



Framework de Ciberseguridad
Ofensiva

NIGHTMARE FRAMEWORK

CIBERSEGURIDAD



Autor: Pablo Díez

Contacto: pablodiez@24@proton.me



Framework de Ciberseguridad Ofensiva

ÍNDICE

01

INTRODUCCIÓN

Una visión general del Framework Nightmare, su objetivo y su importancia en la ciberseguridad ofensiva y las operaciones del red team

02

CARACTERÍSTICAS

Descripción exhaustiva de las funcionalidades clave, que abarca los módulos de comando, la lógica de automatización, la interacción del sistema y los mecanismos de sigilo.

03

INTERFAZ

Presentación visual de las interfaces GUI y CLI, que ilustra la experiencia del usuario, los paneles de control y las capacidades interactivas.

04

LICENCIA Y UTILIZACIÓN

Resumen de los términos legales de uso según el EULA, acciones permitidas, restricciones y condiciones para una aplicación responsable.

05

CONDICIONES DE VENTA.

Aclaración sobre lo que abarca la compra, tipos de licencias (estándar y exclusivas), asistencia postventa y términos de uso.

06

PRECIOS

Modelo de precio fijo para adquisiciones no exclusivas, opciones de exclusividad y condiciones bajo las cuales el framework se retira del mercado.

07

INFORMACIÓN DE CONTACTO

Canales de contacto directo para consultas, adquisiciones y solicitudes de acceso fundamentadas en NDA.







INTRODUCCIÓN

Nightmare Framework: Un robusto framework de ciberseguridad ofensiva

Nightmare es un framework avanzado de **ciberseguridad ofensiva**, diseñado específicamente para llevar a cabo simulaciones de **Amenazas Persistentes Avanzadas (APT)** y **pruebas de penetración** en sistemas de alto nivel. Su arquitectura modular y su **robusto conjunto de herramientas** lo posicionan como la opción ideal para profesionales y empresas de ciberseguridad que buscan realizar evaluaciones de seguridad exhaustivas.

Este framework ha sido concebido para su aplicación en entornos controlados y éticos, permitiendo a los Red Teamers, hackers éticos y consultorías de seguridad detectar vulnerabilidades y reforzar las defensas del sistema.

Características principales:

-  **Comunicación segura:** Intercambio de claves a través de cifrado asimétrico (RSA) y transmisión de mensajes mediante cifrado simétrico (AES).
-  **Persistencia avanzada:** Registro de Windows (sin privilegios de administrador) y basado en servicio (con privilegios elevados).
-  **Dump:** Contraseñas, cookies, software, contraseñas WiFi, procesos, etc.
-  **Arquitectura modular:** carga de módulos (DLL) directamente desde el registro para prevenir la creación de rastros en el disco.
-  **Interfaz gráfica:** Creada de forma manual empleando únicamente llamadas a WinAPI (sin bibliotecas externas).
-  **Entre otros.**

Nightmare está disponible bajo solicitud y se proporciona con un Acuerdo de Confidencialidad (NDA) para asegurar el uso ético y profesional del código fuente.

CARACTERÍSTICAS

Nightmare Framework

✚ Resolución dinámica de dependencias en memoria.

Mi Herramienta de Acceso Remoto (RAT) está concebida para ofrecer máxima eficiencia, portabilidad y discreción. Una de sus principales fortalezas arquitectónicas radica en su gestión de dependencias de terceros: completamente en memoria, sin requerir vinculación tradicional a nivel de sistema ni implementación de DLL.

El ejecutable del cliente tiene un tamaño de solo ~95 KB, pero ofrece soporte completo para bibliotecas robustas como libsodium (cifrado) y cJSON (serialización de datos), gracias al sistema de resolución de dependencias dinámicas en memoria.

¿Qué implica esto para usted?

- **✓ Sin rastro de archivo**
 - Este RAT carga bibliotecas esenciales directamente desde blobs de memoria cifrados. No se generan archivos DLL en el disco. Esto minimiza el impacto en el sistema y disminuye el riesgo de detección por herramientas de seguridad basadas en archivos.
- **✓ Capacidades avanzadas de evasión**
 - A diferencia del malware convencional que utiliza LoadLibrary o DLL visibles, nuestra herramienta simula internamente el cargador de Windows, resolviendo funciones de cargas útiles en memoria. Esto la convierte en una amenaza considerablemente más evasiva para los antivirus (AV) y los sistemas de detección y respuesta de endpoints (EDR) que se basan en firmas y comportamientos.
- **✓ Compacto y autónomo**
 - Todo lo necesario para la ejecución (rutinas de cifrado, funciones de red y gestión de JSON) se integra y se resuelve en memoria durante la ejecución. Esto permite una implementación fluida, incluso en entornos limitados o aislados.
- **✓ Uso mínimo del registro, implementación sin requerir administración**
 - No se necesitan privilegios de instalación ni de administrador para ejecutar el cliente. Todas las bibliotecas externas se cargan de manera dinámica y se resuelven desde la memoria, lo que permite que la herramienta opere de forma independiente del cargador estándar de Windows, garantizando así su total compatibilidad con entornos restringidos y políticas de grupo estrictas.

CARACTERÍSTICAS

Nightmare Framework

🧩 Resolución dinámica de dependencias en memoria.

Cómo funciona (simplificado)

En lugar de depender de Windows para cargar bibliotecas externas, nuestro cliente:

- **Incorpora bibliotecas** internamente como blobs de memoria encriptados.
- Los carga y los asocia en **tiempo de ejecución**, simulando el cargador de **Windows PE**.
- **Resuelve funciones** mediante un solucionador en memoria personalizado (equivalente a **GetProcAddress**).

Esto se realiza de manera transparente, sin requerir DLL adicionales ni modificaciones en el sistema.

Beneficios fundamentales para su organización

Beneficios	Impacto
🔗 Binario independiente	Implementación más sencilla y mínima integración de trabajo.
🕵️ Baja detectabilidad	Alta resistencia a los AV/EDR modernos debido a operaciones exclusivamente en memoria.
🚫 No se requieren DLL externas	No existe el riesgo de que se pierdan o se configuren incorrectamente las dependencias de tiempo de ejecución.
🧩 Flexibilidad en tiempo de ejecución	Admite actualizaciones modulares y la resolución de funciones en tiempo real.
Huella sutil	Cliente completo de menos de 100 KB con función de cifrado y JSON completo.

CARACTERÍSTICAS

Nightmare Framework

Caché permanente

La **caché persistente** almacena datos que se utilizan de manera **recurrente** para **evitar consultas innecesarias, disminuir la carga del sistema y optimizar los tiempos de respuesta**. El framework permite ejecutar comandos sin recurrir a la caché temporal. Este tipo de caché se emplea en **dos áreas fundamentales**:

- **Datos de geolocalización:** En la función de **ejecución basada en la geolocalización**, al seleccionar una **ubicación** en el **mapa**, los **resultados de las consultas de geolocalización** se **almacenan de manera persistente**. Esto **elimina** la **necesidad** de realizar **solicitudes externas** cada vez que se requiere información geográfica, lo que **disminuye el tráfico**.
- **Resultados del escaneo de puertos:** Los resultados de los **escaneos de puertos personalizados**, que **pueden ser lentos** y consumir muchos recursos, se **almacenan en la caché persistente**. Cuando una sesión posterior lleva a cabo el mismo escaneo, se **reutilizan los resultados anteriores, evitando así la necesidad de repetirlo**, a menos que el usuario decida borrarlos o sobrescribirlos explícitamente.



Caché temporal

La **caché temporal** retiene los **resultados de funciones cuyos datos no se anticipa que varíen con frecuencia**. Este método optimiza el tiempo de ejecución al prevenir la ejecución reiterada de funciones que ya han producido resultados, **permitiendo**, a su vez, el **acceso a estos datos** cuando sea necesario. Las siguientes funciones se almacenan temporalmente en esta caché:

- **Escaneo de red**
- **Información del sistema**
- **Verificación del antivirus**
- **Credenciales de WiFi guardadas**
- **Estado de permanencia**
- **Cookies del navegador y volcado de contraseñas**

Este sistema de caché, tanto persistente como temporal, asegura que los datos relevantes y de uso frecuente estén accesibles sin la necesidad de ejecutar funciones de manera reiterada, lo que optimiza la eficiencia general del RAT.

CARACTERÍSTICAS

Nightmare Framework

Comandos por defecto

Los **comandos por defecto** permiten definir una serie de funciones que se ejecutarán **automáticamente** al **iniciarse una sesión**. Una vez configuradas hasta cinco funciones, estas se activarán de **manera secuencial** en el momento en que se establezca la conexión y se complete el protocolo de enlace.

Esta función resulta sumamente útil para la **automatización**, especialmente desde la perspectiva del **administrador de red**. Una vez que se obtiene el acceso, la herramienta puede ser implementada y todas las tareas predefinidas se ejecutarán automáticamente de manera cifrada y controlada, optimizando el proceso.

Ejecución global

Similar a la función de "**comandos por defecto**", esta característica permite la **ejecución global** de hasta cinco tareas configuradas. Optimiza la **automatización** al permitir que todas las funciones necesarias se ejecuten de manera secuencial, eliminando la necesidad de ejecutarlas individualmente.

Ejecución según Geo Posición

La **ejecución geográfica** permite llevar a cabo hasta cinco funciones **en función de la ubicación geográfica** del dispositivo o de su **proveedor de servicios de internet (ISP)**. Esto es particularmente beneficioso para **organizaciones con oficinas interconectadas** en diversas **ubicaciones** (VPN, proxy, túnel, etc.). Una vez que se accede a dispositivos en distintas regiones, las **funciones pueden activarse automáticamente según su información geográfica**. Las opciones disponibles para la ejecución basada en la ubicación incluyen:

- País
- Región
- Ciudad
- ISP (basado en **coordenadas** geográficas)

Esta función permite una ejecución personalizada según la ubicación exacta o el proveedor de red, lo que optimiza la automatización en diversos entornos.

CARACTERÍSTICAS

Nightmare Framework

Funciones de búsqueda

Este framework proporciona una función que permite filtrar sesiones según diferentes criterios. Al iniciar el servidor en modo GUI (interfaz gráfica), se presenta una ventana emergente que permite filtrar por:

- **ID** (Identificación de sesión)
- **Dirección IP** (Dirección del Protocolo de Internet)
- **País**
- **Nombre del ordenador**
- **Sistema operativo**
- **CPU** (unidad central de procesamiento)
- **GPU** (Unidad de procesamiento gráfico)
- **RAM** (Memoria de Acceso Aleatorio)
- **ISP** (Proveedor de Servicios de Internet)

En el modo **CLI (consola)**, las opciones de filtrado son más **restringidas**, permitiéndote filtrar únicamente por: Nombre de PC, país, región, ciudad e ISP.

Esta flexibilidad facilita una gestión más eficiente de las sesiones según su entorno.

Shell remota

La **Shell Remota** permite la **ejecución de comandos** de **PowerShell** de manera remota. En el modo **GUI (Interfaz Gráfica)**, el framework ofrece una ventana de **shell interactiva** con un **historial de comandos**, lo que brinda una **experiencia completamente interactiva**. No obstante, en el modo **CLI (Consola)**, **no** se dispone de **historial de comandos** ni de la capacidad de navegar por los comandos previamente ingresados.

Esta función **establece un proceso** en el que el **servidor gestiona** tanto la **entrada** como la **salida** de comandos, lo que facilita una ejecución y recuperación **sin interrupciones** de resultados previos. Por ejemplo, si se ejecuta ``$p="example"`` y luego se ejecuta ``echo $p``, la salida mostrará el valor de la variable asignada, en este caso, **"example"**.

CARACTERÍSTICAS

Nightmare Framework

Descarga de Archivos

El framework cuenta con una **función específica para descargar archivos** desde la máquina remota, disponible en **dos modalidades**:

- **Interfaz gráfica de usuario (GUI):**
 - Abra el **explorador remoto** (detallado a continuación), donde podrá **descargar archivos de manera sencilla** a través de una interfaz intuitiva.
- **CLI (Consola):**
 - Simplemente **indique el archivo** que **desea descargar** y la **ruta de destino** será un directorio específico denominado **"DATA"**.

Esta función incorpora la **verificación del tamaño** del archivo y presenta una **barra de progreso** en los modos **GUI y CLI** para mejorar la experiencia del usuario.

Subida de Archivos

El framework cuenta con una función específica para cargar archivos en la máquina remota, disponible en **dos modalidades**:

- **Interfaz gráfica de usuario (GUI):**
 - Abra el **explorador remoto** (detallado a continuación), donde podrá **cargar archivos de manera sencilla** a través de una **interfaz intuitiva**.
- **CLI (Consola):**
 - Simplemente **indique el archivo** que desea subir y la **ruta de destino en la que debe guardarse**, y estará listo.

Esta función incorpora la **verificación del tamaño del archivo** en el lado del cliente y presenta una barra de carga en los modos **GUI y CLI** para mejorar la experiencia del usuario.

Función de Ejecución

Esto solo funciona para CLI y permite ejecutar un comando sin utilizar el modo shell.

CARACTERÍSTICAS

Nightmare Framework

Datos del sistema

La función **Información del sistema** ofrece **detalles esenciales** sobre el **hardware** y el **software** del sistema remoto, que incluyen:

- **Sistema operativo**
- **Nombre del ordenador**
- **RAM**
- **UPC**
- **GPU**
- **Espacio en el disco principal**
 - **Espacio disponible en el disco principal**

Esta información se almacena en **caché temporal**, lo que **previene la reejecución** de funciones cuando es poco probable que la salida varíe, **reduciendo** así la **carga** innecesaria en el **sistema remoto**.

Persistencia (sin administrador)

La persistencia **sin privilegios de administrador** se fundamenta en una sencilla entrada del registro y puede ser identificada en aplicaciones de inicio.

Persistencia (Con Administración)

El **mecanismo de persistencia** con permisos de **administrador** se establece mediante la **creación de un servicio de Windows** configurado para **iniciarse automáticamente** al encender el sistema. Este servicio opera bajo la cuenta "**NT AUTHORITY/System**", que representa el **nivel de privilegio más elevado** disponible **en Windows**, otorgando acceso sin restricciones a todo el sistema.

Al ejecutarse con estos permisos elevados, el servicio asegura que el RAT se mantenga activo y operativo incluso tras reiniciar el sistema, sin requerir intervención manual. Este enfoque proporciona una manera sólida y discreta de preservar la persistencia en el sistema de destino.

CARACTERÍSTICAS

Nightmare Framework

✓ Comprobación permisos

Esta función sencilla nos permite, en cualquier momento que sea necesario, **verificar el nivel de permisos que poseemos** en la máquina remota.

🚫 Bloquear y desbloquear 🔒

Para esta función, el framework necesita permisos de administrador en el sistema para poder bloquear o desbloquear con éxito el teclado y el ratón en el sistema remoto.

Esto puede ser útil al ejecutar la función RPD (que se explicará más adelante) para evitar que el usuario interfiera con el control.

🌐 Volcado de navegadores Chromium.

La función "**Volcado de Chromium**" está **diseñada** para **extraer y recuperar datos confidenciales**, como **contraseñas y cookies** almacenadas, de navegadores basados en Chromium, como **Chrome, Brave y Edge**. Al interactuar con los archivos de datos locales del navegador, accede a la **información cifrada del usuario** y utiliza los servicios de descifrado internos del navegador para recuperar dicha información. Este proceso implica la **interacción** con los **recursos del sistema**, incluido el **ElevationService del navegador**, para **extraer y descifrar los datos de manera segura**. Esta función es altamente eficaz para recopilar información crítica, al tiempo que **preserva la integridad del sistema** y asegura que el proceso de recuperación de datos sea **seguro y eficiente**.

Todo **el proceso de descifrado se lleva a cabo en el servidor**, lo que reduce el impacto en el sistema remoto y **contribuye a eludir la detección de las soluciones de seguridad**. Los **datos recuperados se organizan y almacenan en directorios estructurados dentro del entorno del servidor**, lo que facilita un acceso y análisis ágiles. Además, la operación se beneficia de procesos temporales y de una gestión controlada de recursos para asegurar que no queden artefactos residuales tras la extracción, preservando así la discreción operativa y la estabilidad del sistema.

CARACTERÍSTICAS

Nightmare Framework

Volcado de navegadores Gecko.

La función **"Gecko Dump"** está concebida para **extraer y recuperar datos sensibles**, como **contraseñas y cookies** almacenadas, de navegadores basados en Gecko, tales como **Firefox, LibreWolf y WaterFox**.

En este caso, el **proceso de descifrado** se lleva a cabo desde el lado del cliente, ya que **el programa emplea las DLL internas de cada navegador** para acceder a las **funciones** que **descifran las contraseñas** de todos los perfiles identificados que poseen los archivos requeridos.

Al emplear las DLL nativas de los navegadores, el framework **previene la importación de funciones** directamente en el binario, las cuales **podrían ser detectadas por el software antivirus**.

Volcado de contraseñas de WiFi

Se emplea un procedimiento para recuperar las credenciales Wi-Fi almacenadas en un sistema Windows. Para ello, se establece conexión con el servicio de gestión inalámbrica, se enumeran todas las interfaces de red disponibles y se extraen el SSID y la contraseña de cada perfil guardado. La información se analiza a partir de datos XML y se almacena en memoria. Finalmente, se lleva a cabo una adecuada limpieza de los recursos para preservar la estabilidad del sistema.

Exportación de procesos

El cliente documenta todos los procesos en ejecución en el instante en que se invoca esta función. Una vez que tiene todos los procesos enumerados, genera un JSON para serializar el mensaje y enviarlo al servidor, permitiendo así su almacenamiento y visualización de manera eficiente.

Volcado de software.

A través de entradas de registro, se recopila todo el software instalado en el sistema remoto, junto con su versión, para generar un JSON que se enviará al servidor, permitiendo su visualización y almacenamiento de manera conveniente.

CARACTERÍSTICAS

Nightmare Framework

Dump All

La función "Dump All" facilita la recopilación automática de toda la información confidencial en una única operación, diseñada específicamente para optimizar y automatizar los procesos de recolección de datos.

- Contraseñas y cookies de Chromium
- Contraseñas y cookies de Gecko
- Credenciales de WiFi almacenadas
- Procesos en ejecución
- Software instalado
- Datos de la cartera Exodus
- Datos de la cartera Monero

Mostrar "MessageBox"

La función MessageBox proporciona una **capacidad sencilla** para mostrar mensajes emergentes personalizados en el sistema remoto. Inicialmente **incorporada** durante la **fase de desarrollo**, se ha mantenido disponible para casos de uso específicos. Esta función puede emplearse para simular errores del sistema, ofrecer mensajes engañosos que influyan en el comportamiento del usuario (como incitar a ejecutar un archivo .exe o .bat previamente cargado) o generar distracciones controladas durante la interacción. Aunque no es esencial para las operaciones principales, brinda mayor flexibilidad para tácticas de ingeniería social en escenarios autorizados.

Función de captura de pantalla

Genera una **captura de pantalla** de la pantalla principal que se almacenará en la carpeta temporal del usuario HASTA que sea descargada por el servidor; una vez descargada, se eliminará automáticamente.

Esto resulta útil para **conocer las actividades del usuario** sin necesidad de iniciar una **sesión RDP**.

CARACTERÍSTICAS

Nightmare Framework

● Grabación del micrófono

Esta función nos permite, a través de **WMI**, **generar un archivo de audio** de la **duración que deseemos**, siendo un requisito que el sistema **disponga de un micrófono disponible**.

Utiliza automáticamente el **micrófono activo o designado como micrófono principal**.

🔍 Escaner de Red

Esta función lleva a cabo un **escaneo** basado en **ARP** para identificar todos los **dispositivos conectados** a la **red local**. Al ejecutar el RAT en modo **GUI**, se genera un **mapa visual de la red** que proporciona una visión general intuitiva de los dispositivos detectados, optimizando así la navegación y la localización.

El mapa de red ha sido **desarrollado en C++** y aprovecha la **aceleración de hardware** para asegurar una representación fluida y un rendimiento óptimo.

🔍 Función de exploración del host

Esta función **requiere un escaneo ARP previo** de los **dispositivos de red**. En el modo GUI, la opción para llevar a cabo un escaneo de puertos se habilita únicamente tras completar el escaneo de red inicial, lo que asegura un flujo de trabajo eficiente. En el modo CLI, aunque la función puede ser invocada manualmente, **se mostrará una advertencia si aún no se ha realizado un escaneo de dispositivos**.

El proceso de escaneo de puertos **puede requerir un tiempo considerable**, dependiendo del rango seleccionado, ya que **permite** a los usuarios definir el **puerto de inicio** y finalización para un escaneo más **preciso y eficiente**.

Ⓜ Función de Monedero Monero

Esta función emplea el registro del sistema para localizar los archivos **.keys** de Monero. Una vez identificados, los descarga para su análisis posterior.

CARACTERÍSTICAS

Nightmare Framework

Función de la billetera Exodus

Esta función **identifica las rutas de instalación habituales** para localizar los archivos **.seco** de la billetera Exodus, que contienen información esencial. Una vez localizados, la función descarga estos archivos para su **análisis posterior**.

Estas capacidades se **implementaron** como parte del **proceso de desarrollo**, con la comprensión de que **algunas organizaciones pueden poseer criptomonedas como parte de sus operaciones comerciales legítimas**, lo que asegura el cumplimiento de los **frameworks legales pertinentes**.

Detección de software antivirus

A través del **Instrumental de Administración de Windows (WMI)**, esta función detecta **todo el software antivirus presente** en el sistema. Reúne información detallada sobre cada antivirus, incluyendo si la **protección en tiempo real** está habilitada, el **estado de actualización** del software, la **ruta de instalación** y la fecha de la **última actualización**.

Protocolo de Escritorio Remoto (Personalizado)

He creado un **Protocolo de Escritorio Remoto (RDP) ultraligero**, concebido específicamente para **eludir la detección** de software antivirus. Este protocolo personalizado **opera sobre TCP**, lo que **asegura su discreción** y reduce las probabilidades de ser identificado por los sistemas de seguridad. El protocolo ha sido diseñado con un **enfoque en la eficiencia**, manteniendo una estructura ligera para asegurar una **comunicación rápida y fluida**.

Se emplean **cinco tipos de mensajes** diferentes para facilitar el intercambio de datos entre el cliente y el servidor. Estos mensajes están concebidos para asegurar la **eficiencia de la comunicación**, al tiempo que disminuyen la probabilidad de ser identificados por los mecanismos de seguridad convencionales. Lo que lo convierte en una **solución óptima** en entornos donde la **seguridad y la velocidad son esenciales**.

CARACTERÍSTICAS

Nightmare Framework

Función de la cámara web

Esta función abre una ventana específica para mostrar la **transmisión en vivo** de la cámara del cliente. Se desarrolló en **C++** para asegurar la máxima **compatibilidad y configuración**. Antes de intentar acceder a la cámara, la función **comprueba** si el dispositivo está disponible o si otro proceso lo está utilizando, lo que garantiza un funcionamiento estable y previene conflictos.

Si no se detecta ninguna cámara o si ya está ocupada, el sistema maneja la situación de manera eficiente al notificar al servidor, asegurando así la fiabilidad operativa. Esta función prioriza el rendimiento y la compatibilidad, lo que la convierte en una solución sólida para interactuar con el hardware del cliente.

Audio en tiempo real

He diseñado un sistema personalizado basado en sockets que, al conectarse el cliente, inicia la transmisión de datos de audio en tiempo real directamente al servidor. El servidor reproduce este audio mediante la salida predeterminada. Este enfoque asegura una baja latencia y una transmisión continua, lo que facilita la monitorización en tiempo real del entorno de audio del cliente. El sistema ha sido diseñado para ser ligero y eficiente, reduciendo el consumo de recursos y manteniendo una alta fiabilidad durante la transmisión.

Explorador

Esta función está disponible **únicamente en la interfaz gráfica** de usuario (GUI). Se ha creado un servicio de archivos cliente-servidor personalizado que permite llevar a cabo operaciones como **LIST, DOWNLOAD, UPLOAD** y crear carpetas. Toda la **comunicación** se serializa en **JSON** para facilitar el **análisis y la legibilidad** de los mensajes. Tras la inicialización, el cliente envía un **dataset estructurado** que **contienen** información sobre **todos los discos disponibles** para completar adecuadamente la ventana principal.

La **tabla principal** (listview) ofrece dos modos de visualización: **Disk** y **File** view, lo que facilita una **navegación fluida** entre discos, carpetas y archivos.

CARACTERÍSTICAS

Nightmare Framework

Forzar el UAC

Esta función resulta algo intrusiva, ya que solicita de manera continua al usuario privilegios de administrador a través del cuadro de diálogo UAC (Control de Cuentas de Usuario). Funciona en un bucle, requiriendo constantemente la elevación hasta que el usuario concede los derechos de administrador, lo que asegura que finalmente se obtengan los permisos necesarios.

Monitor de CPU

Esta función está disponible únicamente en el modo GUI. Al abrir el panel de control para una sesión individual, se establece una conexión secundaria que supervisa de manera continua el uso de la CPU del sistema. El cliente envía datos de uso de la CPU, medidos en porcentaje, al servidor cada 2 segundos, lo que asegura el seguimiento del rendimiento en tiempo real dentro de la interfaz de la sesión.

Monitor de memoria RAM

Esta función está disponible únicamente en el modo GUI. Al abrir el panel de control para una sesión individual, se establece una conexión secundaria que supervisa de manera continua el uso de RAM del sistema. El cliente envía datos de uso de RAM, medidos en porcentaje, al servidor cada 2 segundos, lo que asegura el seguimiento del rendimiento en tiempo real dentro de la interfaz de la sesión.

Eliminar caché

El único objetivo de esta función es **eliminar la caché de persistencia**. Dado que el sistema utiliza la caché de manera automática siempre que está disponible, no existe la opción de desactivar su uso. Por lo tanto, si el operador desea descartar los datos almacenados en caché o actualizarlos con información reciente, es necesario eliminar la caché manualmente a través de esta función.

CARACTERÍSTICAS

Nightmare Framework

Idle Check

El objetivo primordial de la función de inactividad es monitorizar la latencia de la conexión, asegurando que se mantenga por debajo de los 500 ms. Aunque su uso es opcional, está principalmente integrada en la interfaz gráfica de usuario para verificar de manera continua que la conexión permanezca activa, responda y opere correctamente.

Reconectar

Esta función está concebida para obligar al cliente a reconectarse al servidor cuando la conexión se desincroniza. Esto se logra mediante la creación de un nuevo socket y el establecimiento de una nueva conexión para asegurar una comunicación estable.

Desinstalar

Esta función se ocupa de eliminar todos los artefactos generados por el servidor, incluyendo entradas DLL en el registro, mecanismos de persistencia, asignaciones de memoria y cualquier otro recurso asociado. Su propósito es asegurar la eliminación total y segura de cualquier rastro que permanezca en el sistema.

Cerrar sesión

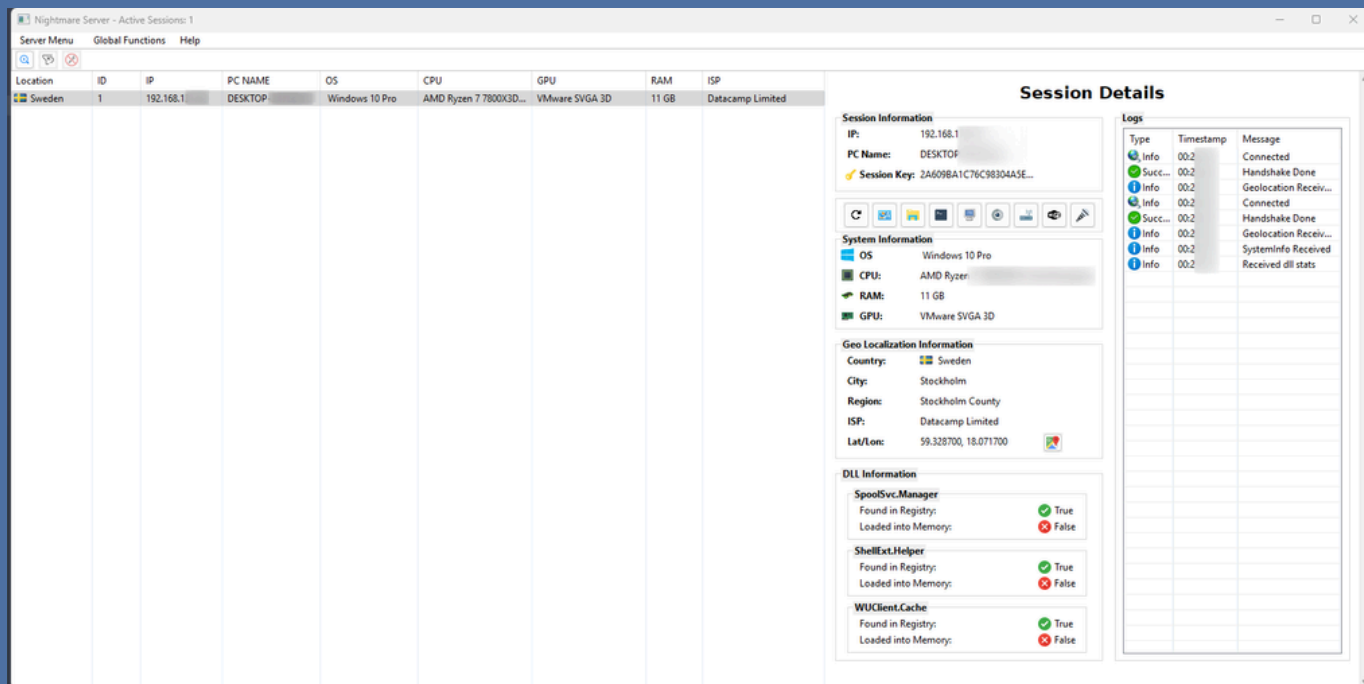
Esta función indica al cliente que debe finalizar la conexión y liberar todos los módulos previamente inyectados en la memoria. Si se ha configurado la persistencia, el sistema restablecerá automáticamente la conexión tras el reinicio, restaurando todos los módulos pertinentes desde el registro.

Con esto, se ha proporcionado una visión general de las funciones principales que ofrece esta herramienta. Hay funciones adicionales más específicas disponibles tanto en la interfaz gráfica de usuario como en la interfaz de línea de comandos (CLI), las cuales están documentadas de manera exhaustiva en el código fuente del proyecto, accesible en formato Markdown.

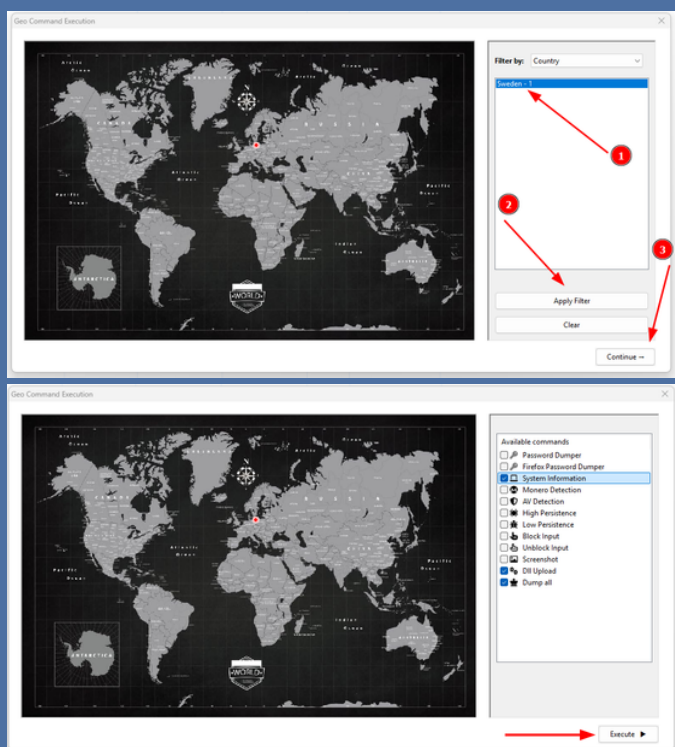
INTERFAZ

Nightmare Framework

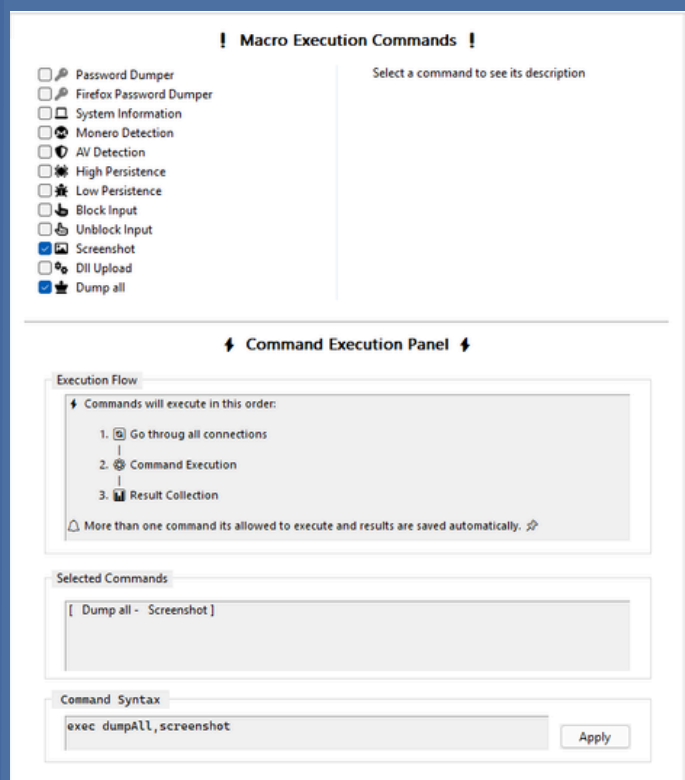
Interfaz principal



Ejecución basado en geoposición



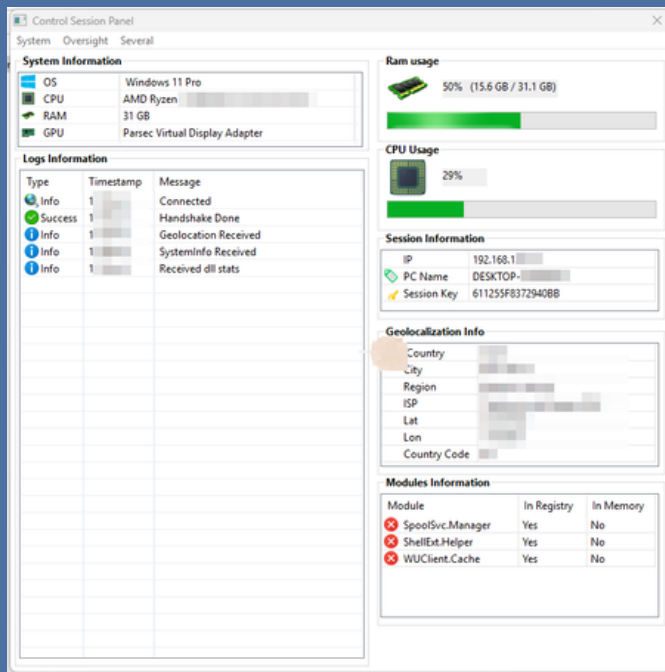
Ejecución Global



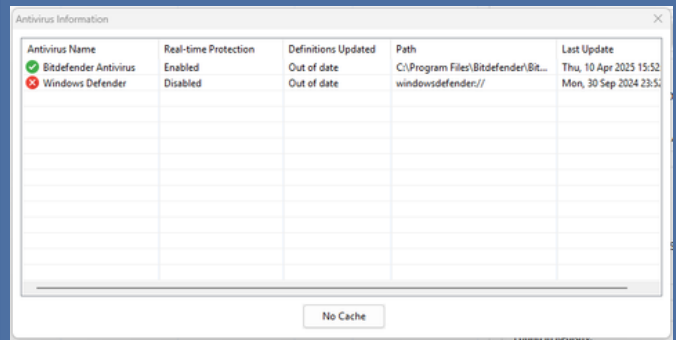
INTERFAZ

Nightmare Framework

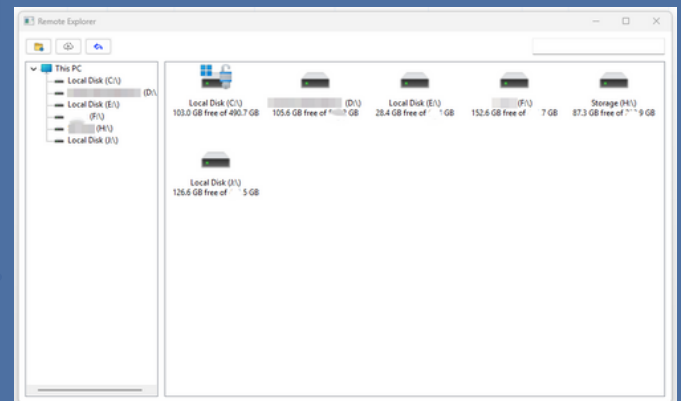
Panel de control de la sesión



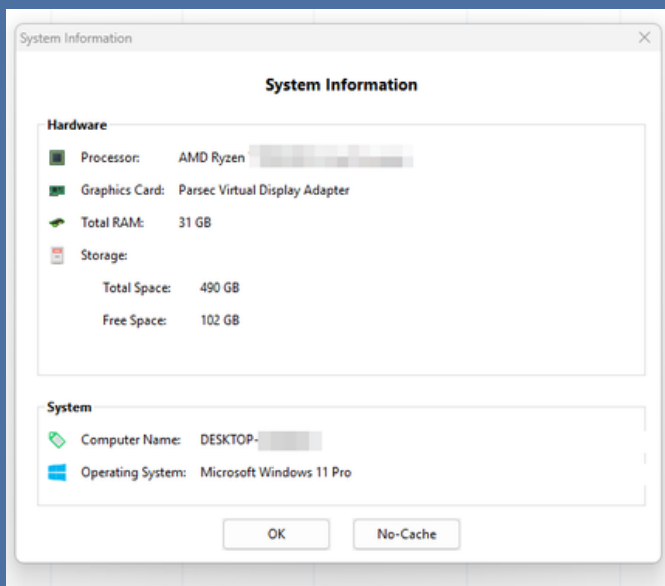
Función de antivirus



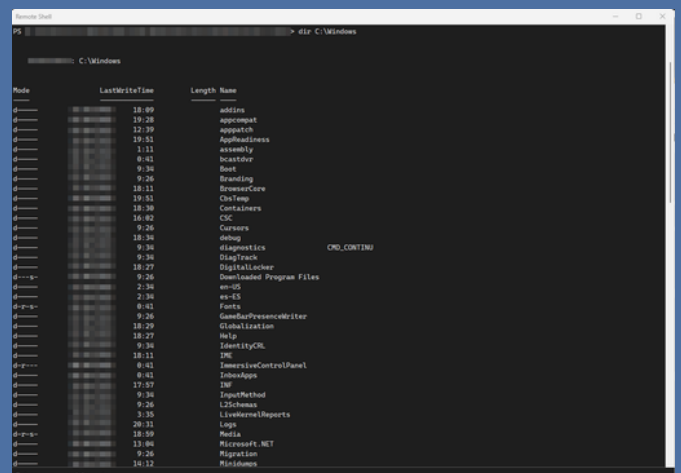
Remote Explorer



Información del sistema



Shell remota



Nightmare Framework

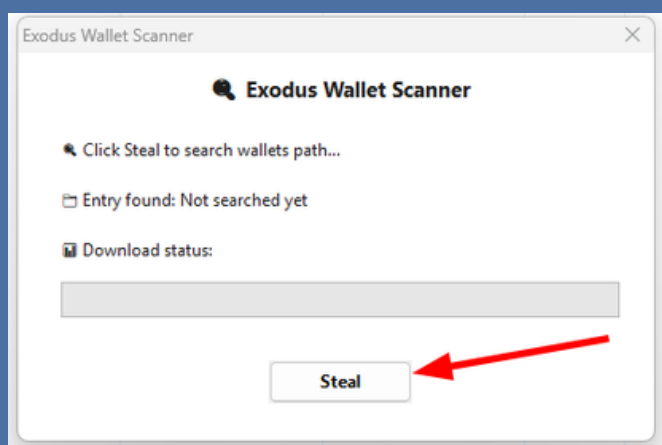
Volcado de software

Name	Version
010 Editor 15.0.1 (64-bit)	15.0.1
[REDACTED]	2025.5.0
[REDACTED]	24.09
[REDACTED]	24.10.34
[REDACTED]	27.0.40.173
[REDACTED]	27.1.1.12
[REDACTED]	0.2.3
[REDACTED]	9.5.0
Git	2.45.1
[REDACTED]	3.0.4.0
Mozilla Firefox (x64 es-ES)	137.0.1
Mozilla Maintenance Service	133.0
[REDACTED]	0.45.0.0
Parsec Virtual USB Adapter Driver	0.3.10.0
[REDACTED]	1.3.3
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
[REDACTED]	
VLC media player	3.0.21
[REDACTED]	8.1.25-0
NVIDIA Nsight Systems 2022.4.2	22.4.2.1
[REDACTED]	17.5.0
Microsoft Visual C++ 2013 x64 Additional Runti...	12.0.40664

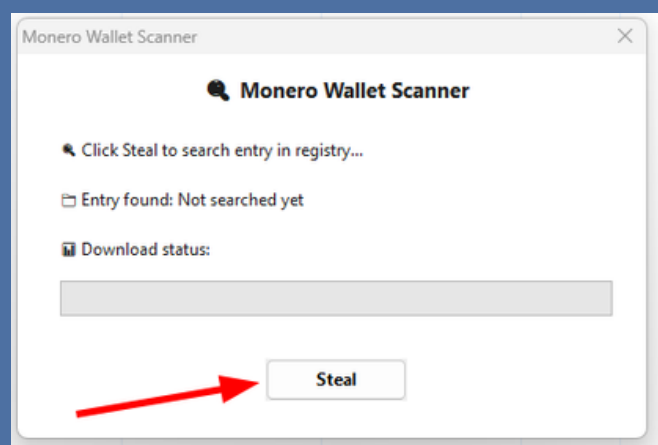
INTERFAZ

Nightmare Framework

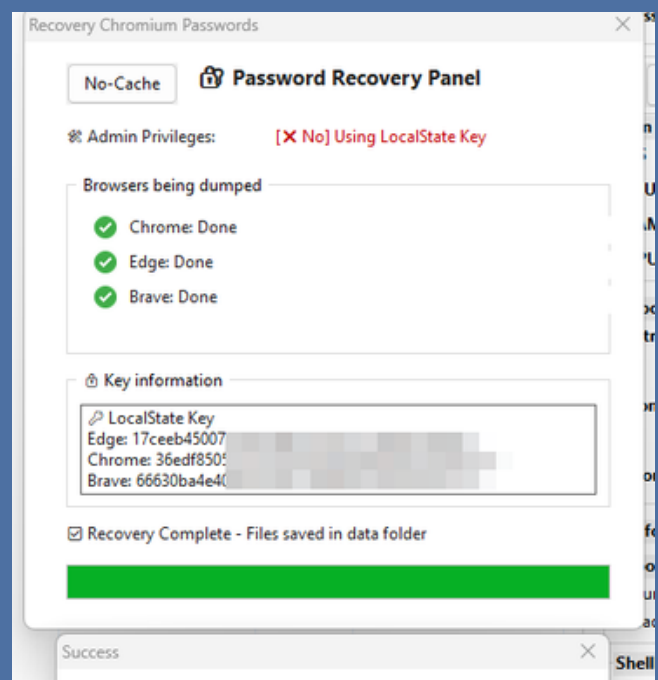
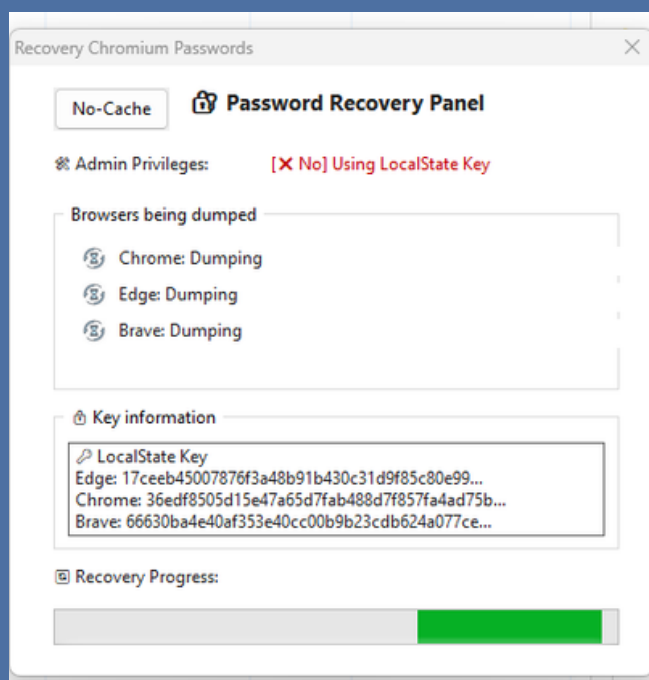
Exodus Wallet



Monero Wallet



Gecko y Chomrium Recovery



Nightmare Framework

Mapa de la red



LICENCIA Y UTILIZACIÓN

ACUERDO DE LICENCIA DE USUARIO FINAL (EULA)

Este software está licenciado, no vendido. Al usar, copiar o modificar este software, usted acepta los siguientes términos:

Uso autorizado: Se le otorga una licencia para usar este software solo en entornos que le pertenezcan o donde tenga permiso explícito por escrito. El uso no autorizado, incluido el uso de este software para actividades maliciosas, está estrictamente prohibido.

1. **Propósito:** Este software está destinado únicamente a fines educativos y de investigación en seguridad dentro de entornos controlados y éticos, como pruebas de penetración o actividades de Red Team. No está destinado para actividades ilegales.
2. **Uso prohibido:** No puede usar este software para:
 - Vigilancia no autorizada
 - Acceso a sistemas o datos sin permiso
 - Distribución de malware o software espía
 - Participación en actividades ilegales o no éticas
 - Violación de leyes locales, nacionales o internacionales
3. **Exención de responsabilidad:** Los desarrolladores de este software no son responsables de ningún daño, consecuencia legal o uso indebido que resulte del uso de este software. Al usar este software, usted acepta la responsabilidad total por su uso y los riesgos asociados.
4. **Sin garantía:** Este software se proporciona "TAL CUAL" sin garantías de ningún tipo. Los desarrolladores no garantizan el rendimiento del software, su comerciabilidad ni su idoneidad para un propósito particular. Úselo bajo su propio riesgo.
5. **Redistribución y modificación:** No puede redistribuir, vender ni modificar el software sin el permiso por escrito del desarrollador. Cualquier modificación es solo para fines personales o educativos y no puede distribuirse comercialmente.

Al usar este software, usted confirma que entiende y acepta cumplir con estos términos.

CONDICIONES DE VENTA.

Disponibilidad del código fuente completo

El código fuente completo está disponible bajo solicitud. Los interesados deben comunicarse conmigo para obtener más información sobre el proceso de adquisición.

Qué incluye la adquisición

Al adquirir el código fuente, el comprador obtendrá:

1. El **código fuente integral** del proyecto.
2. Un **compilador independiente con interfaz gráfica** que simplifica el proceso de **configuración** e instala automáticamente todas las dependencias necesarias, a excepción del instalador de Visual Studio para la compilación en C/C++, que debe ser instalado manualmente.
3. **Documentación exhaustiva**, que incluye **instrucciones** detalladas para la compilación, configuración y utilización del software.

Este paquete asegura que los compradores dispongan de todo lo necesario para compilar, configurar y operar el software de manera efectiva, con mínimas barreras técnicas.

Asistencia postventa

El soporte posventa **está disponible por un periodo limitado de 30 días** a partir de la compra. Durante este tiempo, **proporcionaré asistencia técnica** en caso de que el comprador enfrente dificultades con la instalación, configuración o funcionamiento del software.

El soporte adicional, **las actualizaciones o cualquier personalización del software estarán sujetos a un cargo adicional** y se acordarán de manera separada entre el comprador y el vendedor.

Condiciones complementarias

El código no debe emplearse para actividades ilegales o maliciosas, conforme a lo establecido en el CLUF (Contrato de Licencia de Usuario Final). Cualquier uso inapropiado del software, incluyendo la modificación o redistribución no autorizadas, puede dar lugar a la revocación del soporte técnico y de la licencia del software.

PRECIOS

Precios

El paquete completo tiene un precio establecido para compras estándar (no exclusivas).

Las negociaciones están restringidas únicamente a empresas o individuos que soliciten derechos exclusivos sobre el software.

Términos de venta

- Una adquisición estándar concede una licencia no exclusiva para utilizar el software de acuerdo con los términos establecidos.
- Si se requieren derechos exclusivos, se llevará a cabo una negociación independiente para establecer los términos y precios adecuados.
- **Importante:**
 - Si el código ha sido vendido previamente de manera no exclusiva, se notificará al comprador que solicite la exclusividad sobre la venta anterior.
 - Si el comprador aún desea proceder, se formalizará un contrato de exclusividad y, a partir de ese momento, el software se retirará de manera permanente de la venta.
- El acuerdo de exclusividad incluirá disposiciones precisas en relación con:
 - Declaración de que el código fue vendido con licencias no exclusivas anteriores (si corresponde).
 - Confirmación de que no se llevarán a cabo futuras ventas, transferencias o distribuciones de licencias.

Notas complementarias

- **Garantía del código fuente:** El código se proporciona tal como se describe, sin modificaciones ocultas.
- **Cesión de Derechos:** En las ventas exclusivas, el comprador obtiene los derechos exclusivos de uso comercial, mientras que la propiedad intelectual (autoría) continúa perteneciendo al desarrollador original.
- **Aviso postventa:** Se emitirá un aviso público confirmando la venta en exclusiva.

DATOS DE CONTACTO



Datos de contacto

Para consultas, adquisiciones o información adicional, utilice los siguientes métodos de contacto:

✉ **Correo electrónico:** pablodiez024@proton.me

- 🌐 **GitHub:** <https://github.com/an0mal1a>
- 🌐 **LinkedIn:** <https://www.linkedin.com/in/an0mal1a/>
- **! Importante:**
 - Se atenderán exclusivamente consultas serias y pertinentes al negocio.
 - Todas las comunicaciones se manejan de manera confidencial y segura.
 - No se aceptan mensajes no solicitados ni propuestas irrelevantes.
- **Clave pública PGP:** (opcional; si desea mantener una comunicación cifrada, no olvide adjuntar su clave pública como archivo)

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
xjMEY859TxYJKwYBBAHaRw8BAQdAzPs2wj/f5Utap5yxzYjSrjdCFpEShgDB
XbWpULPUO/HNL3BhYmxvZGllejAyNEBwcm90b24ubWUgPHBhYmxvZGllejAy
NEBwcm90b24ubWU+wowEEBYKAD4FamPOfU8ECwkHCAkQhOsaM7FUNFADFQgK
BBYAAgECGQECGwMCHgEWIQT7DfyqYfcts2wHL2uE6xozsVQ0UAAQWoA/1K0
1yZvbMciaaMdVkeCXRKCvkHRcZs//WQ+8S2koT5TAP0a91niXzBVEGFSdWO+
lioByU0EzVWdu7jZeLeMUyInAc44BGPOfU8SCisGAQQBl1UBBQEBB0CpBT6a
6V2Z+NoKedCYWDjaWa5jqdaKHbLyOV/kOuQzBQMBCAfCeAQYFggAKgUCY859
TwkQhOsaM7FUNFACGwwWIQT7DfyqYfcts2wHL2uE6xozsVQ0UAAAJcwA/Rvr
/sp78c7/A9g2qILxvjCF+s+IBCSqRGRReB6wdcMAP4xli4Ahfp2w6C+hsxB
TI2/+Sdkxm0mPlnQ4xhe48/lCw==
=UqQY
```

-----END PGP PUBLIC KEY BLOCK-----