LogRhythm®

La compañía de inteligencia en seguridad

CÓMO FUNCIONA EL RANSOMWARE

¡El ransomware está ganando ímpetu!

Durante los últimos tres años, el ransomware ha saltado hacia el foco del panorama de amenazas cibernéticas. El FBI prevé que los ataques de ransomware cosecharán más de mil millones de dólares en 2016.[1]

¿Qué es el ransomware?

El ransomware es un software malicioso que permite que un pirata informático restrinja el acceso a la información vital de un individuo o una empresa y, luego, exige cierta forma de pago (usualmente Bitcoins) para liberar la restricción.

209 millones Monto pagado en el T1 de 2016 a delincuentes cibernéticos usando ransomware[1]

Mil millones Estimación del FBI de las pérdidas a ser incurridas en 2016 debido al ransomware[1]

Tiempo desde la infección inicial hasta una demanda de rescate

$ 10–$ 50 millones

Ingresos mensuales estimados para delincuentes cibernéticos gracias al ransomware[3]

72%

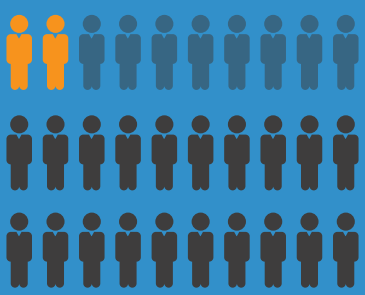
Porcentaje de empresas afectadas por el ransomware que no podían acceder a los datos por, al menos, 2 días luego del ataque[4]

32%

Porcentaje que perdió acceso a sus datos por 5 días o más[4]

86%

Ataques que afectaron a **2** empleados o más[4]



47%

Ataques que afectaron a más de **20** empleados[4]

$ 17 000

Monto pagado por el Centro Médico Hollywood Presbyterian en 2016 para desbloquear archivos y retomar las actividades normales[5]

$ 100 000

Monto que el hospital perdía **POR DÍA** solo por no poder realizar tomografías computadas a pacientes[5]

[1]CNN-Money, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/, 15 de abril de 2016
[2]Security Magazine, "'Ransomware' Attacks to Grow in 2016," 23 de noviembre de 2016
[3]David Common, CBC News, "Ransomware: What You Need to Know," 11 de marzo de 2015
[4]Publicación de blog de Intermedia, "When ransomware strikes your business, are you prepared? Our new report findings may surprise you.", 17 de marzo de 2016
[5]PYMNTS.com, "City Held Hostage – Via Bitcoin Ransomware," 22 de marzo de 2016

LAS 5 FASES
de un ataque de ransomware

Existen 5 fases distintas de un ataque de ransomware [del inglés ransom, «rescate», y ware, por software]. Comprender lo que sucede en cada fase y reconocer los indicadores de compromisos (en inglés, IOC) puede aumentar la probabilidad de una defensa exitosa contra un ataque, o al menos mitigar su efecto.

El plazo de un ataque es muy acotado. A menudo, tiene tan solo 15 minutos desde la explotación e infección hasta la recepción de una nota de rescate. Reconocer los primeros indicadores es clave para tener éxito en detener un ataque.

1

Fase 1: Explotación e infección (T -00:00)
Para que un ataque tenga éxito, el archivo de ransomware malicioso debe ejecutarse en una computadora. Esto se realiza a menudo mediante un correo electrónico con suplantación de identidad o un código malicioso Exploit Kit. En el caso del malware CryptoLocker, el Angler Exploit Kit es un método preferido para obtener la ejecución.

2

Fase 2: Envío y ejecución (T -00:05)
Durante esta fase, los archivos ejecutables reales de ransomware se envían al sistema de la víctima. Tras la ejecución, se implementarán mecanismos de persistencia.

3

Fase 3: Adulteración de las copias de seguridad (T -00:10)
Unos segundos después, el ransomware ataca los archivos y carpetas con copias de seguridad en el sistema de la víctima y los elimina para evitar que se restablezcan desde las copias de seguridad. Esta es una característica única del ransomware; otros tipos de software fraudulento no se molestan en eliminar los archivos con copias de seguridad.

4

Fase 4: Encriptación de archivos (T -02:00)
Cuando las copias de seguridad se eliminan completamente, el malware realizará un intercambio de claves seguro con el servidor de comando y control (C2), lo cual establecerá aquellas claves de encriptación que se utilizarán en el sistema local.

5

Fase 5: Notificación de usuario y limpieza (T -15:00)
Con los archivos de copia de seguridad eliminados y el trabajo sucio de encriptación realizado, se presentan las instrucciones de demanda para extorsión y pagos. Generalmente, se le da a la víctima unos días para pagar. Después de ese momento, el rescate aumenta.

Finalmente, como las grabaciones de Misión Imposible que se autodestruyen, el malware se limpia del sistema para no dejar evidencia forense significativa que ayudaría a crear mejores defensas contra el malware.

Los ataques de ransomware están comenzando a crecer. Debido a que estos ataques son muy lucrativos para los autores, efectivamente se volverán más comunes, más dañinos y más costosos.

El éxito de su organización para defenderse contra un ataque de ransomware depende en gran medida de su nivel de preparación y las herramientas que implementa para monitorear sus sistemas a fin de detectar, responder ante y neutralizar actividad sospechosa.

Aprenda cómo puede detectar y neutralizar rápidamente un ataque de ransomware en **https://logrhythm.com/the-ransomware-threat-ebook/**

LogRhythm®
La compañía de inteligencia en seguridad