Cómo un Ransomware aprovecha una vulnerabilidad para atacar a sus servidores

1. Vulnerabilidad

¿Qué es?

Errores o fallas en la programación o implementación que ponen en riesgo sus sistemas y aplicaciones.
Todo el software tiene vulnerabilidades.

WannaCry/Petya aprovecharon una vulnerabilidad MS17-010

180,000 servidores
en el mundo aún son vulnerables

1.1 Día Cero (0-day)

¿Qué es?

Vulnerabilidad que desconoce tanto fabricante como usuario.

WannaCry/Petya
aprovecharon la falta de parche para atacar.

2. Exploit

¿Qué es?

Programa o código creado para aprovecharse de una vulnerabilidad.

Wannacry/Petya utilizaron

2 exploits públicos: EternalBlue y DoublePulsar.

3. Malware

¿Qué es?

Software de carácter malicioso que busca perjudicar a un sistema o una red.

100 millones
de malware son bloqueados por Trend Micro al año.

3.1. Ransomware

¿Qué es?

Software malicioso que secuestra programas y/o datos y recibe el pago de un rescate para liberarlos.

200,000 sistemas
fueron comprometidos por Ransomware **WannaCry**.

4. Parche de Seguridad

¿Qué es?

Desarrollos que corrigen los fallos de seguridad detectados.

100 a 120 días
tardan en promedio las organizaciones en aplicar parches.

4.1. Parche Virtual

¿Qué es?

Es una capa adicional de seguridad que ayuda a prevenir la explotación de una vulnerabilidad conocida.

El parche virtual blinda a los sistemas y aplicaciones vulnerables hasta que el fabricante libere el parche que corrija los fallos de seguridad detectados.

Información tomada de:

1. Trend Micro Threat Report, 2017.
2. Europol.
3. Trend Micro; Wannacry/Wcry Ransomware cómo defenderse de él; 17 de mayo de 2017 disponible en: http://blog.la.trendmicro.com/wannacrywcry-ransomware-como-defenderse-de-el/

©2017 by Trend Micro Incorporated. Todos los derechos reservados. Trend Micro y el logotipo t-ball de Trend Micro son marcas comerciales y/o marcas registradas de Trend Micro Incorporated. El resto de los nombres de compañías y/o productos pueden ser marcas comerciales o marcas registradas de sus propietarios. La información contenida en este documento está sujeta a cambios sin previo aviso.
[Infografía_Ransomware_110717]

AGENDA TU ANÁLISIS DE VULNERABILIDADES GRATUITO

Diseñar e implementar una estrategia de parcheo virtual eficaz no es fácil.

Por eso estamos aquí para ayudarte, contamos con un equipo de expertos en Parcheo Virtual. Con nuestra experiencia tu ventana de vulnerabilidad sera más corta que con el parche tradicional, lo que reduce en una gran medida la probabilidad de que las bases de datos y las aplicaciones empresariales se vean comprometidas.

PARTNER PLATINUM

http://info.smartekh.com/analisis-de-vulnerabilidades-en-servidores