SoftSecurity
Soluciones innovadoras en Ciberseguridad

BOLETÍN DE SEGURIDAD

Campaña de Ransomware Safe Pay

NOVIEMBRE 2026

El material incluido en este documento es propiedad exclusiva de SOFTSECURITY SAS. Este documento no puede ser divulgado de cualquier manera o a cualquier persona a excepción del destinatario y los empleados o representantes de la firma a quien va dirigido, quienes son los directamente responsables de la evaluación de su contenido. Este documento no puede ser utilizado en cualquier forma diferente al propósito con el que fue distribuido. Se prohíbe terminantemente cualquier uso, reproducción o transmisión no autorizada.

INTRODUCCIÓN

En un mundo cada vez más conectado, la ciberseguridad no es solo responsabilidad del área de TI: es un compromiso de todos. Este boletín tiene como objetivo mantenerte informado sobre las amenazas más recientes, las buenas prácticas de seguridad digital y las acciones clave que puedes tomar para proteger tanto tu información personal como los activos de las organizaciones.

En el siguiente informe se encontrará información sobre amenazas actuales, recomendaciones e indicadores de compromiso.

¿Qué se conoce sobre la amenaza SafePay Ransomware?

SafePay es un grupo de ransomware identificado con alta actividad operativa desde agosto de 2024. A diferencia del ecosistema tradicional que opera bajo el modelo de Ransomware como Servicio (RaaS) mediante redes de afiliados externos, SafePay destaca por operar con un modelo interno cerrado: un único equipo central planifica y ejecuta internamente todas las fases de la intrusión, desde el acceso perimetral inicial hasta la exfiltración masiva, el cifrado y la negociación coercitiva.

A principios de 2025, el grupo contaba con cerca de 200 organizaciones afectadas; sin embargo, para octubre de 2026 la cifra ha escalado a más de 600 víctimas confirmadas a nivel mundial. Esta expansión motivó la emisión de la alerta conjunta internacional AA26-293A por parte de la Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA), el FBI, el Servicio Secreto estadounidense, la Agencia Nacional contra el Crimen del Reino Unido (NCA) y la Policía de Investigación

Análisis del ataque

El análisis exhaustivo de la telemetría y los reportes de respuesta a incidentes revela que SafePay no depende exclusivamente del engaño al usuario final. El actor prioriza la intrusión silenciosa mediante la explotación sistemática de aplicaciones y servicios perimetrales expuestos a Internet, seguida del establecimiento de túneles encubiertos y la manipulación de identidades privilegiadas.

1. Vector de Acceso Inicial y Explotación Perimetral

SafePay obtiene acceso a las infraestructuras corporativas mediante tres mecanismos convergentes:

• Explotación automatizada de vulnerabilidades conocidas: El grupo escanea proactivamente rangos de red buscando dispositivos de borde desactualizados, atacando específicamente cortafuegos Cisco ASA/FTD, plataformas de respaldo Veeam Backup & Replication y firewalls SonicWall SonicOS.

• Fuerza bruta contra servicios VPN: Ataques dirigidos de diccionario y rociado de contraseñas (password spraying) contra portales VPN de acceso remoto que carecen de mecanismos de bloqueo de intentos o autenticación multifactor.

2. Persistencia, Evasión de Defensas y C2 Encubierto

• Despliegue de la puerta trasera QDoor (soc.dll): Para ocultar la ejecución de su código malicioso, SafePay emplea la técnica de vaciado de procesos (Process Hollowing, T1055.012), inyectando el backdoor QDoor dentro de procesos legítimos del sistema operativo como WerFault.exe (Windows Error Reporting).

• Abuso de herramientas legítimas de acceso remoto (RMM): Instalan y configuran utilidades de administración remota como ScreenConnect (establecido como servicio de inicio automático de Windows), AnyDesk y TeamViewer para mantener acceso directo sin despertar sospechas en las soluciones de seguridad perimetral.

• Enmascaramiento (Masquerading, T1036): Renombran sus herramientas para suplantar ejecutables legítimos, tales como Socks_werfault.exe, o ejecutan instancias anómalas de svchost.exe ubicadas fuera del directorio protegido System32.

3. Movimiento Lateral, Exfiltración y Doble Extorsión

Durante la fase interna de la intrusión, SafePay ejecuta un reconocimiento agresivo de la infraestructura de Active Directory:

• Extracción masiva de credenciales: Emplean Mimikatz para volcar contraseñas y hashes de la memoria de procesos críticos (LSASS) y dcsync.exe para simular la replicación de controladores de dominio mediante ataques DCSync (T1003.006).

• Enumeración de recursos de red: Utilizan scripts de PowerShell y herramientas comunitarias como ShareFinder.ps1, SharpShares.exe, netscan.exe y nltest.exe para mapear recursos compartidos y relaciones de confianza interdominio.

• Propagación lateral: Ejecutan comandos remotos y se desplazan a través de la red interna empleando PsExec, WinRM y conexiones SMB nativas.



.

IOCs Indicadores de compromiso y Recomendaciones

Se recomienda fortalecer las capacidades de monitoreo y detección mediante la búsqueda de los siguientes **Indicadores de Compromiso (IoCs)** identificados durante el análisis.

Dirección IP	88[.]119[.]167[.]239	Servidor de Comando y Control (C2) asociado a la puerta trasera soc.dll (QDoor).
Hash SHA-1	b498a2683640c983bb069fa2ea9e67cef4a3797d	locker.dll — Carga ejecutable principal PE32 del ransomware SafePay.
Hash SHA-256	327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917	locker.dll — Archivo ejecutable PE32 utilizado en fases de cifrado local.
Hash SHA-256	a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526	locker.dll — Variante compilada del binario de cifrado.
Hash SHA-256	bbdd3620a67aedec4b9a68b2c9cc880b6631215e129816aea19902a6f4bc6f41	SharpShares.exe — Herramienta para enumeración de recursos de red compartidos.

RECOMENDACIONES Y MEDIDAS DE MITIGACIÓN

SoftSecurity recomienda implementar con carácter prioritario las siguientes medidas técnicas de protección en capas:

- Gestión Prioritaria de Parches y Activos Perimetrales: Aplicar de inmediato las actualizaciones de seguridad en dispositivos de borde expuestos a Internet para corregir las vulnerabilidades explotadas: CVE-2020-3259 y CVE-2023-20269 (Cisco ASA/FTD), CVE-2023-27532 y CVE-2024-40711 (Veeam Backup) y CVE-2024-40766 (SonicWall SonicOS). Aislar o deshabilitar interfaces de administración web expuestas a redes públicas.

- Autenticación Fuerte y Multifactor (MFA): Hacer obligatorio el uso de Autenticación Multifactor (MFA) robusta en todas las conexiones VPN de acceso remoto, portales de correo electrónico, plataformas RMM y accesos administrativos a servidores y servicios en la nube.

- Control y Bloqueo de Herramientas Duales y Software RMM: Restringir mediante directivas de Endpoint (AppLocker, WDAC o EDR) la ejecución no autorizada de herramientas comunes de exfiltración como RClone, WinSCP o b2.exe, así como soluciones de acceso remoto no homologadas corporativamente (AnyDesk, TeamViewer o ScreenConnect no administrado).

Referencias

- BOLETIN COLCERT 20261106