Grupo: Arcus Media Ransomware

Resumen ejecutivo

Arcus Media es un grupo de ransomware detectado a mediados de 2024 y que ha ganado notoriedad durante 2025. Actúa bajo un modelo **Ransomware-as-a-Service (RaaS),** lo que facilita que múltiples afiliados, con distintos niveles de sofisticación, ejecuten ataques a gran escala. Su objetivo principal son organizaciones de sectores como servicios empresariales, manufactura, salud, retail y medios de comunicación, con víctimas registradas en América, Europa y Asia.

A nivel operativo, Arcus Media muestra un alto grado de profesionalización, con **tácticas de evasión y persistencia** similares a las de **familias consolidadas como LockBit o BlackCat**. El grupo elimina copias de seguridad (shadow copies), borra registros de eventos, finaliza procesos críticos y desactiva servicios de seguridad antes del cifrado, asegurando la máxima disrupción de los sistemas afectados.

El principal riesgo que este grupo supone para las organizaciones radica en su **orientación hacia la disrupción del negocio**. Ya que, a diferencia de grupos más centrados en la innovación técnica, Arcus Media optimiza la eficiencia de sus ataques, cifrando parcialmente grandes ficheros para maximizar la velocidad del ataque, apuntando a sistemas críticos (bases de datos, correo, aplicaciones corporativas,…) y destruyendo deliberadamente mecanismos de restauración. Además, su modelo de doble extorsión (cifrar los sistemas y amenazar con la publicación de datos sensibles) puede generar **daños reputacionales y afectación financiera**, especialmente en sectores donde el dato es crucial o en sectores altamente regulados (servicios financieros, salud, tecnología o manufactura).

Grupo de ransomware: Arcus Media

Arcus Media es un grupo de ransomware que opera bajo el modelo Ransomware-as-a-Service (RaaS). Las campañas de Arcus Media se basan en **accesos iniciales** mediante **phishing**, **credenciales comprometidas** o **explotación** de **servicios expuestos** (RDP/VPN). Una vez dentro, los operadores hacen uso de **herramientas legítimas** (living-off-the-land) y **frameworks como Cobalt Strike o Mimikatz** para el movimiento lateral y la recolección de credenciales.

Por último, emplea tácticas de **doble extorsión**, combinando el cifrado de sistemas y la exfiltración de datos. Los archivos cifrados quedan marcados con una extensión específica y se acompaña una nota de rescate con instrucciones de contacto.

Países y sectores afectados

Arcus Media es un grupo emergente de ransomware cuya actividad se ha intensificado durante 2025. Según los datos disponibles, los países donde más actividad se observa incluyen **Brasil, Estados Unidos y Europa** (Francia, España…)

En España, el grupo Arcus Media ha alcanzado al menos **seis víctimas confirmadas**, que abarcan varios sectores clave tales como **tecnología, servicios empresariales, consultoría y educación.** Además, se suma al listado de víctimas una empresa especializada en **ciberseguridad.**

Los **sectores más atacados** por Arcus Media incluyen principalmente **tecnología/TI y servicios empresariales**, seguidos de **agricultura** y **producción de alimentos, transporte y logística**, y **salud**. Esto refleja que el grupo centra sus ataques en organizaciones con alta dependencia tecnológica, aunque también afecta a sectores con información crítica o sensible.

Análisis técnico

Arcus Media es un ransomware que opera como RaaS, accediendo a las redes mediante **credenciales comprometidas o servicios expuestos**. Una vez dentro, se mueve lateralmente, extrae datos y cifra archivos, dejando extensiones propias. También elimina copias de seguridad y detiene servicios críticos para dificultar la recuperación.

El ransomware emplea **cifrado híbrido** basado en **ChaCha20** con **claves protegidas** mediante **RSA-2048**, además de técnicas de cifrado parcial de archivos grandes para acelerar la operación.

Características técnicas principales:

- **Vectores de acceso inicial:** credenciales comprometidas, VPN/RDP expuestos y explotación de vulnerabilidades en aplicaciones empresariales.
- **Movimiento lateral:** uso de credenciales robadas y herramientas de administración remota para expandirse dentro de la red.
- **Exfiltración:** extracción de datos antes del cifrado; en algunos incidentes se han observado utilidades de sincronización y exfiltración (p.ej. Rclone u otras) para transferir datos a destinos remotos.
- **Cifrado:** algoritmo híbrido (cifrado simétrico para archivos + protección de claves con criptografía asimétrica); genera extensiones/nombres de fichero propios para identificar las víctimas.
- **Técnicas de evasión:** eliminación de shadow copies, limpieza de logs y terminación de servicios/backups para impedir la recuperación.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1190** — Exploitation of Public-Facing Application **T1566** — Phishing **T1078** — Valid Accounts
Execution	**T1059.001** — Command and Scripting Interpreter: PowerShell **T1053** — Scheduled Task/Job
Persistence	**T1547.001** — Registry Run Keys / Startup Folder **T1543** — Service Installation
Privilege Escalation	**T1068** —Exploitation for Privilege Escalation **T1548** — Abuse Elevation Control Mechanism
Defense Evasion	**T1070** — Indicator Removal on Host **T1490** — Inhibit System Recovery **T1562.001** — Impair Defenses: Disable or Modify Tools
Discovery	**T1046** — Network Service Scanning **T1016** — System Network Configuration Discovery
Lateral Movement	**T1021** — Remote Services **T1078** — Use of Valid Accounts
Command and Control	**T1071.001** — Application Layer Protocol
Impact	**T1486** — Data Encrypted for Impact **T1485** — Data Destruction

Medidas de mitigación

Proactivas

- ❑ Capacitación a usuarios, filtrado de correos y enlaces sospechosos, uso de MFA y análisis de adjunto. (T1566 – Phishing)
- ❑ Actualizar software y aplicar parches de seguridad. (T1190 – Exploitation of Public-Facing Application)
- ❑ Restringir accesos remotos y usar autenticación multifactor. (T1078 – Valid Accounts, T1021 – Remote Services)
- ❑ Auditar la creación de tareas programadas y restringir privilegios. (T1053 – Scheduled Task / Job)
- ❑ Proteger claves de inicio automático. (T1547 – Registry Run Keys / Startup Folder)
- ❑ Proteger copias de seguridad y monitorizar su eliminación. (T1490 – Inhibit System Recovery)
- ❑ Mantener copias de seguridad seguras y probar restauraciones. (T1486 – Data Encrypted for Impact)

Reactivas

- ❑ Limitar la ejecución de scripts no firmados y registrar su uso. (T1059 – PowerShell / Command Shell)
- ❑ Usar EDR y proteger credenciales en memoria. (T1003 – OS Credential Dumping)

Conclusiones y recomendaciones

Arcus Media se ha consolidado en 2025 como uno de los grupos de ransomware más activos, con amplia presencia en América, Europa y especialmente en España. Su modelo **Ransomware-as-a-Service (RaaS),** basado en operadores y afiliados, le permite escalar ataques y dificultar su atribución. Destaca por su organización, capacidad técnica y variedad de sectores afectados.

Aunque algunos indicios apuntan a que Arcus Media podría compartir infraestructura o metodologías con otros grupos, análisis recientes lo identifican como una **entidad independiente dentro del ecosistema del ransomware**, centrada en la doble extorsión y la explotación de accesos remotos vulnerables.

Para mitigar el riesgo frente a Arcus Media, se **recomienda reforzar la seguridad de accesos externos mediante autenticación multifactor** (MFA), mantener **copias de seguridad**, aplicar **segmentación de red**, **limitar privilegios administrativos y desplegar soluciones de detección y respuesta** (EDR/XDR). Asimismo, la **monitorización continua de amenazas** y **vulnerabilidades** resulta esencial para anticipar posibles intrusiones y minimizar su impacto.

