

10 SEÑALAMIENTOS **PARA PREVENIR INFECCIÓN POR** **RANSOMWARE** **USANDO TU SOLUCIÓN DE** **CIBERSEGURIDAD**



RANSOMWARE

Ransomware es una familia de malware que cifra archivos en las computadoras y servidores de los usuarios finales y posteriormente demandan una forma electrónica de pago a modo de rescate para recuperar los archivos cifrados.

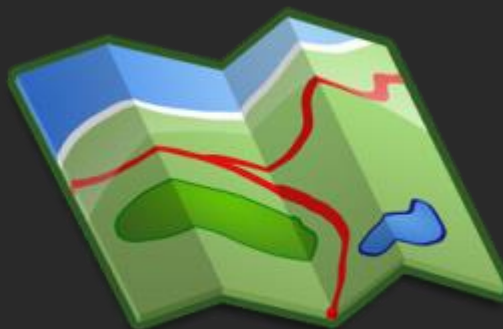
Es una de las amenazas más comunes en el paisaje moderno de amenazas; existen diferentes variantes. **Recuperarse de una infección puede costar mucho dinero, imagen y productividad.**

Lo más recomendable es **configurar adecuadamente nuestras soluciones de ciberseguridad para prevenir y evitar poner en riesgo la información y reputación de nuestra empresa.**

- ❶ Correos electrónicos de Phishing. Contienen archivos adjuntos maliciosos y/o URL maliciosas. DOC`s –PDF`s
- ❷ Kits de Exploit. Distribuyen ransomware explotando vulnerabilidades en servidores web ejecutando scripts maliciosos como Angler, o Neutrino.
- ❸ Ataques dirigidos. Explotan estrategias ciber criminales que inician con Ingeniería Social



Esta amenaza se está convirtiendo en una estrategia cibercriminal y para esto hemos preparado 10 señales importantes que te ayudarán a aprovechar tu solución de ciberseguridad para minimizar al máximo el riesgo de ser atacado.





KITS DE EXPLOITS

1

Es recomendable el uso de una política estricta de protección contra vulnerabilidades, esto ayudará a proteger a tus usuarios.

Para combatir los kits de exploit y vulnerabilidades, existen varias firmas conocidas en las soluciones tecnológicas de hoy en día.



2

CARGAS ÚTILES



Para prevenir la entrega de **payloads maliciosos**, se debe contar con un motor de escaneo de anti-virus de red que inspeccione protocolos conocidos a través de los cuales el contenido viral es transferido incluyendo:

http smtp imap **pop3** ftp **smb**



FILTRADO DE URL

3

Para prevenir las descargas de código malicioso **puedes implementar una estrategia de filtrado de URL.**

Existen categorías de URL específicas donde se ha detectado el mayor riesgo de infección. Puedes empezar bloqueando:

- 0 Malware
- 0 Phishing
- 0 Desconocidas
- 0 DNS Dinámicos
- 0 Proxies
- 0 Questionable
- 0 Parked
- 0 Hacking

4

LISTAS NEGRAS DE REPUTACIÓN

MAX
80



Para prevenir la comunicación a ciertos destinos basados en la reputación de los mismos.



Se recomienda utilizar en tus reglas de seguridad:

LISTAS DINÁMICAS EXTERNAS
BLACKLISTS



TRÁFICO TCP/UDP ESPECÍFICO

5

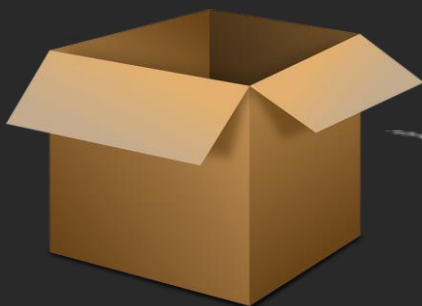
Tanto como sea posible, se debe considerar **bloquear tráfico TCP y UDP desconocido** y solo permitirlo en aplicaciones específicas creando reglas de seguridad particulares.

6

SANDBOXING



Para identificar nuevas variantes de malware, se debe llevar a cabo un análisis de archivos en un **servicio de Sandboxing** (ambiente aislado de prueba).



El paso siguiente se da al crear una firma para ellas y distribuirla en las próximas actualizaciones de la solución.



Para identificar tipos de archivos permitidos y tomar acciones dependiendo las políticas aplicadas, es **recomendable combinar el bloqueo de tipos de archivos con payloads maliciosos (Flash, PDF, Executable, y documentos de Office)** con una política de seguridad que permita la entrada y salida hacia y desde Internet.



La **mayoría de los Ransomware** utilizan correos electrónicos con archivos adjuntos maliciosos, considera bloquear ciertos tipos de archivos a través de SMTP.

Todos los PE (exe, cpl, dll, ocx, sys, scr, drv, efi, fon, pif) HLP, LNK, CHM, BAT, VBE, entre otros.



Bloquear o alertar al identificar archivos cifrados y comprimidos puede reducir el riesgo de infección, también ayuda generar alertas sobre todos los tipos de archivos que no sean bloqueados para tener visibilidad y análisis de los mismos.



DESCIFRADO SSL

8

El descifrado de SSL una parte integral del aseguramiento de una red

Ninguna de las prevenciones anteriores ocurrirán si los datos que pasan por la red se encuentran cifrados.

Recuerda que el descifrado del tráfico puede llegar a ocupar la mayor parte de los recursos de un firewall de nueva generación, por tanto, es importante escoger cuidadosamente el tipo de tráfico a descifrar.

Puedes empezar con categorías de URL Filtering.

9

CALLBACKS



Algunas variantes de **ransomware** se comunican a sitios en la DeepWeb para recibir datos, intercambiando llaves de cifrado de los archivos a secuestrar.



Se deben tomar acciones cuando se detecten solicitudes de DNS sospechosas.

Bloquea las solicitudes a dominios que estén categorizados como maliciosos o **direccionales a una IP falsa o interna (Sinkhole)** y realiza un análisis más exhaustivo.



INTELIGENCIA DE AMENAZAS

10



Un servicio de **inteligencia de amenazas** es ideal para **entender mejor los patrones de comportamiento** de una variante de ransomware en particular.

Revisando los **tags** de las familias de esta amenaza se puede **identificar que características son únicas** dependiendo de su **variante**, esto puede ayudar a reconocer el tipo de organizaciones e industrias a quién se dirige este ransomware



Con esto puedes **medir la cantidad de información que se debe recolectar** para estar **mejor preparados y reforzar las defensas** ante un ataque futuro.



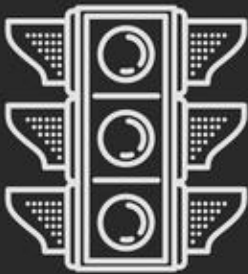
ELIGE LA MEJOR RUTA

para tu estrategia de ciberseguridad



PROTEGE TU RESPALDO

Si se realizan respaldos y se tienen en un lugar seguro, **la recuperación después de una infección tendrá un impacto significativamente menor** en la organización.



PRESTA ATENCIÓN A LOS SEÑALAMIENTOS

Soluciones de ciberseguridad con tecnología de nueva generación especializada **brindan completa visibilidad con alertas para identificar las aplicaciones, usuarios y contenidos** que pasan a través de tu red.



PRUEBA EL PODER DE TECNOLOGÍA DE NUEVA GENERACIÓN

Reconociendo los niveles de seguridad que manejan en tu organización podrás mejorar la competitividad y fortalecer tu estrategia disminuyendo la superficie de ataque de Ransomware.

Agenda tu prueba de manejo encendiendo el motor aquí



