Informe de Análisis de Malware - LexCorp

Autor: Nicolas Veragara

Fecha: 23/12/2025

Incidente: 20-23 de junio de 2021

1. DATOS DE LA MUESTRA ANALIZADA

Nombre archivo: Ransomware.wannacry.exe.malz
Fecha analisis: 03 de noviembre de 2025
Sistema operativo: Windows 10 Professional (64-bit)
MD5: DB349897C3702275EA1D184TSC89EBA
Veredicto: ACTIVIDAD MALICIOSA (Ransomware)

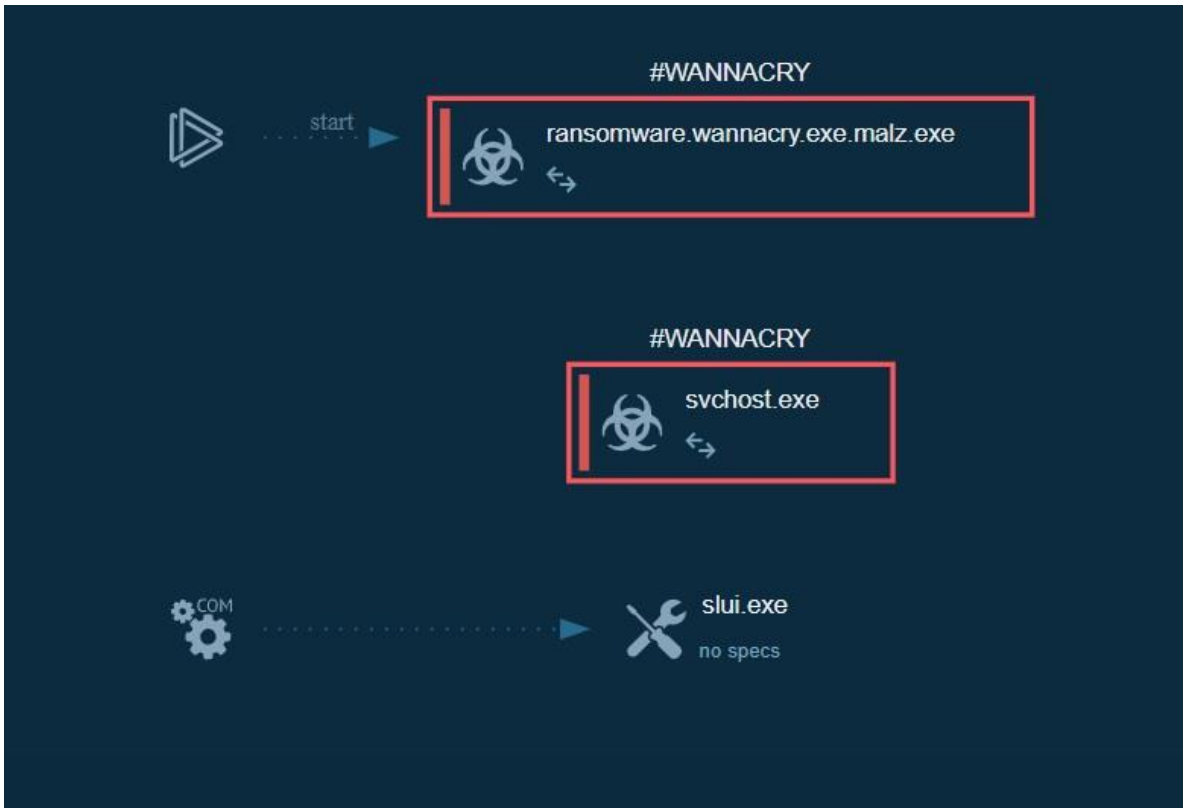
2. INFORMACIÓN ESTÁTICAENCONTRADA

Tipo archivo: PE32 ejecutable para Windows
Se hace pasar por: Microsoft® Disk Defragmenter (suplantación)
Compañía falsa: Microsoft Corporation
Timestamp: 2010-11-20 09:03:08

3. COMPORTAMIENTO OBSERVADO(ANÁLISIS DINÁMICO)

I)WANNACRY detectado - Ransomware confirmado
II)Se disfraza como utilidad legítima de Windows
III)Consulta información del sistema (nombre equipo, idiomas)
IV)Se comunica con internet para activar cifrado

DIAGRAMA DEL COMPORTAMIENTO:



4. ACTIVIDAD DE RED DETECTADA

Conexiones principales:
Dominio sospechoso:
www.luqeafsodp9fjaposdfj1gosurj1aewrvergwea.com
IP: 104.16.167.228
Propósito: Killswitch (interruptor de activación)

Amenazas de red detectadas:
ET MALWARE Possible WannaCry DNS Lookup
ET MALWARE WannaCry Ransomware Killswitch Domain HTTP Request

5. HIPÓTESIS DEL INCIDENTELEXCORP

¿Cómo entró el malware?

Probablemente a través de:

Correo electrónico con archivo adjunto malicioso
Descarga involuntaria desde internet
USB infectado conectado a un equipo

¿Cómo se propagó a toda la empresa?

El malware WannaCry aprovecha una vulnerabilidad en Windows llamada **EternalBlue**que permite propagarse automáticamente entre equipos conectados en red. ComoLexCorp tenía:

Windows Server 2003/2012 (vulnerables)
Windows 7/10 (algunos sin actualizar)

El malware saltó de equipo en equipo sin necesidad de intervención humana.

¿Qué hizo en cada equipo?

Cifró todos los archivos importantes
Mostró mensaje de rescate
Intentó desactivar copias de seguridad

6. IMPORTANCIA DE LOS BACKUPS RESTAURADOS

¿Por qué fue crucial restaurar desde elbackup del 19 de septiembre?

Única recuperación sin pagar rescate: Sin backup, los archivos eran irrecuperables
Estado pre-infección: El backup del 19/09 tenía los archivos SIN cifrar
Lección aprendida: Necesidad de backups regulares para toda la empresa

7. CONCLUSIONES

Comportamiento del malware: Ransomware que se propaga automáticamente porred y cifra archivos
Nombre general: WannaCry
Investigación del malware: Ransomware famoso de 2017 que usa la vulnerabilidadEternalBlue para propagarse rápidamente en redes corporativas
Tipo de malware: Ransomware (software de rescate)

Recomendaciones para LexCorp:

1) Aplicar todos los parches de seguridad a servidores y equipos
2) Implementar backups regulares para el 100% de los equipos
3) Capacitar empleados en identificar correos sospechosos
4) Segmentar la red para limitar propagación de malware

8. Herramientas

1) *sandbox ANY.RUN*