

Resumen ejecutivo

Play Ransomware (también llamado Play o Playcrypt) es un grupo cibercriminal con motivación económica activo al menos desde junio de 2022, especializado en campañas de ransomware de **doble y múltiple extorsión** contra organizaciones de todo el mundo. Entre sus víctimas se incluyen administraciones públicas, infraestructuras críticas, entidades financieras, empresas industriales, educativas y sanitarias en Norteamérica, Sudamérica, Europa y Australia.

Desde el punto de vista técnico, Play destaca por el **uso de vulnerabilidades conocidas** en productos corporativos como FortiOS y Microsoft Exchange (ProxyNotShell), el **abuso de servicios como RDP o VPN** y el **uso de credenciales válidas robadas** para el acceso inicial a las redes internas de las víctimas.

Una vez alcanzado el acceso inicial, el ransomware ataca sistemas Windows, Linux y ESXi. Combinando herramientas de post-explotación muy maduras (Cobalt Strike, SystemBC, Empire, Mimikatz, PsExec,...) para obtener la persistencia y un **cifrado híbrido AES-256/RSA-2048** con cifrado intermitente para evadir las soluciones de seguridad basadas en detección de patrones de cifrado masivo. Además, una vez exfiltrados los datos utiliza un portal en la red Tor ("Play News") donde publica los datos de las víctimas que se niegan a pagar.

La combinación de capacidades técnicas avanzadas, selección de objetivos de alto valor, evolución hacia un modelo RaaS y un volumen creciente de víctimas sitúa a Play actualmente entre los grupos de **ransomware más relevantes y peligrosos** para empresas e instituciones públicas.

Grupo de ransomware: Play

Play Ransomware es un grupo con motivación de obtener **beneficios económicos** mediante la extorsión a organizaciones medianas y grandes. Fue detectado por primera vez en junio de 2022 y su nombre procede de la extensión ".PLAY" que añade a los archivos cifrados. El grupo es también conocido por nombres como Playcrypt y combina el cifrado y exfiltración de datos sensibles junto a la amenaza de publicarlo para incrementar la presión sobre las víctimas. El grupo mantiene un **sitio de fuga de datos en Tor** llamado "Play News", donde lista víctimas, publica contadores de tiempo y difunde parte de la información robada para maximizar el impacto reputacional y obligar a la negociación.

Actualmente Play está adaptando su modelo criminal independiente hacia un **modelo RaaS** (Ransomware as a Service) con TTP homogéneas aplicadas por distintos operadores afiliados y playbooks reutilizables, lo que aumenta el potencial de expansión de sus campañas.

Países y sectores afectados

Las campañas de Play Ransomware han tenido un **alcance geográfico amplio**, impactando a multitud de empresas e infraestructuras críticas en Norteamérica, Sudamérica, Australia y Europa. Destacando países particularmente afectados como Estados Unidos, Canadá, Reino Unido, Alemania, Francia, Australia y Sudáfrica, entre otros.


En cuanto a los **sectores más afectados**, Play muestra un patrón de ataque orientado a **entidades con capacidad de pago y alto impacto operativo**. Las víctimas incluyen instituciones y empresas de sectores como **sanidad, servicios financieros, educación, telecomunicaciones, transporte, medios de comunicación, empresas de tecnología y defensa**.


Análisis técnico


Play Ransomware inicia sus intrusiones principalmente mediante el abuso de credenciales válidas, phishing, la explotación de servicios expuestos a Internet (RDP/VPN) y especialmente vulnerabilidades conocidas en FortiOS y Microsoft Exchange. Una vez dentro del entorno, el grupo realiza tareas de reconocimiento para enumerar la infraestructura y evadir las defensas mediante el uso de herramientas legítimas del sistema, scripts de PowerShell y técnicas de living-off-the-land.

Posteriormente, emplea herramientas de mando y control y post-explotación para facilitar el movimiento lateral, la persistencia y la escalada de privilegios. Antes de ejecutar el cifrado, filtra información sensible para habilitar la doble extorsión, comprimiendo los datos y transfiriéndolos a infraestructuras bajo su control. El impacto final se materializa mediante ransomware que utiliza cifrado híbrido AES-256/RSA-2048, renombrando los archivos con la extensión “.PLAY”.

Características técnicas principales:

 **Vector de acceso inicial:** El ransomware se dirige a sistemas Microsoft Windows en entornos corporativos y a sistemas Linux/VMware ESXi orientada al cifrado de máquinas virtuales y recursos asociados.

 **Herramientas:** Emplea un conjunto de herramientas como frameworks de post-explotación, utilidades de enumeración, malware de credenciales, herramientas de manipulación del sistema y software legítimo para empaquetar y transferir información.

 **Cifrado:** Esquema de cifrado híbrido basado en AES-256 y RSA-2048, utilizando un cifrado intermitente por bloques para evadir mecanismos de detección basados en análisis estático o heurístico.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	T1078 – Valid Accounts T1190 – Exploit Public Facing Application T1133 – External Remote Services T1059.001 – Command and Scripting Interpreter: PowerShell
Execution	T1053.005 – Scheduled Task/Job: Scheduled Task T1203 – Exploitation for Client Execution T1204.002 – User Execution: Malicious File T1047 – Windows Management Instrumentation
Persistence	T1547.001 – Registry Run Keys / Startup Folder T1112 – Modify Registry
Privilege Escalation	T1055 – Process Injection: Dynamic-link Library Injection T1055.012 – Process Hollowing
Defense Evasion	T1562.001 – Impair Defenses: Disable or Modify Tools T1070.001 – Indicator Removal: Clear Windows Event Logs
Credential Access	T1552 – Unsecured Credentials T1003 – OS Credential Dumping
Discovery	T1016 – System Network Configuration Discovery T1518.001 – Software Discovery: Security Software Discovery
Lateral Movement	T1570 – Lateral Tool Transfer
Collection	T1560.001 – Archive Collected Data: Archive via Utility
Command and Control	T1484.001 – Domain Policy Modification: Group Policy Modification
Exfiltration	T1048 – Exfiltration Over Alternative Protocol
Impact	T1078 – Data Encrypted for Impact

Medidas de mitigación

Proactivas

- ❑ Implementar MFA para reducir el impacto del robo de credenciales y acceso no autorizado. (T1555 - Credentials from Password Stores)
- ❑ Bloquear macros y deshabilitar contenido activo en documentos Office provenientes de correo electrónico. (T1203 - Exploitation for Client Execution)
- ❑ Activar listas de aplicaciones permitidas (allowlisting) para impedir la ejecución de binarios desconocidos. (T1047 - Windows Management Instrumentation)
- ❑ Restringir privilegios y aplicar un modelo de mínimos privilegios para evitar persistencia y ejecución de componentes dañinos. (T1562 - Impair Defenses)

Reactivas

- ❑ Usar EDR o antivirus con capacidades de detección de *malware* y *herramientas post-explotación*. (T1203 - Exploitation for Client Execution)
- ❑ 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)
- ❑ Habilitar reglas de Reducción de Superficie de Ataque (ASR) para evitar la ejecución de archivos dañinos. (T1204.002 - User Execution: Malicious File)

Conclusiones y recomendaciones

Play Ransomware se ha consolidado en pocos años como un **grupo de referencia** dentro del ecosistema de ransomware global, combinando TTP maduras, una **orientación clara a objetivos de alto valor** y un ciclo de innovación técnica que incluye técnicas avanzadas de evasión y la expansión a plataformas como ESXi.

Para reducir la exposición a ataques como Play Ransomware y reforzar la seguridad de los sistemas, se recomienda adoptar un enfoque integral que combine prevención, detección y respuesta. Esto incluye priorizar la **gestión de vulnerabilidades** en servicios expuestos a Internet y la **reducción de la superficie de ataque**, especialmente en accesos remotos como RDP y VPN, incorporando **autenticación multifactor**. Asimismo, es fundamental fortalecer la **gestión de identidades mediante políticas de contraseñas robustas**, el **principio de mínimo privilegio** y la **revisión periódica de cuentas privilegiadas**. La resiliencia operativa debe garantizarse mediante **copias de seguridad** seguras, offline e inmutables, con pruebas regulares de restauración. Finalmente, resulta clave contar con planes de respuesta a incidentes bien definidos y fomentar la concienciación del personal.

