

Resumen ejecutivo

SafePay es un grupo cibercriminal que opera bajo el modelo de **Ransomware-as-a-Service** (RaaS), dificultando de este modo la atribución directa de sus ataques y amplificando el alcance y la velocidad de propagación del malware.

Desde mediados de 2024, SafePay ha sido vinculado con al menos 250 ataques exitosos, afectando a empresas en Estados Unidos, Europa y Asia. Sus campañas han demostrado un enfoque selectivo y dirigido hacia sectores estratégicos, como, por ejemplo, **servicios financieros, sanidad, tecnología, manufactura y educación**. Esto refleja una comprensión profunda del valor de los datos en estos sectores y una clara intención de maximizar el impacto financiero y reputacional sobre sus posibles víctimas. Para ello, el grupo emplea entre sus tácticas un esquema de **doble extorsión** en el que la amenaza de publicación de datos sensibles en la dark web se suma al cifrado de los sistemas comprometidos.

Una característica destacada de SafePay es su enfoque operativo metódico. En muchos casos, los ataques son precedidos por una etapa de **reconocimiento y recopilación de información**, lo cual les permite identificar empresas y sectores clave y planificar los ataques de una manera más estratégica. Este nivel de planificación, junto con las capacidades técnicas demostradas y su capacidad de evolución, indica una **madurez operativa superior** a la media.

Por ello, se recomienda a las organizaciones implementar una defensa en profundidad, priorizando la monitorización, la detección de movimientos laterales, la segmentación de red y la capacidad de respuesta rápida.

Actor de amenazas: SafePay

SafePay ha logrado consolidarse en pocos meses como una organización cibercriminal con operaciones sostenidas y metódicas. A diferencia de otros colectivos de ransomware menos organizados, destaca por su:

- ❑ Modelo de negocio RaaS, que permite a afiliados lanzar ataques en su nombre, aumentando la escala de campañas.
- ❑ Actividad constante en foros clandestinos, donde publican datos filtrados como presión hacia las víctimas.
- ❑ Capacidad de adaptación sectorial, ajustando técnicas según el sector y el tamaño de la organización objetivo.
- ❑ Metodología previa de reconocimiento, que les permite elegir objetivos con datos de mayor valor o con menor capacidad defensiva.

Países y sectores afectados






SafePay ha centrado sus ataques en organizaciones situadas en América del Norte, Europa y Asia, con un número significativo de víctimas en Estados Unidos, Reino Unido, Alemania, España y Canadá. En cuanto a los sectores afectados, destacan principalmente los de servicios financieros, sanidad, educación, manufactura y tecnología. El grupo ha demostrado una capacidad notable para adaptar sus ataques a diferentes industrias, maximizando así el impacto operativo financiero y reputacional sobre sus objetivos.

Durante 2025, el grupo ha atacado varias organizaciones españolas, entre ellas Cámara Valencia, Avance Agrícola SL, Solge, Grupo Azpiaran, entre otras. Estos incidentes han evidenciado la necesidad de fortalecer las defensas en ciberseguridad.

Análisis técnico

SafePay utiliza un flujo de ataque estructurado que combina accesos iniciales mediante credenciales comprometidas, movimientos laterales con herramientas legítimas del sistema y la posterior exfiltración y cifrado de información crítica. Este modus operandi, reforzado con técnicas avanzadas de evasión y persistencia, le permite operar con un alto grado de efectividad y baja detección por las defensas tradicionales.

Características técnicas principales:

-  Acceso inicial mediante **credenciales comprometidas y uso de herramientas RDP/VPN**.
-  Técnicas de evasión a través **herramientas legítimas** (LOLT), desactivación de antivirus, borrado de logs,...
-  SafePay aplica un modelo de **dobles extorsión**: primero cifra los datos de la víctima y, si no se realiza el pago, amenaza con divulgar públicamente los datos exfiltrados en la dark web.
-  **Exfiltración de datos** a través del uso de protocolos HTTPS/SFTP hacia servidores controlados por el atacante.
-  Uso de **técnicas de persistencia** en los sistemas comprometidos a través de la instalación de scripts y modificación de claves de registro.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	T1078 – Valid Accounts
Execution	T1059 – Command and Scripting T1059.001 – PowerShell T1059.003 – Windows Command Shell T1202 – System Binary Proxy Execution
Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism: Bypass UAC
Defense Evasion	T1562.001 – Impair Defenses: Disable or Modify Tools T1070.004 – File Removal
Credential Access	T1003 – OS Credential Dumping
Discovery	T1135 – Network Share Discovery T1482 – Domain Trust Discovery
Lateral Movement	T1021 – Remote Services
Collection	T1560.001 – Archive Collected Data: Archive via Utility
Exfiltration	T1048 – Exfiltration Over Alternative Protocol T1048.003 – Exfiltration Over Web Service
Impact	T1486 – Data Encrypted for Impact T1490 – Inhibit System Recovery

Medidas de mitigación

Proactivas

- ❑ Implementar autenticación multifactor (MFA) para evitar accesos no autorizados (T1078 - Valid Accounts)
- ❑ Evita la ejecución de código no autorizado o dañino en los sistemas mediante el uso de control de aplicaciones y bloqueo de scripts. (T1059.003 – Windows Command Shell)
- ❑ Utilizar el nivel de cumplimiento más alto para UAC cuando sea posible. (T1548.002 – Abuse Elevation Control Mechanism: Bypass UAC)
- ❑ Auditar los cambios en herramientas de seguridad y configurar alertas ante modificaciones o desactivaciones para detectar actividad dañina. (T1562.001 - Impair Defenses: Disable or Modify)
- ❑ Segmentar la red para limitar el descubrimiento. (T1482 – Domain Trust Discovery)
- ❑ Considerar deshabilitar o restringir el protocolo NTLM y la autenticación de tipo WDigest. Evitar el uso de la misma credencial en diferentes cuentas corporativas. (T1003 - OS Credential Dumping)
- ❑ Evitar el acceso remoto innecesario a recursos compartidos de archivos, hipervisores, sistemas sensibles, etc. (T1021 – Remote Services)

Reactivas

- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos, desactivar PowerShell cuando no sea necesario o usar el modo "Constrained Language" para restringir el acceso (T1059.001 - Command and Scripting Interpreter: PowerShell).

Conclusiones y recomendaciones

SafePay representa una amenaza significativa para organizaciones e infraestructuras críticas debido a su enfoque técnico profesionalizado, su uso de técnicas avanzadas de evasión y su modelo de doble extorsión. A pesar de ser un grupo relativamente reciente, su impacto operativo ha sido considerable, destacando su capacidad para explotar accesos remotos inseguros y su madurez operativa.

Se recomienda a las organizaciones implementar controles estrictos de acceso remoto, como autenticación multifactor (MFA) y segmentación de red, junto con la implementación de servicios de ciberinteligencia que monitoricen de manera periódica posibles credenciales expuestas en foros clandestinos. Además, es crucial implementar estrategias de defensa en profundidad y adoptar un enfoque proactivo y coordinado en ciberseguridad para mitigar sus efectos y proteger los activos más sensibles.

