#1 Choice of DIGITAL WORLD

eScan™
Anti-Virus & Content Security

RANSOMWARE

eScan debuta nueva Tecnología para la detección y mitigación

www.latam.escanav.com

Ransomware empezó a adquirir prominencia alrededor del año 2012 sembrando terror y pánico allá donde se pululara. A diferencia del Troyano o demás software malicioso que se mantenían ocultos en el segundo plano mientras robaban datos importantes, Ransomware anunciaba claramente su presencia.

Desde el principio, a Ransomware se le consideraba un malware muy sofisticado dadas sus capacidades de encriptación. Con el paso de tiempo y valiéndose de nuevas tácticas, los creadores de Ransomware empezaron a identificar archivos importantes que serían el blanco de sus ataques. Debido a que numerosas bibliotecas de encriptación estaban ya disponibles en la red, no hacía falta que el programador fuese un experto en encriptación e incluso los script kiddies, (los falsos hackers o hackers inexpertos) podían crear su propio ransomware. Lo que básicamente interesaba al autor de ransomware era:

1. Colarse en el sistema

2. Encriptar los archivos en base a las extensiones.

3. Transferir las claves de encriptación otra vez al servidor CNC.

Ransomware se presentaba de varias formas, empezando por binarias comprimidas y luego como macros incrustados en archivos Docx o Doc (cuando las empresas de seguridad informática comenzaron a bloquearlas). Muy recientemente, nos hemos encontrado con que el Ransomware, en su más última versión, se está propagando mediante scripts basados en Java, VB y Powershell.

Para combatir a esta última variante de Ransomware, las empresas de seguridad informática empezaron a bloquear los motores de scripting. Nos preguntamos, '' ¿Hasta cuándo durará este juego del gato y ratón?'' A los investigadores, les ha resultado cada vez más difícil encontrar una solución que pare a Ransomware en seco.

Los sistemas convencionales de recuperación de datos se basan en el hecho de que solo ciertas carpetas se consideran importantes y ante ataques de malware se inicia la recuperación de carpetas pre-configuradas. Sin embargo, Ransomware está centrado en archivos y en algunos casos encriptará todos

los archivos de fotos y dejará las miniaturas para que te des cuenta de lo que puedes llegar a perder si no pagas el rescate.

Nosotros en eScan, hemos estado persiguiendo el Ransomware a varios niveles, hemos estado analizándolo, hemos estado estudiándolo y hemos estado buscando maneras de detectar y mitigar esta amenaza. eScan debuta ahora **Proactive Behavioral Analysis Engine (PBAE)** que monitorea la actividad de todos los procesos en el equipo cliente y cuando PBAE encuentra indicios de comportamiento que se parecen a una infección de Ransomware, se activa una alarma y el proceso que tenía un comportamiento similar a Ransomware queda completamente inactivo. De esta forma, se impide que Ransomware cause estragos en redes corporativas.

No obstante, a Ransomware se le conoce por encriptar archivos que se ubican en recursos compartidos de la red. En tales casos, cuando un sistema infectado y no protegido accede a los recursos compartidos de la red de un sistema protegido e intenta modificar los archivos que se encuentran ahí, PBAE invalidará la sesión de red inmediatamente.

En nuestra lucha contra el Ransomware, hemos creado un mecanismo oculto de respaldos que se activa durante posibles ataques de ransomware y que permite al usuario superar tales ataques de ransomware.

Con **Proactive Behavioral Analysis Engine (PBAE)**, eScan es capaz de proteger sistemas y redes corporativas con relativa facilidad frente a ataques de Ransomware como Locky, Zepto, Crysis, Crypto por nombrar unos cuantos. Hasta la fecha, PBAE, la revolucionaria tecnología de eScan ha podido detectar y detener miles de ataques de Ransomware por todo el mundo. En eScan, seguimos trabajando duro para ir por delante de posibles nuevas variantes de Ransomware que salgan a la luz.