

OBTENER ACCESO AL SISTEMA OBJETIVO MEDIANTE TROYANOS

Un troyano informático es un programa con código malicioso o dañino contenido dentro de programación o datos aparentemente inofensivos, de tal forma que el programa puede obtener el control y causar daños como, por ejemplo, arruinar la tabla de asignación de archivos del disco duro.

ESCENARIO DE LABORATORIO

Los atacantes utilizan caballos de Troya digitales para engañar a la víctima para que realice una acción predefinida en un ordenador. Los troyanos se activan cuando los usuarios realizan acciones específicas predefinidas, como instalar involuntariamente un programa malicioso o hacer clic en un enlace malicioso, y una vez activados, pueden conceder a los atacantes acceso ilimitado a todos los datos almacenados en los sistemas de información comprometidos y causar daños potencialmente inmensos. Por ejemplo, los usuarios podrían descargar un archivo que parece ser una película, pero que, al abrirse, desencadena un peligroso programa que borra el disco duro o envía números de tarjetas de crédito y contraseñas al atacante. Los troyanos funcionan al mismo nivel de privilegios que las víctimas. Por ejemplo, si una víctima tiene privilegios para eliminar archivos, transmitir información, modificar archivos existentes e instalar otros programas (como programas que proporcionan acceso no autorizado a la red y ejecutan ataques de elevación de privilegios), una vez que el troyano infecte ese sistema, poseerá los mismos privilegios. Además, puede intentar explotar vulnerabilidades para aumentar su nivel de acceso, incluso más allá del usuario que lo ejecuta. Si tiene éxito, el troyano podría utilizar el aumento de privilegios para instalar otros códigos maliciosos en la máquina de la víctima. Un auditor de seguridad experto o un hacker ético deben asegurarse de que la red de la organización está a salvo de los ataques de troyanos encontrando máquinas vulnerables a estos ataques y asegurándose de que las herramientas antivirus están correctamente configuradas para detectar dichos ataques. Las tareas de laboratorio de este ejercicio demuestran la facilidad con la que los hackers pueden acceder a los sistemas objetivo de la organización y crear un canal de comunicación encubierto para transferir datos confidenciales entre el ordenador víctima y el atacante.

OBJETIVOS DEL LABORATORIO

- Obtener el control de una máquina víctima utilizando el troyano njRAT RAT
- Ocultar un troyano utilizando SwayzCryptor y hacerlo indetectable para varios programas antivirus.
- Crear un servidor troyano con el troyano Theef RAT

ENTORNO DE LABORATORIO

Para llevar a cabo este laboratorio, necesitas:

- Máquina virtual Windows 11
- Máquina virtual Windows 10
- Navegadores web con conexión a Internet
- Privilegios de administrador para ejecutar las herramientas

VISIÓN GENERAL DE LOS TROYANOS

En la mitología de la Antigua Grecia, los griegos ganaron la guerra de Troya con la ayuda de un caballo gigante de madera que los griegos construyeron para ocultar a sus soldados. Los griegos dejaron el caballo frente a las puertas de Troya. Los troyanos, pensando que era un regalo de los griegos que habían dejado antes de retirarse aparentemente de la guerra, llevaron el caballo a su ciudad. Por la noche, los soldados

griegos ocultos salieron del caballo de madera y abrieron las puertas de la ciudad a sus soldados, que finalmente destruyeron la ciudad de Troya. Así, tomando como referencia este mito, un troyano informático es un programa en el que un código malicioso o dañino está contenido dentro de programación o datos aparentemente inofensivos, de tal forma que puede obtener el control y causar daños como, por ejemplo, arruinar la tabla de asignación de archivos del disco duro.

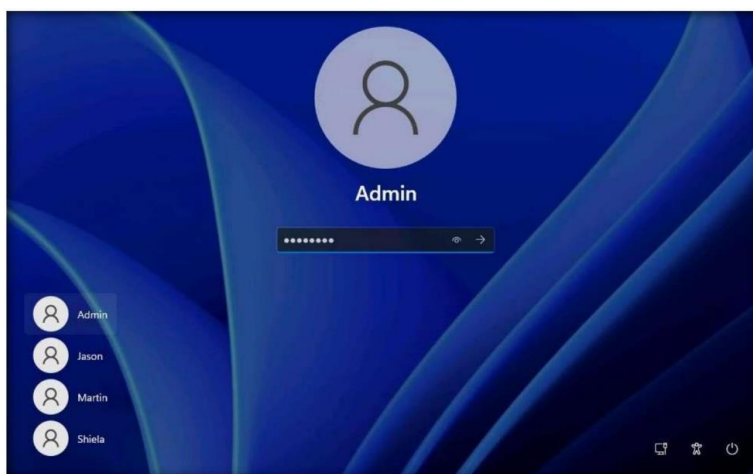
TAREAS DE LABORATORIO TAREA 1: OBTENER EL CONTROL DE UNA MÁQUINA VÍCTIMA UTILIZANDO EL TROYANO RAT NJRAT

Los atacantes utilizan troyanos de acceso remoto (RAT) para infectar la máquina objetivo y obtener acceso administrativo. Los RAT ayudan a un atacante a acceder de forma remota a toda la interfaz gráfica de usuario y controlar el ordenador de la víctima sin que ésta sea consciente de ello. Pueden realizar filtrado y captura de cámara, ejecución de código, keylogging, acceso a archivos, sniffing de contraseñas, gestión del registro y otras tareas. El virus infecta a las víctimas a través de ataques de phishing y descargas drive-by y se propaga a través de llaves USB infectadas o unidades en red. Puede descargar y ejecutar malware adicional, ejecutar comandos shell, leer y escribir claves del registro, capturar pantallas, registrar pulsaciones de teclas y espiar cámaras web. njRAT es un RAT con potentes capacidades de robo de datos. Además de registrar las pulsaciones del teclado, es capaz de acceder a la cámara de la víctima, robar credenciales almacenadas en los navegadores, cargar y descargar archivos, realizar manipulaciones de procesos y archivos y ver el escritorio de la víctima. Esta RAT puede utilizarse para controlar Botnets (redes de ordenadores), permitiendo al atacante actualizar, desinstalar, desconectar, reiniciar y cerrar la RAT, y cambiar el nombre de su ID de campaña. Además, el atacante puede crear y configurar el malware para que se propague a través de unidades USB con la ayuda del software del servidor de Comando y Control.

Aquí utilizaremos el troyano njRAT para obtener el control de una máquina víctima.

Nota: Las versiones del cliente o host creado y la apariencia del sitio web pueden diferir de lo que se muestra en esta tarea. Sin embargo, el proceso real de creación del servidor y el cliente es el mismo, como se muestra en esta tarea. Nota: En esta tarea de laboratorio, utilizaremos el equipo Windows 11 {10.10.1.11} como equipo atacante y el equipo Windows 10 {10.10.1.22} como equipo víctima.

1. Encienda las máquinas virtuales Windows 11 y Windows 10.
2. Cambie a la máquina virtual Windows 11.
3. Abra el usuario administrador e introduzca la contraseña y pulse Intro para iniciar sesión.



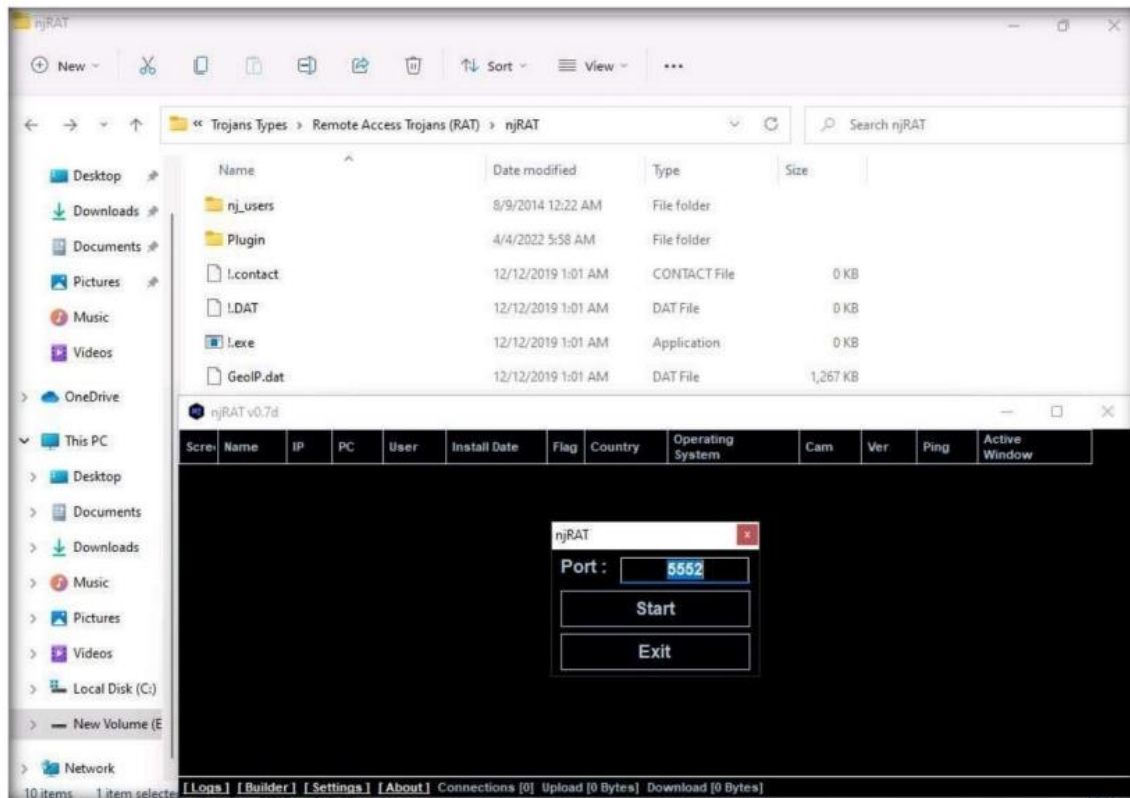
4. Vaya a C:\Tools\Remote Access Trojans (RAT)\njRAT y haga doble clic en njRAT v0.7d.exe.

NOTA: SI APARECE UNA VENTANA DE CONTROL DE CUENTAS DE USUARIO, HAGA CLIC EN SÍ.

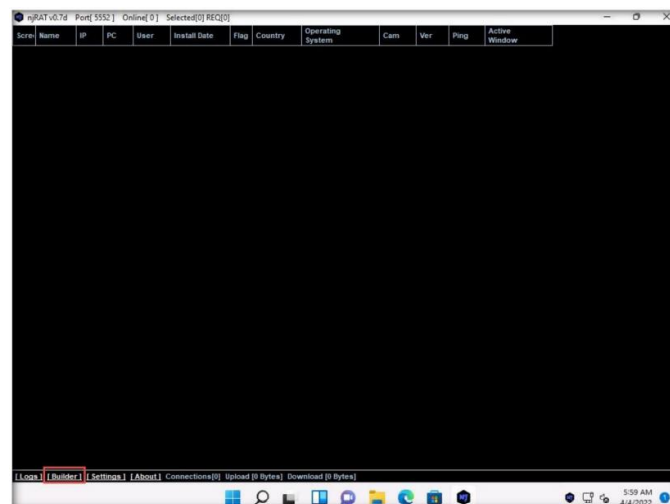
NOTA: SI APARECE UNA VENTANA EMERGENTE ABRIR ARCHIVO - ADVERTENCIA DE SEGURIDAD, HAGA CLIC EN EJECUTAR.

5. Aparecerá la GUI njRAT junto con una ventana emergente njRAT, donde deberá especificar el puerto que desea utilizar para interactuar con la máquina víctima. Introduzca el número de puerto y haga clic en Iniciar.

6. En esta tarea, se ha elegido el número de puerto por defecto 5552.

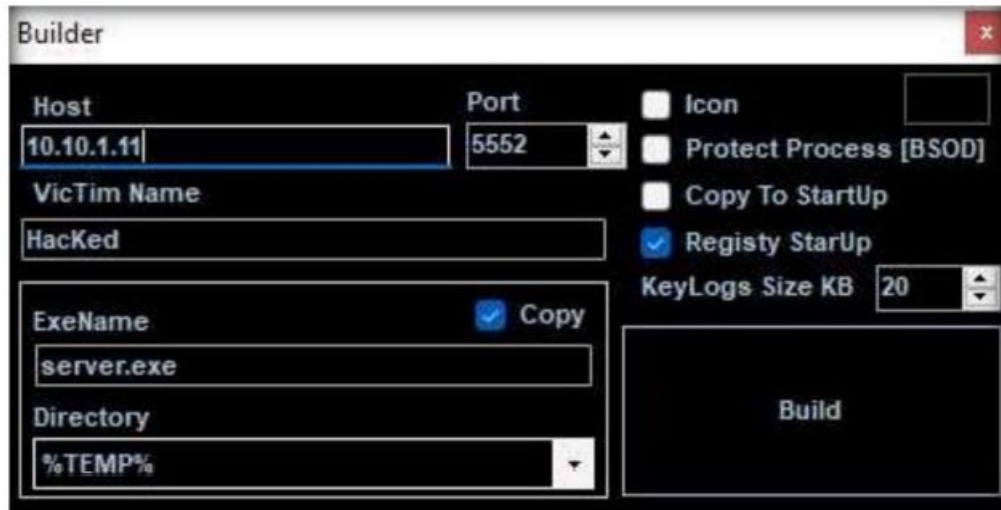


7. Aparecerá la GUI njRAT; haga clic en el enlace Builder situado en la esquina inferior izquierda de la GUI para configurar los detalles del exploit.



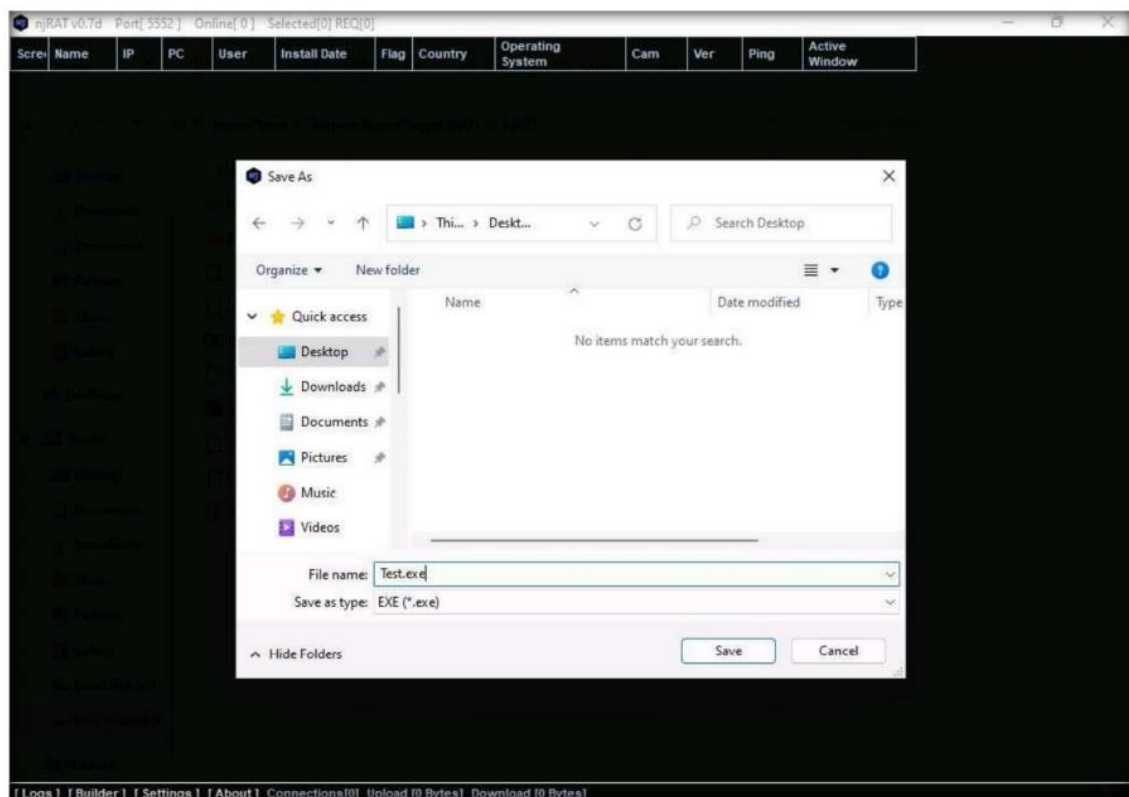
8. Aparece el cuadro de diálogo Builder; introduzca la dirección IP de la máquina Windows 11 (máquina atacante) en el campo Host, marque la opción Registry StarUp, deje los demás ajustes por defecto y haga clic en Build.

NOTA: EN ESTA TAREA, LA DIRECCIÓN IP DE LA MÁQUINA WINDOWS 11 ES 10.10.1.11.



9. Aparecerá la ventana Guardar como; especifique una ubicación para almacenar el servidor, cámbiele el nombre y haga clic en Ahorra.

10. En este laboratorio, la ubicación de destino elegida es Escritorio, y el archivo se llama Test.exe.



11. Una vez creado el servidor, aparece la ventana emergente ¡HECHO!; haga clic en Aceptar.

12. Ahora, utilice cualquier técnica para enviar este servidor al objetivo previsto a través del correo electrónico o cualquier otra fuente (en tiempo real, los atacantes envían este servidor a la víctima).

NOTA: EN ESTA TAREA, COPIAMOS EL ARCHIVO TEST.EXE A LA UBICACIÓN DE RED COMPARTIDA PARA COMPARTIR EL ARCHIVO.

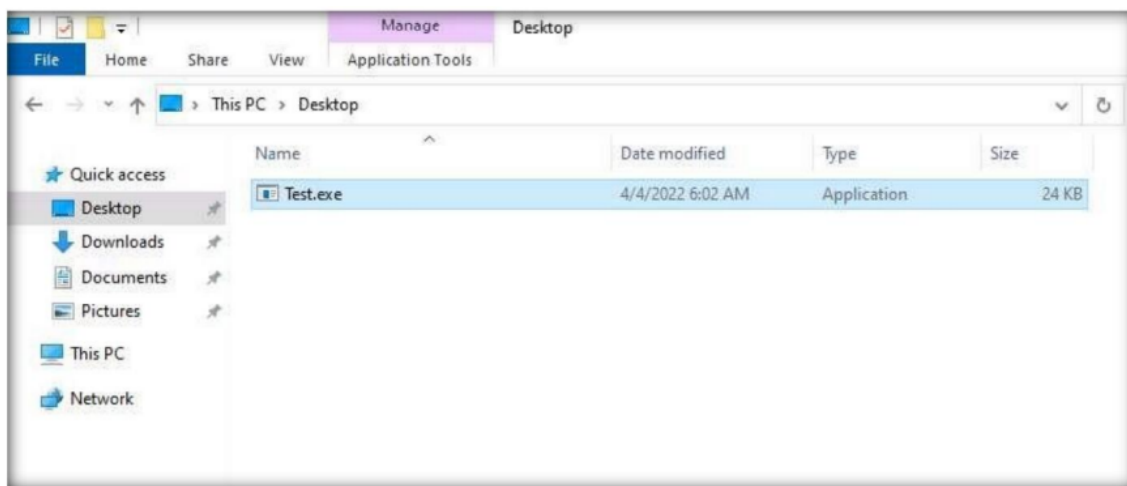
13. Cambie a la máquina virtual Windows 10. escriba la contraseña y pulse Intro.

NOTA: APARECE LA PANTALLA REDES, HAGA CLIC EN SÍ PARA PERMITIR QUE SU PC SEA DETECTABLE POR OTROS PC Y DISPOSITIVOS DE LA RED.

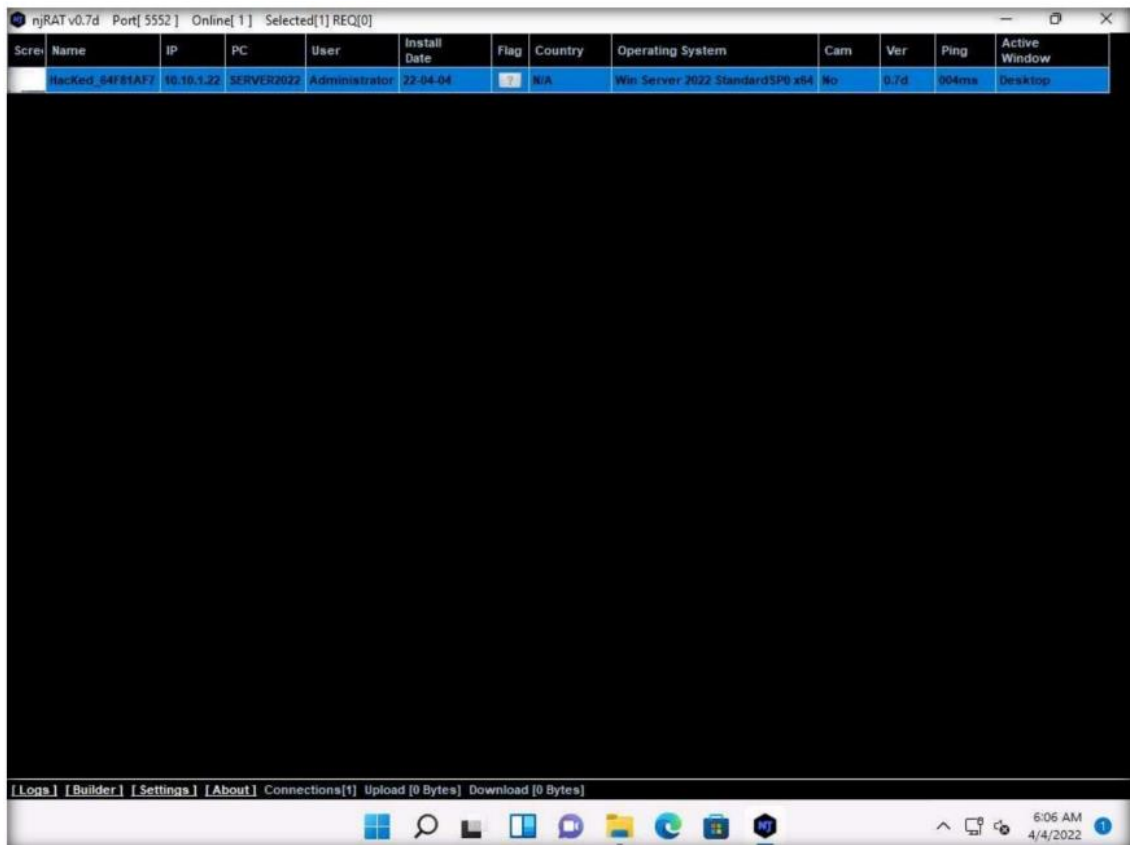
14. Navegue hasta la ubicación de red compartida y, a continuación, copie y pegue el archivo ejecutable (Test.exe) en el escritorio de Windows 10.

15. Aquí, estás actuando como un atacante que entra en la máquina Windows 11 para crear un servidor malicioso, y como una víctima que entra en la máquina Windows 10 y descarga el servidor.

16. Haga doble clic en el servidor (Test.exe) para ejecutar este ejecutable malicioso.



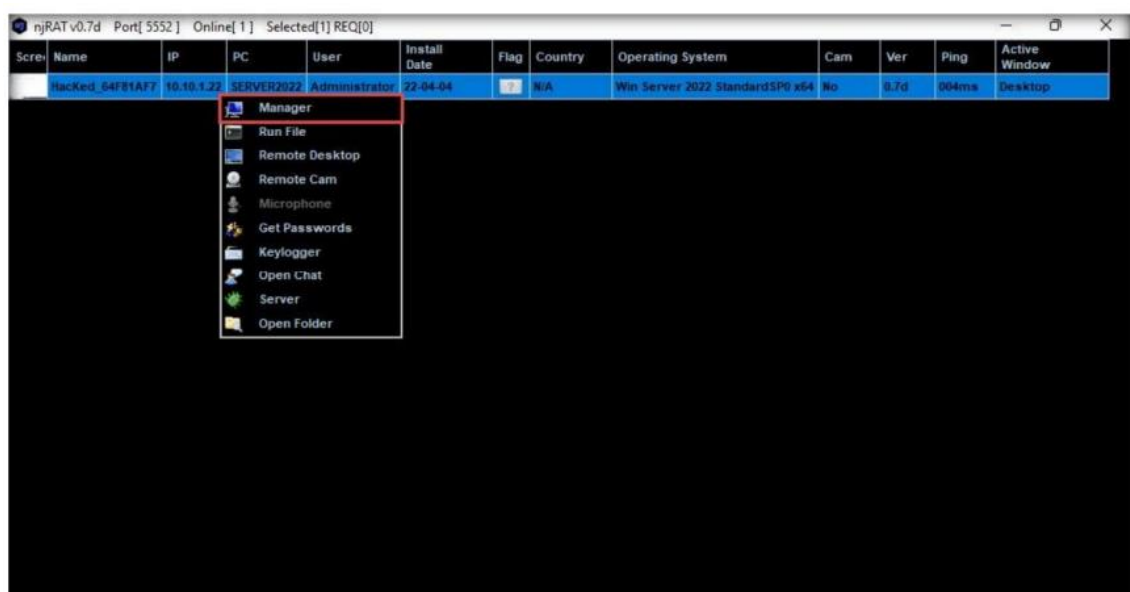
17. Vuelva a la máquina virtual Windows 11. Maximice la ventana de njRAT GUI. Tan pronto como la víctima (aquí, usted) hace doble clic en el servidor, el ejecutable comienza a ejecutarse y el cliente njRAT (njRAT GUI) que se ejecuta en Windows 11 establece una conexión persistente con la máquina víctima, como se muestra en la captura de pantalla.



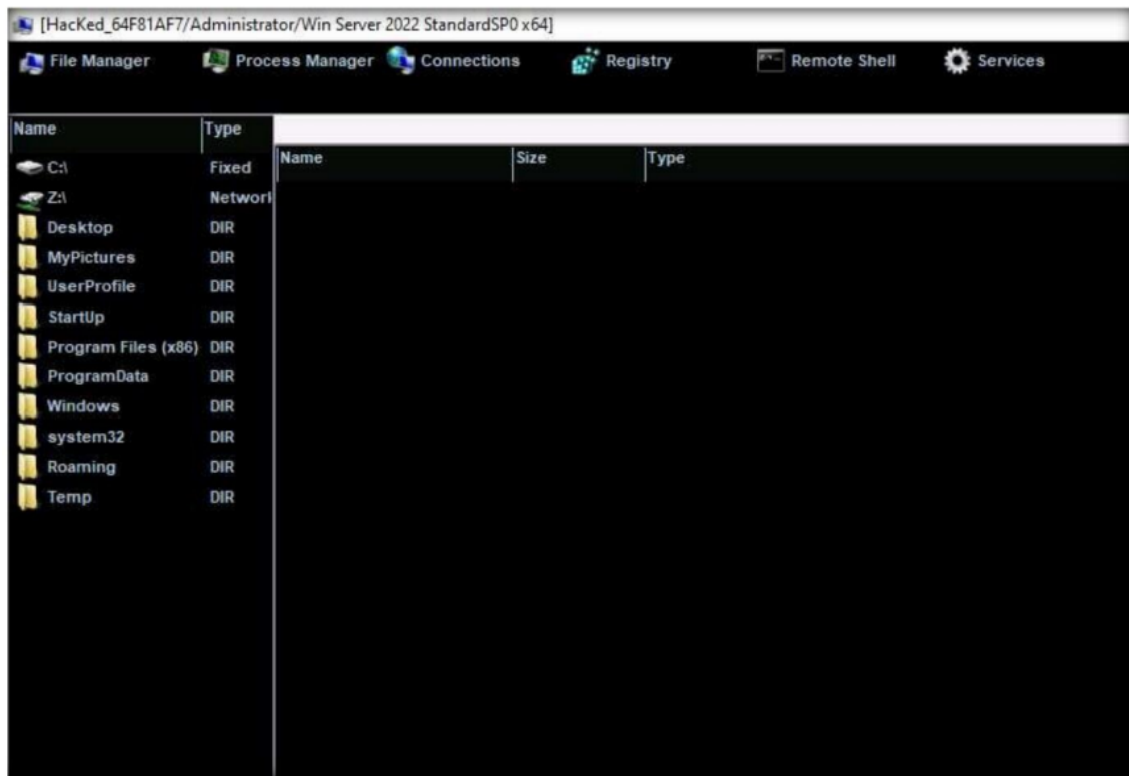
18. A menos que el atacante que trabaja en la máquina con Windows 11 desconecte el servidor por su cuenta, la máquina víctima permanecerá bajo su control.

19. La GUI muestra los detalles básicos de la máquina, como la dirección IP, el nombre de usuario y el tipo de sistema operativo.

20. Haga clic con el botón derecho del ratón en el nombre de la víctima detectada y haga clic en Administrador.



21. La ventana del gestor aparece con el Gestor de Archivos seleccionado por defecto

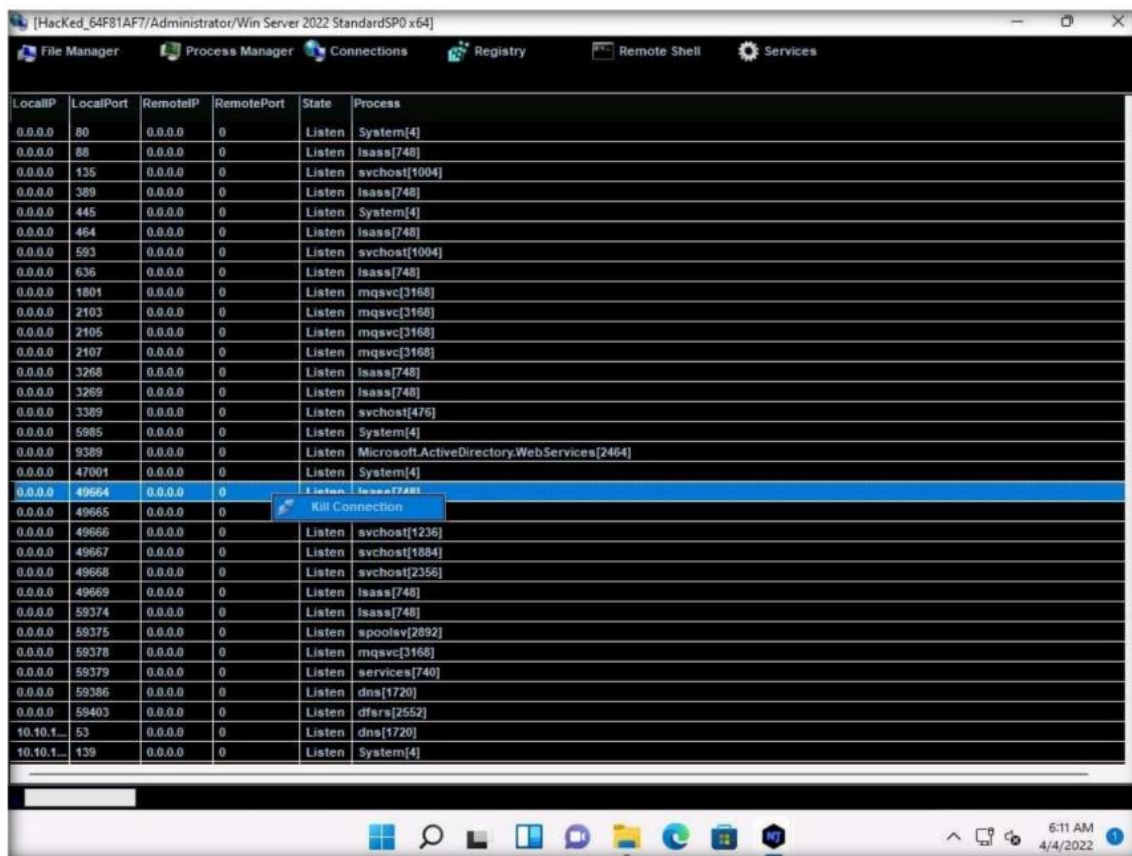


22. Haga doble clic en cualquier directorio del panel izquierdo (aquí, ProgramData); todos sus archivos y directorios asociados aparecerán en el panel derecho. Puede hacer clic con el botón derecho en un directorio seleccionado y manipularlo utilizando las opciones contextuales.

23. Haga clic en Administrador de procesos. Se le redirigirá al Administrador de procesos, donde puede hacer clic con el botón derecho en un proceso seleccionado y realizar acciones, como Matar, Eliminar y Reiniciar.

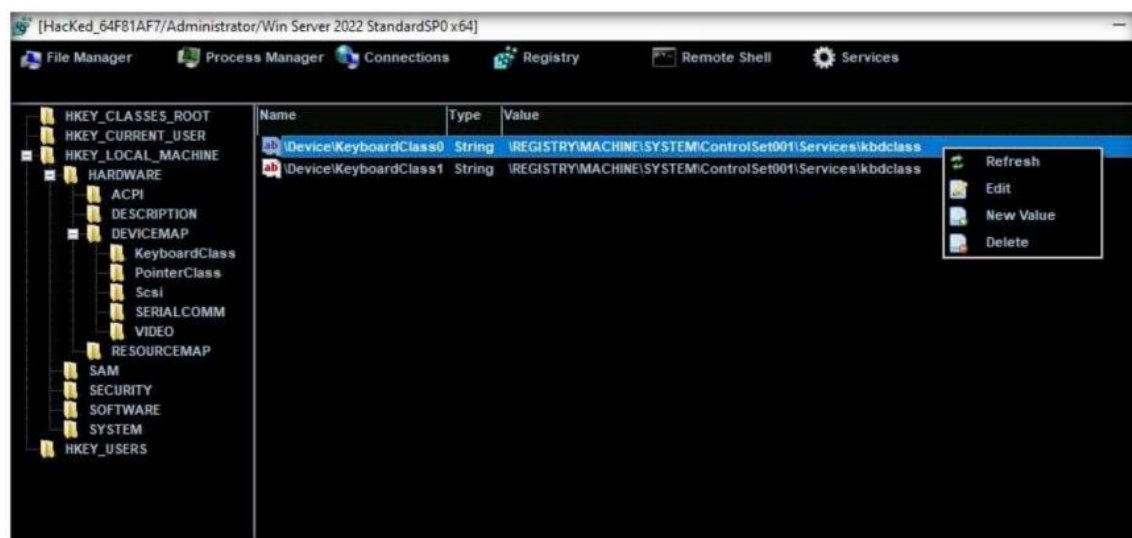


24. Haga clic en Conexiones, seleccione una conexión específica, haga clic con el botón derecho sobre ella y haga clic en Matar conexión. Esto mata la conexión entre dos máquinas que se comunican a través de un puerto en particular.



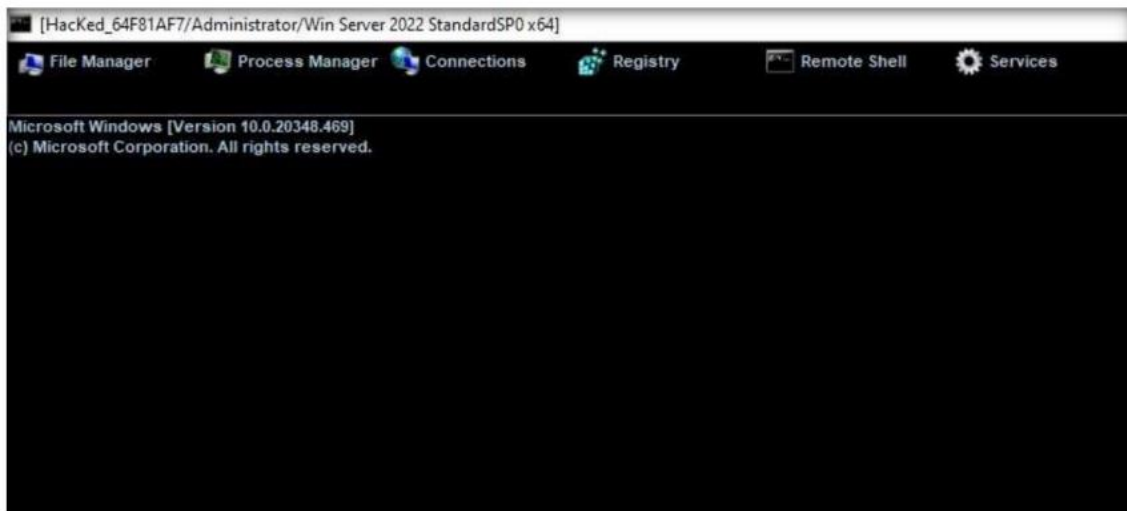
25. Haga clic en Registro, elija un directorio de registro del panel izquierdo y haga clic con el botón derecho en sus archivos de registro asociados.

26. Aparecen algunas opciones para los archivos; puede utilizarlas para manipularlos.

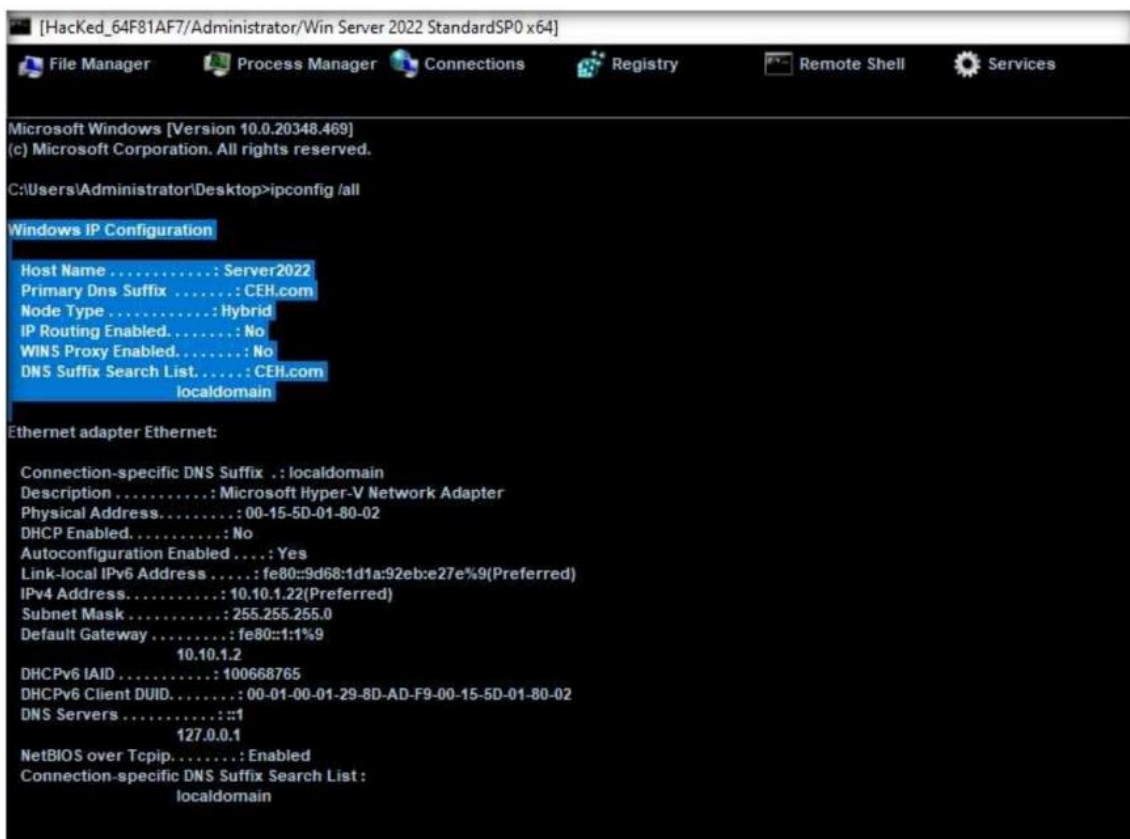


27. Haga clic en Remote Shell. Esto inicia un símbolo del sistema remoto para la máquina víctima (Windows 10).

28. En el campo de texto presente en la sección inferior de la ventana escriba el comando.



29. Esto muestra todas las interfaces relacionadas con la máquina víctima, como se muestra en la captura de pantalla.



30. Del mismo modo, puede emitir todos los demás comandos que se pueden ejecutar en el símbolo del sistema de la máquina víctima.

31. Del mismo modo, haga clic en Servicios. Podrá ver todos los servicios que se están ejecutando en la máquina víctima. En esta sección, puede utilizar las opciones para iniciar, pausar o detener un servicio.



32. Cierre la ventana del Gestor.

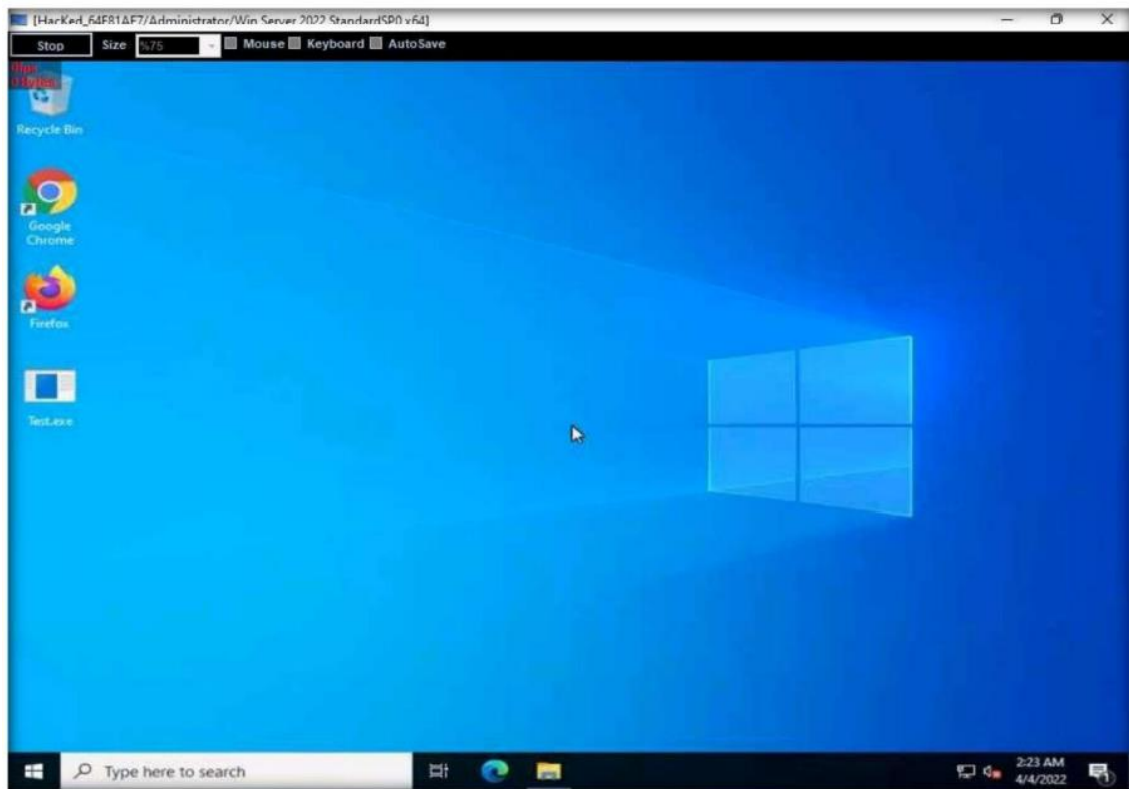
33. Haga clic con el botón derecho del ratón en el nombre de la víctima y seleccione Escritorio remoto.



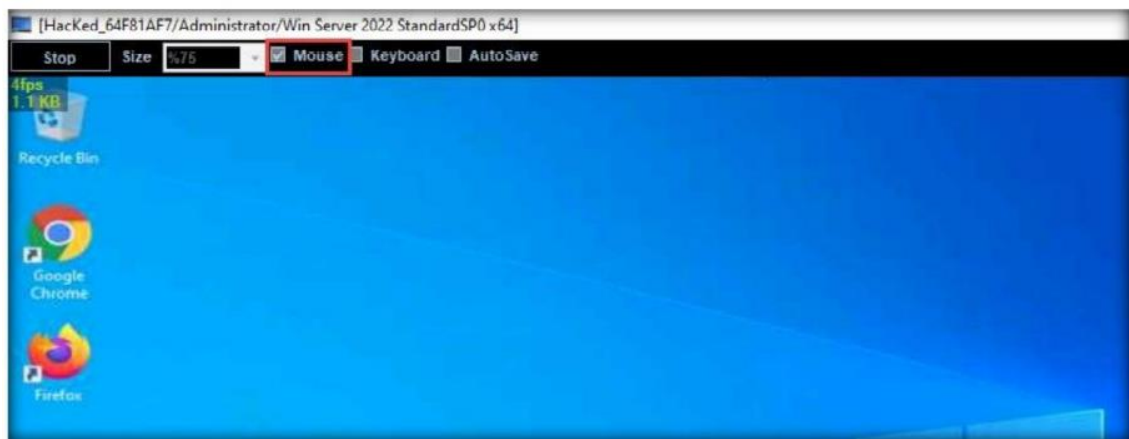
34. Esto inicia una conexión de escritorio remoto sin que la víctima sea consciente de ello.

35. Aparecerá una ventana de Escritorio Remoto; sitúe el cursor del ratón en la zona superior central de la ventana. Aparece una flecha hacia abajo; haga clic en ella.

NOTA: LA PANTALLA PUEDE TARDAR UN POCO EN APARECER.



36. Aparecerá un panel de control de escritorio remoto; marque la opción Ratón.



37. Ahora, podrás interactuar remotamente con la máquina víctima usando el ratón.

NOTA: SI DESEA CREAR ARCHIVOS O ESCRIBIR SCRIPTS EN EL EQUIPO VÍCTIMA, DEBERÁ ACTIVAR LA OPCIÓN TECLADO.

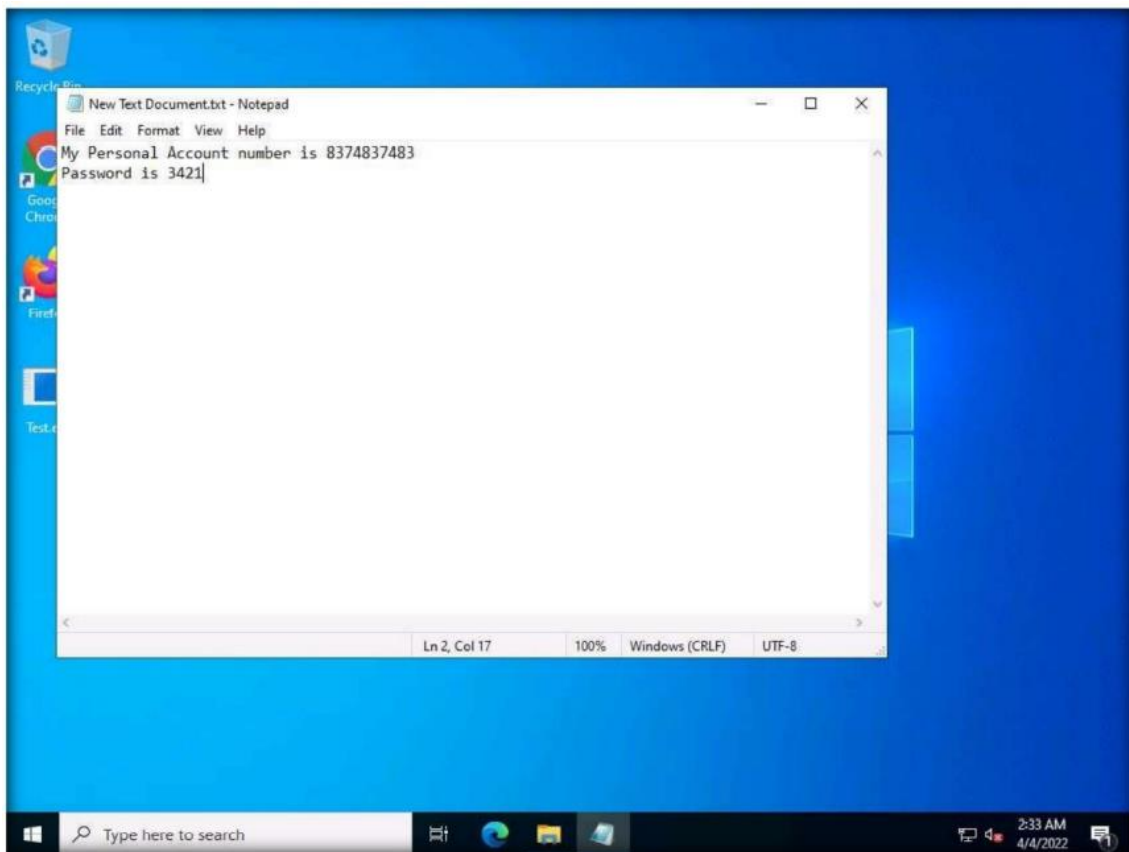
38. Una vez completada la tarea, cierre la ventana de Escritorio Remoto.

NOTA: SI APARECE UNA VENTANA EMERGENTE HACKED, HAZ CLIC EN CONTINUAR PARA CERRARLA.

39. En la página mismo haga clic con el botón derecho del ratón sobre la víctima nombre, y seleccione Remoto Cam y Micrófono para espiarlos y rastrear conversaciones de voz.



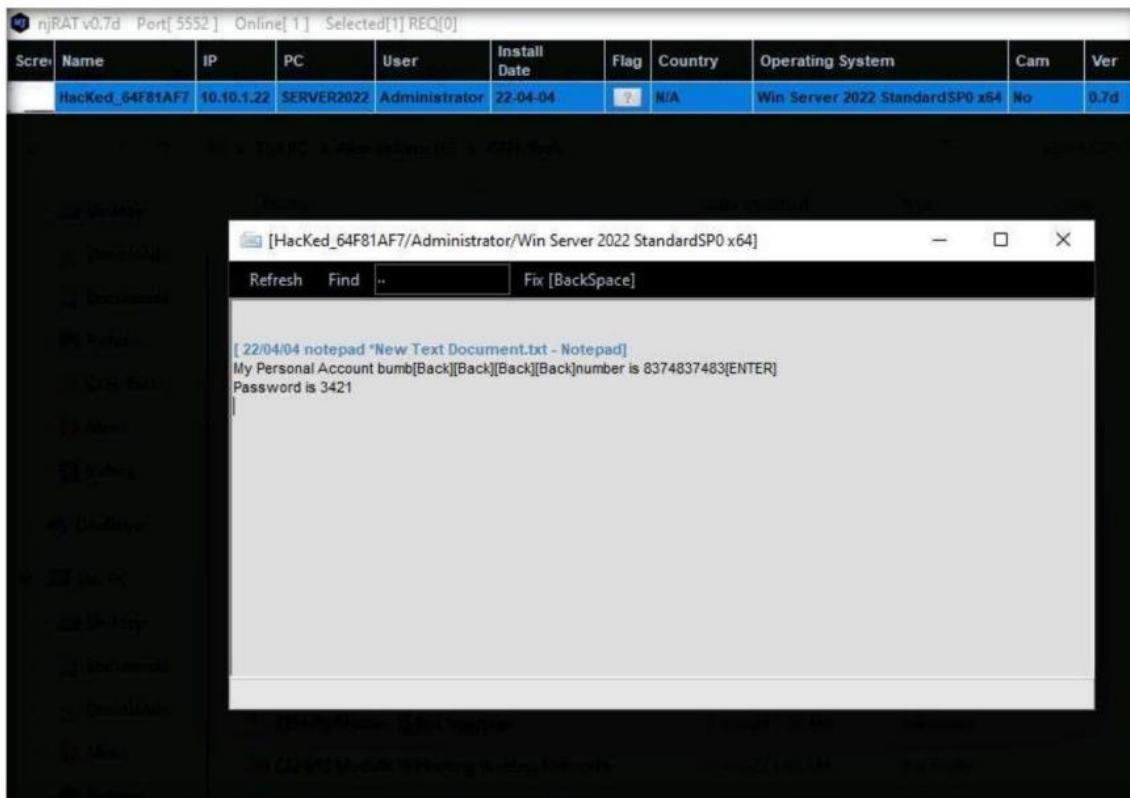
40. Cambie a la máquina virtual Windows 10. Suponga que es un usuario legítimo y realiza algunas actividades, como iniciar sesión en cualquier sitio web o escribir algún texto en documentos de texto.



41. Vuelva a la máquina virtual Windows 11, haga clic con el botón derecho en el nombre de la víctima y haga clic en Registrador de teclas.

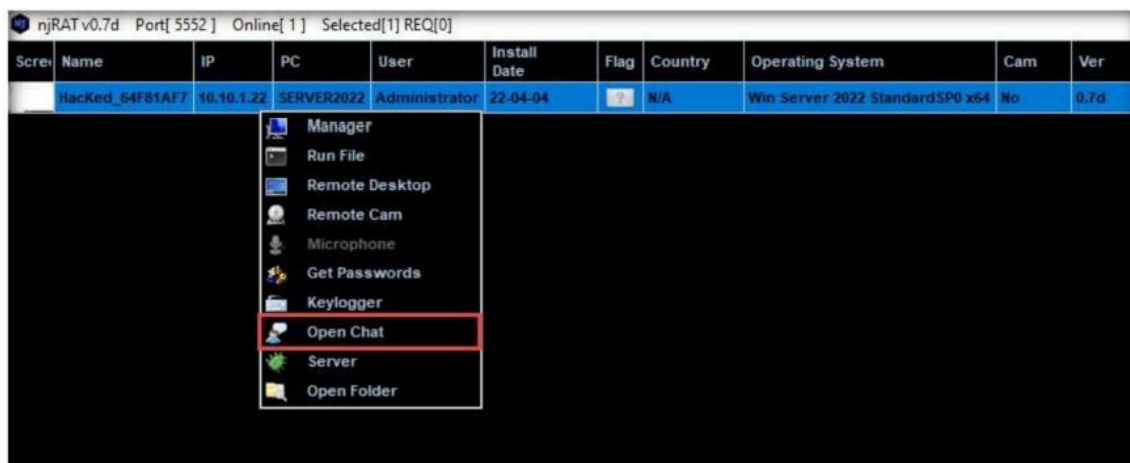
42. Aparecerá la ventana Keylogger; espere a que se cargue.

43. La ventana muestra todas las pulsaciones de teclas realizadas por la víctima en Windows Server 2022, como se muestra en la captura de pantalla.



44. Cierra la ventana del Registrador de teclas.

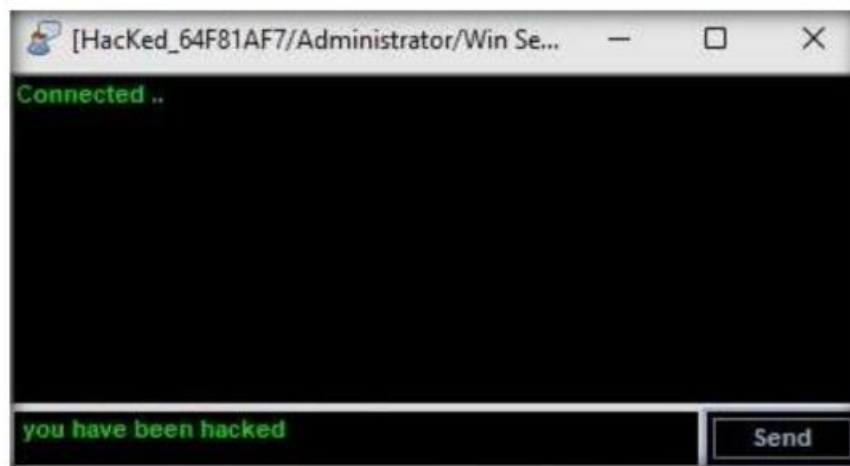
45. Haga clic con el botón derecho del ratón en el nombre de la víctima y haga clic en Abrir chat.



46. Aparecerá una ventana emergente de Chat; introduce un apodo (aquí, Hacker) y haz clic en Aceptar.

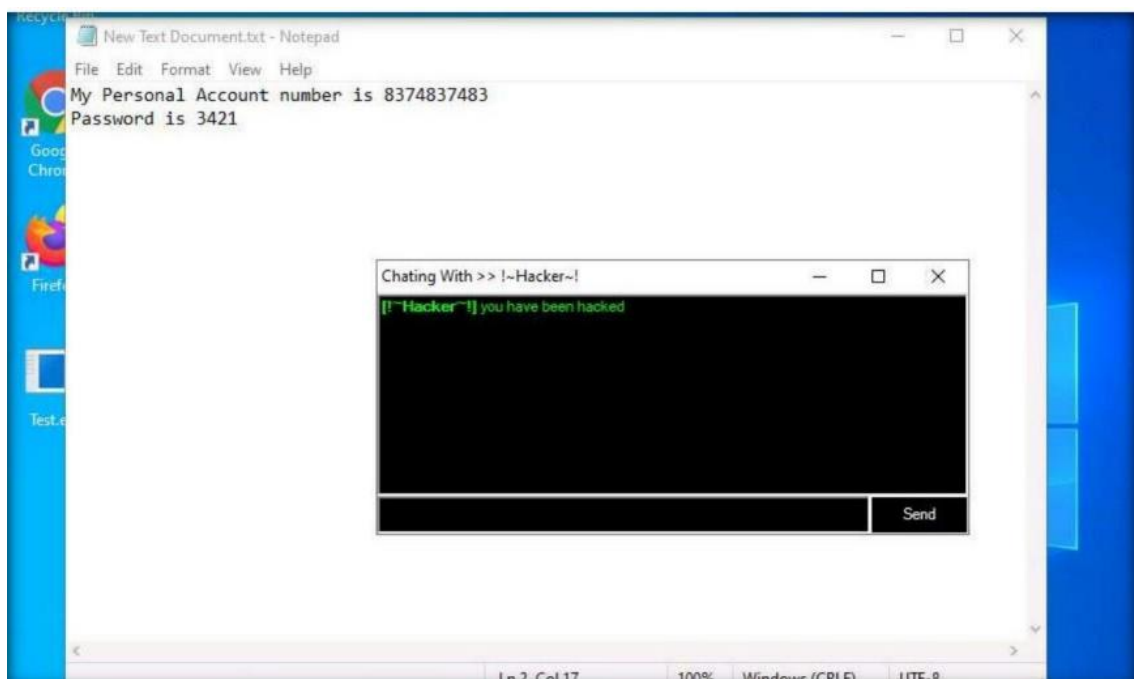


47. Aparecerá un cuadro de chat; escriba un mensaje y haga clic en Enviar.



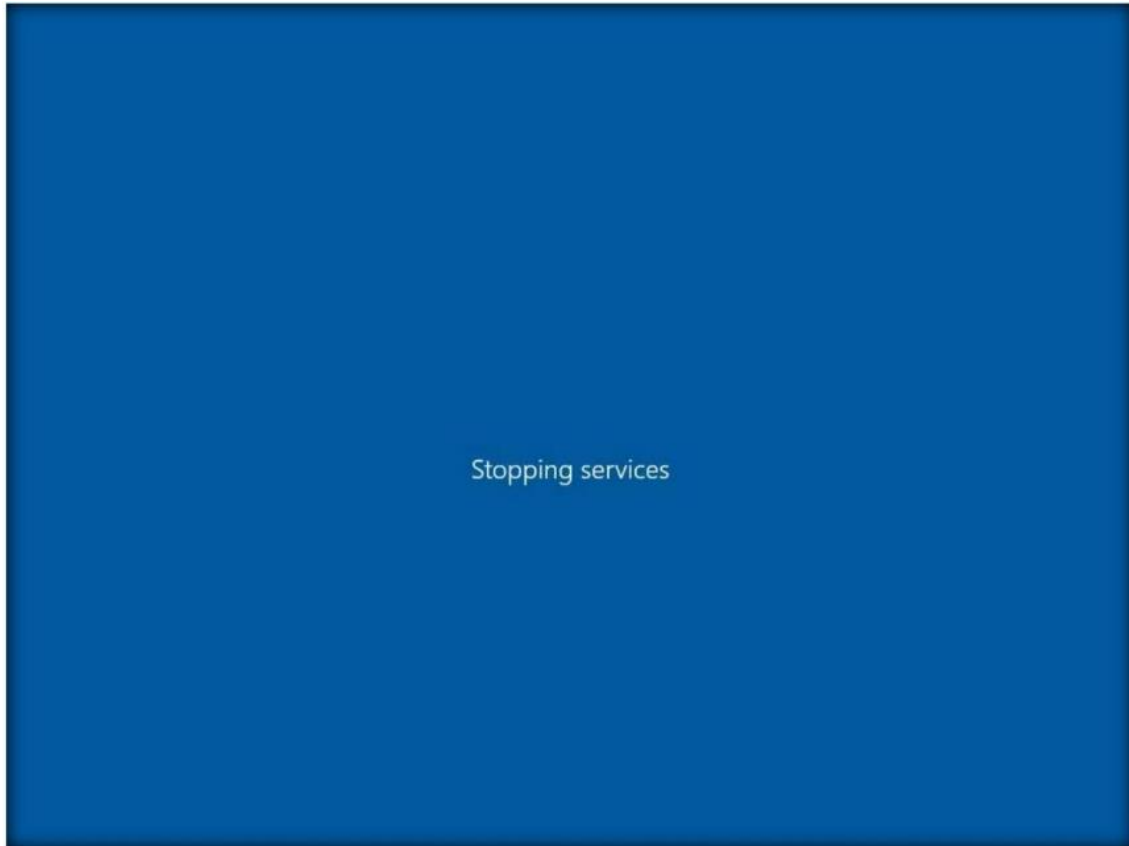
48. En tiempo real, tan pronto como el atacante envía el mensaje, aparece una ventana emergente en la pantalla de la víctima (Windows 10), como se muestra en la captura de pantalla.

49. Cambie a la máquina virtual Windows 10, puede observar el mensaje del hacker aparece en la pantalla.



50. Al ver esto, la víctima se pone alerta e intenta cerrar el chatbox. Independientemente de lo que haga la víctima, el chatbox permanece abierto mientras el atacante lo utilice.

51. Sorprendida por el comportamiento, la víctima (usted) intenta romper la conexión reiniciando la máquina. Tan pronto como esto sucede, njRAT pierde su conexión con Windows 10, ya que la máquina se apaga en el proceso de reinicio.



52. Vuelva a la máquina atacante (Windows 11); puede ver que se ha perdido la conexión con la máquina víctima.



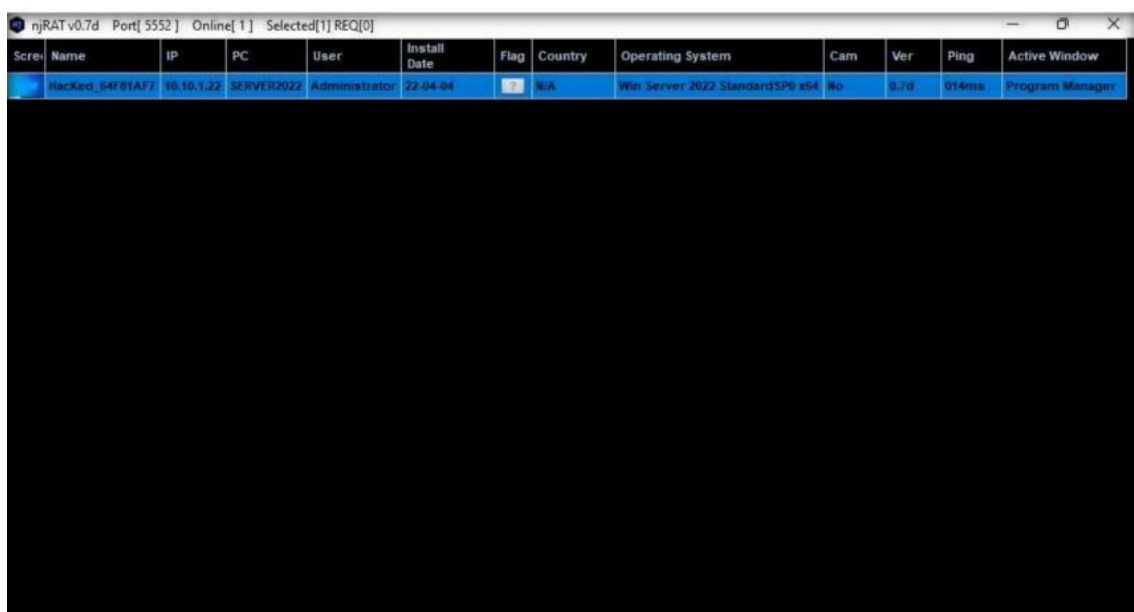
53. Sin embargo, tan pronto como la víctima inicia sesión en su máquina, el cliente njRAT establece automáticamente una conexión con la víctima, como se muestra en la captura de pantalla.

54. Cambie a la máquina víctima (Windows 10), escriba la contraseña y pulse Intro.



55. Vuelva a la máquina atacante (Windows 11); puede ver que la conexión se ha restablecido con la máquina víctima.

NOTA: PUEDE LLEVAR ALGÚN TIEMPO ESTABLECER UNA CONEXIÓN CON LA VÍCTIMA.



56. El atacante, como de costumbre, hace uso de la conexión para acceder a la máquina víctima de forma remota y realizar actividades maliciosas.

57. Una vez finalizado este laboratorio, cambie a la máquina virtual Windows 10, inicie el Administrador de tareas, haga clic en Más detalles y busque el proceso server.exe (32 bits) y haga clic en Finalizar tarea.

Name	Status	CPU	Memory
Client for NFS service		0%	0.9 MB
CTF Loader		0%	2.6 MB
Distributed File System Replicati...		0%	6.1 MB
Domain Name System (DNS) Se...		0%	117.2 MB
Google Crash Handler		0%	0.4 MB
Google Crash Handler (32 bit)		0%	0.5 MB
Host Process for Windows Tasks		0%	1.7 MB
Message Queuing Service		0%	2.7 MB
Microsoft Distributed Transactio...		0%	2.3 MB
Microsoft.ActiveDirectory.WebS...		0%	15.4 MB
Microsoft® Volume Shadow Co...		0%	1.2 MB
MoUSO Core Worker Process		0%	2.2 MB
Runtime Broker		0%	1.6 MB
Runtime Broker		0%	4.6 MB
Runtime Broker		0%	2.0 MB
Search		0%	0 MB
server.exe (32 bit)		0%	0.8 MB
SMShost.exe		0%	3.5 MB
SMShost.exe (3)		0%	6.2 MB
SNMP Service		0%	3.1 MB

58. Esto concluye la demostración de cómo crear un troyano utilizando el troyano njRAT para obtener el control de una máquina víctima.

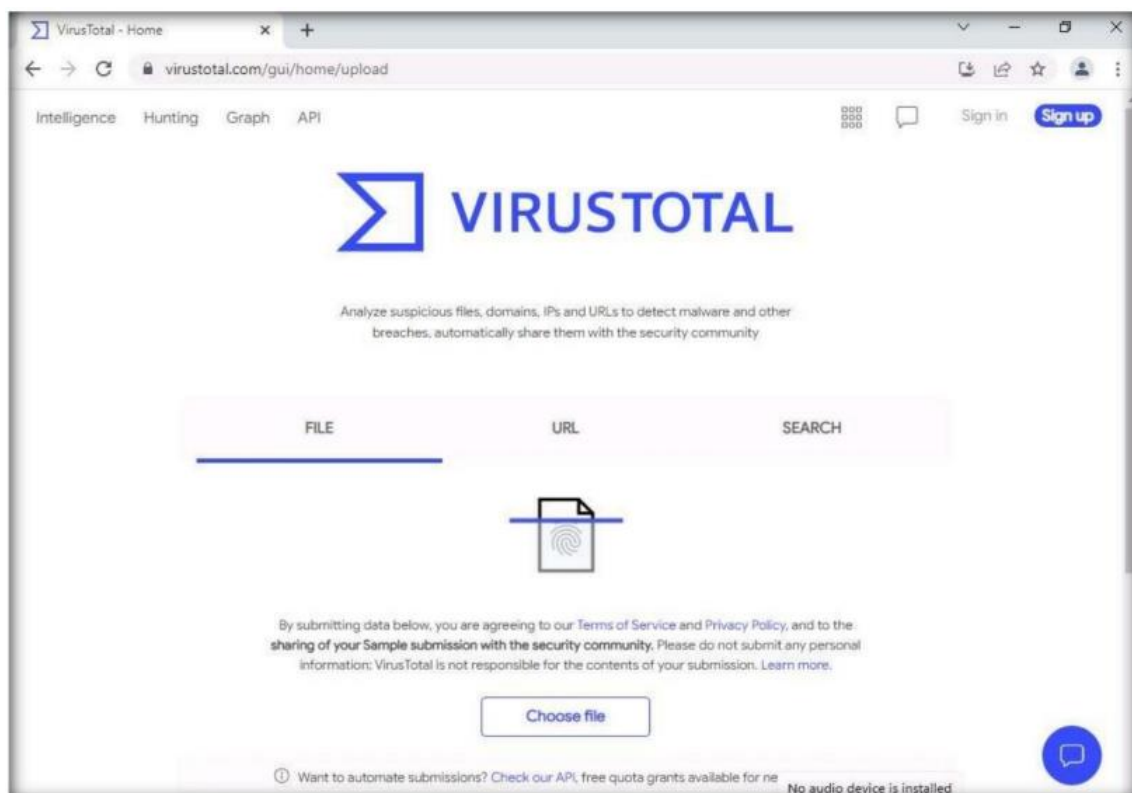
59. Cierre todas las ventanas abiertas en todas las máquinas.

TAREA 2: OCULTAR UN TROYANO USANDO SWAYZCRYPTOR Y HACERLO INDETECTABLE PARA VARIOS PROGRAMAS ANTIVIRUS

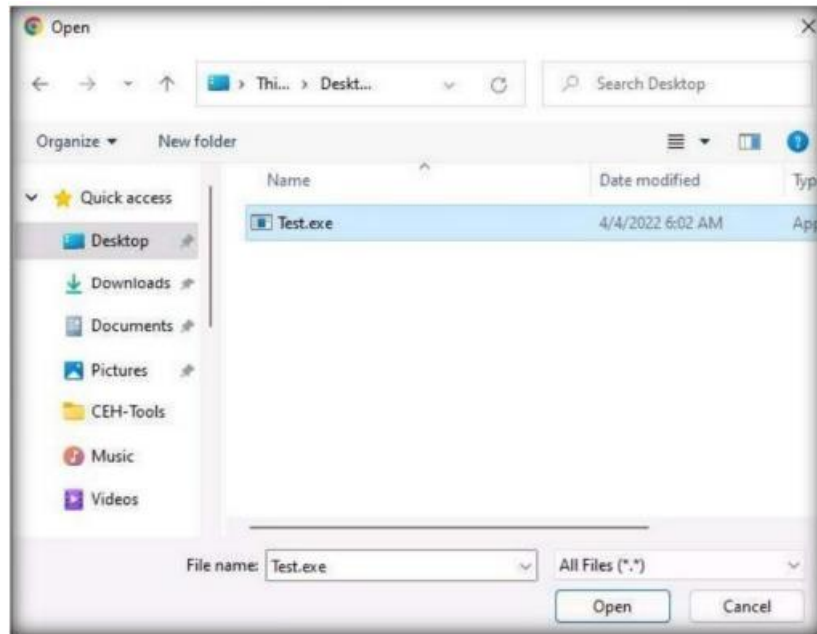
En la actualidad, numerosos programas antivirus están configurados para detectar programas maliciosos como troyanos, virus y gusanos. Aunque los especialistas en seguridad actualizan constantemente las definiciones de virus, los hackers intentan continuamente evadirlas o eludirlas. Uno de los métodos que utilizan los atacantes para eludir los antivirus es "criptar" (abreviatura de "cifrar") los archivos maliciosos utilizando criptadores totalmente indetectables (FUD). El cifrado de estos archivos les permite alcanzar sus objetivos y, de este modo, hacerse con el control total de la máquina de la víctima. Crypter es un software que encripta el código binario original del archivo .exe para ocultar virus, spyware, keyloggers y RATs, entre otros, en cualquier tipo de archivo para hacerlos indetectables por los antivirus. SwayzCryptor es un encriptador (o "crypter") que permite a los usuarios encriptar el código fuente de sus programas.

Aquí, utilizaremos el SwayzCryptor para ocultar un troyano y hacerlo indetectable por el software antivirus.

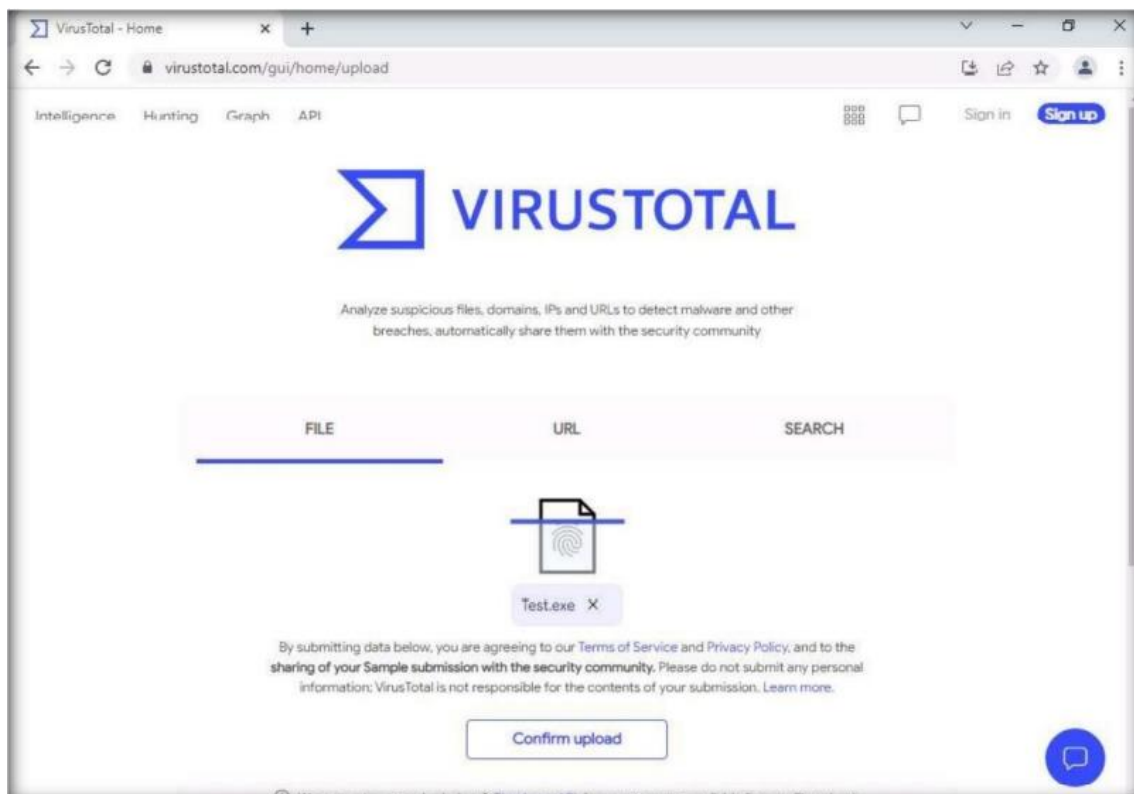
1. Cambie a la máquina virtual Windows 11, abra cualquier navegador web (aquí, Google Chrome). En la barra de direcciones del navegador coloque el cursor del ratón y escriba <https://www.virustotal.com> y pulse Intro.
2. Aparece el sitio principal de análisis de VirusTotal; haga clic en Elegir archivo para cargar un archivo de virus.



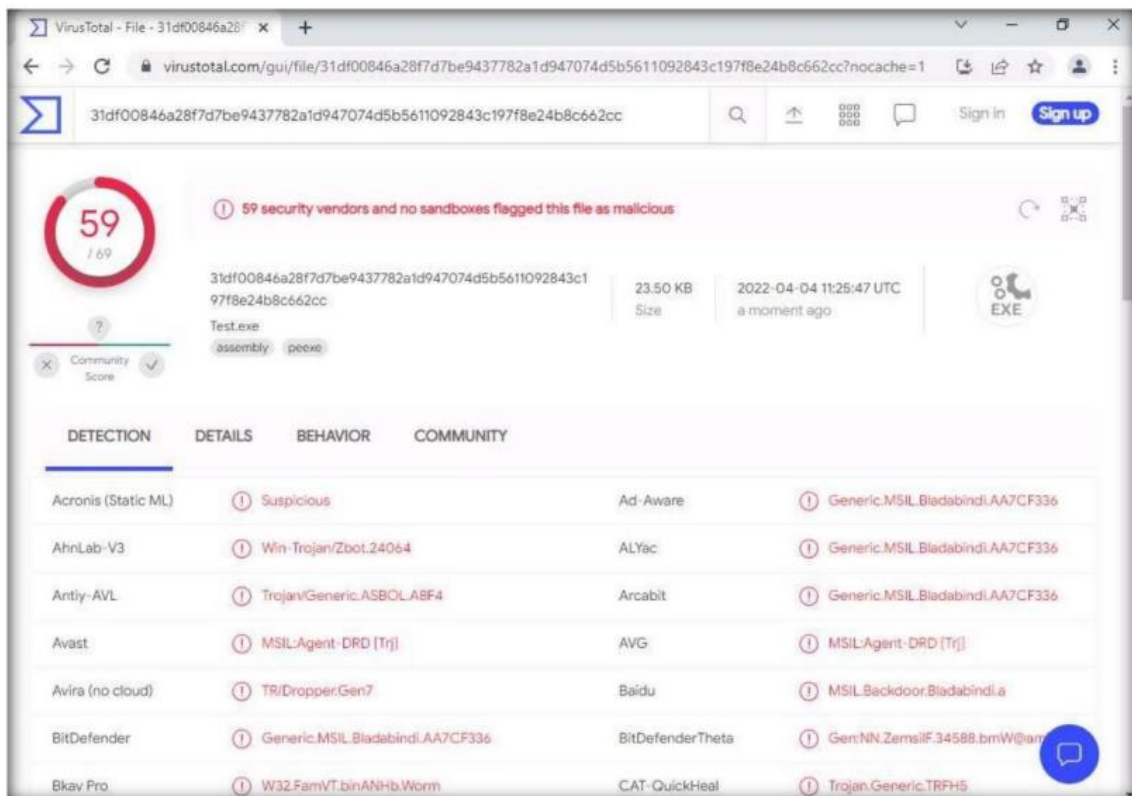
3. Aparecerá un cuadro de diálogo Abrir; vaya a la ubicación donde guardó el archivo malicioso Test.exe en la tarea anterior (Escritorio), selecciónelo y haga clic en Abrir.



4. Haga clic en Confirmar carga en la página de VirusTotal.



5. VirusTotal carga el archivo y lo escanea con los distintos programas antivirus de su base de datos. Una vez completado el escaneo, aparece el resultado del escaneo, como se muestra en la captura de pantalla.

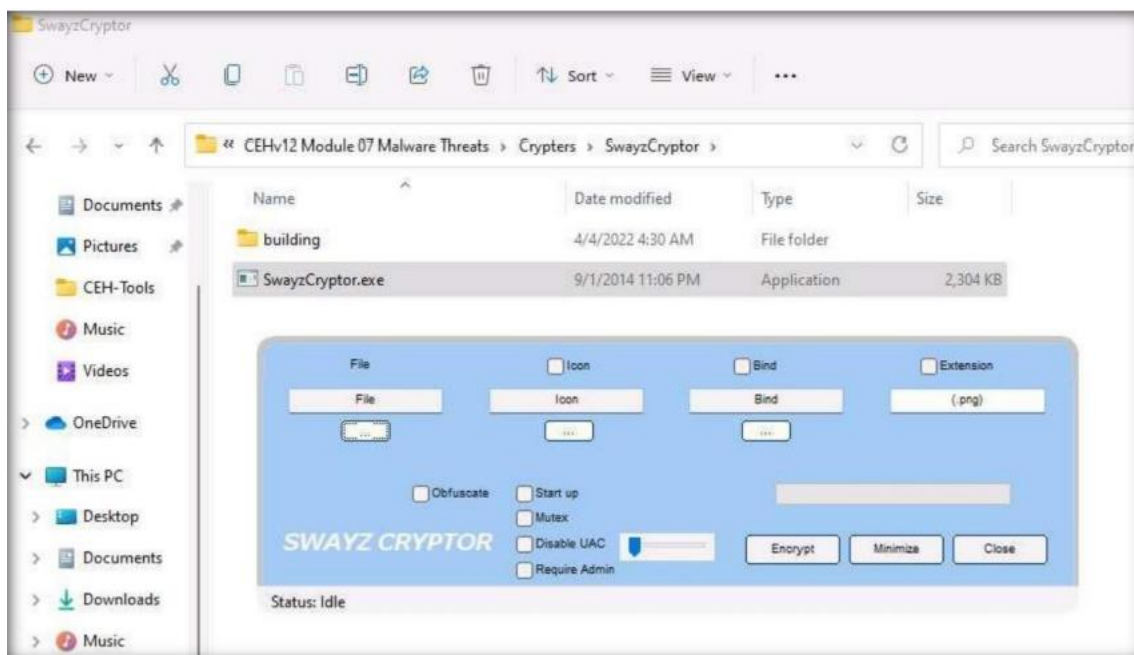


6. Puede ver que 59 de 69 programas antivirus han detectado Test.exe como un archivo malicioso. Minimice la ventana del navegador web.

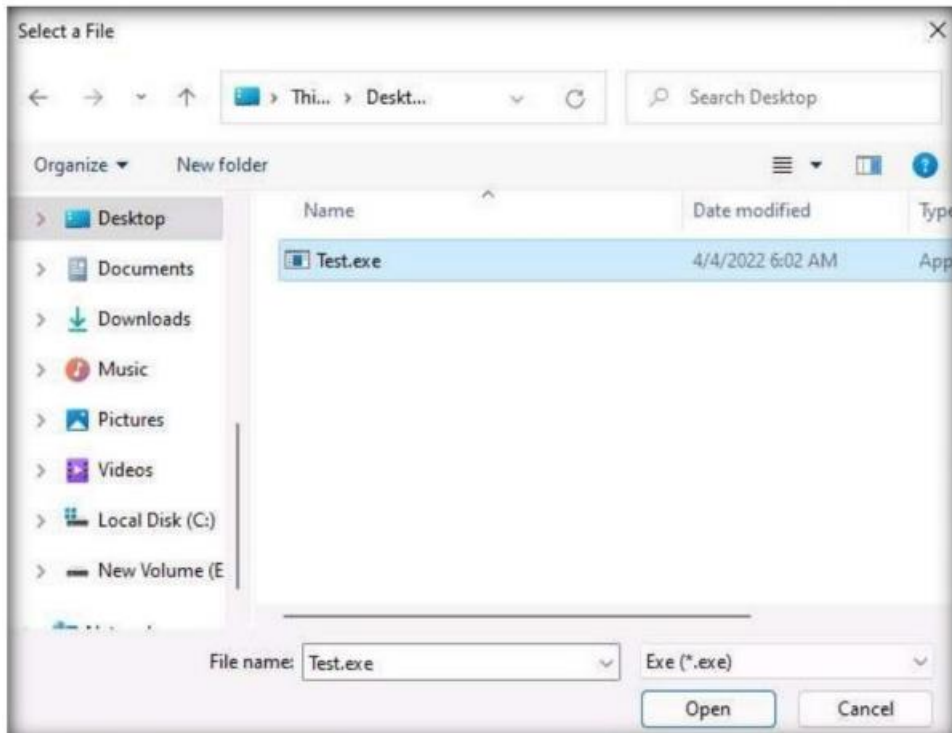
NOTA: EL RATIO DE DETECCIÓN PUEDE VARIAR AL REALIZAR ESTA TAREA.

7. Vaya a C:\Tools\Crypters\SwayzCryptor y haga doble clic en SwayzCryptor.exe.

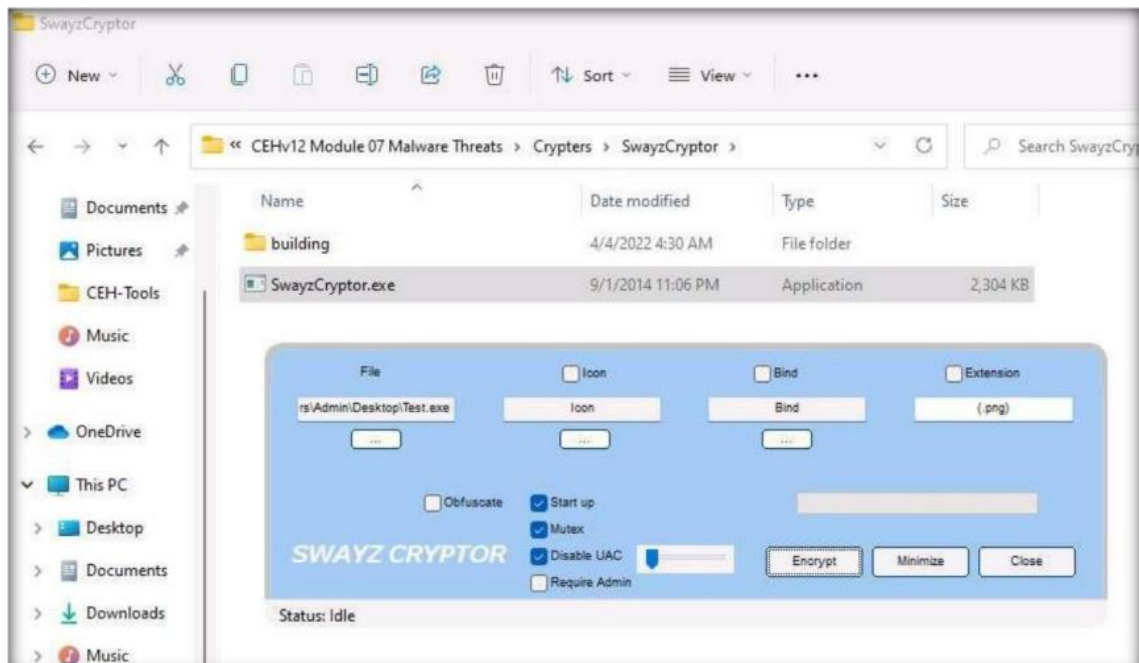
8. Aparecerá la interfaz gráfica de usuario de SwayzCryptor; haz clic en el icono con forma de elipse situado debajo de Archivo para seleccionar el archivo troyano.



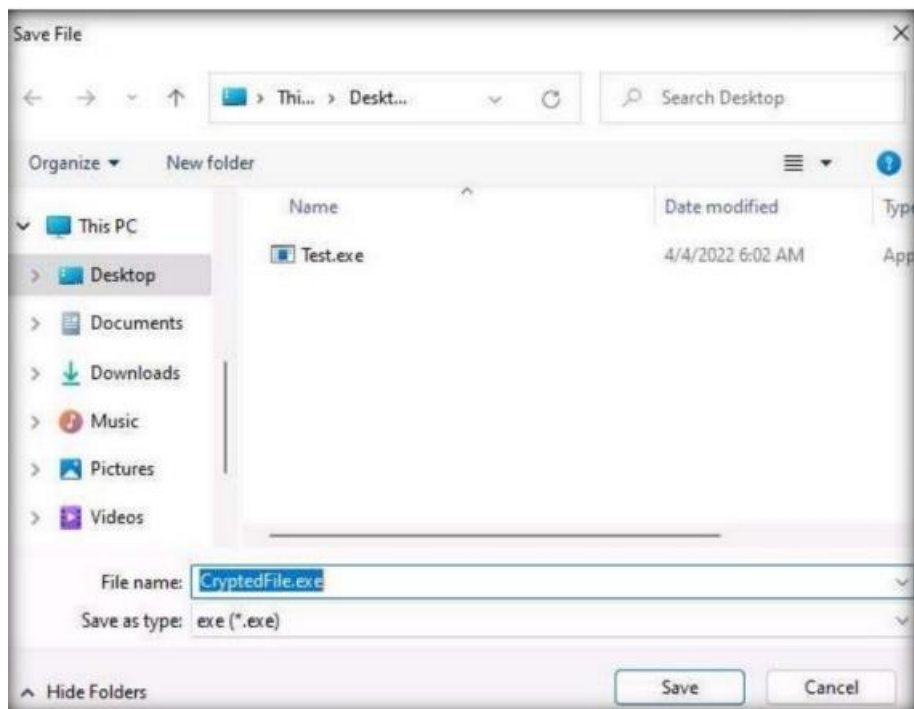
9. Aparecerá el cuadro de diálogo Seleccionar un archivo; vaya a la ubicación de Test.exe (Escritorio), selecciónelo y haga clic en Abrir.



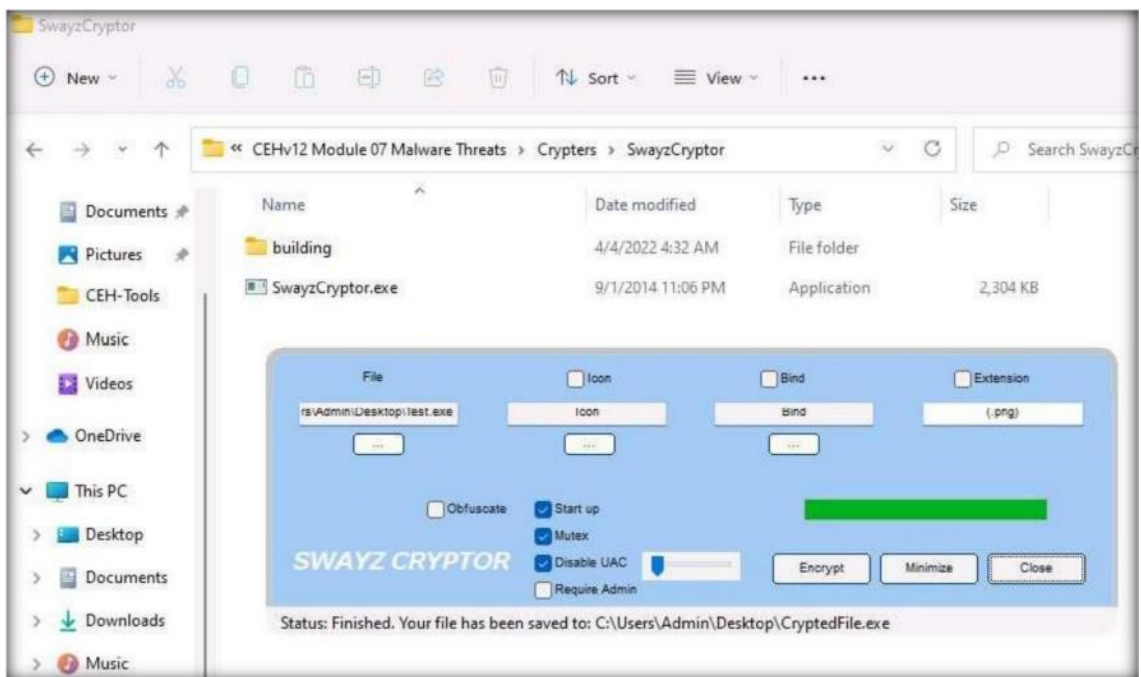
10. Una vez seleccionado el archivo, marque las opciones Arrancar, Mutex y Desactivar UAC y, a continuación, haga clic en Cifrar.



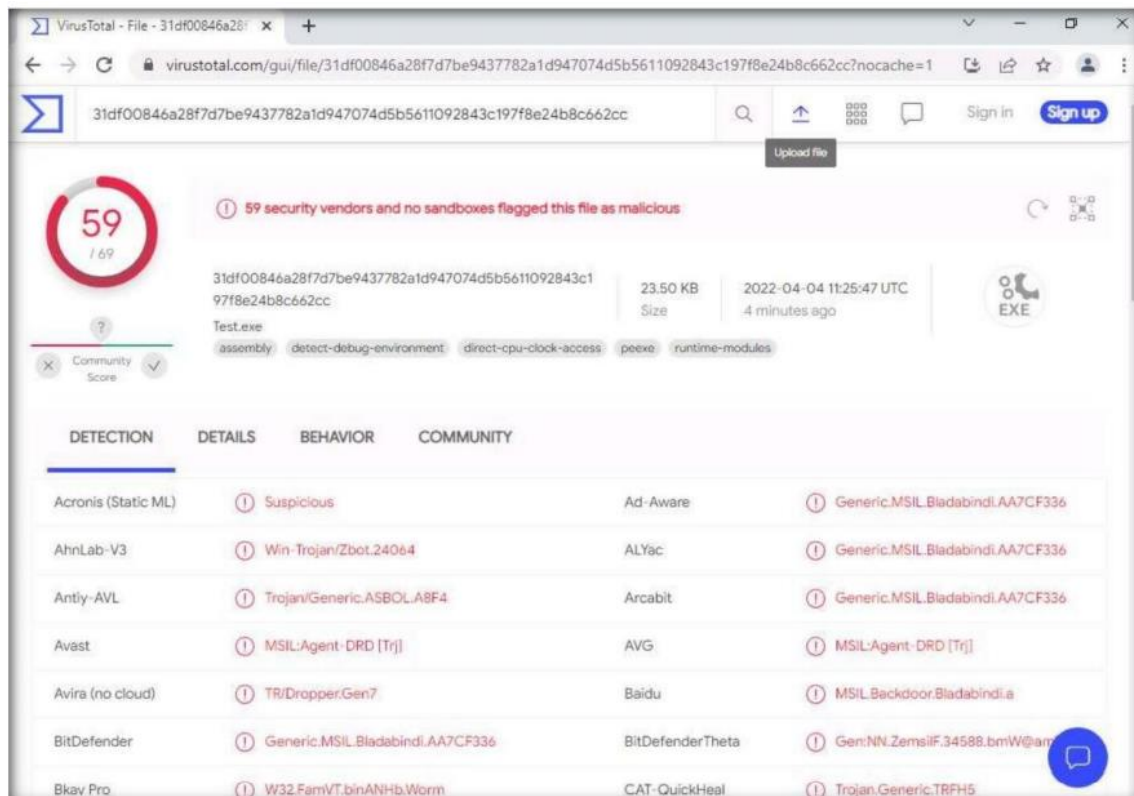
11. Aparecerá el cuadro de diálogo Guardar archivo; seleccione la ubicación en la que desea guardar el archivo cifrado (aquí, Escritorio), deje el nombre del archivo en su valor predeterminado (CryptedFile) y haga clic en Encrypt.



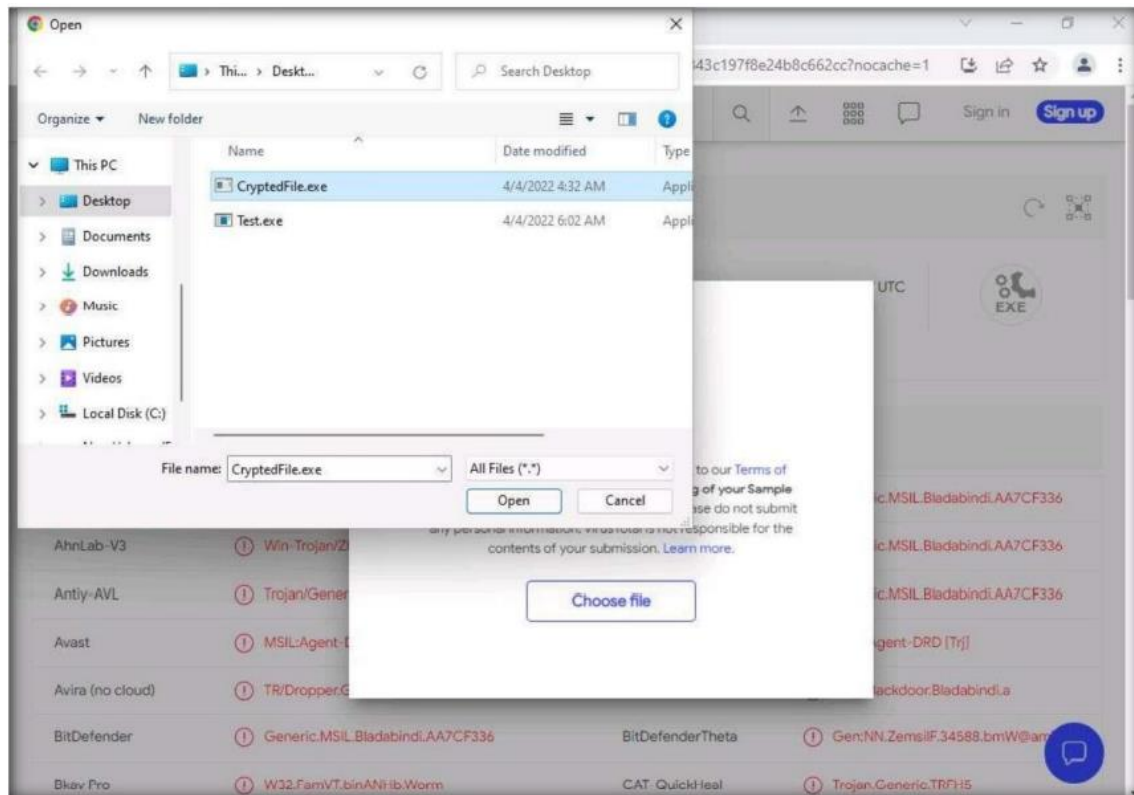
12. Una vez finalizado el cifrado, haga clic en Cerrar.



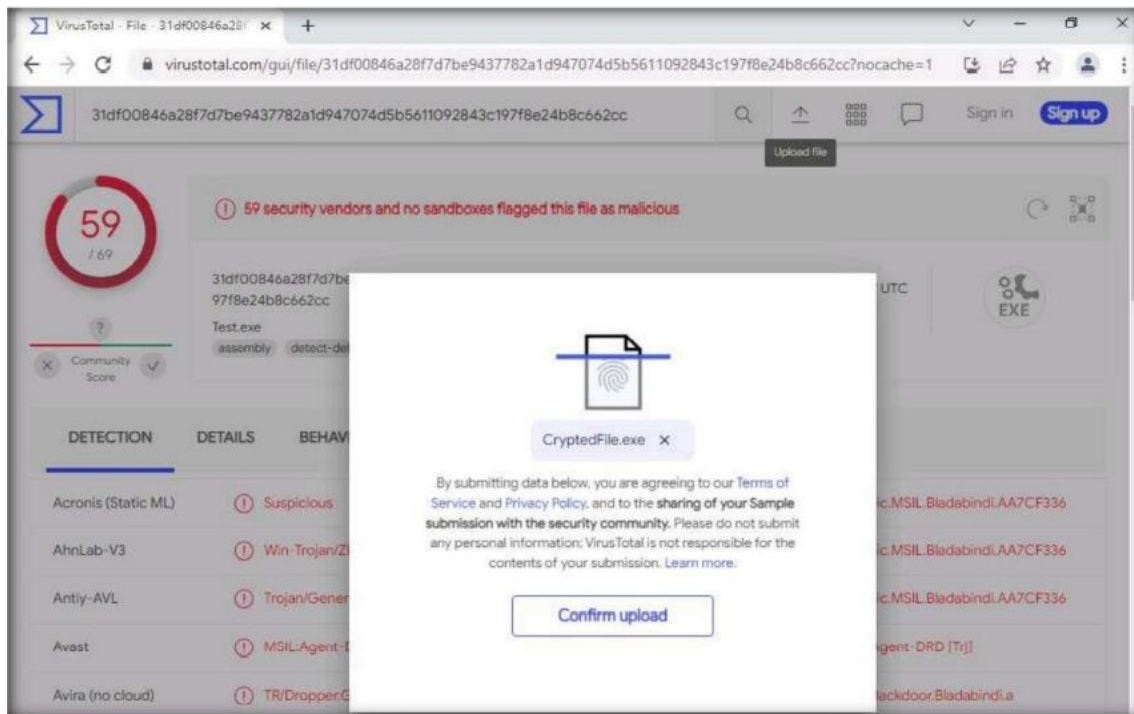
13. Maximiza el navegador web (aquí, Google Chrome). En la página de análisis de VirusTotal, haz clic en el icono Subir archivo en la esquina superior derecha de la página.



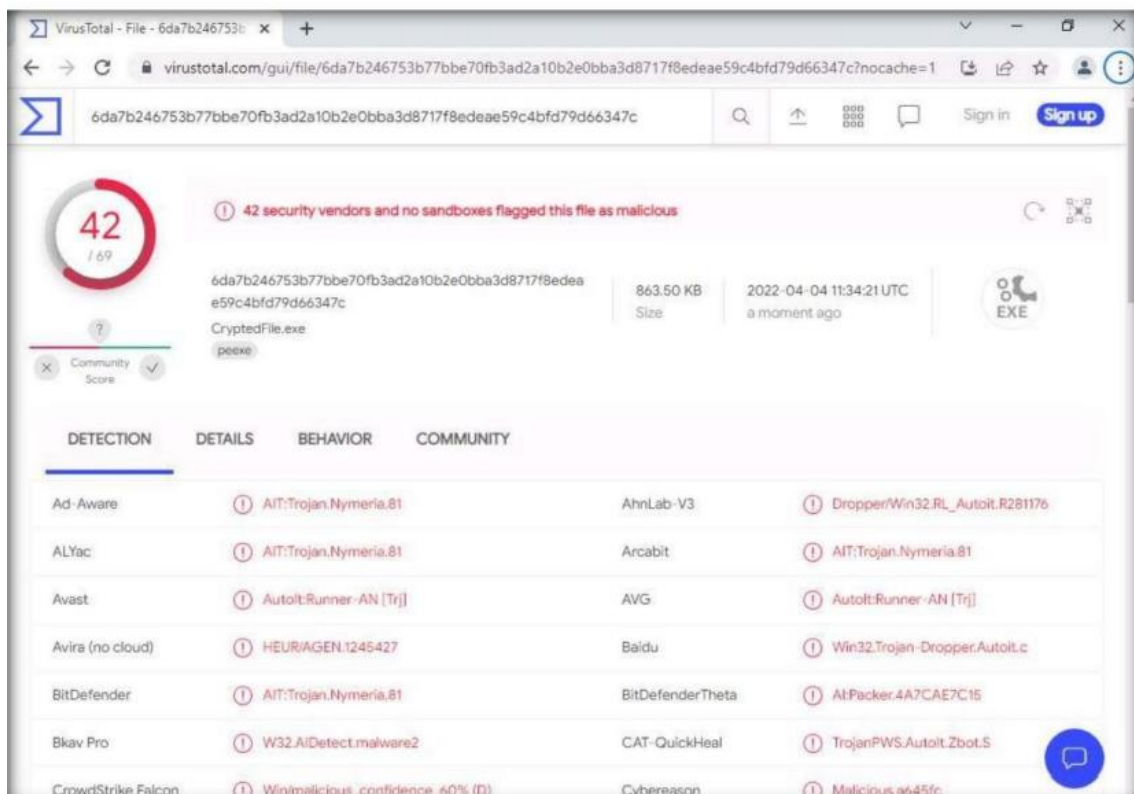
14. Aparecerá un cuadro de diálogo Abrir; vaya a la ubicación donde guardó el archivo cifrado CryptedFile.exe (Escritorio), seleccione el archivo y haga clic en Abrir.

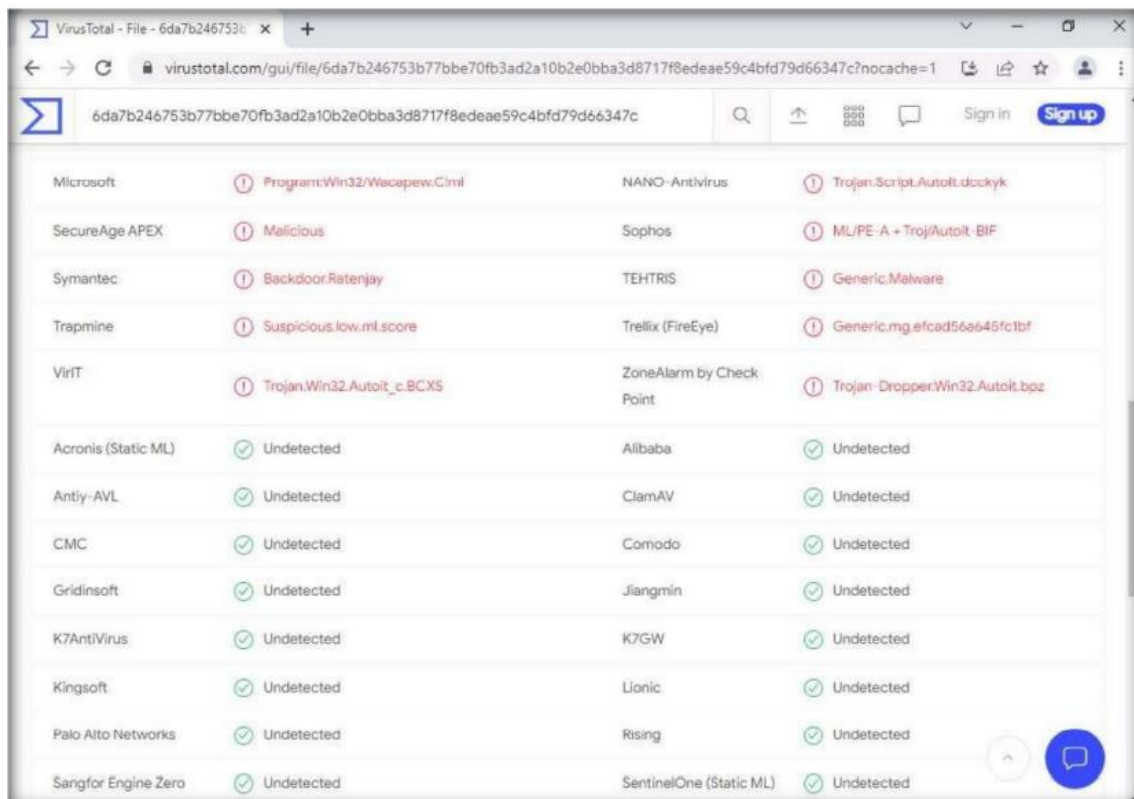


15. Haga clic en Confirmar carga.



16. VirusTotal carga el archivo y comienza a escanearlo con los distintos programas antivirus de su base de datos. Una vez finalizado el análisis, aparece el resultado del análisis, como se muestra en la captura de pantalla.



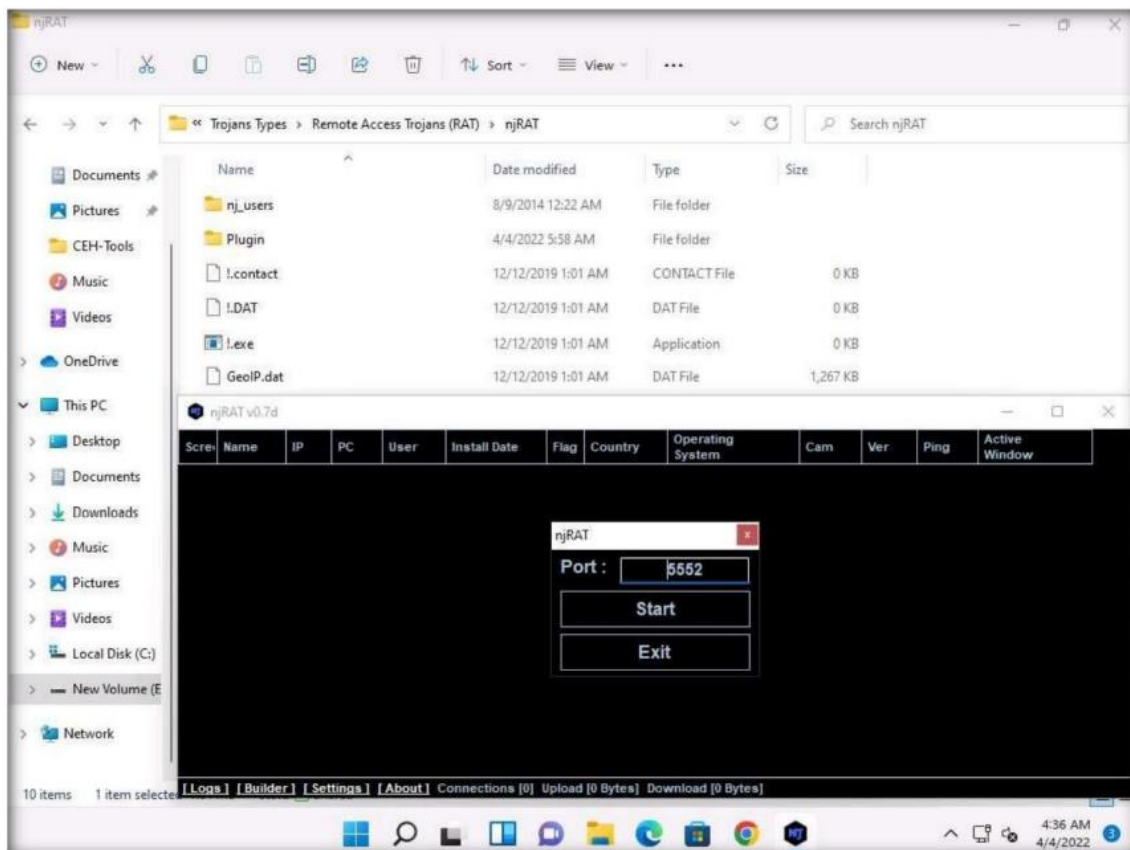


17. Sólo unos pocos programas antivirus han detectado CryptedFile.exe como un archivo malicioso. Minimice o cierre la ventana del navegador.

18. Ahora, probaremos el funcionamiento de un archivo Crypted (CryptedFile.exe).

19. Vaya a C:\Tools\Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT, haga doble clic en el archivo njRAT v0.7d.exe e inicie njRAT eligiendo el número de puerto predeterminado 5552 y, a continuación, haga clic en Iniciar.

20. En este ejercicio, ya hemos creado un archivo cifrado (CryptedFile.exe), construido utilizando njRAT.



21.Utilizar cualquier técnica para enviar CryptedFile.exe al objetivo previsto, a través de correo electrónico o cualquier otra fuente (en tiempo real, los atacantes envían este servidor a la víctima). Nota: En esta tarea, copiamos el archivo CryptedFile.exe a la ubicación de red compartida para compartir el archivo.

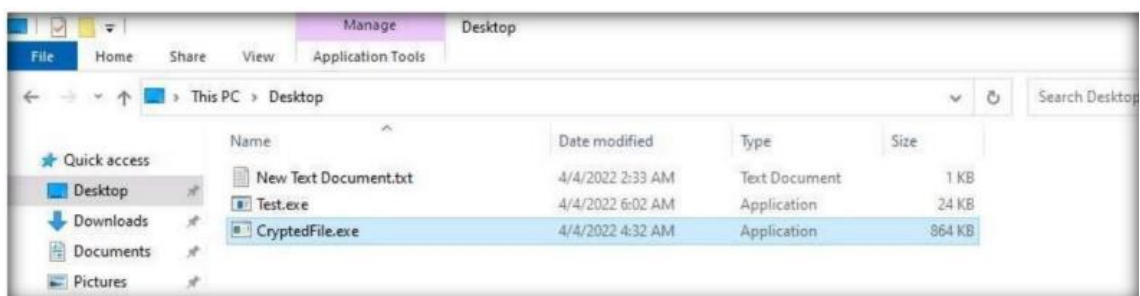
22.Cambie a la máquina virtual Windows 10.

23.Navegue hasta la ubicación de red compartida y, a continuación, Copie y Pegue el archivo ejecutable (CryptedFile.exe), en el que el atacante (aquí, usted) envió el ejecutable del servidor, en el Escritorio de Windows 10.

24.Aquí, estás actuando tanto como el atacante que inicia sesión en la máquina Windows 11 para crear un servidor malicioso y como la víctima que inicia sesión en la máquina Windows 10 y descarga el servidor.

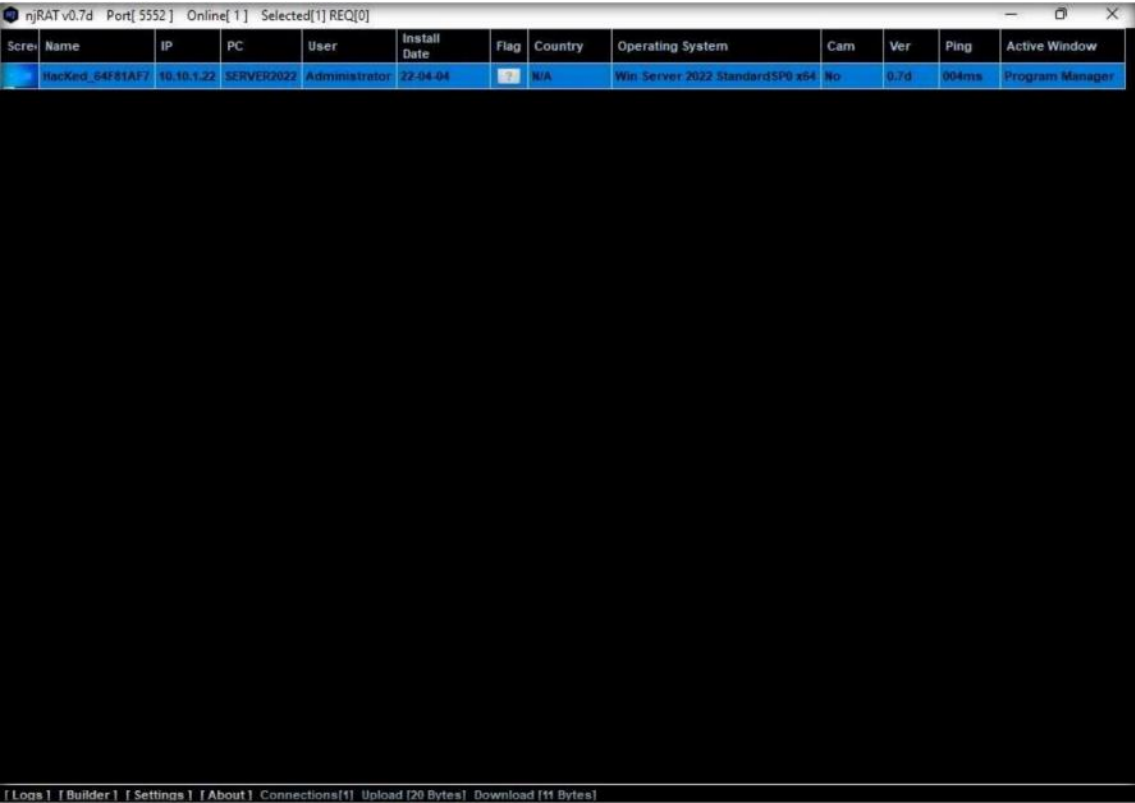
25.Haga doble clic en CryptedFile.exe para ejecutar este ejecutable malicioso.

NOTA: SI DEBE REINICIAR EL EQUIPO PARA DESACTIVAR EL CONTROL DE CUENTAS DE USUARIO, APARECERÁ UN MENSAJE EMERGENTE EN LA ESQUINA INFERIOR DERECHA DE LA VENTANA.



26.Tan pronto como la víctima (aquí, usted) hace doble clic en el servidor, el ejecutable comienza a ejecutarse, y el cliente njRAT (njRAT GUI} que se ejecuta en la máquina Windows 11 establece una conexión persistente con la máquina víctima.

27. Cambie a la máquina virtual Windows 11 y en la ventana njRAT podrá observar que se ha establecido la conexión con la máquina víctima.



28.A menos que el atacante que trabaja en la máquina con Windows 11 desconecte el servidor por su cuenta, la máquina víctima permanecerá bajo su control.

29.De este modo, ha creado un troyano indetectable que puede eludir los programas antivirus y cortafuegos, así como utilizarse para mantener una conexión persistente con la víctima.

30. Una vez finalizado este laboratorio, cambie a la máquina virtual Windows Server 2022, inicie el Administrador de tareas, haga clic en Más detalles y busque el proceso server.exe (32 bits}, y haga clic en Finalizar tarea en la máquina Windows 10.

31. Esto concluye la demostración de cómo ocultar un troyano usando SwayzCryptor para hacerlo indetectable a varios programas antivirus.

TAREA 3: CREAR UN SERVIDOR TROYANO UTILIZANDO EL TROYANO THEEFRAT

Theef es un troyano de acceso remoto escrito en Delphi. Permite a atacantes remotos acceder al sistema a través del puerto 9871. Theef es una aplicación basada en Windows tanto para el cliente como para el servidor. El servidor de Theef es un virus que se instala en un ordenador objetivo, y el cliente de Theef es lo que luego se utiliza para controlar el virus.

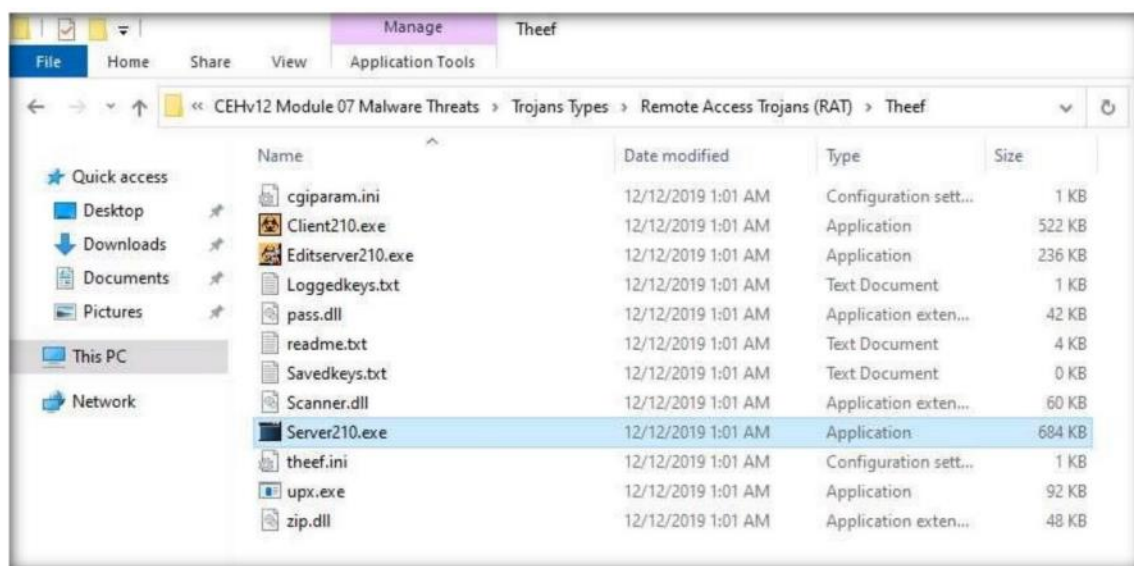
1. Generalmente, un atacante puede enviar un ejecutable de servidor a la máquina víctima e inducir a la víctima a ejecutarlo. En este laboratorio, a efectos de demostración, ejecutaremos directamente el archivo en la máquina víctima, Windows 10.

2. Cambie a la máquina Windows 10.

NOTA: APARECE LA PANTALLA REDES, HAGA CLIC EN SÍ PARA PERMITIR QUE SU PC SEA DETECTABLE POR OTROS PC Y DISPOSITIVOS DE LA RED.

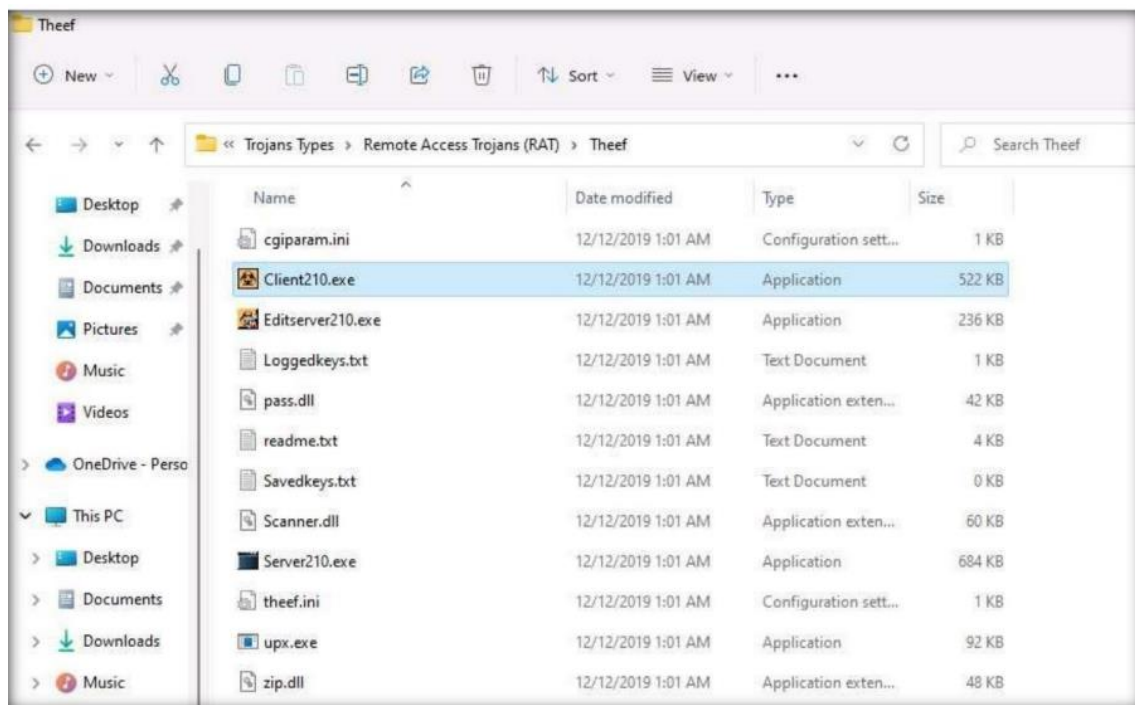
3. Vaya a C:\Tools\Trojans Types\Remote Access Trojans (RAT)\Theef y haga doble clic en Server210.exe para ejecutar el troyano en la máquina víctima.

NOTA: SI APARECE UNA VENTANA EMERGENTE ABRIR ARCHIVO - ADVERTENCIA DE SEGURIDAD, HAGA CLIC EN EJECUTAR.

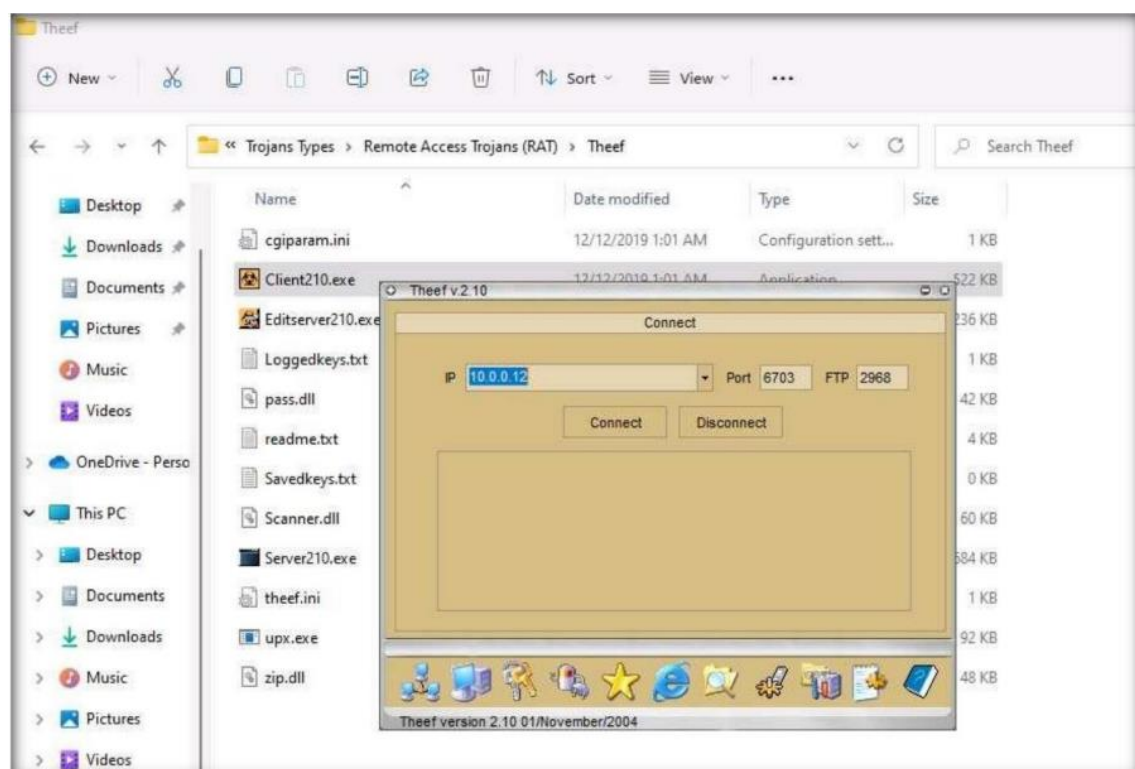


4. Ahora, cambie a la máquina virtual Windows 11 (como atacante).

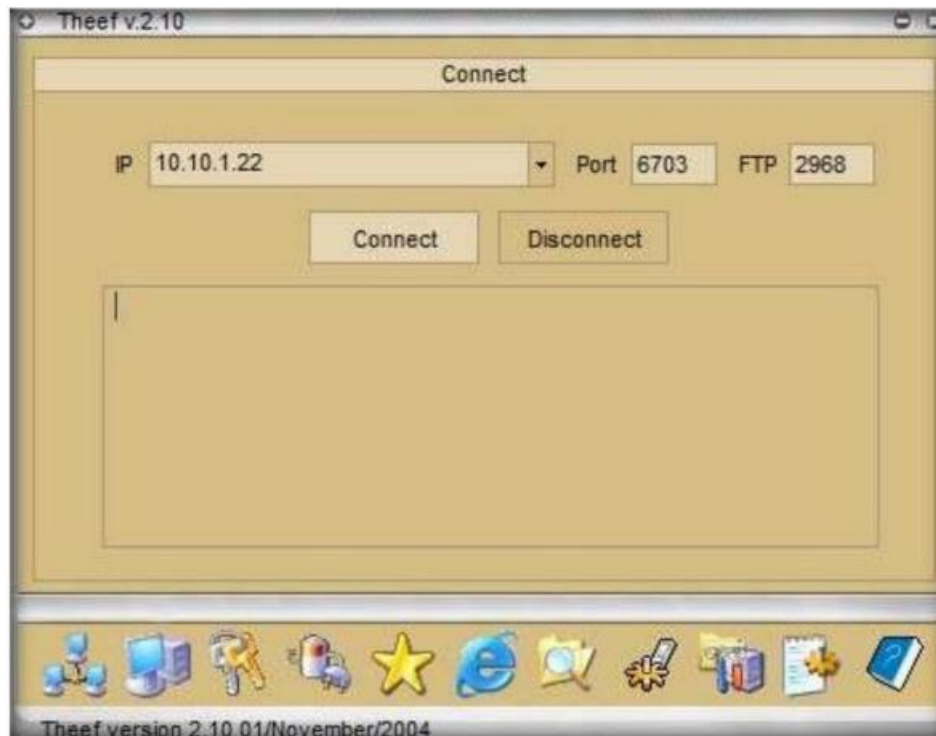
5. Vaya a C:\Tools\Trojans Types\Remote Access Trojans (RAT)\Theef y haga doble clic en Client210.exe para acceder a la máquina víctima de forma remota.



6. Aparece la ventana principal de Theef, como se muestra en la captura de pantalla.



7. Introduzca la dirección IP del equipo de destino (aquí, Windows 10) en el campo IP {10.10.1.22}, y deja los campos Puerto y FTP por defecto; haz clic en Conectar.



8. Ahora, desde Windows 11, has establecido con éxito una conexión remota con la máquina Windows 10.



9. Para ver la información del ordenador, haga clic en el icono Información del ordenador { } en la parte inferior de la ventana.



10. En Información del ordenador, puede ver Detalles del PC, Información del sistema operativo, Inicio y Red haciendo clic en sus respectivos botones.

11. Aquí, por ejemplo, al seleccionar Detalles del PC se muestra información relacionada con el ordenador.



12. Haga clic en el icono Espía () para realizar diversas operaciones en el equipo de destino.

13. Puede realizar varias operaciones como capturar pantallas, registrar claves, ver procesos, ver el administrador de tareas, usar la cámara web y usar el micrófono en la máquina víctima seleccionando sus respectivas opciones.

14. Aquí, por ejemplo, al seleccionar Administrador de tareas se ven las tareas que se están ejecutando en el equipo de destino.



15. En la ventana del Administrador de tareas, haga clic en el icono Actualizar para obtener la lista de procesos en ejecución.




16. Seleccione un proceso (tarea); haga clic en el icono Cerrar ventana (para finalizar la tarea en el equipo de destino).



17. Cierre la ventana del Administrador de tareas. Nota: Las tareas que se ejecutan en el administrador de tareas pueden variar al realizar esta tarea.
18. En el menú Espía, haga clic en Registrador de teclas para registrar las pulsaciones de teclas realizadas en la máquina víctima.



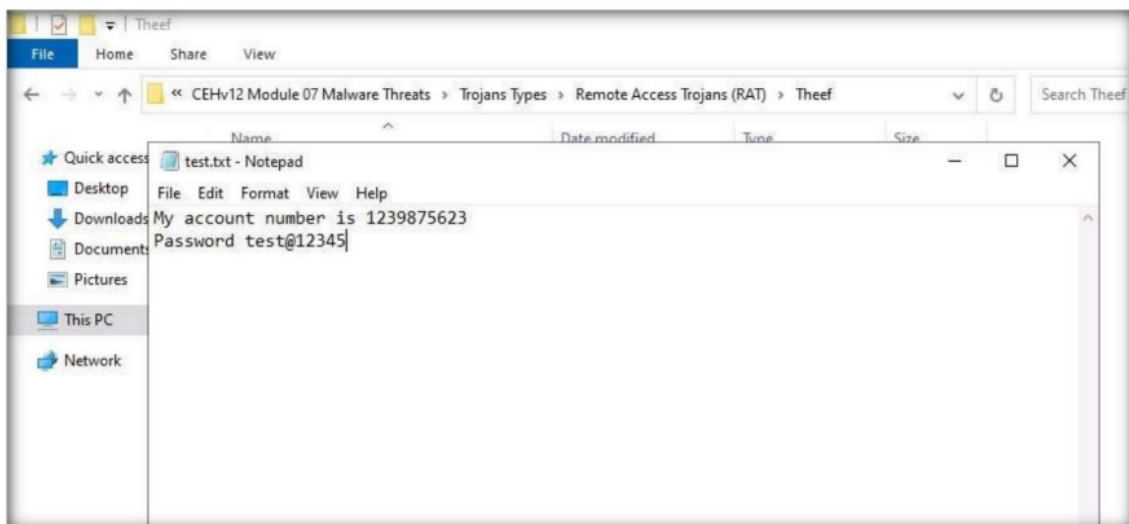
19. Aparecerá la ventana emergente Keylogger; haga clic en el icono Inicio () para leer las pulsaciones de teclado de la máquina víctima.



20. Cambie a la máquina virtual Windows 10.

21. Abra una ventana del navegador y navegue por algunos sitios web o abra un documento de texto y escriba alguna información sensible.

NOTA: AQUÍ, ESTAMOS CREANDO UN ARCHIVO DE BLOC DE NOTAS (TEST.TXT), SIN EMBARGO, USTED PUEDE REALIZAR ALGUNA OTRA ACTIVIDAD.



22. Vuelva a la máquina atacante (Windows 11) para ver las pulsaciones de teclas grabadas de la máquina víctima en la ventana de Theef Keylogger.



23. Cierre la ventana de Theef Keylogger.

24. Del mismo modo, puede acceder a los detalles de la máquina víctima haciendo clic en los distintos iconos.

25. Cierre todas las ventanas abiertas en los equipos Windows 11 y Windows 10.

26. Apague las máquinas virtuales Windows 11 y Windows 10.