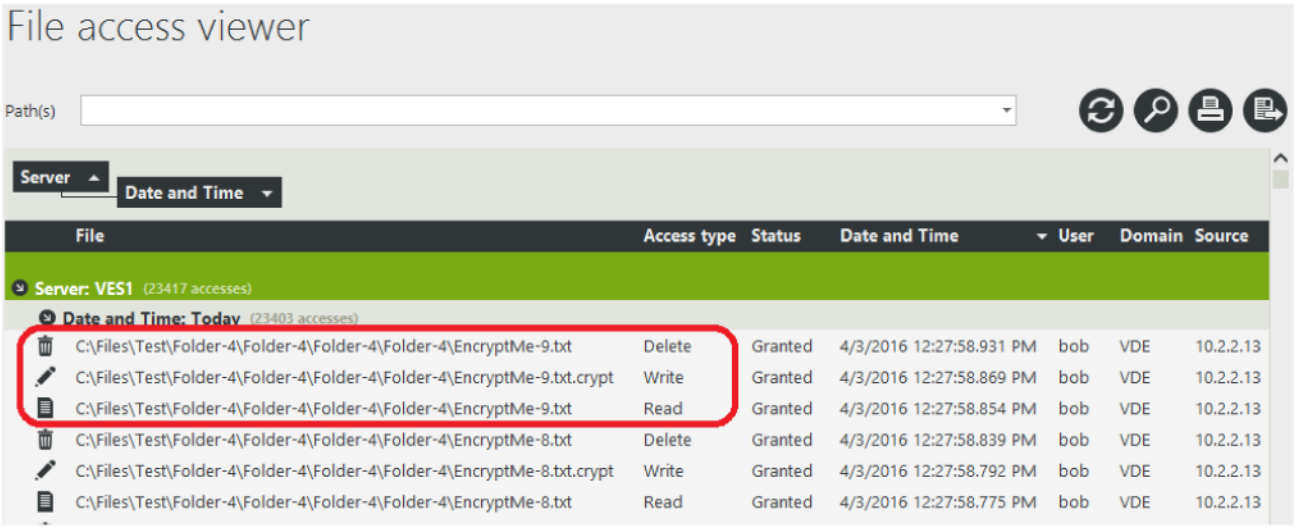
Inmediatamente revisamos la carpeta raíz y vemos que las extensiones de los archivos cambiaron y que si tratamos de mostrar el contenido solo podremos ver valores aleatorios.



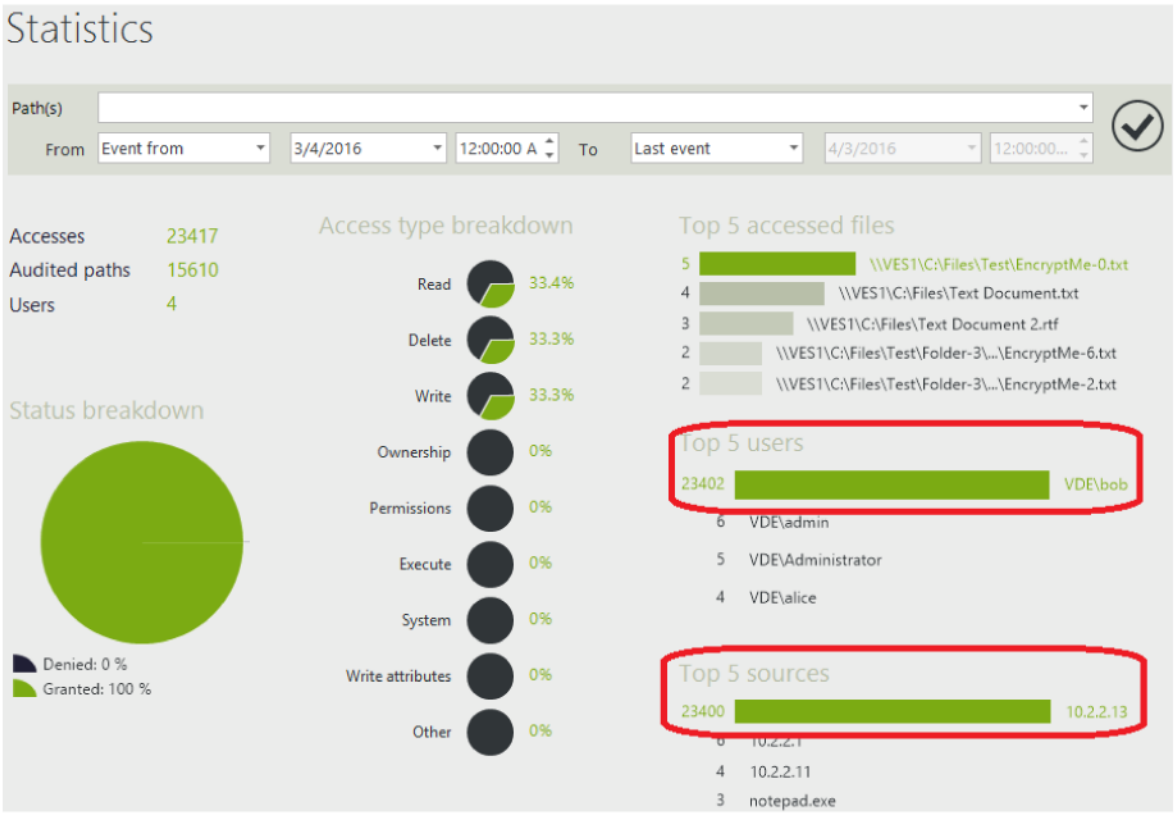
Luego verificamos el correo del administrador y veremos las tres alertas como era de esperarse. Sin embargo también obtenemos alertas sucesivas a cada minuto, ya que la encripción tomo más tiempo que el período de latencia (más de un minuto en este caso).



En el visor de accesos de FileAudit vemos la confirmación de lo que sospechamos. Por cada archivo, el archivo es leído, un nuevo archivo creado y el archivo original borrado.



Si vemos las estadísticas en FileAudit, el usuario responsable de la encripción masiva y la IP se encuentran en el Top 5.



2.5 ¿Es la simulación de ransomware realística?

La prueba fue exitosa, pero ¿fue esta simulación similar a un ataque real de un ransomware?

Algunas descripciones indican que CryptoWall, un ransomware común y peligroso, es capaz de encriptar 230 GB de datos en dos horas, lo que da una taza de 30 MB/s.

Por ejemplo un promedio de 200KB por archivo, si encriptamos una carpeta de 7810 archivos por un total de 1.5GB con la herramienta de simulación, tardaría unos 40 segundos. Esto equivale a una velocidad de encripción de 40 MB/s o 200 archivos por segundo (o 12.000 por minuto). Lo que sugiere que la simulación fue similar a un ataque real.

Adicionalmente, se sabe que los ransomware utilizan encripción AES 256, como lo hace nuestra herramienta. Por lo que no hay motivo por el cual deberíamos obtener una diferencia de velocidad.

El intervalo por defecto de FileAudit de 100 accesos por minuto ejecutará la alerta. Por supuesto que el tamaño de archivos puede variar, afectando la velocidad de archivos que por minuto se puede cambiar, pero se sabe que el ransomware encripta los primeros megas de archivos grandes. Como el intervalo es 100 veces menor al que podemos esperar durante un ataque hay un margen para trabajar con esto.

También existe un detalle menor para mencionar sobre la herramienta de simulación. Los archivos encriptados son creados con el mismo nombre pero la extensión ".crypt" es agregada. Esto es específico para nuestra simulación. Los ransomware pueden tener un comportamiento distinto. Las nuevas extensiones pueden ser diferentes y a veces los nombres de los archivos encriptados también lo son. Esto hace difícil localizar un archivo específico entre todos los archivos encriptados. En cualquier caso, esto no afecta a la detección de FileAudit.

Como punto final, en la simulación la encripción toma lugar en una sola carpeta auditada por FileAudit. Pero en un ambiente real se necesita configurar FileAudit en todas las carpetas compartidas por el servidor, ya que la encripción de archivos no auditados por FileAudit permanecerá no detectada.

3 Conclusión

Ahora ya sabemos cómo detectar la encripción hecha por un ransomware en una red con FileAudit

Sin embargo, como en todo entorno seguro, no se debe confiar en una sola línea de defensa. La seguridad en profundidad es integral a una estrategia robusta de protección, y la última línea debe ser siempre un backup. FileAudit puede solamente detectar un ataque una vez que la encripción ha comenzado. Entonces aunque pueda detener un ransomware a tiempo, siempre habrá archivos que restaurar.

4 Integraciones y aplicaciones de los Tokens USB / Smartcards de Macroseguridad.org

MacroSeguridad ha desarrollado varias guías de integración para utilizar sus dispositivos criptográficos con las aplicaciones de uso común. Los Tokens USB y SmartCards le permiten robustecer la seguridad de dichas aplicaciones de modo totalmente transparente. Si desea conocer mayor información al respecto de estas guías puede visitar:

http://www.macroseguridad.net/documentacion

Para mayor información o dudas sobre esta guia contacte al equipo de Tecnología de MacroSeguridad.org por el medio que usted prefiera:

- Mail: soporte@macroseguridad.net
- Portal de soporte: https://soporte.macroseguridad.la
- Web: www.macroseguridad.net