RANSOMWARE

INCIDENTES NOTABLES

En la primera mitad de 2019, los ciberdelincuentes fueron más selectivos sobre sus objetivos de ransomware, concentrándose principalmente en multinacionales, empresas e incluso organizaciones gubernamentales. Su modus operandi implicaba enviar a los empleados correos electrónicos de phishing personalizados, explotar las brechas de seguridad para obtener acceso a la red y luego moverse lateralmente dentro de la red.

El ransomware LockerGoga , por ejemplo, golpeó a una empresa manufacturera noruega y detuvo la producción en varias de sus plantas en marzo, lo que finalmente resultó en más de 55 millones de dólares en pérdidas financieras . Y la ciudad de Baltimore, Maryland, había incurrido en US $ 5,3 millones en costos de recuperación después de que sus sistemas fueron infectados con el ransomware RobbinHood en mayo.

Evidentemente, algunas organizaciones municipales fueron presionadas para que simplemente pagaran los rescates con la esperanza de restaurar rápidamente los sistemas afectados utilizados para sus servicios públicos. En particular, tres municipios en Florida fueron atacados por ataques de ransomware separados en el transcurso de varias semanas: Riviera Beach , por una variante de ransomware no identificada, y Lake City y Key Biscayne , ambos por el notorio ransomware Ryuk .

Riviera Beach
US $ 600,000
29 de mayo

Lake City
US $ 460,000
10 de junio

Key Biscayne
No se informó pago
el 23 de junio

Estos ataques de alto perfil y pagos de alto valor estuvieron en línea con el fuerte aumento en nuestras detecciones generales de ransomware desde la segunda mitad de 2018 hasta la primera mitad de 2019, aunque la cantidad de nuevas familias de ransomware disminuyó.

77%↑
Detecciones generales de ransomware en comparación con la segunda mitad de 2018

55%↓
Nuevas familias de ransomware en comparación con la segunda mitad de 2018

RUTINAS COMPLEJAS

También observamos rutinas destructivas más allá del cifrado de archivos. Algunas variantes de ransomware, incluidos los ejemplos a continuación, se diseñaron con características notables que disminuyeron las posibilidades de que las víctimas recuperen archivos y sistemas.

Ryuk
- Llega por correo no deseado
- Puede hacer que los sistemas infectados no se puedan iniciar

LockerGoga
- Llega a través de credenciales comprometidas
- Modifica las contraseñas de las cuentas de usuario de los sistemas infectados, evita que los sistemas infectados se reinicien

RobbinHood
- Llega a través de escritorios remotos no seguros o troyanos
- Cifra cada archivo con una clave única

BitPaymer
- Llega a través de cuentas comprometidas y correos electrónicos que contienen Dridex
- Abusos de la herramienta PsExec

MegaCortex
- Llega a través de controladores comprometidos
- Desactiva ciertos procesos

Nozelesn
- Llega por correo no deseado
: su descargador de troyanos, Nymaim, utiliza técnicas sin archivos para cargar el ransomware.