Boletín de setiembre

MEDIDAS DE PROTECCIÓN CONTRA MALWARE TIPO RANSOWARE

Un malware (software malicioso) tipo Ransomware es un cryptovirus, que fue creado para extorsionar a los usuarios de equipos informáticos.

Nadie puede predecir de antemano la aparición de un ransomware en su PC, este virus revela su presencia sólo después de que encripta los archivos. Y eventualmente mostrará en el escritorio un mensaje solicitando un rescate para el descifrado.

El cifrado de los archivos afectados está basado en técnicas de criptografía tal como los que se usan en procesos de CriptoMoneda, Firmas o Certificados digitales.

El proceso de infección está basado en facilitar el ingreso del malware (software malicioso) a través de una descargar no controlada desde una página web, abrir archivos de emails desconocidos o introducir un dispositivo USB infectado previamente.

La activación de este virus, es progresiva, pues requiere configurar condiciones adecuadas en la PC, pero una vez logrado, el proceso de encriptación de los archivos existentes en especial documentos y fotos es muy violento y rápido, expandiéndose por todas las carpetas locales y externas compartidas en la PC.

La versión de estos virus muta permanentemente al igual que sus técnicas de encriptación, por lo que, los antivirus tradicionales no lo detectan, y el proceso inverso de desencriptación queda permanentemente bajo investigación. Esta es la característica que los ciberdelincuentes usan para exigir pagos por el rescate de los archivos encriptados.

ver: https://www.pcissuessolution.com/es/como-eliminar-kvag-file-virus-y-restaurar-archivos

MEDIDAS PARA PREVENIR VIRUS EN LAS PCs:

I. Capacitación al personal. Como medida preventiva

El personal debe saber cómo reconocer una amenaza de virus en cualquiera de sus variantes y como proceder para reducir el riesgo de infección generalizadas, para Realizaremos una capacitación para el uso seguro de los servicios y accesos a internet y elementos externos a la red de datos de la oficina.

II. Copias de seguridad más frecuentes y fuera de la oficina

Se debe establecer un protocolo de copias de seguridad, que se lleve a cabo de manera exhaustiva y recurrente.

Dicho protocolo involucra, Una copia local en la misma PC o recurso compartido, Una copia seguridad en otra PC o servidor, que solo se active para el momento requerido de las copias de seguridad de PCs de la red de datos y una tercera copia, desde el servidor backup, pero con almacenamiento externo a la oficina (por parte de uno de los administradores del negocio), con lo cual no solo se protege la información existente de virus, sino también de siniestros que podrían ocurrir.

III. Mejorar el ecosistema informático

1. Actualización del sistema y aplicaciones. Mantener el sistema operativo actualizado con los últimos parches de seguridad y todas las aplicaciones que tengamos instaladas es el mejor punto de partida. (Pero ello exige Sistemas Operativos licenciados).
2. Línea de defensa. Conviene instalar y mantener una solución antimalware, incluyendo un cortafuego (Configuración hardware y software) correctamente configurado para permitir el acceso exclusivo de las aplicaciones y servicios necesarios.
3. Herramienta Anti Ransom (Software especializado – actualmente solo con licencias de pago). Es una herramienta específica contra este tipo de ataques, que tratará de bloquear el proceso de cifrado de un ransomware (monitorizando "honey files"). Realizará un dump de la memoria del código dañino en el momento de su ejecución, en el que con suerte hallaremos la clave de cifrado simétrico que estuviera empleándose.
4. Filtro antispam. Muchos de los ataques por Ransomware se distribuyen a través de campañas masivas de correo electrónico. Además de estos filtros, debes seguir los consejos generales como no pinchar en enlaces o abrir archivos adjuntos de remitentes desconocidos.
5. Bloqueadores de JavaScript. Aplicaciones como Privacy Manager bloquean la ejecución de todo código JavaScript sospechoso de poder dañar el equipo del usuario. Esto ayuda a minimizar la posibilidad de quedar infectado a través de la navegación web.
6. Políticas de seguridad. Herramientas como AppLocker, Cryptoprevent, o CryptoLocker Prevention Kit facilitan el establecimiento de políticas que impiden la ejecución de directorios comúnmente utilizados por el ransomware, como App Data, Local App Data, etc. (Lamentablemente, todas ellas son licencias de pago).
7. Cuentas con privilegios. No utilizar cuentas con privilegios de administrador. El 86% de las amenazas contra Windows se pueden esquivar en caso de utilizar un usuario común en lugar de un administrador. Por eso es importante utilizar para tareas comunes un usuario común y solo dejar el administrador para cuando se vaya a hacer una serie de tareas relacionadas con la manipulación del sistema.
8. Extensiones de archivos. Mostrar las extensiones para tipos de ficheros conocidos es una buena práctica para identificar los posibles ficheros ejecutables que quieran hacerse pasar por otro tipo de fichero. No es raro ver a un fichero .exe con el icono de un documento de Word. Si no se ve la extensión, el usuario posiblemente no pueda distinguir si es un documento de Word o un ejecutable malicioso, aunque también es bueno recordar que un documento de Microsoft Office también puede contener malware.
9. Máquinas virtuales. Emplear máquinas virtuales para aislar el sistema principal es otra técnica efectiva. En un entorno virtualizado la acción de los ransomware no suele materializarse.
10. Backup. Realizar copias de seguridad de los datos importantes como tarea de mantenimiento regular es la medida más efectiva para minimizar los daños en caso de ser infectado. La copia de seguridad debe alojarse en un medio externo distinto al del equipo para poder recuperar los archivos desde un sitio "limpio" y no tener que pagar el "rescate" exigido por estos ciberdelincuentes.