

Resumen ejecutivo

El grupo **SpaceBears** ha emergido como una nueva y sofisticada amenaza de **ransomware**, estrechamente vinculada con el Ransomware as a Service Phobos. Este grupo, que utiliza un **modelo de extorsión doble**, combina el cifrado de datos con amenazas de filtración pública de dicha información, aumentando así la presión sobre las víctimas. A lo largo de 2024, SpaceBears ha logrado atraer la atención por las agresivas campañas de ataques realizadas y por su capacidad para afectar tanto a **pequeñas como a grandes organizaciones**. Además, este actor de amenazas muestra signos de estar bien organizada, cuenta con una red de soporte global y hace uso de un sitio web en la dark web para filtrar los datos robados.

Entre las medidas técnicas desplegadas, se caracteriza por utilizar un vector de entrada a través de la **explotación de vulnerabilidades en el protocolo RDP** (Remote Desktop Protocol) y el uso de **correos electrónicos dañinos** (phishing). Además, utiliza **tácticas de evasión avanzadas** para evitar la detección y maximizar la efectividad del ataque.

SpaceBears representa un riesgo significativo, ya que este grupo impacta en la **disponibilidad** de los datos al cifrarlos y afecta a la **integridad y confidencialidad de la información** en el caso que se produzca su publicación. Además, SpaceBears puede exponer a sus víctimas a cuantiosas pérdidas económicas, daño a su reputación y posibles sanciones regulatorias. Por ello, **SpaceBears es una amenaza de alto nivel** para las organizaciones y deben implantar las medidas de seguridad recomendadas en este informe para prevenir y mitigar esta amenaza.

Grupo de ransomware: SpaceBears

SpaceBears es un grupo que apareció en abril de 2024, **afiliado al malware Phobos**, una de las familias de ransomware como servicio (RaaS) más activas en la actualidad.

SpaceBears utiliza un **modelo de doble extorsión**, combinando el **cifrado de información** de la víctima con la **amenaza de filtración** de los datos sensibles robados. Para ello, SpaceBears utiliza un sitio web de filtraciones en la dark web donde publica parte de la información robada y presiona a las organizaciones para que paguen el rescate, amenazando con hacer pública más información si no se cumple con sus demandas.

Una característica distintiva de SpaceBears es su **enfoque "corporativo"** en la presentación de su sitio de filtraciones, utilizan imágenes empresariales y un tono profesional que imita el estilo de una empresa legítima, lo que puede aumentar la presión sobre las víctimas al presentar sus demandas de manera más formal y estructurada. Este enfoque refleja una estrategia de extorsión calculada y profesional, diseñada para maximizar la efectividad de sus ataques.





Países y sectores afectados

Las víctimas de SpaceBears incluyen organizaciones que van desde pequeñas y medianas empresas hasta algunas de mayor tamaño. Los sectores más afectados incluyen el de las **tecnologías de la información, manufactura y servicios profesionales**, los cuales son objetivos frecuentes debido a sus vulnerabilidades en la gestión de los datos y en las infraestructuras de red. En términos geográficos, SpaceBears ha afectado a organizaciones en diversas regiones, aunque su actividad se concentra principalmente en **América del Norte y Europa**. Actualmente **España** ha registrado un total de **cinco víctimas**, de las cuales tres han sido en el último mes, lo que indica una tendencia en alza de sus ataques en este país.

Análisis técnico

SpaceBears utiliza correos **phishing** o explota las **vulnerabilidades conocidas en el protocolo RDP** para infiltrarse en las redes de las víctimas, una técnica comúnmente asociada con el ransomware Phobos. Una vez dentro, el ransomware SpaceBears **desactiva las copias de seguridad de volumen y otros mecanismos de protección de datos**, lo que dificulta la recuperación de la información sin el pago del rescate. Además, al igual que otras variantes de ransomware, SpaceBears puede emplear técnicas de evasión avanzadas para evitar la detección y maximizar la efectividad del ataque. Por último, el ransomware realiza el **cifrado de los datos** y realiza la **doble extorsión** para obtener beneficios económicos.

Características técnicas principales:

-  **Ransomware basado en Phobos:** SpaceBears utiliza el mismo código base que el ransomware Phobos, lo que le permite una distribución rápida y eficiente.
-  **Explotación de vulnerabilidades RDP:** Emplea vulnerabilidades en el protocolo RDP para obtener acceso remoto a las redes de las víctimas, aprovechando configuraciones inseguras o credenciales débiles.
-  **Desactivación de copias de seguridad:** Elimina las copias de seguridad y bloquea la restauración de datos sin el rescate.
-  **Uso de cifrado robusto:** Utiliza una combinación de AES-256 para el cifrado simétrico y RSA-1024 para el cifrado asimétrico.
-  **Modelo de doble extorsión:** SpaceBears ha adoptado el modelo de doble extorsión que no solo cifra los archivos de las víctimas, sino que también amenaza con publicar datos sensibles en caso de no recibir el rescate.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	T1133 – External Remote Services T1566.001 – Phishing: Spearphishing Attachment
Execution	T1059.003 – Command and Scripting Interpreter: Windows Command Shell T1204.002 – User Execution: Malicious File
Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Privilege Escalation	T1134 – Access Token Manipulation T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control
Defense Evasion	T1562.004 – Impair Defenses: Disable or Modify System Firewall T1562.001 – Impair Defenses: Disable or Modify Tools T1070.001 – Indicator Removal: Clear Windows Event Logs T1218.010 – System Binary Proxy Execution: Mshta
Credential Access	T1003.001 – OS Credential Dumping: LSASS Memory
Discovery	T1049 – System Network Connections Discovery T1057 – Process Discovery T1083 – File and Directory Discovery
Lateral Movement	T1021.001 – Remote Services: Remote Desktop Protocol
Collection	T1560.001 – Archive Collected Data: Archive via Utility
Command and Control	T1071.002 – Application Layer Protocol: Ingress Tool Transfer
Exfiltration	T1048 – Exfiltration Over Alternative Protocol
Impact	T1486 – Data Encrypted for Impact T1490 – Inhibit System Recovery

Medidas de mitigación

Proactivas

- Restringir accesos remotos y aplicar autenticación multifactor. (T1133/T1021 - External Remote Services/ Remote Desktop Protocol)
- Monitorizar y proteger claves de inicio automático. (T1547.001 - Registry Run Keys / Startup Folder)
- Utilizar el control de aplicaciones cuando sea apropiado y eliminar herramientas desactualizadas o que no sean imprescindibles. (T1562.001 - Impair Defenses)
- Habilitar ASR y Credential Guard, restringir NTLM y WDigest, y usar contraseñas únicas. (T1003.001 - OS Credential Dumping: LSASS Memory)
- Restringir privilegios, segmentar la red, controlar accesos remotos y auditar consultas y accesos a archivos. (T1083 - File and Directory Discovery)
- Prevenir la ejecución de código no autorizado implementando control de aplicaciones, bloqueo de scripts y otros mecanismos de prevención de ejecución. (T1059.003 - Command and Scripting Interpreter: Windows Command Shell)

Reactivas

- Habilitar reglas de Reducción de Superficie de Ataque (ASR) para evitar la ejecución de archivos dañinos. (T1204 - User Execution: Malicious File)
- Utilizar dispositivos de red y software de endpoints para filtrar el tráfico de entrada, salida y lateral de la red. (T1048 - Exfiltration Over Alternative Protocol)

Conclusiones y recomendaciones

SpaceBears plantea un riesgo alto a las organizaciones, no solo por los daños directos del cifrado de datos y la extorsión financiera, sino también por las posibles consecuencias hacia la disponibilidad y confidencialidad de la información y las repercusiones en términos de reputación y confianza. Los grupos como SpaceBears utilizan la ingeniería social y explotan vulnerabilidades en la infraestructura de seguridad, sobre todo aquellas relacionadas con el acceso remoto, para infiltrarse en redes corporativas de manera eficiente con el objetivo de cifrar su información y extorsionar a las organizaciones.

Por todo ello, SpaceBears representa una amenaza avanzada que exige una respuesta integral y proactiva. Las organizaciones deben estar preparadas para enfrentarse a un ataque de esta magnitud mediante la implementación de tecnologías de seguridad avanzadas, la formación continua de su personal y la planificación de estrategias de recuperación ante desastres.

