IT & Security Consultores Ltda.
NIT 811.031.833-3
*Soluciones Antivirus Multinivel *Consultoría en Seguridad Informática
*Recuperación Avanzada de Datos *Mantenimiento Integrado de Software y Hardware
*Soporte Técnico y Capacitación

NUEVA OLEADA DE RANSOMWARE

Calle 37 No 79-17 Laureles Tels. 604 45 41 Ext. 203
Medellín – Colombia E-mail: mvargas@its-consultores.com

IT & Security Consultores Ltda.
NIT 811.031.833-3
*Soluciones Antivirus Multinivel *Consultoría en Seguridad Informática
*Recuperación Avanzada de Datos *Mantenimiento Integrado de Software y Hardware
*Soporte Técnico y Capacitación

NUEVA OLEADA DE RANSOMWARE

Con este boletín queremos que nuestros clientes estén en alerta ante una reciente oleada de ataques de ransomware que se han venido presentando especialmente desde esta semana, varias empresas fueron fuertemente afectadas por no contar con un esquema de seguridad adecuado o porque contaban con uno o más puntos del esquema de seguridad funcionando incorrectamente.

Por lo tanto el mensaje es a no bajar la guardia y a verificar que todos los puntos del esquema de protección de la empresa están funcionando correctamente, lamentablemente muchas empresas sólo actúan cuando ya han sido afectadas, cuando se dan cuenta que el ransomware ha destruido absolutamente todo, por eso queremos que sean conscientes de que lo mejor es actuar lo más pronto posible para evitar ser afectados.

Calle 37 No 79-17 Laureles Tels. 604 45 41 Ext. 203
Medellín – Colombia E-mail: mvargas@its-consultores.com

Ransomware Rapid

El ransomware que afectó a varias empresas de Antioquia (en realidad de toda Sudamérica) esta semana se le ha dado el nombre de Rapid porque los archivos que cifra los deja con extensión .rapid, sin embargo no queremos hacer énfasis en esta variante de ransomware en específico porque realmente no tiene nada especial que lo diferencie de otras variantes, es decir, no infecta de una forma nueva, no cifra archivos de una forma nueva, no tiene nada de especial, simplemente que como es una variante nueva es posible que no la detecten muchos antivirus o que no la detecte ningún antivirus.

¿Cómo infectó a las empresas este ransomware? Por escritorio remoto, a todas las empresas afectadas se les cifraron los servidores que tenían el escritorio remoto publicado de forma insegura, lo que hacen los cibercriminales es sondear en todo el internet en busca de servicios activos escuchando y en el momento en el que encuentran un escritorio remoto publicado, lo atacan de diferentes formas hasta vulnerarlo y así ganar acceso para infectarlo. Esto no es algo nuevo, desde hace muchos años ha sido peligroso publicar servidores de esta forma, sólo que ahora el riesgo es mayor por la existencia del ransomware.

Por eso es que realmente en lo que queremos hacer énfasis es que así como a estas empresas el ransomware Rapid las afectó por tener publicado el escritorio remoto de un servidor, las pudo haber afectado cualquier otra variante que hubiera intentado ejecutar la infección por la misma vía.

Es por esto que nuevamente hacemos un llamado para que entiendan que publicar un escritorio remoto de un servidor para todo el internet -es decir que se pueda acceder desde todo el internet- es muy peligroso, por eso hay técnicas para hacer esto pero de forma SEGURA, por ejemplo establecer una VPN para que no haya necesidad de publicar el servidor, esta y otras técnicas las mencionamos detalladamente en el boletín anterior de febrero. (Si desea se lo podemos reenviar)

Finalmente los invitamos a que revisen su esquema de seguridad o a que se apoyen en nosotros para que logren identificar cuáles pueden ser los puntos más débiles y así poder posteriormente reforzarlos, recuerden que la seguridad siempre debe ser **PRE-VEN-TI-VA.**

Calle 37 No 79-17 Laureles Tels. 604 45 41 Ext. 203
Medellín – Colombia E-mail: mvargas@its-consultores.com

Enlaces con mayor información sobre el ransomware Rapid

https://www.bleepingcomputer.com/news/security/rapid-ransomware-continues-encrypting-new-files-as-they-are-created/

https://www.redeszone.net/2018/01/24/rapid-nuevo-ransomware-cifrar-equipo/

https://howtoremove.guide/rapid-ransomware/

https://myspybot.com/rapid-ransomware/