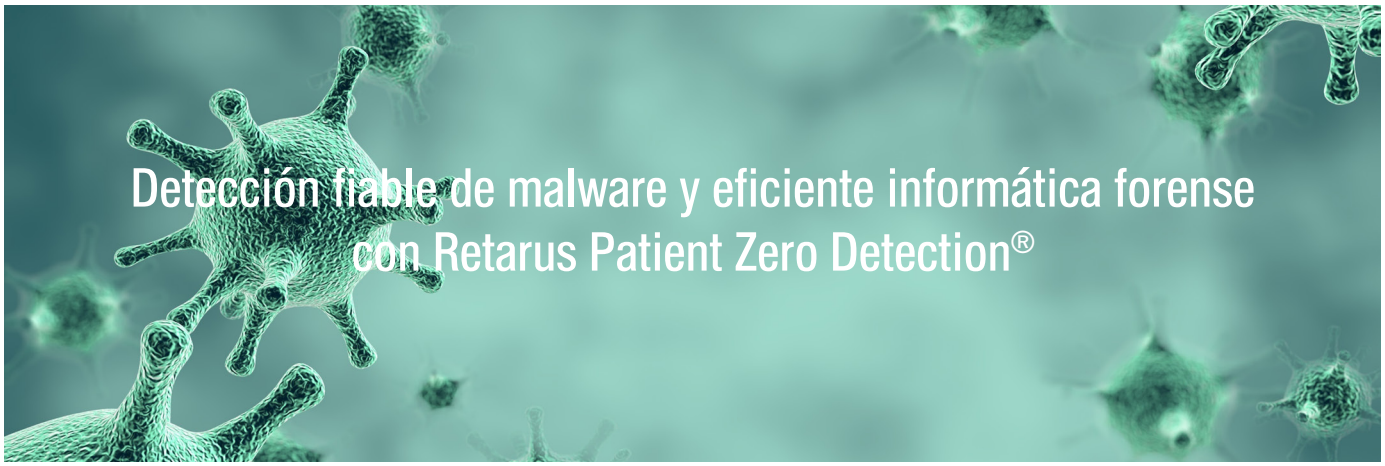

Detección fiable de malware y eficiente informática forense con Retarus Patient Zero Detection®

El reto

Las medidas de protección simples han dejado de ser suficiente. El número de virus nuevos que atacan diariamente la infraestructura corporativa a través del correo electrónico es demasiado elevado. Una vez que el malware ha entrado en la red, es importante reducir al mínimo sus consecuencias. Solo mediante la identificación rápida de los destinatarios afectados (los denominados "pacientes cero") efectuada por la informática forense pueden aplicarse contramedidas a tiempo para evitar interferencias importantes. Al mismo tiempo, la configuración del sistema debe optimizarse continuamente para proporcionar una protección completa contra las amenazas futuras.

La situación de partida

Desafortunadamente, la mayor parte del correo electrónico consiste en spam, virus o ataques de phishing dirigidos. Cada día se registran más de 390.000 casos de malware nuevos en todo el mundo. Esto se traduce en una media de alrededor de 270 nuevas variantes de virus por minuto. Por lo general, las soluciones de seguridad de correo electrónico filtran de forma fiable los mensajes infectados. Sin embargo, incluso los mejores filtros antivirus no pueden ofrecer una protección totalmente efectiva puesto que, cuando aparece un malware nuevo por primera vez, su firma sigue siendo desconocida. Es por ello que muchas empresas utilizan exploradores antivirus instalados localmente o soluciones complejas de Sandboxing además de las soluciones basadas en la nube. Pero incluso en este caso, los administradores y los destinatarios de nuevos virus a menudo se percatan de su existencia cuando ya es demasiado tarde y el malware ya ha causado daños. Además, el origen del ataque, en su mayor parte desconocido, obstaculiza en suma medida la aplicación de la informática forense.

La solución

Los **Retarus Email Security Services** brindan una protección fiable contra ataques de malware gracias a la protección antivirus de varios niveles, los filtros inteligentes de spam y phishing y la exclusiva característica Attachment Blocker. Por ejemplo, el probado sistema de exploración cuádruple de Retarus ya ofrece un elevado nivel de protección al filtrar alrededor de un 35 % más de virus que las soluciones de protección antivirus convencionales que utilizan solo dos exploradores. En combinación con la patentada tecnología **Patient Zero Detection®** de Retarus, las empresas pueden proteger aún mejor su infraestructura contra ataques y detectar además malware no conocido.

Beneficios para el cliente

- Máxima protección de la infraestructura informática
- Respuesta rápida a los ataques
- Informática forense sencilla
- Comunicación empresarial eficiente
- Optimización duradera del sistema

Resumen de ventajas

- Detección fiable de destinatarios de malware no detectado inicialmente
- Alerta inmediata
- Entrega de correo electrónico sin retraso
- Informes y análisis detallados
- Integración perfecta con **Retarus Enterprise Email Encryption**

El escenario de aplicación

Los Retarus Email Security Services acceden a varios exploradores antivirus en paralelo con reglas de filtrado actualizadas continuamente y, de este modo, detectan de forma fiable la mayoría de los programas maliciosos peligrosos. La innovadora tecnología Patient Zero Detection® de Retarus también identifica los correos electrónicos peligrosos que ya se han entregado y facilita así la informática forense. Para ello se genera una huella digital de todos los archivos adjuntos cuando se recibe el correo electrónico y se almacena en una base de datos de la infraestructura de Retarus. Este procedimiento no causa retrasos en la entrega. En cuanto un explorador antivirus detecta posteriormente un código malicioso en un archivo adjunto similar para otro destinatario, Retarus compara esta huella con todos los datos almacenados en la base de datos. El correo electrónico infectado se elimina inmediatamente. Si la firma coincide con una ya guardada, se notifica inmediatamente a los administradores responsables y, opcionalmente, a todos los destinatarios anteriores. La **Patient Zero Detection® Real-Time Response** permite el procesamiento basado en reglas de los hallazgos para identificar correos electrónicos potencialmente peligrosos en el buzón de un usuario y moverlos o eliminarlos automáticamente.

Las empresas pueden identificar los sistemas afectados en muy poco tiempo y adoptar las medidas adecuadas antes de que los virus se propaguen por la red corporativa. El correo electrónico infectado se puede eliminar a tiempo antes de que se abra. En el caso de que un archivo adjunto afectado ya se haya ejecutado, Retarus Patient Zero Detection® también facilita la informática forense. Los informes y análisis detallados proporcionan indicios concretos sobre qué archivos deben analizarse en busca de virus. Para mejorar la protección del sistema en caso de futuros ataques, la configuración de filtro de Retarus Email Security también puede optimizarse de forma permanente con la información proporcionada por Patient Zero Detection.

¿Sabía que...?

Según Kaspersky, el coste medio de un ataque cibernético para las grandes empresas es de unos 861.000 dólares.

Otros escenarios

Cifrado seguro
Los datos confidenciales nunca deben caer en las manos equivocadas. Con **Retarus Email Encryption**, las empresas pueden proteger la confidencialidad de sus comunicaciones e implementar fácilmente las leyes de protección de datos aplicables.

Cuarentena inteligente de mail
Los resúmenes de correo electrónico proporcionan rápidamente a las empresas una visión general de los virus y el spam interceptados. Los correos electrónicos clasificados como spam pueden ponerse en cuarentena sin acceso al portal.

Bloqueador de adjuntos
Con el **Attachment Blocker** de Retarus, las empresas pueden mejorar aún más su infraestructura contra ataques de malware. Esta característica impide la recepción de todos los tipos de archivos adjuntos que el administrador clasifica como no fiables.