CSIRT Salud

Boletín informativo

CSIRTSALUD-AL-20260417-93

TLP: CLEAR

Alerta ID:	093
Fecha del reporte:	17/04/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	SpankRAT explota los procesos del Explorador de Windows
Herramienta de detección	N/A
Activo involucrado:	
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema digital sobre la identificación de un nuevo toolkit de acceso remoto denominado SpankRAT, el cual abusa de procesos legítimos del sistema operativo Windows —particularmente explorer.exe— para lograr persistencia, evadir controles de seguridad basados en reputación y mantener un canal oculto de comando y control (C2) con los atacantes.

Descripción:

SpankRAT es un troyano de acceso remoto (RAT) desarrollado en lenguaje Rust y estructurado en dos componentes principales: un cargador inicial (SpankLoader) y un agente persistente (rmm_agent.dll / RmmAgentCore). Este toolkit fue identificado y analizado por el equipo de investigación de ANY.RUN, que lo catalogó como una amenaza sigilosa de alto riesgo debido

a su capacidad de enrutar el tráfico de mando y control a través de procesos de confianza del sistema operativo Windows.

La característica distintiva de SpankRAT es que, una vez instalado, inyecta su DLL maliciosa dentro del proceso legítimo explorer.exe, de modo que las comunicaciones C2 generadas por el malware aparentan provenir de un binario propio y firmado del sistema operativo. Esto permite eludir controles de detección basados en reputación, retrasar la respuesta del SOC y reducir significativamente la visibilidad de la actividad maliciosa, ya que las alertas suelen ser despriorizadas al asociarse con un proceso considerado confiable.

El agente completo soporta 18 comandos distintos del servidor, otorgando a los atacantes un control remoto integral sobre el sistema comprometido: desde la ejecución arbitraria de comandos y manipulación del registro hasta el control de servicios de Windows, operaciones sobre archivos y enumeración del software instalado. La comunicación con el C2 se realiza a través del protocolo WebSocket sobre el puerto 9000, utilizando un esquema de mensajería basado en JSON.

Consecuencias de la explotación

La explotación exitosa de esta amenaza puede traducirse en impactos significativos tanto a nivel técnico como operativo para las entidades afectadas. Entre las principales consecuencias se destacan las siguientes:

- **Compromiso total del endpoint:** el atacante obtiene control remoto pleno sobre el equipo infectado, con capacidad de ejecutar comandos arbitrarios, cargar archivos y manipular servicios, procesos y registros del sistema.
- **Evasión prolongada de detección:** al enmascararse dentro de explorer.exe y mantenerse por debajo de los umbrales de detección de soluciones antimalware

tradicionales, la amenaza puede permanecer activa durante semanas o meses (dwell time elevado) antes de ser identificada.

- **Persistencia resistente:** la creación de la tarea programada RmmAgentCore con disparador de inicio de sesión garantiza que el malware se reactive en cada arranque del sistema, incluso si se interrumpe el proceso principal.
- **Exfiltración de información sensible:** el agente permite listar, leer y cargar archivos desde el equipo, facilitando la extracción de historias clínicas, información administrativa, datos personales de pacientes, credenciales o información financiera de la entidad.
- **Movimiento lateral y escalamiento:** con la elevación a UAC mediante Start-Process -Verb RunAs y el uso de SeDebugPrivilege, los atacantes pueden pivotar a otros sistemas dentro de la red y obtener acceso privilegiado a activos críticos.
- **Impacto operacional:** la capacidad de detener, reiniciar o deshabilitar servicios de Windows y terminar procesos puede derivar en interrupciones de sistemas de información hospitalaria (SIH), HIS, bases de datos clínicas o plataformas de atención al usuario.
- **Riesgo regulatorio y reputacional:** la posible afectación de datos sensibles de pacientes implica incumplimientos frente a la Ley 1581 de 2012 de Protección de Datos Personales y demás normatividad aplicable al sector salud, además de un impacto reputacional relevante.

Indicadores de compromiso (IoC)

A continuación se listan los indicadores técnicos asociados a la actividad del toolkit SpankRAT identificados durante el análisis. Se recomienda incorporarlos a las plataformas SIEM, EDR, IDS/IPS, firewalls perimetrales y feeds de inteligencia de amenazas de cada entidad.

Tipo de indicador	Valor
Servidor C2 (HTTP staging + WebSocket)	45.131.214[.]132:9000
Servidor C2 alterno (WebSocket)	166.1.144[.]109:9000
Hash SHA-256 del agente	f0afbbb3c80e5347191452f2f3b147627e9d1ae4d60b61d6da900a60b35eec95
Archivo malicioso (loader)	RmmAgentCore.exe
Archivo malicioso (payload)	rmm_agent.dll
Variante independiente	arc_agent.exe
Ruta de despliegue (drop path)	C:\ProgramData\
Mecanismo de persistencia	Tarea programada: RmmAgentCore (logon trigger, highest privileges)
Proceso objetivo de inyección	explorer.exe
Endpoint WebSocket C2	ws://<C2>:9000/ws/agent
Patrón URL de staging	*/download/rmm_agent.dll*
Rutas de compilación (Rust/Cargo)	C:\Users\spank\.cargo\ | /root/.cargo/

Nota: las direcciones IP están neutralizadas con corchetes ([.]) para evitar su resolución accidental. Antes de aplicarlas en un entorno productivo deben ser normalizadas a su formato estándar.

Modo de explotación del ataque

La cadena de ataque de SpankRAT puede dividirse en cinco fases claramente identificadas, las cuales se describen a continuación en detalle:

Fase 1 – Entrega y ejecución inicial (SpankLoader)
El ataque comienza con la ejecución del componente SpankLoader, un loader de primera etapa ligero y especializado en preparar el entorno antes del despliegue del payload principal. Este componente realiza una petición HTTP no cifrada al servidor C2 para recuperar el archivo rmm_agent.dll, lo que facilita su identificación mediante reglas de inspección de tráfico en el perímetro.

El patrón de URL característico durante esta etapa responde a la forma */download/rmm_agent.dll*, dato clave para la caza de amenazas (threat hunting) dentro de los registros de proxies, firewalls y telemetría EDR.

Fase 2 – Escalamiento de privilegios
Una vez en ejecución, SpankLoader solicita y habilita el privilegio SeDebugPrivilege sobre el token de acceso del proceso. Este privilegio permite al atacante abrir procesos protegidos con permisos extendidos (incluyendo la posibilidad de leer y escribir en su memoria) y es un prerrequisito técnico para realizar la inyección de DLL sobre explorer.exe.

Despliegue del payload e inyección en explorer.exe
SpankLoader deposita la DLL maliciosa rmm_agent.dll dentro del directorio C:\ProgramData\ y la inyecta sobre el proceso explorer.exe utilizando técnicas clásicas de DLL injection. Esta técnica es particularmente peligrosa por tres motivos:

1. La actividad de red del malware aparenta provenir de un binario propio y firmado del sistema operativo (explorer.exe), evadiendo controles basados en reputación y listas blancas de procesos.
2. Las soluciones EDR que aplican reglas de perfilamiento por proceso pueden despriorizar alertas originadas en explorer.exe, al considerarlo un proceso legítimo del sistema.
3. Se dificulta la atribución forense, dado que el tráfico saliente malicioso se mezcla con el tráfico legítimo del Explorador de Windows.

Fase 4 – Persistencia mediante tarea programada

Para garantizar que el acceso se mantenga incluso tras reinicios del sistema, SpankLoader crea la tarea programada RmmAgentCore con las siguientes características:

- **Disparador (trigger):** inicio de sesión de usuario (logon trigger).
- **Nivel de privilegios:** ejecución en el nivel más alto disponible (Run with highest privileges).
- **Acción:** ejecución del binario del loader (RmmAgentCore.exe).

Esta configuración asegura que el agente se reactive en cada inicio de sesión del usuario con privilegios elevados, sin depender exclusivamente de que explorer.exe permanezca infectado.

Fase 5 – Establecimiento del canal C2 y control remoto

Instalado dentro de explorer.exe, el agente establece una conexión persistente por WebSocket hacia el servidor de comando y control en ws://<C2>:9000/ws/agent, utilizando un protocolo de mensajería basado en JSON. A partir de ese momento, el atacante dispone de 18 comandos distintos mediante los cuales puede operar el equipo de manera remota.

Todas las interacciones con el sistema operativo son ejecutadas a través de PowerShell con los parámetros -NoProfile -NonInteractive -ExecutionPolicy Bypass, evitando el uso del perfil del usuario, inhibiendo sesiones interactivas y saltando las políticas de ejecución de scripts de

PowerShell. Asimismo, el agente realiza un fingerprinting del sistema operativo consultando directamente el registro para obtener el número de build y el nombre del producto.

El siguiente cuadro resume las capacidades operacionales ofrecidas por el agente una vez establecida la conexión con el C2:

Categoría	Capacidades soportadas
Gestión de sesión	Registro del agente y envío de telemetría periódica (heartbeat) incluyendo uso de CPU, memoria RAM, disco y tiempo de actividad.
Ejecución remota	Ejecución arbitraria de comandos con retorno de stdout y código de salida; elevación a UAC mediante Start-Process -Verb RunAs.
Operaciones sobre archivos	Listar, leer, cargar, eliminar y renombrar archivos, así como crear directorios sobre el sistema comprometido.
Control de procesos	Enumeración de procesos (PID, nombre, memoria, usuario, CPU) y terminación arbitraria de procesos.
Servicios de Windows	Listado de servicios e iniciar, detener o reiniciar cualquier servicio del sistema operativo.
Manipulación del registro	Operaciones CRUD completas sobre el registro de Windows: leer claves y valores, establecer, crear y eliminar entradas.
Tareas programadas	Listar, ejecutar y habilitar o deshabilitar tareas programadas del sistema.
Inventario de software	Enumeración completa del software instalado en el equipo comprometido.

vulnerabilidades asociadas

A diferencia de campañas centradas en la explotación de CVE específicos, la amenaza SpankRAT no se apoya en la explotación de una vulnerabilidad publicada con identificador CVE. Su efectividad no reside en un fallo concreto de software, sino en el abuso de características legítimas del sistema operativo Windows y en debilidades de configuración y visibilidad típicas de los entornos corporativos. Los mecanismos aprovechados son los siguientes:

- **Abuso de SeDebugPrivilege:** privilegio legítimo del sistema operativo que, cuando se concede a procesos o cuentas sin restricción suficiente, permite inyección de código en procesos de otros usuarios o de mayor integridad. No es una vulnerabilidad, sino una capacidad legítima mal gobernada.
- **Inyección de DLL en procesos de confianza (T1055.001):** técnica clásica de evasión que explota la ausencia de controles estrictos sobre la integridad de los procesos del sistema (por ejemplo, políticas de protección de integridad como PPL o protecciones contra carga de DLLs no firmadas).
- **Ejecución de PowerShell con políticas laxas:** uso del parámetro -ExecutionPolicy Bypass, el cual permite saltar políticas de ejecución de scripts cuando no se cuenta con controles complementarios como Constrained Language Mode, AppLocker o Windows Defender Application Control (WDAC).
- **Creación de tareas programadas con privilegios elevados:** abuso de la capacidad del Programador de Tareas de Windows para crear tareas con el nivel de privilegios más alto, en ausencia de controles GPO que restrinjan esta operación a administradores monitoreados.

- **Tráfico WebSocket saliente no inspeccionado:** debilidad perimetral frecuente en la que las comunicaciones ws:// o wss:// hacia puertos no estándar (como el 9000/TCP) no son sometidas a inspección profunda ni a análisis de reputación, lo que permite su uso como canal C2.
- **Ausencia de detección conductual:** dependencia exclusiva de soluciones antimalware basadas en firmas o en reputación, que al momento del análisis no detectaban la mayoría de muestras de SpankRAT en VirusTotal.

Con el propósito de facilitar la operacionalización de la información dentro de los programas de detección y respuesta del sector salud, a continuación se presenta el mapeo de la amenaza frente al marco MITRE ATT&CK for Enterprise:

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Initial Access (TA0001)	T1190 / T1566	Entrega inicial del componente SpankLoader mediante canales HTTP no cifrados, potencialmente a través de ingeniería social o explotación de servicios expuestos.
Execution (TA0002)	T1059.001	Ejecución a través de PowerShell con parámetros -NoProfile, -NonInteractive y -ExecutionPolicy Bypass para evadir controles de script y políticas de ejecución.
Persistence (TA0003)	T1053.005	Creación de la tarea programada RmmAgentCore configurada con disparador de inicio de sesión (logon trigger) y ejecución en el nivel de privilegios más alto.
Privilege Escalation (TA0004)	T1134 / T1134.001	Manipulación de tokens de acceso; SpankLoader habilita el privilegio SeDebugPrivilege para poder abrir procesos protegidos y realizar inyección de código.
Defense Evasion (TA0005)	T1055.001	Inyección de DLL (rmm_agent.dll) en el proceso legítimo explorer.exe para enmascarar la actividad maliciosa bajo un binario firmado de confianza.

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Defense Evasion (TA0005)	T1036.005	Coincidencia de nombre de ejecución con procesos legítimos del sistema (Masquerading), aprovechando la reputación de explorer.exe para evadir controles.
Discovery (TA0007)	T1057 / T1082 / T1012 / T1518	Enumeración de procesos, servicios, información del sistema, claves de registro y software instalado para reconocimiento y perfilamiento del host.
Collection (TA0009)	T1005 / T1119	Listado, lectura y transferencia de archivos desde el sistema comprometido mediante los comandos remotos del agente (read, upload, list).
Command and Control (TA0011)	T1071.001 / T1095 / T1573	Comunicaciones con el C2 a través de protocolo WebSocket (ws://) sobre el puerto 9000 con protocolo de mensajería basado en JSON.
Exfiltration (TA0010)	T1041	Exfiltración de datos y resultados de comandos a través del mismo canal C2 establecido por WebSocket.
Impact (TA0040)	T1489 / T1529	Capacidad de detener o reiniciar servicios de Windows y terminar procesos en ejecución, lo que habilita acciones disruptivas en el equipo comprometido.

Recomendaciones de detección y mitigación

Los equipos de operaciones de seguridad (SOC, Blue Team) deben implementar y ajustar reglas de detección conductuales en sus plataformas SIEM y EDR, orientadas a identificar los patrones característicos de SpankRAT. Entre las reglas prioritarias se encuentran:

- Detección de inyecciones de DLL sobre el proceso explorer.exe realizadas desde procesos no confiables o desde rutas atípicas como C:\ProgramData\.
- Alertamiento sobre la creación de tareas programadas con nivel de privilegios más alto (highest privileges) y disparador de inicio de sesión, especialmente con nombres como RmmAgentCore.

- Monitoreo de conexiones salientes por WebSocket (ws://) hacia puertos no estándar (como el 9000/TCP) originadas desde explorer.exe u otros procesos de sistema que no son navegadores.
- Búsqueda proactiva (threat hunting) de peticiones HTTP GET con patrones de URL como */download/rmm_agent.dll* en logs de proxy, firewall, IDS y telemetría EDR.
- Alertamiento sobre ejecuciones de PowerShell con la combinación de parámetros -NoProfile -NonInteractive -ExecutionPolicy Bypass, particularmente cuando son invocadas por procesos hijos de explorer.exe.
- Monitoreo de eventos de escalamiento mediante SeDebugPrivilege y del uso del comando Start-Process -Verb RunAs desde sesiones no administrativas.
- Bloqueo o detección de los IoC listados, incluyendo los servidores C2 45.131.214[.]132 y 166.1.144[.]109 en puerto 9000.
- Hashing y revisión de integridad de archivos nuevos en C:\ProgramData\, especialmente RmmAgentCore.exe, rmm_agent.dll y arc_agent.exe.
- Incorporación del hash f0afbbb3c80e5347191452f2f3b147627e9d1ae4d60b61d6da900a60b35eec95 a las listas de denegación de ejecución y reglas YARA corporativas.

Recomendaciones de prevención y mitigación

En paralelo a la detección, se recomienda aplicar las siguientes medidas de fortalecimiento (hardening) y prevención:

1. Restringir el uso del privilegio SeDebugPrivilege únicamente a cuentas de administración controladas a través de políticas de grupo (GPO) y monitorear su asignación y uso.
2. Implementar AppLocker o Windows Defender Application Control (WDAC) para limitar la ejecución de binarios y DLLs a ubicaciones y firmantes autorizados.

3. Habilitar Constrained Language Mode en PowerShell y activar la auditoría de scripts y ejecución de módulos (ScriptBlock Logging y Module Logging).
4. Aplicar bloqueo de ejecución de binarios desde rutas sensibles como C:\ProgramData\, C:\Users\Public\ y perfiles de usuario no administrativos.
5. Configurar el firewall perimetral y las soluciones de inspección de tráfico para bloquear conexiones WebSocket no autorizadas hacia puertos no estándar y hacia reputaciones bajas.
6. Deshabilitar protocolos HTTP salientes hacia servidores con reputación desconocida o implementar inspección profunda de paquetes (DPI) que permita detectar transferencias de archivos ejecutables o DLLs.
7. Reforzar los permisos sobre el Programador de Tareas de Windows, restringiendo la creación de tareas con privilegios elevados a cuentas auditadas.
8. Incorporar soluciones de análisis dinámico tipo sandbox (como ANY.RUN, Joe Sandbox, Cuckoo) en los flujos de triage del SOC, dado que las muestras de SpankRAT evaden detección estática en VirusTotal.
9. Mantener actualizadas las soluciones EDR/XDR con capacidades conductuales e integrar feeds de inteligencia de amenazas actualizados que incluyan los IoC de esta campaña.
10. Aplicar el principio de mínimo privilegio en estaciones de trabajo: los usuarios finales no deben operar con cuentas de administrador local.

Recomendaciones de respuesta ante compromiso

En caso de confirmarse o sospecharse compromiso por SpankRAT, se recomienda ejecutar el siguiente procedimiento de contención y erradicación:

1. Aislar de inmediato el equipo afectado de la red (aislamiento lógico vía EDR o físico), evitando el apagado para preservar evidencia volátil.

2. Capturar memoria RAM y artefactos forenses clave (imagen del disco, logs de eventos de Windows, logs de PowerShell y tarea programada RmmAgentCore) antes de realizar cualquier acción de remediación.
3. Eliminar la tarea programada maliciosa RmmAgentCore y revisar la existencia de tareas adicionales creadas por el atacante.
4. Eliminar los archivos rmm_agent.dll, RmmAgentCore.exe y arc_agent.exe de la ruta C:\ProgramData\ y de cualquier otra ruta donde se identifiquen.
5. Validar la ausencia de inyecciones residuales en explorer.exe mediante herramientas forenses (por ejemplo, Volatility, Process Hacker, PE-sieve) y reiniciar el equipo.
6. Restablecer las credenciales de todos los usuarios que hayan iniciado sesión en el equipo afectado, así como los secretos y tokens que pudieran haber estado expuestos.
7. Revisar los logs de comunicaciones salientes hacia las IPs 45.131.214[.]132 y 166.1.144[.]109 en puerto 9000 para identificar otros equipos potencialmente comprometidos dentro de la red.
8. Reportar el incidente al CSIRT Salud y, según corresponda, a colCERT y a la Superintendencia de Industria y Comercio cuando exista afectación de datos personales conforme a la Ley 1581 de 2012.
9. Considerar la reinstalación completa del sistema operativo cuando existan indicios de compromiso prolongado o cuando no sea posible validar la integridad total del equipo.

Conclusiones

SpankRAT representa una amenaza relevante para los entornos Windows corporativos y, particularmente, para las entidades del sector salud colombiano, debido a su combinación de técnicas sigilosas (inyección en explorer.exe, comunicaciones WebSocket, abuso de tareas programadas) y su baja tasa de detección en soluciones antimalware tradicionales. El abuso

de procesos legítimos del sistema operativo como canal de C2 evidencia la necesidad de migrar hacia modelos de seguridad basados en análisis conductual y telemetría de endpoint, complementados con inspección dinámica de amenazas.

Fuentes:

- Cyber Security News. SpankRAT Exploits Windows Explorer Processes for Stealth and Delayed Detection. Abril de 2026. Disponible en: https://cybersecuritynews.com/spankrat-exploits-windows-process/
- ANY.RUN – Análisis técnico del toolkit SpankRAT.
- MITRE ATT&CK Framework for Enterprise – https://attack.mitre.org/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.