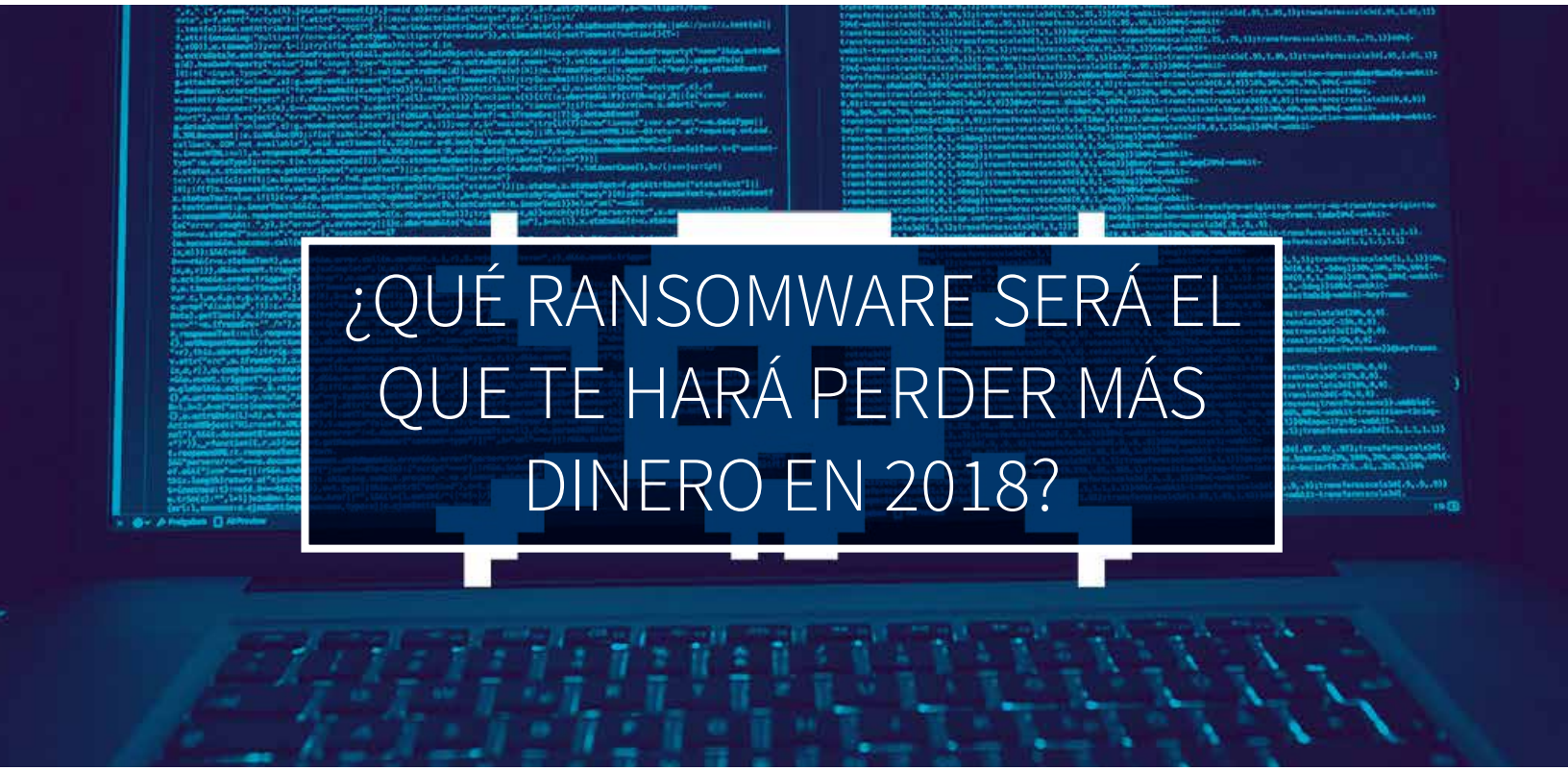
Managed secure IT | no matter what



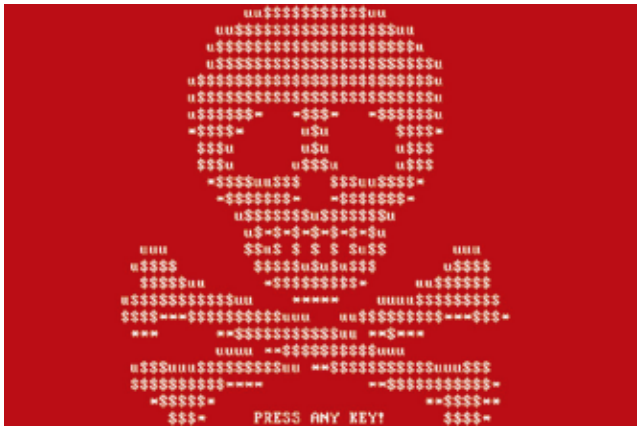
¿QUÉ RANSOMWARE SERÁ EL QUE TE HARÁ PERDER MÁS DINERO EN 2018?

2017 fue un año en el que el ransomware y los ataques en los que se usó, adquirieron un protagonismo infame que solo hizo que miles de empresas de todo el mundo perdieran millones de dólares en cuestión de segundos.

Sin embargo, también hizo que expertos en ciberseguridad en todo el mundo, encontraran nuevas maneras de protegernos de los cibercriminales.

No obstante, los analistas indican que en 2018, al menos 75% de las empresas de toda escala y giro estarán en la mira de los hackers, quienes con cada semana que pasa, encuentran nuevas y más letales maneras de violar su ciberseguridad y hacer dinero fácil.

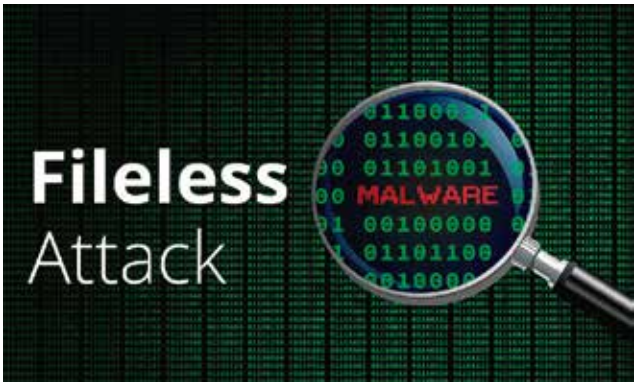
Por ello, de acuerdo al análisis de expertos en ciberseguridad de todo el mundo, se hizo una lista del ransomware que más dinero podría hacerte perder en 2018, en caso de ser afectado por uno.



Fileless

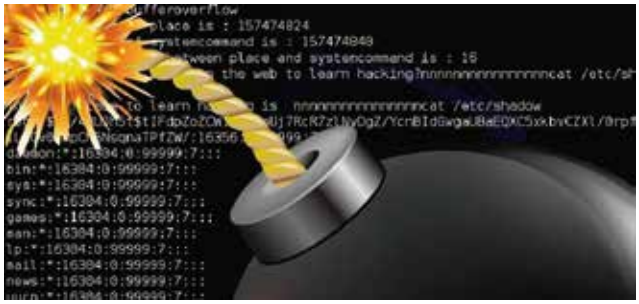
En 2017 era virtualmente desconocida, pero en 2018 comenzó a ponerse de moda entre los cibercriminales. Se trata de un malware que ataca los equipos de una empresa a través de su memoria RAM para robar datos directo desde los servidores de la misma.

Los Fileless fueron creados como una respuesta a los cada vez más sofisticados métodos de protección mediante machine learning y por ello atacan a una empresa sin necesidad de ser descargados a la memoria ROM de un equipo.



Exploits

Ningún cerco de seguridad es perfecto y son esas mínimas, casi imperceptibles, fallas, las que hacen que los hackers se infiltren en un sistema y lo ataquen desde dentro. Para evitar este tipo de brechas, hace falta contar con un experto en ciberseguridad que eche mano de no una, sino devarias herramientas de monitoreo y prevención, para evitar que los cibercriminales tomen por sorpresa la red de un negocio.



Keyloggers

En 2017 el nombre del juego de los hackers era hacer dinero, pero en 2018 buscan algo más. Se acabaron los días en los que los cibercriminales simplemente secuestraban los sistemas o programas de una empresa para obtener un beneficio económico pues, según los expertos de todo el mundo, las empresas ya son afectadas mediante otros métodos de infección masiva de equipos a través de keyloggers o software para minar criptomonedas.

Para contrarrestar este tipo de ataques, hace falta buscar la orientación de un grupo de expertos que se mantenga actualizado en cuanto a las nuevas tendencias de ciberataques y a los mejores métodos de protección contra estos.

Cabe resaltar que continuar confiando en métodos on-premise para trabajar o almacenar información confidencial, solo expone a las empresas a las ciberamenazas de la era digital, por lo que se recomienda comenzar a buscar ayuda de expertos certificados para migrar todas las operaciones de un negocio a la Nube.

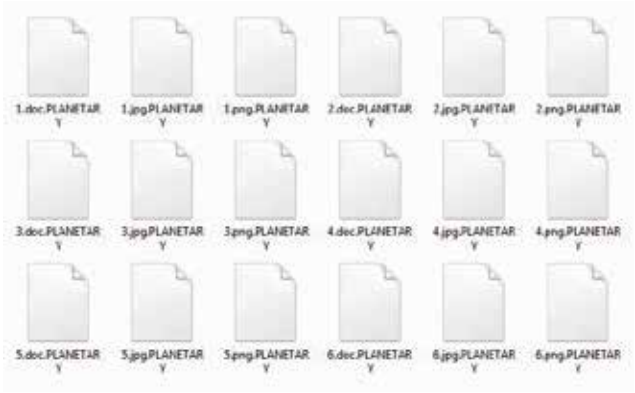
Security

Se sabe que aproximadamente 81% de los ataques masivos de ransomware llegan desde los servidores físicos de una empresa, mientras que el 19% sobrante se mantiene protegido en el ecosistema de la Nube.

HC7

En 2017 fueron los ransomware NotPetya y WannaCry, los más letales para el mundo empresarial, pero los cibercriminales preparan herramientas mucho más devastadoras como el HC7 Planetary y todas sus variantes.

Este malware es casi indetectable y, de acuerdo a informes de seguridad de varios expertos, es el primero en incluir la criptomoneda Ethereum como forma de pago para el rescate.



HC7 infecta las computadoras de una empresa a través de sesiones de acceso remoto, y luego acceden al sistema central de forma manual para ejecutar el ransomware que secuestra todos los equipos dentro de una red.

Se sabe que con este ransomware, se cobran no menos de $500 USD por liberar una sola computadora, y al menos 5 mil por todas las que hay en un piso de oficinas. Sin embargo, en empresas con cientos de sucursales de todo el mundo, el precio del rescate podría ascender a varios miles de millones de dólares.

Se sabe que en 2018, los cibercriminales intensificarán el uso de criptomonedas, por lo que el número de ataques contra empresas de todo tipo y tamaño, se triplicará para finales del año en curso.

Desde los ataques de WannaCry y NotPetya, el número de incidencias de brechas de seguridad a empresas se ha multiplicado aproximadamente 1.900%, así que si no quieres convertirte en parte de esta estadística, te recomendamos buscar la orientación de un experto que te ayudará a mantenerte seguro mientras continúas creciendo en el mundo digital.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.