Grupo de ransomware: DeadLock

Resumen ejecutivo

DeadLock es una familia de ransomware orientada al **cifrado de información y a la extorsión económica**, caracterizada por renombrar los archivos comprometidos con un identificador único de víctima y la extensión .dlock. El malware emplea **múltiples vectores de infección**, incluyendo copias ilegales de software, adjuntos de correos dañinos infectados y descargas engañosas, lo que permite a los atacantes comprometer tanto equipos personales como estaciones de trabajo corporativas. Una vez obtenida la ejecución en el sistema víctima, DeadLock procede al cifrado de los ficheros de usuario y genera una nota de rescate con las instrucciones del pago a través de criptomonedas.

Para las organizaciones DeadLock supone un **riesgo severo** debido a su capacidad de provocar **interrupciones operativas críticas**, pérdida permanente de información, impacto en la continuidad del negocio y potencial daño reputacional. Por ello, DeadLock debe considerarse una **amenaza de alto riesgo para cualquier organización**, especialmente aquellas con controles de seguridad débiles, prácticas ineficientes de gestión de parches, dependencias operativas críticas de datos locales o con una cultura de ciberseguridad no madura.

Su mitigación requiere un enfoque centrado en la prevención, la realización de copias de seguridad robustas y aisladas, y la detección temprana mediante soluciones de seguridad basadas en comportamiento.

Grupo de ransomware: DeadLock

El ransomware DeadLock se especializa en el cifrado de archivos con el **objetivo de extorsionar económicamente a las víctimas**. El malware asigna a cada víctima un identificador único que forma parte tanto del nombre de los archivos cifrados como de la nota de rescate, lo cual permite a los atacantes gestionar las extorsiones de forma individualizada y correlacionar pagos con claves de descifrado específicas.

DeadLock se caracteriza por emplear múltiples **vectores de infección y técnicas de ingeniería social**, lo que manifiesta su capacidad operativa en entornos con una escasa madurez en materia de ciberseguridad. Una vez ejecutado, el ransomware **cifra los archivos de la víctima** (los renombra con la extensión ".dlock" y el identificador correspondiente) y despliega una **nota de rescate** que exige el pago en criptomonedas (como Bitcoin o Monero). Además, proporciona un canal de comunicación mediante la aplicación de mensajería anónima Session Messenger para negociar el rescate.

DeadLock se posiciona por tanto como un **malware de baja o media complejidad técnica, pero de alta eficacia operativa** debido a su amplio vector de distribución y modelo de extorsión personalizado.

Países y sectores afectados

DeadLock puede ser considerado como un **grupo oportunista y de ámbito internacional**, ya que no restringe su actividad a un país o sector especifico. Sin embargo, este ransomware verifica el idioma del sistema durante su ejecución y se detiene si detecta configuraciones basadas en el alfabeto cirílico.

Este comportamiento refleja la práctica de algunos malware, que evitan deliberadamente atacar ciertos países o regiones para reducir la atención de las autoridades locales o evitar repercusiones en sus propias jurisdicciones.

Análisis técnico

Desde el punto de vista técnico, la cadena de ataque de DeadLock **se inicia a través de la ejecución voluntaria por parte del usuario** de un fichero dañino. También se contempla la infección a través de unidades **USB infectadas y portales de soporte técnico falsos** que inducen a descargar “parches” que en realidad son el cargador del ransomware.

Una vez obtenida la ejecución en el sistema víctima, DeadLock procede al **cifrado de los ficheros de usuario**, cifrando cada fichero con la extensión .dlock. Tras el cifrado, el malware genera una nota de rescate en texto plano y modifica el fondo de escritorio para confirmar visualmente el compromiso.

En cuanto al comportamiento posterior a la fase de cifrado, el ransomware puede seguir cifrando nuevos archivos, recolectando credenciales, habilitando puertas traseras o intentando realizar movimientos laterales hacia otros equipos de la red local o recursos compartidos.

Características técnicas principales:

- **Cifrado:** DeadLock cifra archivos y los renombra añadiendo un identificador único a cada víctima junto a la extensión .dlock..
- **Acceso inicial:** Mediante ficheros dañinos ejecutados por usuarios, USB infectados y portales de soporte falsos.
- **Perfil del operador:** Evita el cifrado de ficheros en sistemas configurados con el alfabeto cirílico
- **Uso de herramientas Living Off the Land:** Uso de herramientas legítimas del sistema para el escaneo o descubrimiento de equipos.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1078** — Valid Accounts **T1133** — External Remote Services
Execution	**T1047** — Windows Management Instrumentation **T1059.003** — Command and Scripting Interpreter: Windows Command **T1106** — Native API
Persistence	**T1543.003** — Create or Modify System Process: Windows Service
Privilege Escalation	**T1055** — Process Injection
Defense Evasion	**T1006** — Direct Volume Access **T1027.013** — Encrypted/Encoded File **T1027.015** — Compression **T1497.001** — Virtualization/Sandbox Evasion: System Checks **T1562.001** — Impair Defenses: Disable or Modify Tools **T1622** — Debugger Evasion
Credential Access	**T1003** — OS Credential Dumping
Discovery	**T1046** — Network Service Discovery **T1082** — System Information Discovery **T1083** — File and Directory Discovery **T1135** — Network Share Discovery **T1614** — System Location Discovery
Lateral Movement	**T1021.001** — Remote Services
Collection	**T1039** — Data from Network Shared Drive
Command and Control	**T1219** — Remote Desktop Software
Impact	**T1486** — Data Encrypted for Impact **T1489** — Service Stop

Medidas de mitigación

Proactivas

- ❑ Implementar autenticación multifactor y formación frente a phishing. (T1078 – Valid Accounts)
- ❑ Restringir scripts y macros no firmados y controlar el uso de intérpretes como PowerShell o CMD. (T1059 – Command and Scripting Interpreter)
- ❑ Limitar cuentas con privilegios. (T1562 – Impair Defenses)
- ❑ Aplicar el principio de mínimo privilegio, segmentar la red y monitorizar accesos a recursos compartidos. (T1083 – File and Directory Discovery, T1135 – Network Share Discovery)
- ❑ Mantener copias de seguridad offline y probar restauraciones periódicas. (T1486 – Data Encrypted for Impact)
- ❑ En Windows, habilitar las reglas de reducción de superficie de ataque (ASR) para proteger LSASS y evitar el robo de credenciales. (T1003 - OS Credential Dumping)

Reactivas

- ❑ Usar antivirus con AMSI, aplicar reglas ASR y formar a los usuarios para bloquear archivos ofuscados. (T1027 - Obfuscated Files or Information)
- ❑ Usar soluciones de filtrado web basados en categorías y reputación. (T1133 – External Remote Services)

Conclusiones y recomendaciones

DeadLock representa una **amenaza significativa dentro del panorama actual de ransomware** debido a su enfoque oportunista, sus múltiples vectores de entrada basados en ingeniería social y su capacidad de cifrado. Además, la utilización de un identificador individual por víctima, junto con canales de comunicación anónimos, permite a los operadores gestionar con precisión el proceso de extorsión, reforzando su modelo de cobro por la clave de descifrado. Sin embargo, dicho pago no garantiza la recuperación de datos ni la eliminación del riesgo, dado que los grupos pueden retener acceso a sistemas comprometidos o reutilizar las credenciales obtenidas.

DeadLock debe considerarse un riesgo de alto impacto para los entornos corporativos y organizaciones. Por este motivo, se recomienda llevar a cabo copias de seguridad confiables, aisladas y probadas; aplicar de forma estricta el principio de mínimo privilegio y el control de macros y scripts; deshabilitar la ejecución automática de medios extraíbles y llevar a cabo campañas de concienciación para los usuarios.

