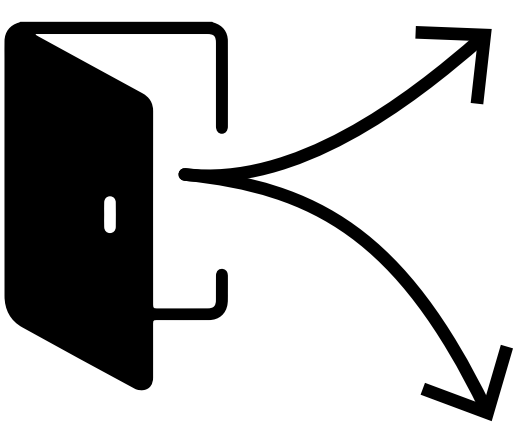
AVG Business

Supervivencia del ransomware: Jigsaw

Con 120 millones de nuevas muestras de ransomware solo en 2015, es una de las amenazas a la seguridad de más rápido crecimiento en la web. Jigsaw, es la versión de ransomware más reciente y avanzada, que secuestra su equipo y elimina archivos hasta que paga todo el dinero. La prevención es la clave para evitar estos ataques. Lo invitamos a sobrevivir al ransomware.

¿Cómo se introduce Jigsaw?

Es 80 % más probable que el ransomware ataque a las empresas; por lo tanto, capacite a sus empleados, usuarios o clientes sobre cómo identificarlo antes de que se convierta en un problema.



Correo electrónico

Los correos electrónicos maliciosos son algunos de los puntos de entrada de ransomware más comunes. Qué buscar:

- Un vínculo malicioso
- Un archivo adjunto con código malicioso en el interior, disfrazado como un archivo .pdf, Word, Excel o .zip
- Líneas del asunto sospechosas o confusas

Sitio web

A veces, una página web puede ser un punto de entrada. Esté atento a lo siguiente:

- Ventanas emergentes o banners publicitarios
- Vínculos que apuntan a ransomware
- Imágenes que se conectan con ransomware

En caso de duda, cierre siempre el sitio web o la ventana emergente.

¿Qué sucede cuando se infecta con Jigsaw?

72:00

72 horas; generalmente tiene 72 horas para pagar el rescate, normalmente en Bitcoin.

00:60

60 minutos; cada hora y al inicio, Jigsaw elimina archivos para presionarlo a que pague.

1-1000

De 1 a 1000; la velocidad a la cual se eliminan los archivos es exponencial, desde un simple archivo hasta miles de archivos a la vez.

¿Por qué Bitcoin?

Bitcoin es una moneda digital que admite transacciones de punto a punto sin la necesidad de un banco o una empresa de tarjetas de crédito.

No se puede hacer un seguimiento del pago, lo cual hace que sea más difícil que se involucre la policía o que los bancos congelen los pagos.

No hay supervisión de su pago, por lo tanto no hay garantía.

El Bitcoin está disponible sobre todo en la web oscura.

No le dé oportunidad al ransomware

La prevención es la mejor protección

Al realizar copias de respaldo de manera regular, educar a sus empleados y usar protección de niveles múltiples, puede proteger su empresa contra el ransomware. No todas las soluciones antivirus son capaces de analizar archivos a un nivel que realmente prevenga un ataque de ransomware. Asegúrese de que el software antivirus es capaz de escanear archivos .zip, metadatos, contenido y comportamiento.

Proteja su empresa en 5 pasos simples

1. Realice una copia de respaldo de los archivos en una unidad externa
2. Capacite a los empleados para que sepan a qué tienen que estar atentos
3. Implemente políticas para administrar el ransomware
4. Actualice todo el software a las versiones más recientes
5. Utilice protección AV de niveles múltiples

Confíe en AVG para proteger su empresa

AVG Internet Security y AntiVirus Business Edition utilizan un enfoque de capas múltiples para detectar y eliminar el ransomware. Cuando un archivo pasa satisfactoriamente a través de un nivel de análisis es dirigido hacia otra capa. AVG identifica proactivamente las muestras nuevas de malware y nuestros algoritmos avanzados reducen los tiempos de análisis.

No deje que su empresa sea chantajeada.

Diríjase a www.antivirusavg.es o comuníquese con su socio de seguridad para empresas de AVG autorizado

#securitysimplified

The Online Security Company™
Devices. Data. People.™