# Remcos RAT

CYBERZAINTZA-MALWARE-REMCOS

**TLP: CLEAR**

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

## TABLA DE CONTENIDO

## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## 1. Resumen ejecutivo

El RAT Remcos ha emergido como una herramienta de ciberespionaje y cibercrimen versátil y peligrosa, destacando su capacidad para control remoto, captura de datos sensibles y despliegue de cargas adicionales. Su distribución a través de técnicas sofisticadas de phishing, páginas web comprometidas y explotación de vulnerabilidades refleja su adaptabilidad y capacidad de infección.

Se ha observado su uso en diversas campañas globales, como, por ejemplo, contra organizaciones ucranianas a través de correos electrónicos (phishing) en febrero de 2023 o contra empresas europeas de diferentes sectores a través de ficheros adjuntos infectados que descargan el malware Remcos.

Además, debido al fácil acceso a este software, se ha podido observar que el RAT Remcos ha afectado a varios países alrededor del mundo. Entre ellos, se han identificado ataques específicos en Europa y Estados Unidos, y a sectores tan diversos como instituciones financieras, gobiernos, medios de comunicación, … Estos ataques globales reflejan la amplia distribución y el uso versátil de Remcos en diferentes tipos de campañas maliciosas.

Por último, indicar que la capacidad de robo de información confidencial de Remcos RAT puede llevar al uso ilegitimo de estos datos sensibles, produciendo posibles chantajes o el uso de los datos de la organización para su utilización en otros ataques sofisticados a gran escala. Pudiendo provocar un daño irreparable a las organizaciones afectadas por este malware.

## 2. Análisis técnico

### Introducción

Remcos (acrónimo de Remote Control & Surveillance Software) es un software de vigilancia y herramienta comercial de acceso remoto (RAT) desarrollado por la empresa de ciberseguridad Breaking Security asentada en Roma (Italia). Dicha empresa vende y distribuye este sofware como una herramienta legítima en su sitio web (https://breakingsecurity.net/remcos/) a través de un modelo freemium con una versión pro a un precio aproximado entre 79 € y 1295 €, dependiendo del tiempo de suscripción y licenciamiento. Además, se permite el pago a través de pasarelas de pago y criptomonedas.

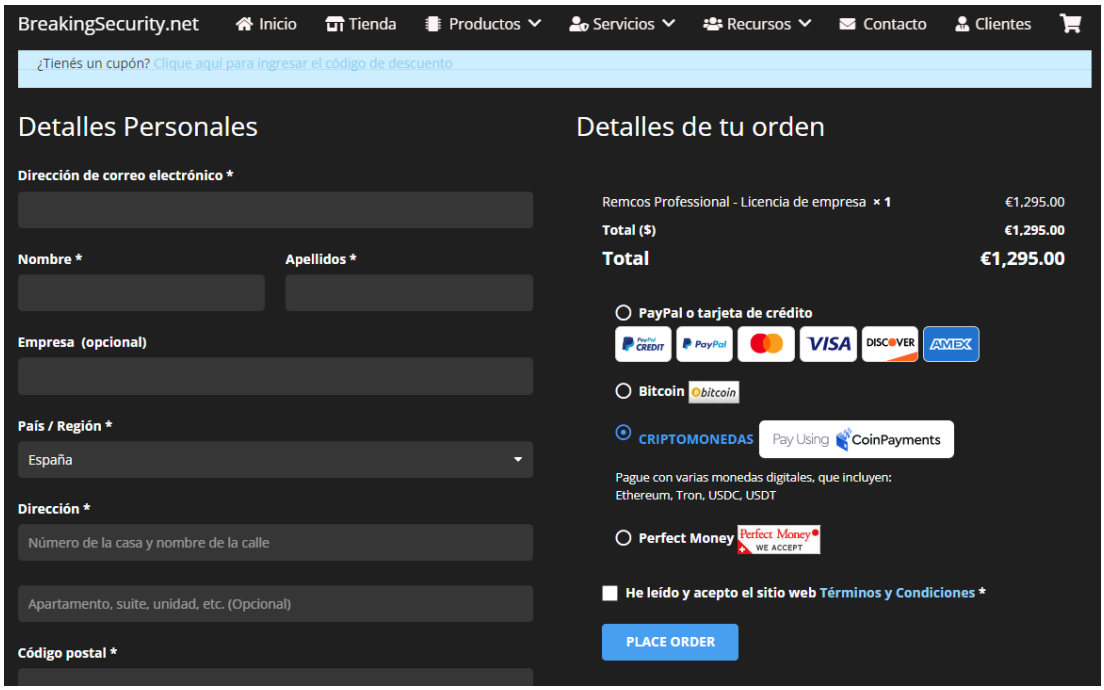



Ilustración 1: Pagina de pago del malware Remcos

Remcos es un software completamente nativo, desarrollado para versiones de Windows, desde Windows XP hasta Windows 11, tanto para plataformas de 32 como de 64 bits. Y permite obtener de forma remota el control total de otro equipo informático.

Esta aplicación está desarrollada utilizando dos lenguajes de programación: C++ para el Agente y Delphi para el Controlador. A pesar de ofrecer acceso a una amplia gama de funciones, el Agente de Remcos, mantiene un tamaño reducido, aproximadamente 482 kb.

Su arquitectura está basada en un modelo agente – controlador:

- Controlador: Permite la administración y control de los sistemas remotos infectados a través de las funcionalidades y características desplegados en cada agente. Y la obtención de toda la información detallada del equipo infectado y la actividad que está realizando.

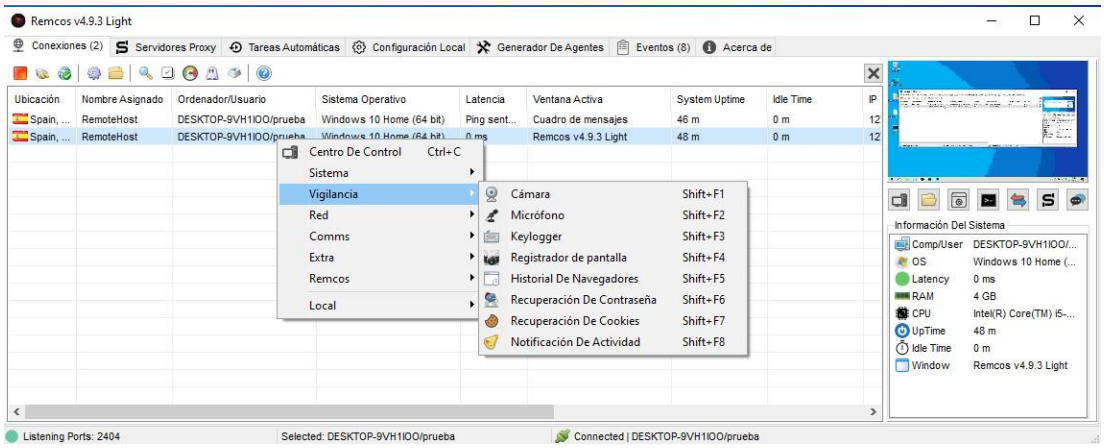



Ilustración 2: Pantalla del controlador del malware Remcos

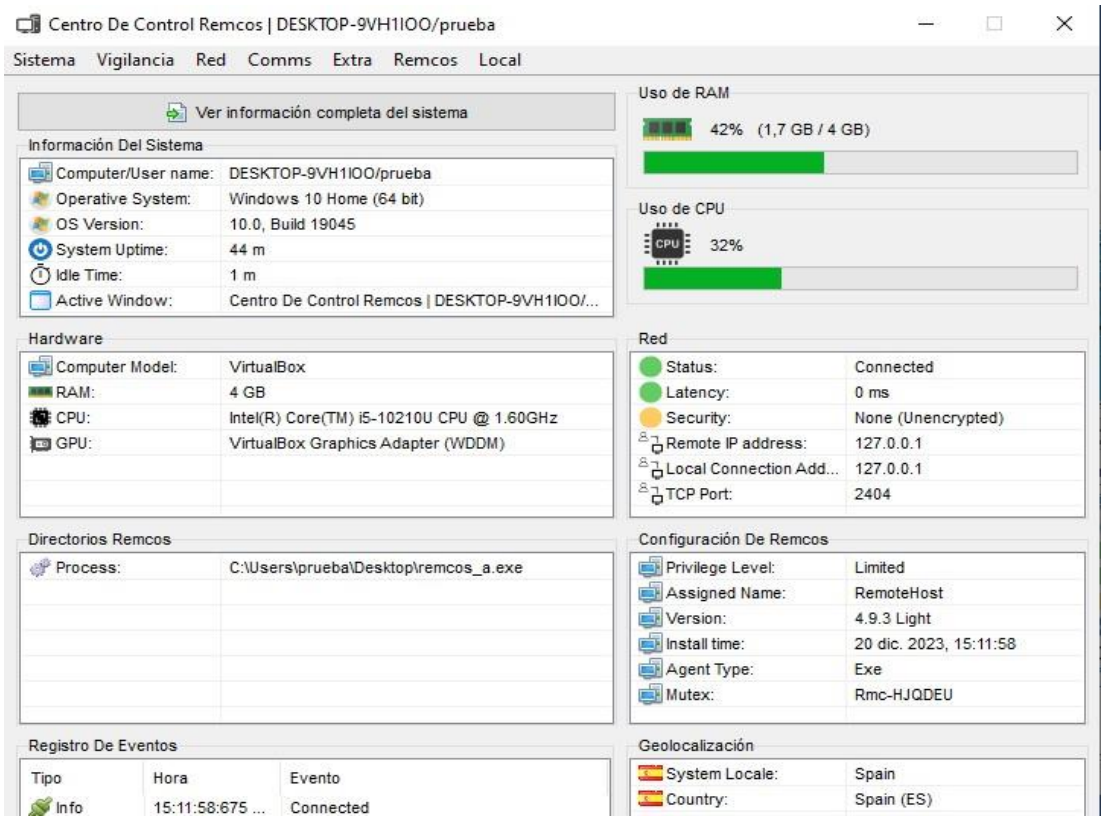



Ilustración 3: Centro de control de un agente

- Agente: Instalados en cada equipo infectado remoto, con la capacidad de ocultamiento en los sistemas, permite la recolección y envío de la información robada, así como la ejecución de los comandos recibidos desde el controlador. Los agentes son creados desde el controlador con las características, funcionalidades y configuraciones de comunicación definidas por el atacante. Además, Remcos RAT permite la creación de perfiles con configuraciones predefinidas para usarlas en compilaciones de agentes posteriores.

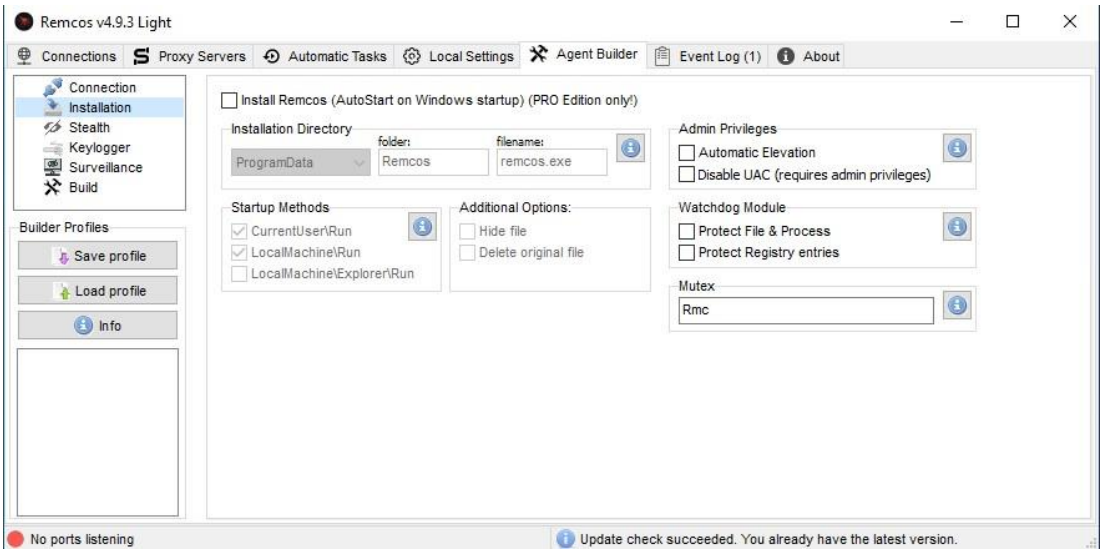



Ilustración 4: Configuración de un agente de Remcos

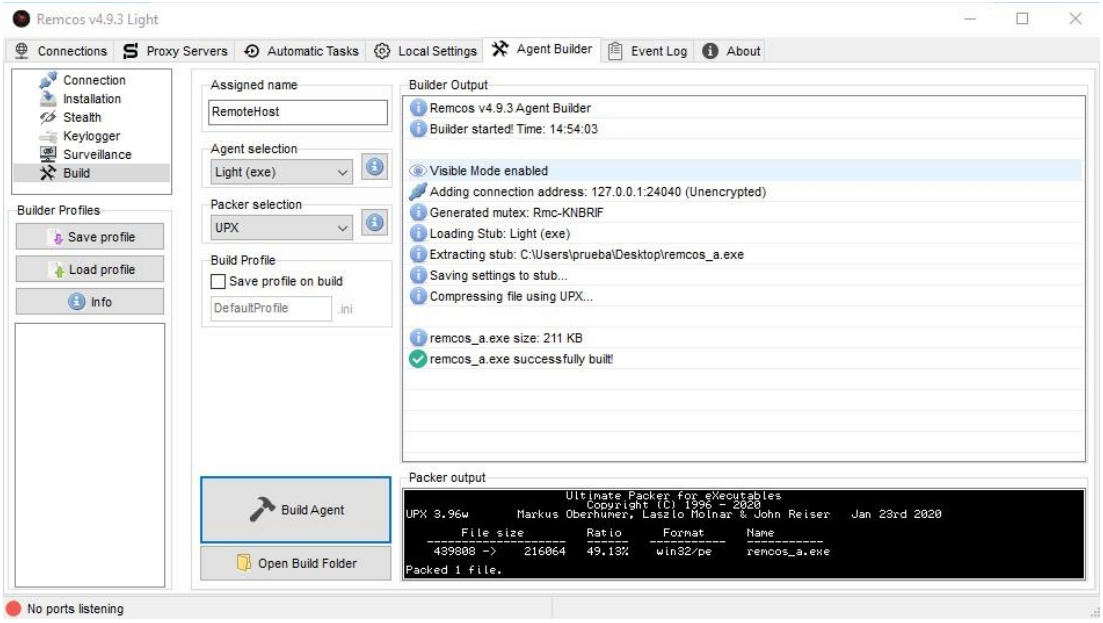



Ilustración 5: Creación del agente instalable de Remcos

Si el agente del sistema infectado está compilado en modo visible se podrá visualizar y verificar que la conexión ha sido establecida con el controlador, como, por ejemplo

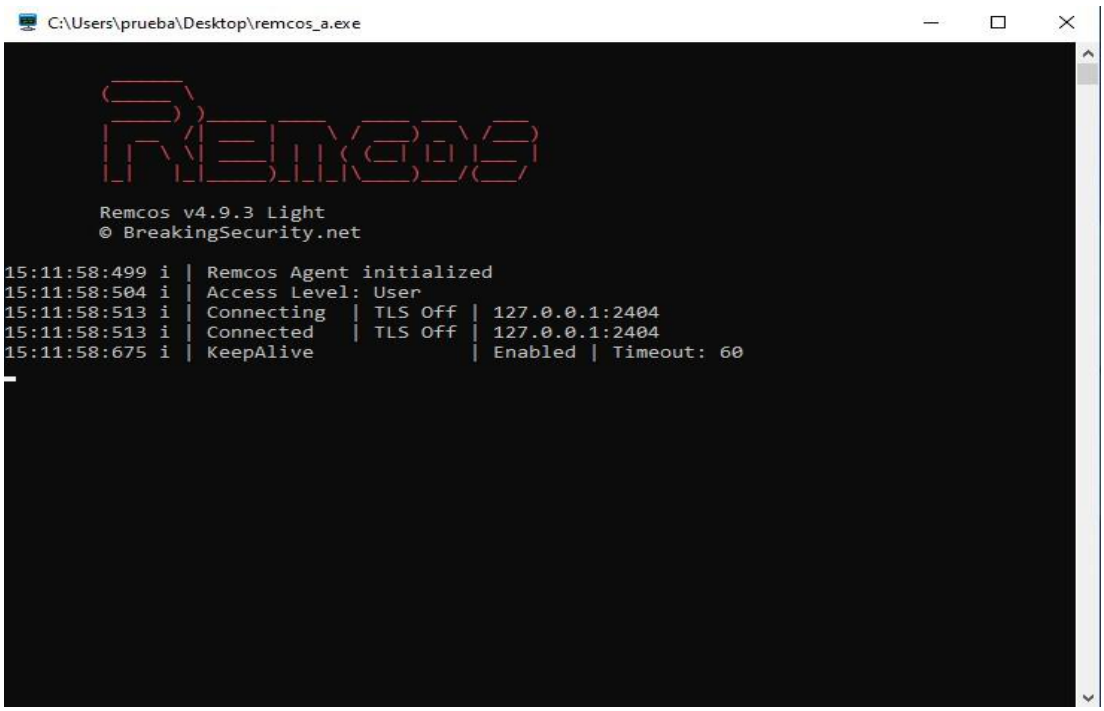



Ilustración 6: Agente desplegado en la maquina victima

En cuanto a las comunicaciones entre el agente y el controlador, Remcos utiliza una conexión TCP cifrada TLS v1.3, utilizando cifrado AES-128 y sin servidores intermedios, lo que proporciona las siguientes funcionalidades:

1. Conexión cifrada: Los datos transmitidos entre el Controlador y el Agente son cifrados con un algoritmo AES-128, lo que evita ataques de tipo man in the middle o interceptación de los datos a través de sniffing.
2. Autenticación mutua de las comunicaciones mediante certificados TLS: Tanto el controlador Remcos como el agente se autentican entre sí, permitiendo al controlador asegurarse de que la conexión llega desde un Agente previamente registrado y al agente le permite asegurarse de que esté conectado con el controlador correcto.
3. Protección del controlador frente a accesos no autorizados: El uso del controlador puede estar protegido por contraseña para evitar que un usuario no autorizado se haga con el control del controlador y los agentes.

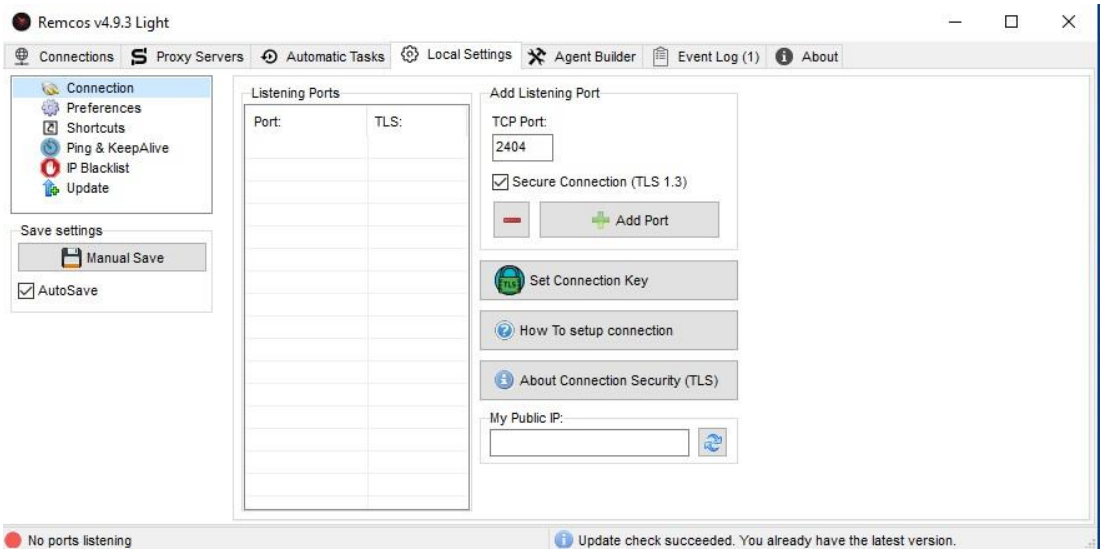



Ilustración 7: Configuración de la configuración

Remcos permite obtener las siguientes capacidades y funcionalidades en el equipo remoto con el objetivo de ocultarse, obtener información y ejecutar diferentes acciones:

- Obtener capturas de pantalla remotas: permite ver y controlar las pantallas remotamente.

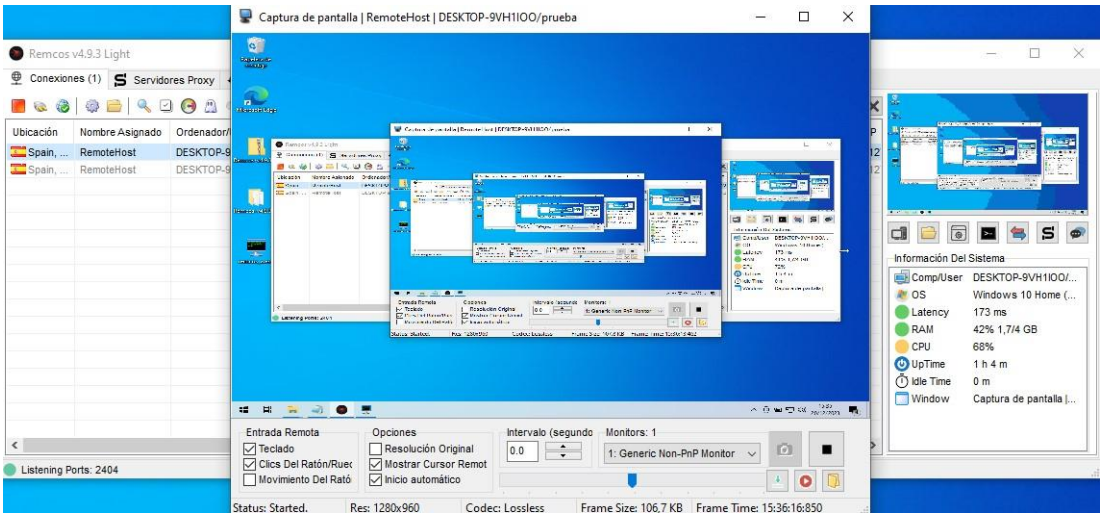



Ilustración 8: Captura de pantalla remota

- Administrar remotamente procesos y archivos.

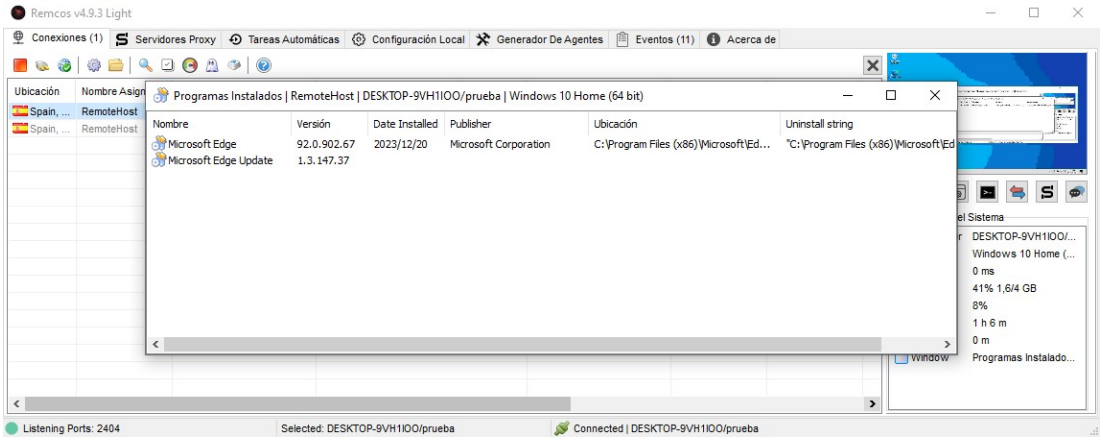



Ilustración 9: Captura de programas instalados

- Editar el registro del equipo remoto.

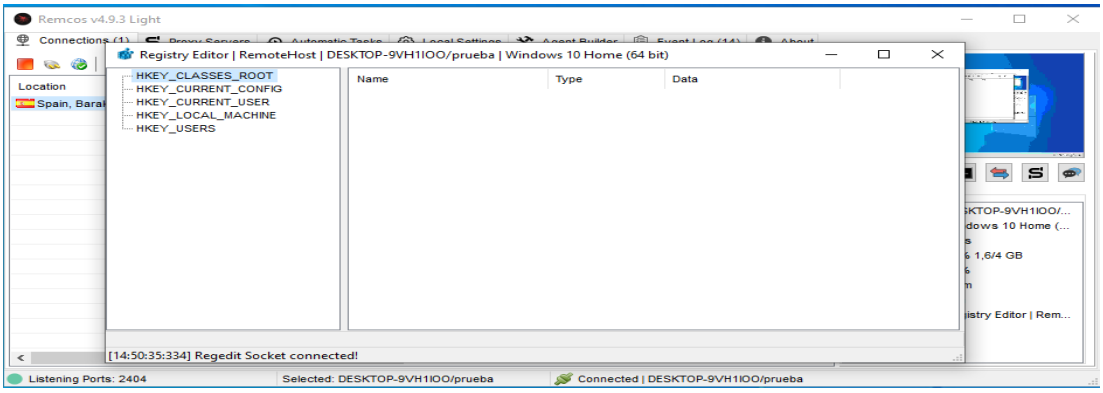



Ilustración 10: Edición remota del registro

- Ejecutar la línea de comando de forma remota: Abre una Shell en el sistema infectado, permitiéndole usar su línea de comando de forma remota.

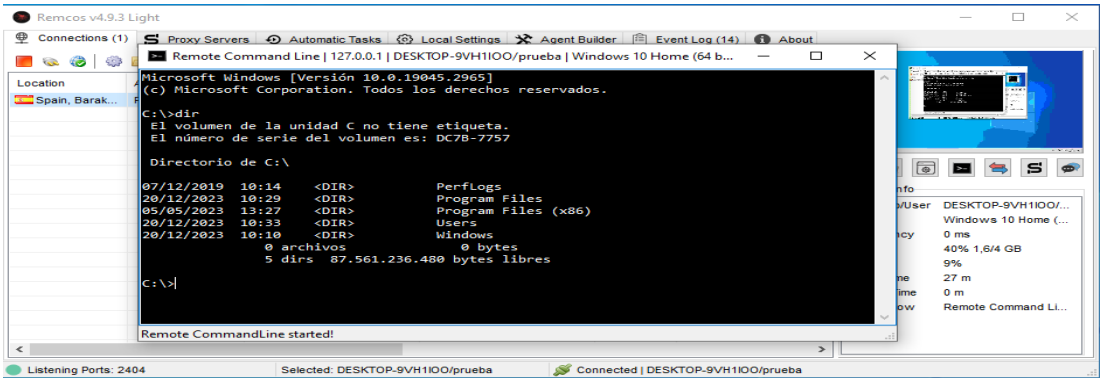



Ilustración 11: Ejecución remota de la línea de comandos

- Registrar las teclas pulsadas y acceder al portapapeles.
- Capturar audio e imágenes a través de la webcam del equipo infectado.

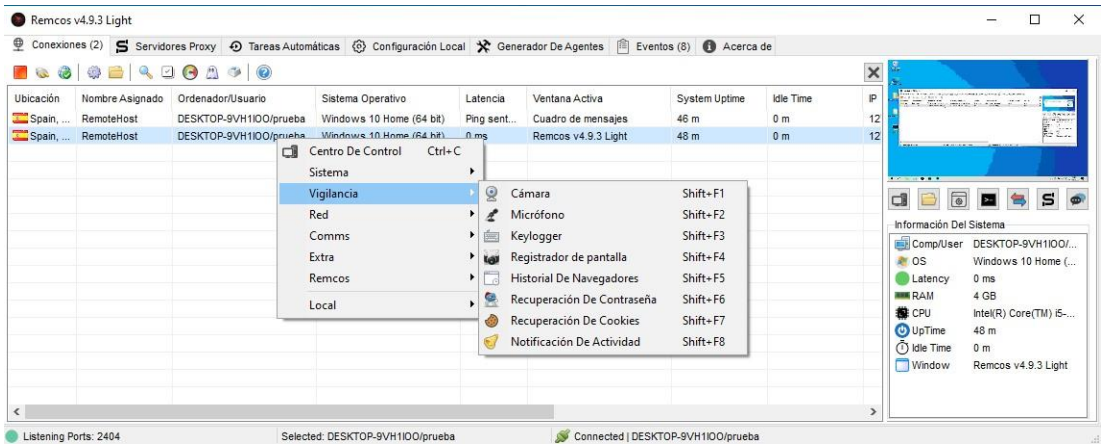



Ilustración 12: Opciones para la vigilancia del sistema remoto

- Extraer contraseñas de los navegadores instalados en el equipo remoto.
- Redireccionar peticiones DNS a una dirección IP controlada por el atacante.

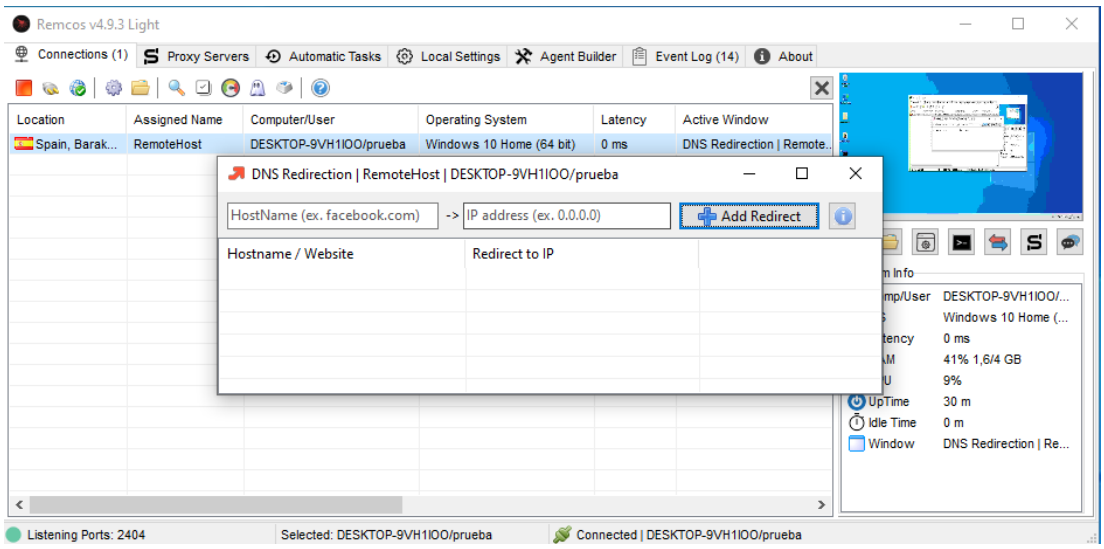



Ilustración 13: Configuración del redireccionamiento DNS

- Enviar chats y mensajes, proporcionando un canal de comunicación con la maquina remota.

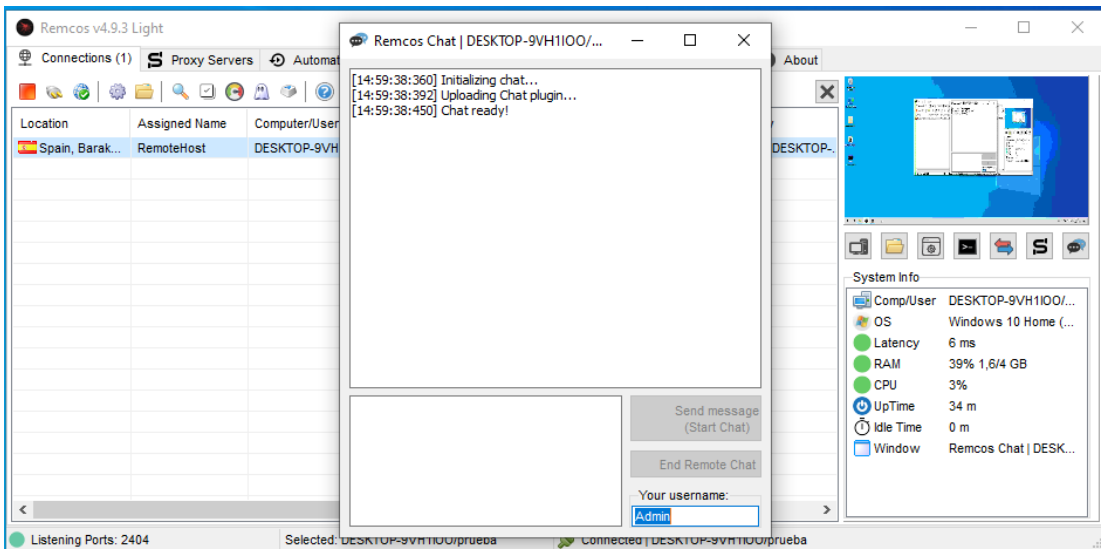



Ilustración 14: Creación de un canal de chat con la maquina remota

- Ejecutar scripts remotamente (VBScript, JavaScript, Batch)

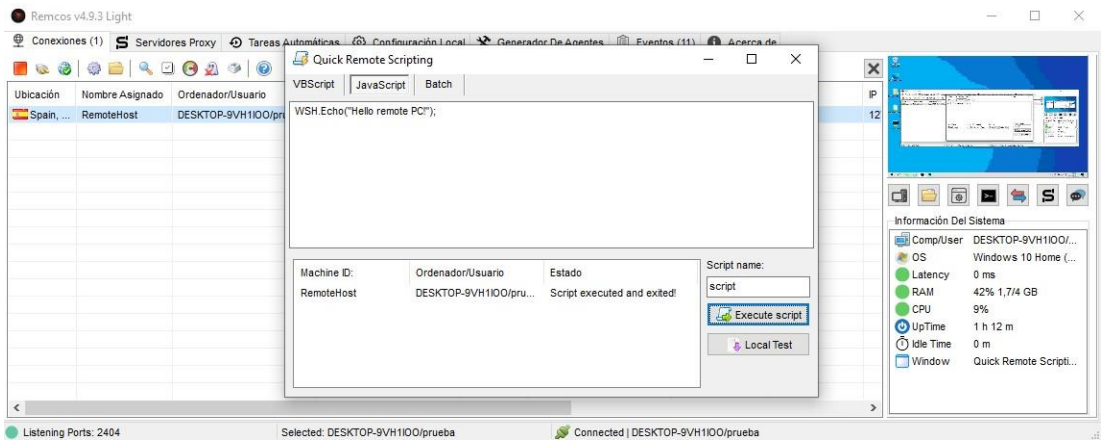



Ilustración 15: Consola de ejecución de scripts

- Descargar ficheros remotos o locales

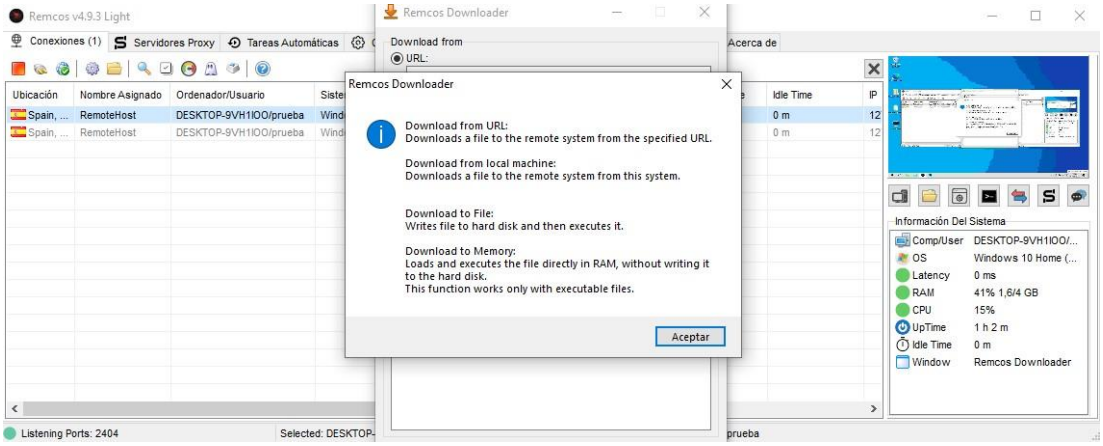



Ilustración 16: Descarga de ficheros remotos

- Cargar DLLs en el sistema remoto

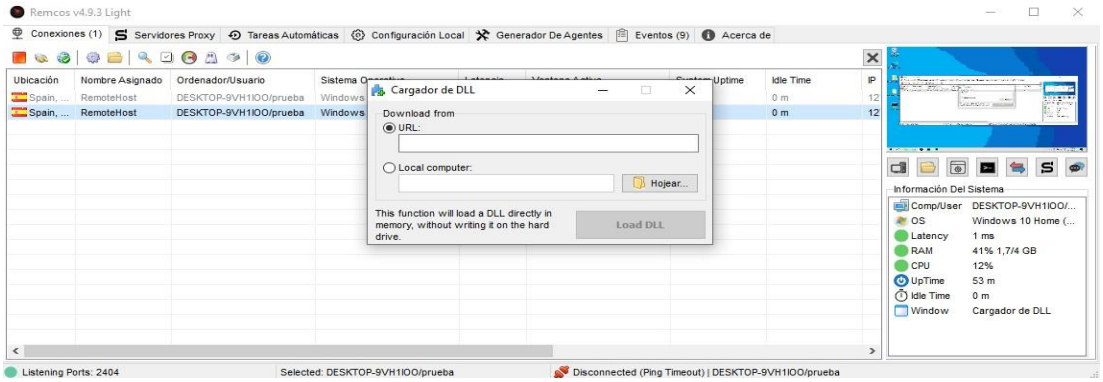



Ilustración 17: Consola de ejecución de DLLS en el equipo remoto

- Obtener privilegios de administrador y deshabilitar UAC (Control de cuentas de usuario)

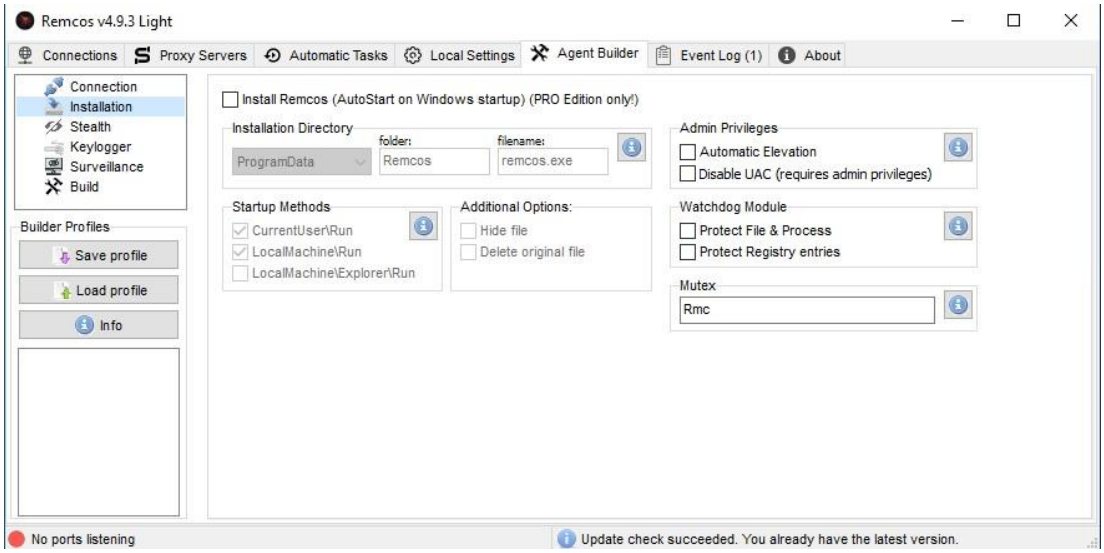



Ilustración 18: Configuración de administración de privilegios

- Crear y mantener la persistencia en la máquina de destino
- Borrar el fichero original una vez instalado Remcos RAT
- Ejecutarse como un proceso legítimo (por ejemplo, inyección en un proceso de Windows)

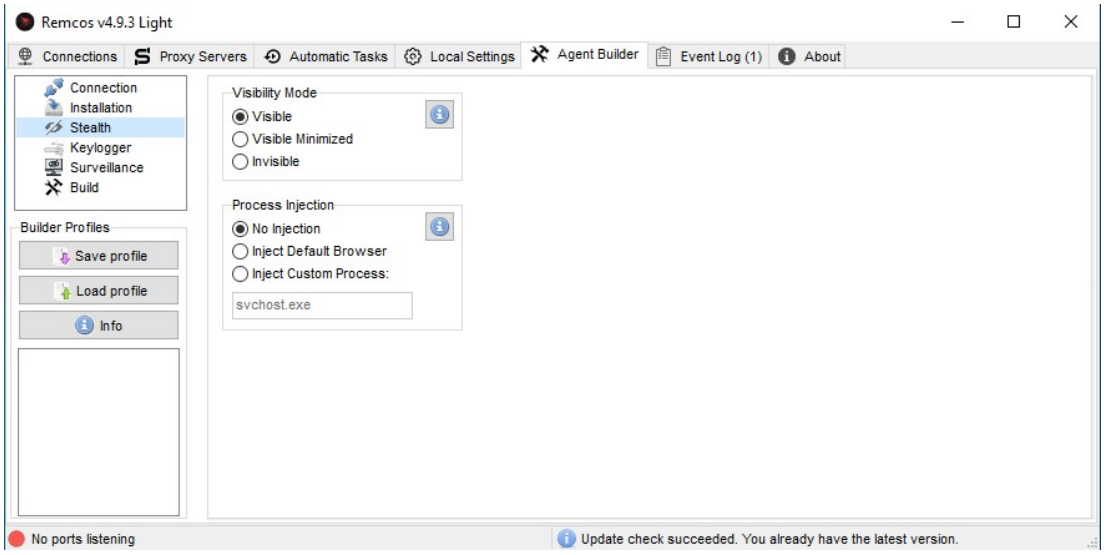



Ilustración 19: Configuración para evadir detecciones en el equipo remoto

- Ejecutarse en segundo plano sin mostrar su actividad al usuario.
- Limpiar logs o registros del sistema: Cada vez que se inicia el agente de Remcos, se eliminarán todas las contraseñas e inicios de sesión almacenados en el navegador.

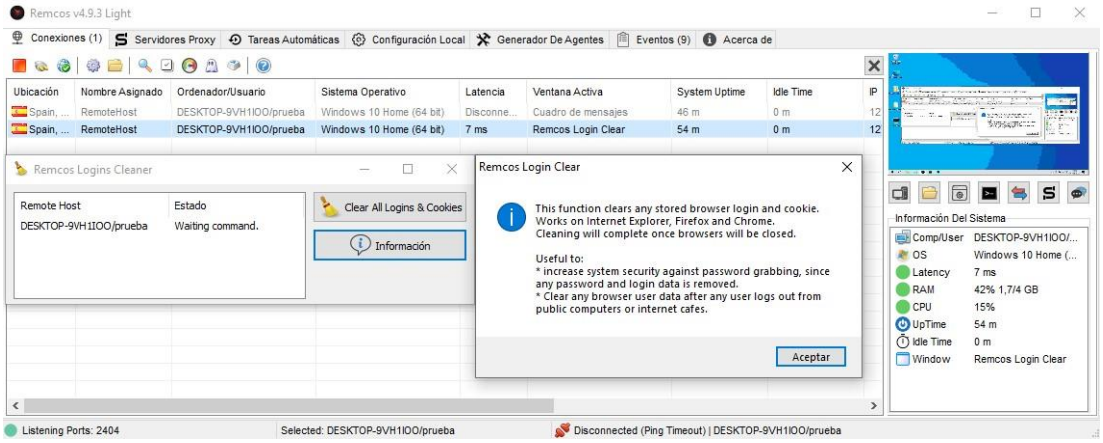



Ilustración 20: Consola para la limpieza de los registros del sistema remoto

- Apagar el equipo remoto o descargar nuevas funcionalidades y actualizaciones para ampliar sus capacidades.

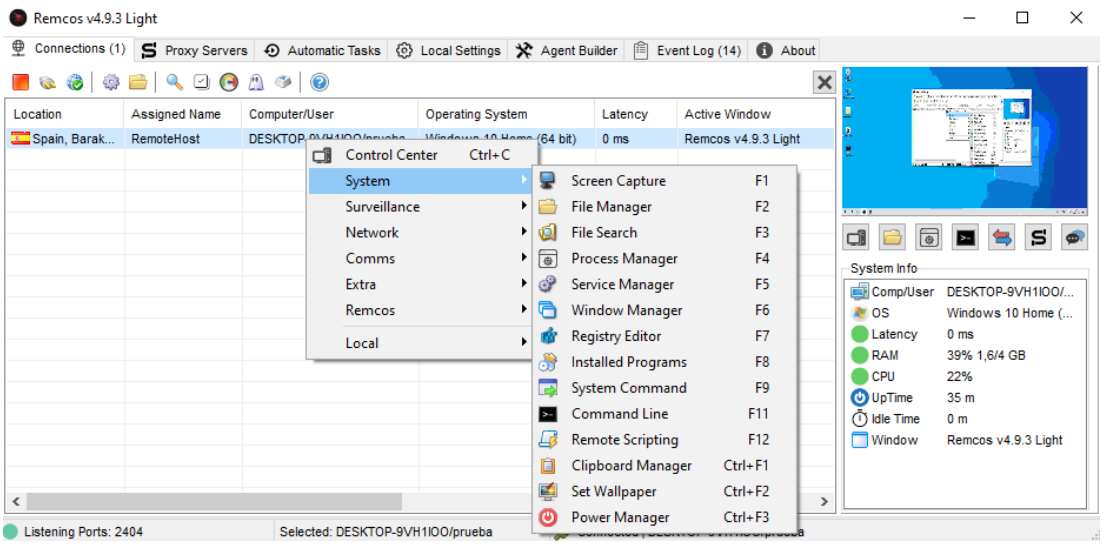



Ilustración 20: Consola para la limpieza de los registros del sistema remoto

## Analisis de Breaking Security

Si bien la empresa Breaking Security, creadora del RAT Remcos, asegura que la venta de su software es exclusivamente para usos legítimos y que revocará las licencias de los usuarios que no sigan su EULA (https://breakingsecurity.net/es/terms/), desde finales de 2016 se ha detectado la presencia de dicho software en foros de hacking y se ha utilizado en campañas de ciberataques brindando a los atacantes la capacidad para tomar el control de un equipo remoto, vigilar la actividad de la víctima y robar cualquier información confidencial que esté disponible en él. Todo ello sin

invertir recursos en desarrollar una herramienta propia con las mismas capacidades.

Además, mencionar que Breaking Security también ofrece otros softwares que pueden ser usados por atacantes para llevar a cabo ataques o ser utilizados conjuntamente con Remcos para aumentar sus capacidades de infección, evasión de medidas de seguridad o capacidad de vigilancia. Ejemplos de estos softwares son:

- Viotto keylogger: keylogger para sistemas Windows con capacidad para registrar y enviar las pulsaciones de teclas, tomar capturas de pantalla, capturar la información del portapapeles, registrar las aplicaciones abiertas, …
- Poseidon Mailer: SMTP Mailer que permite la generación de campañas de correo y el envío masivo de emails.
- Viotto Binder: Instalador de software desarrollado en VB6.
- …

Analizando la página web de Breaking Security se puede ver que no muestra información sobre la empresa o autores del software. Analizando el dominio “breakingsecurity.net” se ha podido observar que está registrado en la empresa registrante canadiense Tucows y la información sobre el contacto técnico o administrativo es privado. El dominio resuelve a la dirección IP “192.124.249.19” perteneciente a la empresa sucuri security encargada de proporcionar una capa de seguridad a la web y dificultando el análisis de la autoría del código de Remcos y de la empresa Breaking Security.

Analizando los cambios producidos en la web durante los últimos años (2012-2023) se ha podido observar que durante el año 2012 el autor apodado “Viotto” publicó un texto autobiográfico donde describía su afición por el malware y sus primeros pasos.

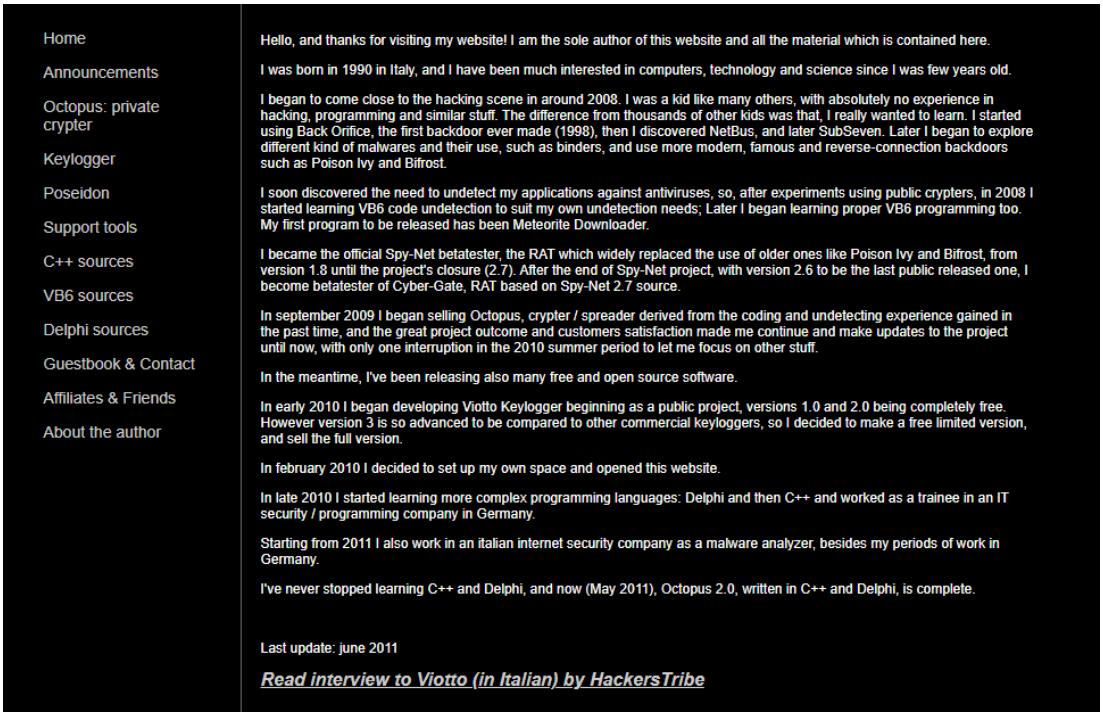



Ilustración 21: Autobiografía del autor de Remcos RAT

Además, se puede observar el grupo de foros de hacking y páginas web en el que el autor participaba:

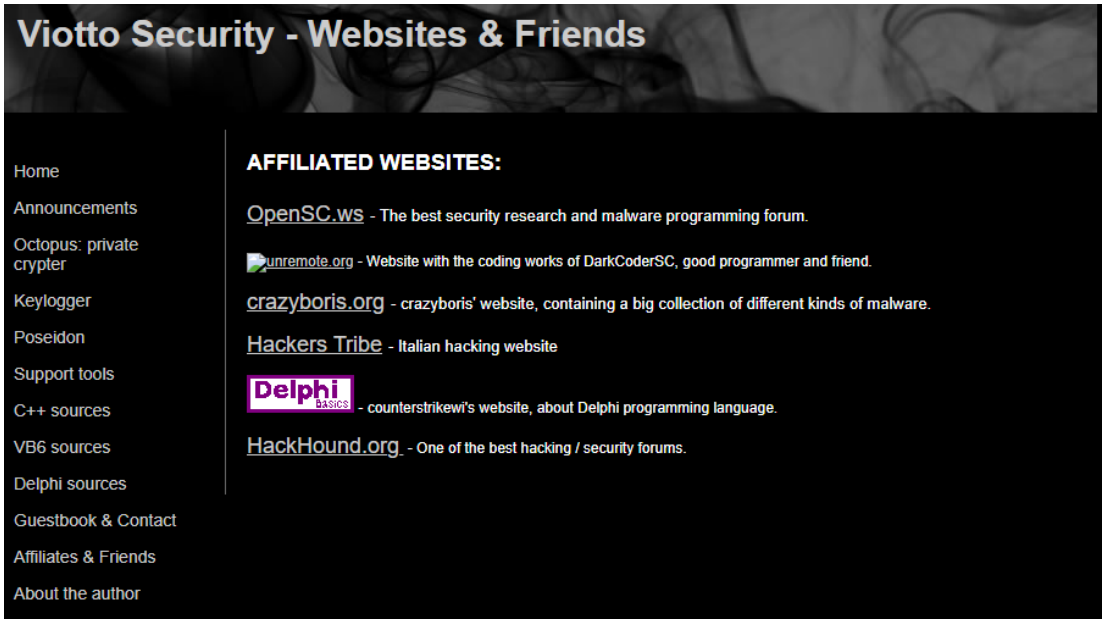



Ilustración 22: Websites afiliadas

Asociado a dicho usuario y pagina web se ha podido encontrar otros nombres de dominios que ya no están activos o que actualmente redirigen a la página web principal https://breakingsecurity.net/, como son:

- Breaking-security.net
- Viotto-security.net

Además, se han encontrado diferentes correos electrónicos de contacto o soporte en la página web a lo largo de los últimos años:

- viotto24@hotmail.it
- admin@breakingsecurity.net
- abuse@breakingsecurity.net

Por último, se ha podido identificar que en junio del año 2020 la empresa Breaking Security tenía un identificador VAT asociado (DE308884780) que actualmente ya no está registrado.

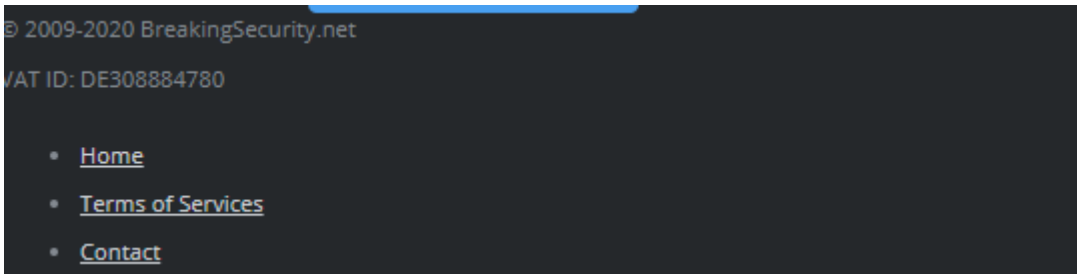



Ilustración 23: Numero de VAT

## Flujo de infección

Por la información obtenida a través de fuentes públicas y debido a su fácil descarga y ejecución, el malware Remcos RAT se puede propagar a través de múltiples formas de infección o conjuntamente con otros malwares. Pero de manera más generalizada la vía de entrada para la infección se produce a través de correos electrónicos de Phishing. Utilizando documentos adjuntos maliciosos, a menudo con temáticas de negocios, para engañar a los usuarios a que ejecuten el documento ofimático. Una vez ejecutado el documento ofimático infectado se descarga un powershell que descarga el malware Remcos y lo instala en la maquina remota victima para tomar control de ella.

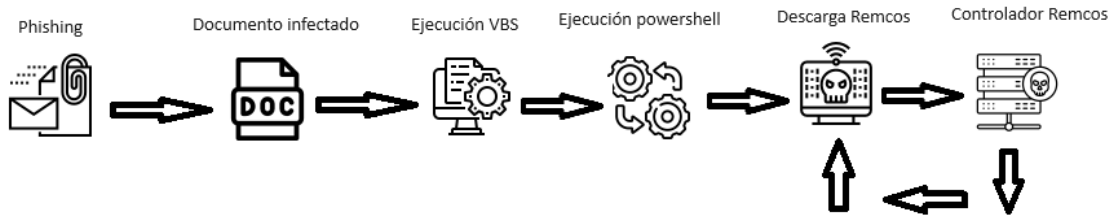



Ilustración 24: Flujo de infección

## Análisis técnico

La muestra analizada corresponde con malware Remcos RAT. Se trata de un fichero ejecutable (application/x-dosexec) para la plataforma Windows, cuya firma SHA256 es la siguiente:

6c040340e398600d3f192f83b9cdb219171108c5d7d8ca14813fa48d326d1a8b

El binario está desarrollado en C++ y se detecta a través de entropía un posible packer en las secciones text y sdata.

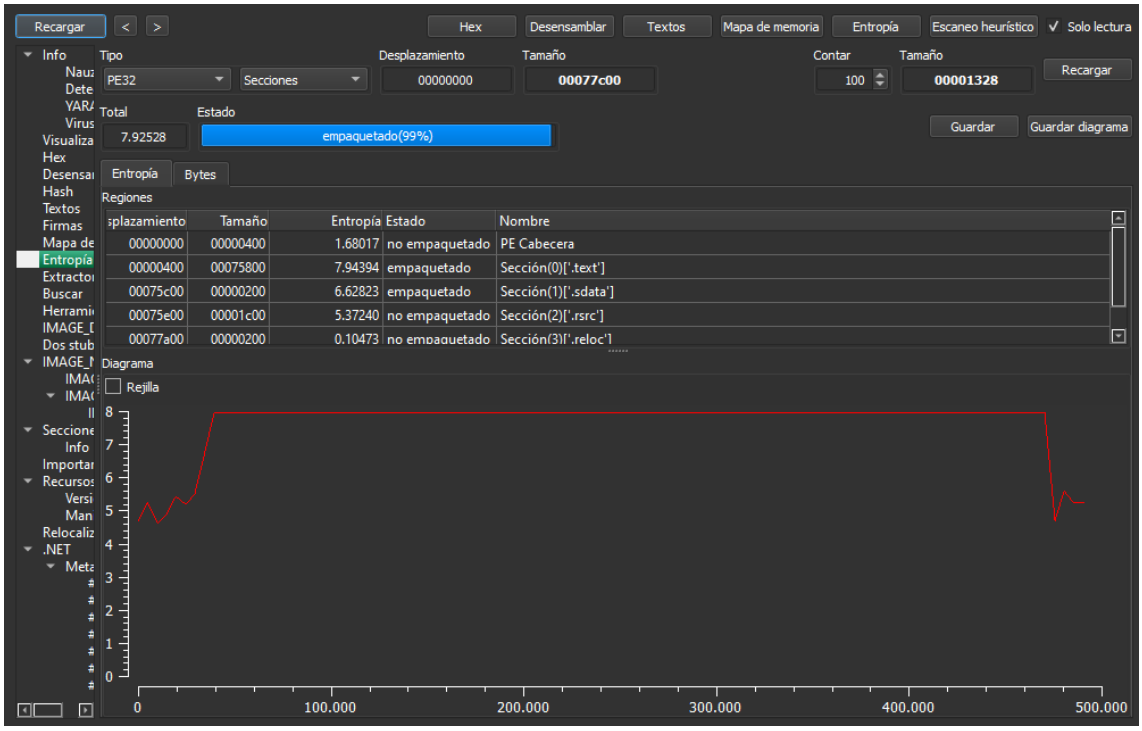



Ilustración 25: Entropía del binario

Identificando por firmas como posibles protectores “Crypto Obfuscator for .NET” o “.NET Reactor”.

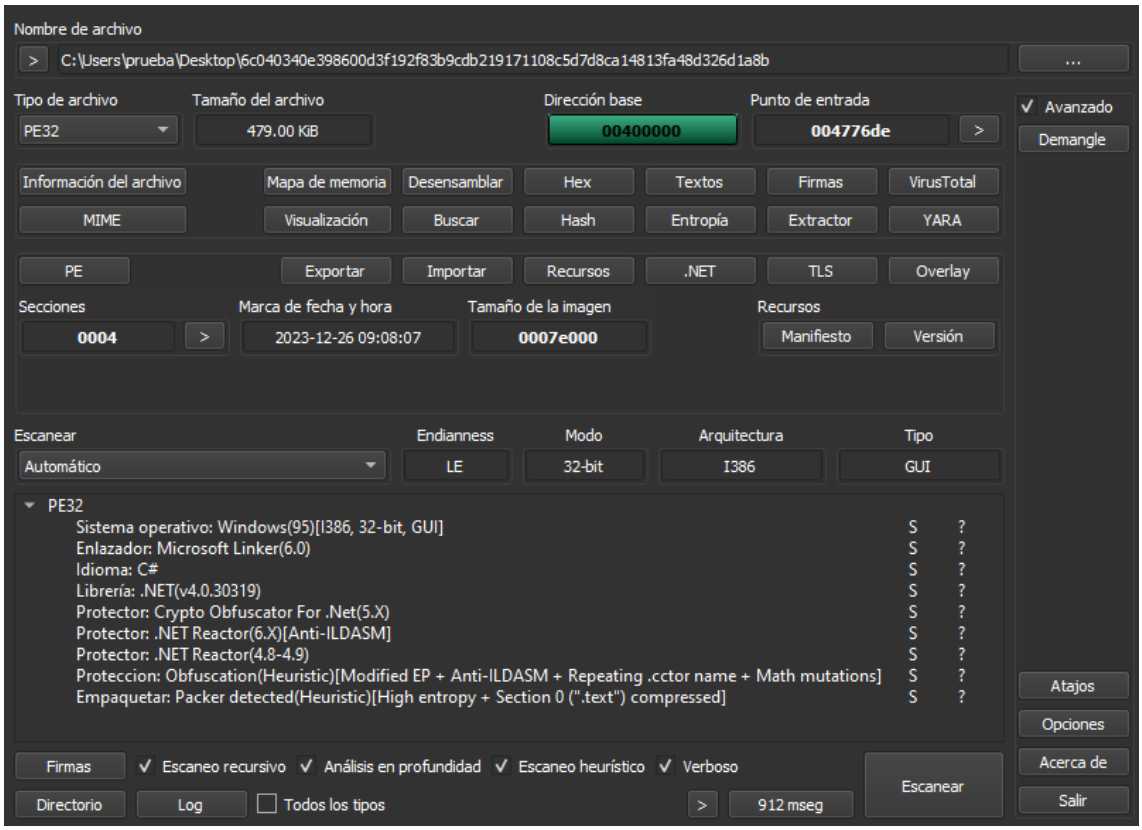



Ilustración 26: Detección de packers

Una vez ejecutado el binario dañino en un entorno Windows controlado (sandbox) se ha podido observar que el ejecutable inicial realiza una inyección del RAT Remcos en el proceso legitimo aspnet_compiler.exe.

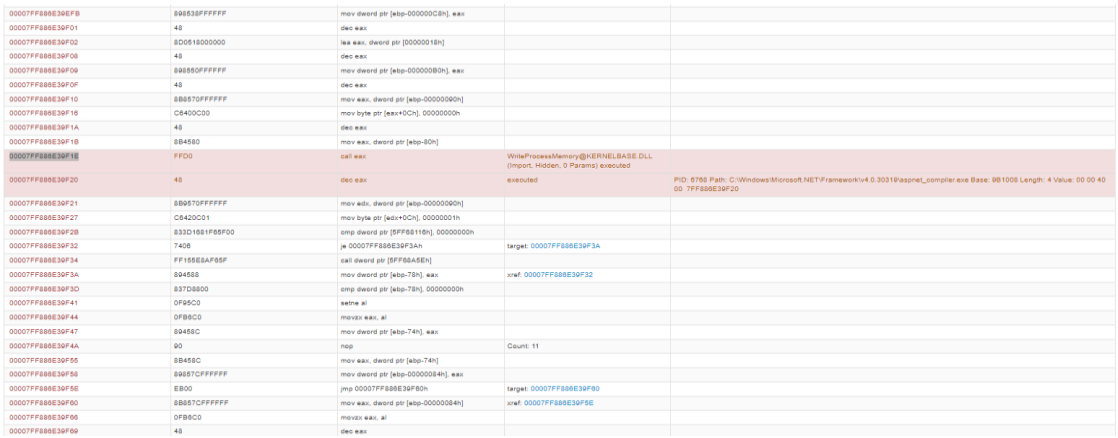


Ilustración 27: Inyección del malware

También podemos observar que Remcos RAT tiene capacidades de evasión medidas de análisis, como por ejemplo el uso de funciones sleep para intentar consumir el tiempo destinado a la ejecución del malware dentro de máquinas de sandbox.

| | | | | |
|---|---|---|---|---|
| 0040F853 | 83C420 | add esp, 20h | | |
| 0040F856 | 68B80B0000 | push 00000BB8h | xref: 0040F7F2 | |
| 0040F85B | FF15F8924500 | call dword ptr [004592F8h] | Sleep@KERNELBASE.DLL (Import, Hidden, 0 Params) executed | |
| 0040F861 | E95CFFFFFF | jmp 0040F7C2h | target: 0040F7C2 executed | Time: -3000 TID: 6012 40F861 |
| 0040F866 | 83EC1C | sub esp, 1Ch | xref: 0040F7ED | |
| 0040F869 | 8BCC | mov ecx, esp | | |

Ilustración 28: Evasión de sandboxing

Posteriormente el RAT Remcos realiza un escalado de privilegios dentro del sistema para intentar obtener permisos para la vigilancia y obtención de información.

| | | | |
|---|---|---|---|
| 004074FD | 55 | push ebp | xref: 004075DE |
| 004074FE | 8BEC | mov ebp, esp | |
| 00407500 | 81EC30020000 | sub esp, 00000230h | |
| 00407506 | 56 | push esi | |
| 00407507 | 57 | push edi | |
| 00407508 | 681C634600 | push 0046631Ch | ASCII "[+] ucmAllocateElevatedObject" |
| 0040750D | E887BCFEFF | call 00407200h | target: 00407200 |
| 00407512 | 8365FC00 | and dword ptr [ebp-04h], 00000000h | |
| 00407516 | BFE8634600 | mov edi, 004663E8h | UTF-16 "{3E5FC7F9-9A51-4367-9063-A120244FBEC7}" |
| 0040751B | 57 | push edi | UTF-16 "{3E5FC7F9-9A51-4367-9063-A120244FBEC7}" |
| 0040751C | BE05400080 | mov esi, 80004005h | |
| 00407521 | E826A50300 | call 0043BAD6h | _wcslen@LIBCMT.LIB (Import, Unknown Params) target: 0043BAD6 |
| 00407526 | 59 | pop ecx | |
| 00407527 | 59 | pop ecx | |
| 00407528 | 83F840 | cmp eax, 40h | |
| 0040752B | 7773 | jnbe 004075A0h | target: 004075A0 |
| 0040752D | 8D4DD8 | lea ecx, dword ptr [ebp-28h] | |
| 00407530 | E85BFCFFFF | call 00407190h | target: 00407190 |
| 00407535 | 8D85D0FDFFFF | lea eax, dword ptr [ebp-00000230h] | |
| 0040753B | C745D824000000 | mov dword ptr [ebp-28h], 00000024h | ASCII "$" (Chunk) |
| 00407542 | 683C634600 | push 0046633Ch | UTF-16 "Elevation:Administrator!new:" |
| 00407547 | 50 | push eax | |
| 00407548 | C745EC04000000 | mov dword ptr [ebp-14h], 00000004h | |
| 0040754F | E85D350200 | call 0043F809h | target: 0043F809 |
| 00407554 | 8D85D0FDFFFF | lea eax, dword ptr [ebp-00000230h] | |
| 0040755A | 57 | push edi | UTF-16 "{3E5FC7F9-9A51-4367-9063-A120244FBEC7}" |
| 0040755B | 50 | push eax | |
| 0040755C | E86E350200 | call 0043F82Bh | target: 0043F82B |
| 00407561 | 6878634600 | push 00466378h | ASCII "[+] CoGetObject" |
| 00407566 | E887BCFEFF | call 00407200h | target: 00407200 |
| 0040756B | 83C414 | add esp, 14h | |
| 0040756E | 8D45FC | lea eax, dword ptr [ebp-04h] | |
| 00407571 | 50 | push eax | |
| 00407572 | 6818654600 | push 00466518h | |
| 00407577 | 8D45D8 | lea eax, dword ptr [ebp-28h] | |
| 0040757A | 50 | push eax | |
| 0040757B | 8D85D0FDFFFF | lea eax, dword ptr [ebp-00000230h] | |

Ilustración 29: Escalado de privilegios

El malware tiene la funcionalidad de recuperar credenciales de diferentes navegadores (Chrome, Firefox y Microsoft Edge) con la intención de robar información. Para ello Remcos accede a los siguientes ficheros para acceder a las credenciales:

- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
- C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\3nxxd8pi.default-release\places.sqlite
- C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
- C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\3nxxd8pi.default-release\key4.db
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data
- C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data

Un ejemplo de la ejecución donde el malware accede a los ficheros Login Data de Chrome que guardan las credenciales del navegador:

| | | | |
|---|---|---|---|
| 0040BA18 | 53 | push ebx | |
| 0040BA19 | 6878694600 | push 00466978h | ASCII "\AppData\Local\Google\Chrome\User Data\Default\Login Data" |
| 0040BA1E | 68B4694600 | push 004669B4h | ASCII "UserProfile" |
| 0040BA23 | E8B2060300 | call 0043C0DAh | target: 0043C0DA |
| 0040BA28 | 59 | pop ecx | |
| 0040BA29 | 50 | push eax | |
| 0040BA2A | 8D4DD0 | lea ecx, dword ptr [ebp-30h] | |
| 0040BA2D | E890CFFFFF | call 00402093h | target: 00402093 |
| 0040BA32 | 8BD0 | mov edx, eax | |
| 0040BA34 | 8D4DE8 | lea ecx, dword ptr [ebp-18h] | |
| 0040BA37 | E830AEFEFF | call 00406383h | target: 00406383 |
| 0040BA3C | 59 | pop ecx | |
| 0040BA3D | 8D4DD0 | lea ecx, dword ptr [ebp-30h] | |
| 0040BA40 | E84DD4FFFF | call 00401FD8h | target: 00401FD8 |
| 0040BA45 | 8D4DE8 | lea ecx, dword ptr [ebp-18h] | |
| 0040BA48 | E84CD4FFFF | call 00401FABh | target: 00401FAB |
| 0040BA4D | 50 | push eax | |
| 0040BA4E | FF1588924500 | call dword ptr [00459288h] | DeleteFileA@KERNEL32.DLL (Import, Unknown Params) |
| 0040BA54 | 85C0 | test eax, eax | Return Compare (DeleteFileA) |
| 0040BA56 | 7521 | jne 0040BA79h | target: 0040BA79 |
| 0040BA58 | FF1568924500 | call dword ptr [00459268h] | GetLastError@KERNEL32.DLL (Import, Unknown Params) |
| 0040BA5E | 48 | dec eax | |
| 0040BA5F | 83E801 | sub eax, 01h | |
| 0040BA62 | 7409 | je 0040BA6Dh | target: 0040BA6D |
| 0040BA64 | 83E801 | sub eax, 01h | |
| 0040BA67 | 7409 | je 0040BA6Dh | target: 0040BA6D |
| 0040BA69 | 32DB | xor bl, bl | |
| 0040BA6B | EB25 | jmp 0040BA92h | target: 0040BA92 |
| 0040BA6D | 83EC18 | sub esp, 18h | xref: 0040BA62 0040BA67 |
| 0040BA70 | 8BCC | mov ecx, esp | |
| 0040BA72 | 68C0694600 | push 004669C0h | ASCII "[Chrome StoredLogins not found]" |
| 0040BA77 | EB0A | jmp 0040BA83h | target: 0040BA83 |
| 0040BA79 | 83EC18 | sub esp, 18h | xref: 0040BA56 |
| 0040BA7C | 8BCC | mov ecx, esp | |
| 0040BA7E | 68E4694600 | push 004669E4h | ASCII "[Chrome StoredLogins found, cleared!]" |
| 0040BA83 | E890CFFFFF | call 00402093h | xref: 0040BA77 target: 00402093 |
| 0040BA88 | E84B070000 | call 0040C1D8h | target: 0040C1D8 |

Ilustración 30: Robo de credenciales

También Remcos RAT tiene la funcionalidad de robar credenciales en cuentas de mensajerías instantáneas como, por ejemplo: Google Talk, MSN Messenger y Paltalk. Para ello el malware intenta acceder a las claves de registro siguientes para intentar obtener la información:

- HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Dynamic Salt
- HKEY_CURRENT_USER\Software\Paltalk

Así como acceder al registro del sistema para obtener las credenciales de posibles clientes de correo instalados en el ordenador remoto:

- HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
- HKEY_CURRENT_USER\Software\IncrediMail\Identities
- HKEY_CURRENT_USER\Software\Microsoft\Windows Live Mail

Como se ha mencionado anteriormente Remcos utiliza métodos para capturar la información que el usuario ha tecleado (keylogger) y recopilar información de diferentes ubicaciones, como por ejemplo páginas o portales de inicio de sesión. El siguiente código ejecutado por el malware permite recuperar información sobre el teclado del sistema infectado:

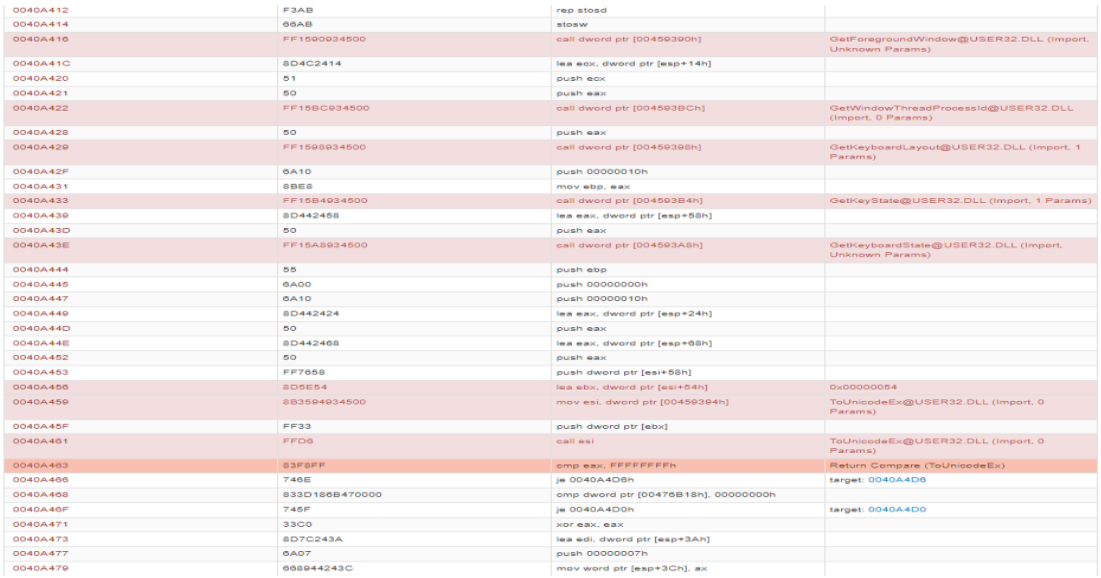
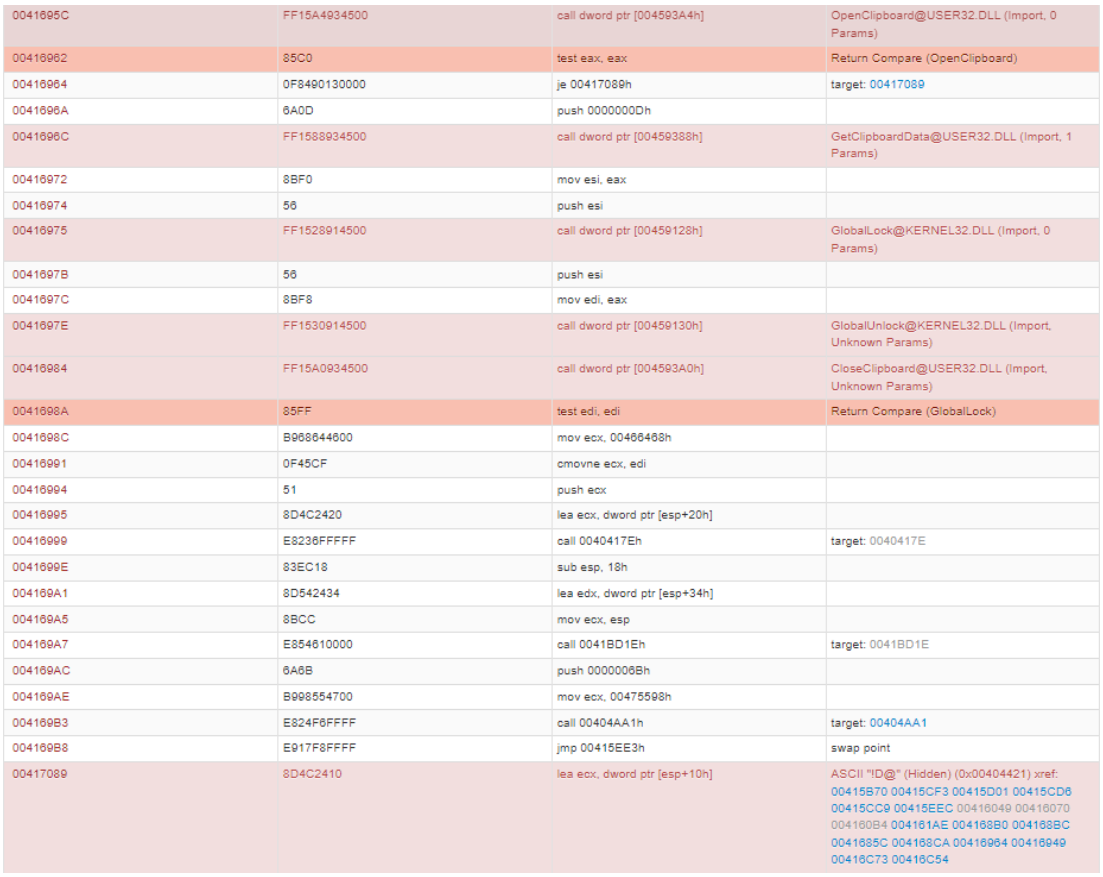



Ilustración 31: Keylogger

De la misma forma Remcos RAT recopila la información del portapapeles para el robo de información:



| | | | |
|---|---|---|---|
| 0041695C | FF15A4934500 | call dword ptr [004593A4h] | OpenClipboard@USER32.DLL (Import, 0 Params) |
| 00416962 | 85C0 | test eax, eax | Return Compare (OpenClipboard) |
| 00416964 | 0F8490130000 | je 00417089h | target: 00417089 |
| 0041696A | 6A0D | push 0000000Dh | |
| 0041696C | FF1588934500 | call dword ptr [00459388h] | GetClipboardData@USER32.DLL (Import, 1 Params) |
| 00416972 | 8BF0 | mov esi, eax | |
| 00416974 | 56 | push esi | |
| 00416975 | FF1528914500 | call dword ptr [00459128h] | GlobalLock@KERNEL32.DLL (Import, 0 Params) |
| 0041697B | 56 | push esi | |
| 0041697C | 8BF8 | mov edi, eax | |
| 0041697E | FF1530914500 | call dword ptr [00459130h] | GlobalUnlock@KERNEL32.DLL (Import, Unknown Params) |
| 00416984 | FF15A0934500 | call dword ptr [004593A0h] | CloseClipboard@USER32.DLL (Import, Unknown Params) |
| 0041698A | 85FF | test edi, edi | Return Compare (GlobalLock) |
| 0041698C | B968644600 | mov ecx, 00466468h | |
| 00416991 | 0F45CF | cmovne ecx, edi | |
| 00416994 | 51 | push ecx | |
| 00416995 | 8D4C2420 | lea ecx, dword ptr [esp+20h] | |
| 00416999 | E8236FFFFF | call 0040417Eh | target: 0040417E |
| 0041699E | 83EC18 | sub esp, 18h | |
| 004169A1 | 8D542434 | lea edx, dword ptr [esp+34h] | |
| 004169A5 | 8BCC | mov ecx, esp | |
| 004169A7 | E854610000 | call 0041BD1Eh | target: 0041BD1E |
| 004169AC | 6A6B | push 0000006Bh | |
| 004169AE | B998554700 | mov ecx, 00475598h | |
| 004169B3 | E824F6FFFF | call 00404AA1h | target: 00404AA1 |
| 004169B8 | E917F8FFFF | jmp 00415EE3h | swap point |
| 00417089 | 8D4C2410 | lea ecx, dword ptr [esp+10h] | ASCII "ID@" (Hidden) (0x00404421) xref: 00415B70 00415CF3 00415D01 00415CD6 00415CC9 00415EEC 00416049 00416070 004160B4 004161AE 004168B0 004168BC 0041685C 004168CA 00416964 00416949 00416C73 00416C54 |

Ilustración 32: Robo de información del portapapeles

Durante la ejecución de Remcos RAT se ha podido observar que el malware hace una recopilación de la información del sistema operativo infectado, accediendo a la siguiente información:

- Hora local del sistema infectado a través de la función del sistema Windows GetLocalTime:

| | | | |
|---|---|---|---|
| 00404F80 | 50 | push eax | |
| 00404F81 | FF15E4924500 | call dword ptr [004592E4h] | GetLocalTime@KERNEL32.DLL (Import, Unknown Params) |
| 00404F87 | 8BD7 | mov edx, edi | |
| 00404F89 | 8D4DD8 | lea ecx, dword ptr [ebp-28h] | |
| 00404F8C | E815750100 | call 0041BB8Eh | target: 0041BB8E |
| 00404F91 | 83EC18 | sub esp, 18h | |
| 00404F94 | BA10604600 | mov edx, 00466010h | ASCII "KeepAlive \| Enabled \| Timeout: " |
| 00404F99 | 8BCC | mov ecx, esp | |
| 00404F9B | 50 | push eax | |
| 00404F9C | E8AD080000 | call 004052FDh | target: 004052FD |

Ilustración 33: Hora local del sistema

- Recopilación de los servicios ejecutados en el sistema remoto a través de la función OpenSCManager, que establece una conexión con el administrador de controles de servicio para obtener la información:

| | | | |
|---|---|---|---|
| 0041A75E | FF1520904500 | call dword ptr [00459020h] | OpenSCManagerA@ADVAPI32.DLL (Import, Unknown Params) |
| 0041A764 | 8BD8 | mov ebx, eax | |
| 0041A766 | 85DB | test ebx, ebx | Return Compare (OpenSCManagerA) |
| 0041A768 | 7511 | jne 0041A77Bh | target: 0041A77B |
| 0041A76A | 6868644600 | push 00466468h | |
| 0041A76F | 8BCF | mov ecx, edi | |
| 0041A771 | E8236FFFFF | call 0040417Eh | target: 0040417E |
| 0041A776 | E9C2020000 | jmp 0041AA3Dh | target: 0041AA3D |
| 0041A77B | 8D4C244C | lea ecx, dword ptr [esp+4Ch] | xref: 0041A768 |
| 0041A77F | E8FE65FFFF | call 00401F86h | target: 00401F86 |
| 0041A784 | 8D442420 | lea eax, dword ptr [esp+20h] | |
| 0041A788 | 896C2418 | mov dword ptr [esp+18h], ebp | |
| 0041A78C | 50 | push eax | |
| 0041A78D | 8D442418 | lea eax, dword ptr [esp+18h] | |
| 0041A791 | 896C2418 | mov dword ptr [esp+18h], ebp | |
| 0041A795 | 50 | push eax | |
| 0041A796 | 8D442420 | lea eax, dword ptr [esp+20h] | |
| 0041A79A | 896C2428 | mov dword ptr [esp+28h], ebp | |
| 0041A79E | 50 | push eax | |
| 0041A79F | 55 | push ebp | |
| 0041A7A0 | 8D8424A4000000 | lea eax, dword ptr [esp+000000A4h] | |
| 0041A7A7 | 50 | push eax | |
| 0041A7A8 | 6A03 | push 00000003h | |
| 0041A7AA | 6A3B | push 0000003Bh | |
| 0041A7AC | 53 | push ebx | |
| 0041A7AD | FF1538904500 | call dword ptr [00459038h] | EnumServicesStatusW@ADVAPI32.DLL (Import, 0 Params) |
| 0041A7B3 | 85C0 | test eax, eax | Return Compare (EnumServicesStatusW) |
| 0041A7B5 | 0F8566020000 | jne 0041AA21h | target: 0041AA21 |
| 0041A7BB | FF1568924500 | call dword ptr [00459268h] | GetLastError@KERNEL32.DLL (Import, Unknown Params) |
| 0041A7C1 | 3DEA000000 | cmp eax, 000000EAh | Return Compare (GetLastError) |

Ilustración 34: Recopilación de servicios ejecutados en la maquina remota

- Leer, crear, borrar y modificar ficheros en el sistema remoto a través de las siguientes funciones del sistema Windows remoto: ”FindFirstFileW, FindNextFileW, RemoveDirectoryW, SetFileAttributesW, DeleteFileW, GetLastError, FindClose, RemoveDirectoryW, FindClose,”
- Enumerar los procesos corriendo en la maquina infectada remota a través de la función de Windows Process32.

| | | | |
|---|---|---|---|
| 0040F4D5 | FF15D0904500 | call dword ptr [004590D0h] | Process32FirstW@KERNEL32.DLL (Import, 0 Params) |
| 0040F4DB | EB6E | jmp 0040F54Bh | target: 0040F54B |
| 0040F4DD | 8D8424AC000000 | lea eax, dword ptr [esp+000000ACh] | xref: 0040F55C |
| 0040F4E4 | 50 | push eax | |
| 0040F4E5 | 8D4C241C | lea ecx, dword ptr [esp+1Ch] | |
| 0040F4E9 | E8236FFFFF | call 0040417Eh | target: 0040417E |
| 0040F4EE | 8D442460 | lea eax, dword ptr [esp+60h] | |
| 0040F4F2 | 50 | push eax | |
| 0040F4F3 | 8D4C241C | lea ecx, dword ptr [esp+1Ch] | |
| 0040F4F7 | E87F66FEFF | call 00402305h | target: 00402305 |
| 0040F4FC | 8BF8 | mov edi, eax | |
| 0040F4FE | 8D4C2418 | lea ecx, dword ptr [esp+18h] | |
| 0040F502 | 8D442464 | lea eax, dword ptr [esp+64h] | |
| 0040F506 | 50 | push eax | |
| 0040F507 | E878030000 | call 004022CAh | target: 004022CA |
| 0040F50C | 8BF0 | mov esi, eax | |
| 0040F50E | 8D4C2418 | lea ecx, dword ptr [esp+18h] | |
| 0040F512 | 8D442468 | lea eax, dword ptr [esp+68h] | |
| 0040F516 | 50 | push eax | |
| 0040F517 | E87F66FEFF | call 00402305h | target: 00402305 |
| 0040F51C | FF37 | push dword ptr [edi] | |
| 0040F51E | 8D4C2470 | lea ecx, dword ptr [esp+70h] | |
| 0040F522 | FF36 | push dword ptr [esi] | |
| 0040F524 | FF30 | push dword ptr [eax] | |
| 0040F526 | E804D6FEFF | call 00409BDBh | target: 00409BDB |
| 0040F52B | 83C40C | add esp, 0Ch | |
| 0040F52E | 8D9424C8040000 | lea edx, dword ptr [esp+000004C8h] | |
| 0040F535 | 8D4C2418 | lea ecx, dword ptr [esp+18h] | |
| 0040F539 | E81B020000 | call 0040B9CCh | target: 0040B9CC |
| 0040F53E | 84C0 | test al, al | |
| 0040F540 | 754B | jne 0040F58Dh | target: 0040F58D |
| 0040F542 | 8D4C2418 | lea ecx, dword ptr [esp+18h] | |
| 0040F546 | E899E6FEFF | call 00401F09h | target: 00401F09 |
| 0040F54B | 8D842488000000 | lea eax, dword ptr [esp+00000088h] | xref: 0040F4DB |
| 0040F552 | 50 | push eax | |
| 0040F553 | 55 | push ebp | |
| 0040F554 | FF15CC904500 | call dword ptr [004590CCh] | Process32NextW@KERNEL32.DLL (Import, 2 Params) |
| 0040F55A | 85C0 | test eax, eax | Return Compare (Process32NextW) |

Ilustración 34: Procesos corriendo en la maquina remota

- Obtener información del sistema infectado, como, por ejemplo, uso de la cpu, número de serie del equipo, nombre del equipo, nombre de usuario. Por ejemplo, en el siguiente código se muestra que el malware Remcos RAT ha ejecutado la función del sistema “GetComputerNameExW” para extraer el nombre de la maquina remota y la función del sistema “GetUserNameW” para extraer el nombre de usuario.
-

| | | | | |
|---|---|---|---|---|
| 0041B62A | FF15084B4700 | call dword ptr [00474B08h] | GetComputerNameExW@KERNELBASE.DLL (Import, Hidden, 3 Params) executed | |
| 0041B630 | 8D45F8 | lea eax, dword ptr [ebp-08h] | executed | Path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CCG 41B630 |
| 0041B633 | C745F800010000 | mov dword ptr [ebp-08h], 00000100h | | |
| 0041B63A | 50 | push eax | | |
| 0041B63B | 8D85A8FDFFFF | lea eax, dword ptr [ebp-00000258h] | | |
| 0041B641 | 50 | push eax | | |
| 0041B642 | FF150C904500 | call dword ptr [0045900Ch] | GetUserNameW@ADVAPI32.DLL (Import, Hidden, 0 Params) executed | |
| 0041B648 | 8D85A8FDFFFF | lea eax, dword ptr [ebp-00000258h] | executed | 41B648 |

Ilustración 34: Nombre de maquina

Durante la ejecución del malware Remcos RAT se ha podido extraer el fichero de configuración del malware el cual nos indica muchas de las configuraciones

presentes en el agente, como por ejemplo el dominio del controlador “top.noforabusers1.xyz:2090” y la versión del malware “4.9.3 Pro”.

El fichero de configuración puede encontrarse en la sección de recursos del binario desempaquetado, el recurso se llama “settings” y está cifrado con un cifrado RC4. La longitud de la clave es el primer byte del recurso y los siguientes bytes hasta la longitud del primer byte es la clave:


```
{"Version": "4.9.3 Pro",
"Host:Port:Password": "top.noforabusers1.xyz:2090:1",
"Assigned name": "RemoteHost",
"Connect interval": "1",
"Install flag": "Disable",
"Setup HKCU\\Run": "Enable",
"Setup HKLM\\Run": "Enable",
"Install path": "Application path",
"Copy file": "remcos.exe",
"Startup value": "Disable",
"Hide file": "Disable",
"Mutex": "Rmc-1IWDHQ",
"Keylog flag": "0",
"Keylog path": "Application path",
"Keylog file": "logs.dat",
"Keylog crypt": "Disable",
"Hide keylog file": "Disable",
"Screenshot flag": "Disable",
"Screenshot time": "10",
"Take Screenshot option": "Disable",
"Take screenshot title": "",
"Take screenshot time": "5",
"Screenshot path": "AppData",
"Screenshot file": "Screenshots",
"Screenshot crypt": "Disable",
```

"Mouse option": "Disable",

"Delete file": "Disable",

"Audio record time": "5"}

## Comunicaciones realizadas por el malware

Dentro de las conexiones realizadas desde el sistema infectado se ha podido observar la comunicación hacía el dominio legítimo “geoplugin.net” encargado de extraer la geolocalización de la maquina infectada. La petición y respuesta realizada es la siguiente:

| Bytes transferred | Direction | Data |
|---|---|---|
| 71 | OUT | GET /json.gp HTTP/1.1<br>Host: geoplugin.net<br>Cache-Control: no-cache |
| 1162 | IN | HTTP/1.1 200 OK<br>date: Wed, 27 Dec 2023 10:51:14 GMT<br>server: Apache<br>content-length: 954<br>content-type: application/json; charset=utf-8<br>cache-control: public, max-age=300<br>access-control-allow-origin: *<br>Data Raw: 7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 32 31 32 2e 31 30 32 2e 34 31 2e 32 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 32 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 73 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 73 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 3c 5c 2f 61 3e 2e 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 69 74 79 22 3a 22 44 61 6c 6c 61 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 22 3a 22 54 65 78 61 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 43 6f 64 65 22 3a 22 54 58 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 54 65 78 61 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 61 72 65 61 43 6f 64 65 22 3a 22 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 6d 61 43 6f 64 65 22 3a 22 36 32 33 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 55 53 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 4e 61 6d 65 22 3a 22 55 6e 69 74 65 64 20 53 74 61 74 65 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 69 6e 45 55 22 3a 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 65 75 56 41 54 72 61 74 65 22 3a 66 61 6c 73 65 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 43 6f 64 65 22 3a 22 4e 41 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 4e 61 6d 65 22 3a 22 4e 6f 72 74 68 20 41 6d 65 72 69 63 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 61 74 69 74 75 64 65 22 3a 22 33 32 2e 37 37 39 37 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 6e 67 69 74 75 64 65 22 3a 22 2d 39 36 2e 38 30 32 32 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 63 61 74 69 6f 6e 41 63 63 75 72 61 63 79 52 61 64 69 75 73 22 3a 22 32 30 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 74 69 6d 65 7a 6f 6e 65 22 3a 22 41 6d 65 72 69 63 61 5c 2f 43 68 69 63 61 67 6f 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 55 53 44 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 22 3a 22 24 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 5f 55 54 46 38 22 3a 22 24 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 6e 76 65 72 74 65 72 22 3a 30 0a 7d<br>Data Ascii: { "geoplugin_request":"212.102.41.2", "geoplugin_status":200, "geoplugin_delay":"1ms", "geoplugin_credit":"Some of the returned data includes GeoLite2 data created by MaxMind, available from <a href='https:\/\/www.maxmind.com'>https:\/\/www.maxmind.com<\/a>.", "geoplugin_city":"Dallas", "geoplugin_region":"Texas", "geoplugin_regionCode":"TX", "geoplugin_regionName":"Texas", "geoplugin_areaCode":"", "geoplugin_dmaCode":"623", "geoplugin_countryCode":"US", "geoplugin_countryName":"United States", "geoplugin_inEU":0, "geoplugin_euVATrate":false, "geoplugin_continentCode":"NA", "geoplugin_continentName":"North America", "geoplugin_latitude":"32.7797", "geoplugin_longitude":"-96.8022", "geoplugin_locationAccuracyRadius":"20", "geoplugin_timezone":"America\/Chicago", "geoplugin_currencyCode":"USD", "geoplugin_currencySymbol":"$", "geoplugin_currencySymbol_UTF8":"$", "geoplugin_currencyConverter":0} |

Ilustración 35: Comunicaciones realizadas por el agente

Además, se ha resuelto la petición DNS del dominio “top.noforabusers1.xyz” resolviendo hacía la dirección IP “91.92.252.36”. Siendo el controlador del agente instalado en la maquina remota.

| Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|
| 1.1.1.1 | 192.168.2.9 | 0x281 | No error (0) | top.noforabusers1.xyz | | 91.92.252.36 | A (IP address) | IN (0x0001) | false |
| 1.1.1.1 | 192.168.2.9 | 0xa958 | No error (0) | geoplugin.net | | 178.237.33.50 | A (IP address) | IN (0x0001) | false |

Ilustración 36: Comunicaciones realizadas por el agente

La dirección IP dañina 91.92.252.36 está alojada en Bulgaria y pertenece al ASN THEZONEBG, por otro lado, la dirección IP benigna 178.237.33.50 está alojada en Países Bajos y pertenece al ASN ATOM86-ASATOM86NL.

## 3. Vulnerabilidades explotadas

Como se ha mencionado al principio de este documento, la facilidad de acceso al Remcos RAT ha propiciado que los atacantes distribuyan este malware de múltiples formas, aunque la forma más habitual de entrega es a través de phishing que contienen documentos ofimáticos dañinos adjuntados.

Por ello, se ha podido detectar a través de fuentes públicas y análisis externos que dichos documentos ofimáticos aprovechan vulnerabilidades conocidas de Microsoft Office para ejecutar su carga dañina y llevar a cabo la actividad deseada por el atacante. A continuación, se muestran dos vulnerabilidades que una vez explotadas descargan en la máquina de la víctima el malware Remcos:

- **Vulnerabilidad en productos Microsoft (CVE-2017-11882):** Esta vulnerabilidad permite que un atacante ejecute código arbitrario de forma remota (RCE) a través de errores de manejo de objetos en la memoria RAM. Un atacante puede explotar esta vulnerabilidad mediante la creación de un archivo dañino y persuadir a la víctima para que lo abra, a menudo a través de un correo electrónico o desde un sitio web comprometido. Si la víctima tiene derechos de administrador, esto podría llevar el control total del sistema, incluyendo la instalación de programas, alteración o eliminación de datos, y creación de nuevas cuentas de usuario. El software afectado por esta vulnerabilidad es: Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1 y Microsoft Office 2016.
- **Vulnerabilidad en Microsoft Office y múltiples versiones de Windows (CVE-2017-0199):** Esta vulnerabilidad permite que un atacante ejecute código arbitrario de forma remota (RCE) a través de un documento manipulado en las siguientes versiones de software, Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1 y Windows 8.1. Esta vulnerabilidad ha sido activamente explotada durante los últimos años con el objetivo de descargarse malware como por ejemplo Remcos o Dridex.

## 3. Técnicas MITRE ATT&CK

| MITRE ATT&CK | | |
|---|---|---|
| **Táctica** | **Técnica** | **Mitigaciones** |
| **TA0001 Initial Access** | T1566.001 Spearphishing Attachment | **M1049: Antivirus/Antimalware**: Anti-virus can also automatically quarantine suspicious files. |
| | | **M1017: User Training:** Users can be trained to identify social engineering techniques and spearphishing emails. |
| | T1566 Phishing | **M1021 Restrict Web-Based Content:** Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. |
| | | **M1049: Antivirus/Antimalware**: Anti-virus can automatically quarantine suspicious files. |
| | | **M1017: User Training:** Users can be trained to identify social engineering techniques and phishing emails. |
| | | **M1054 Software Configuration:** Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intraorg and cross domain) to perform similar message filtering and validation.(Citation: Microsoft Anti Spoofing)(Citation: ACSC Email Spoofing). |
| | | **M1031 Network Intrusion Prevention:** Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity. |
| | T1190 Exploit Public-Facing Application | **M1048 Application Isolation and Sandboxing:** Application isolation will limit what other processes and system features the exploited target can access. |

| | | |
|---|---|---|
| | | **M1050 Exploit Protection:** Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application. |
| | | **M1030 Network Segmentation:** Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure. |
| | | **M1026 Privileged Account Management:** Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. |
| | | **M1051 Update Software:** Update software regularly by employing patch management for externally exposed applications. |
| | | **M1016 Vulnerability Scanning:** Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure. |
| | T1189 Drive-by Compromise | **M1048 Application Isolation and Sandboxing:** Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems. |
| | | **M1050 Exploit Protection:** Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. Many of these protections depend on the architecture and target application binary for compatibility. |
| | | **M1021 Restrict Web-Based Content:** For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process. |
| | | **M1051 Update Software:** Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on. |

| | | |
|---|---|---|
| | T1106 Native API | **M1040 Behavior Prevention on Endpoint:** On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office VBA macros from calling Win32 APIs. |
| | | **M1038 Execution Prevention:** Identify and block potentially malicious software executed that may be executed through this technique by using application control tools, like Windows Defender Application Control, AppLocker, or Software Restriction Policies where appropriate. |
| **TA0002 Execution** | T1059 Command and Scripting Interpreter | **M1049 Antivirus/Antimalware:** Anti-virus can be used to automatically quarantine suspicious files. |
| | | **M1040 Behavior Prevention on Endpoint:** On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual Basic and JavaScript scripts from executing potentially malicious downloaded content. |
| | | **M1045 Code Signing:** Where possible, only permit execution of signed scripts. |
| | | **M1042 Disable or Remove Feature or Program:** Disable or remove any unnecessary or unused shells or interpreters. |
| | | **M1038 Execution Prevention:** Use application control where appropriate. For example, PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., Add-Type). |
| | | **M1026 Privileged Account Management:** When PowerShell is necessary, consider restricting PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration. PowerShell JEA (Just Enough Administration) may also be used to sandbox administration and limit what commands admins/users can execute through remote PowerShell sessions. |
| | | **M1021 Restrict Web-Based Content:** Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. |

| | | |
|---|---|---|
| | T1569.002 Service Execution | **M1040 Behavior Prevention on Endpoint:** On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running. |
| | | **M1026 Privileged Account Management:** Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. |
| | | **M1022 Restrict File and Directory Permissions:** Ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level. |
| **TA0003 Persistence** | T1543.003 Windows Service | **M1047 Audit:** Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. |
| | | **M1040 Behavior Prevention on Endpoint:** On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system. On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed service drivers. |
| | | **M1045 Code Signing:** Enforce registration and execution of only legitimately signed service drivers where possible. |
| | | **M1028 Operating System Configuration:** Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed. |
| | | **M1018 User Account Management:** Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. |
| **TA0004 Privilege Escalation** | T1548.002 Bypass User Account Control | **M1047 Audit:** Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate. |
| | | **M1026 Privileged Account Management:** Remove users from the local administrator group on systems. |
| | | **M1051 Update Software:** Consider updating Windows to the latest version and patch level to utilize the latest protective measures against UAC bypass. |

| | | |
|---|---|---|
| | | **M1052 User Account Control:** Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking. |
| | T1134 Access Token Manipulation | **M1026 Privileged Account Management:** Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runas. |
| | | **M1018 User Account Management:** An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require. |
| | T1543.003 Windows Service | **M1047 Audit:** Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. |
| | | **M1040 Behavior Prevention on Endpoint:** On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system. On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed service drivers. |
| | | **M1045 Code Signing:** Enforce registration and execution of only legitimately signed service drivers where possible. |
| | | **M1028 Operating System Configuration:** Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed. |
| | | **M1018 User Account Management:** Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. |

| | | |
|---|---|---|
| | T1055 Process Injection | **M1040 Behavior Prevention on Endpoint:** Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process. For example, on Windows 10, Attack Surface Reduction (ASR) rules may prevent Office applications from code injection. |
| | | **M1026 Privileged Account Management:** Utilize Yama (ex: /proc/sys/kernel/yama/ptrace_scope) to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced access control and process restrictions such as SELinux, grsecurity, and AppArmor. |
| **TA0005 Defense Evasion** | T1562.001 Disable or Modify Tools | **M1038 Execution Prevention:** Use application control where appropriate, especially regarding the execution of tools outside of the organization's security policies (such as rootkit removal tools) that have been abused to impair system defenses. Ensure that only approved security applications are used and running on enterprise systems. |
| | | **M1022 Restrict File and Directory Permissions:** Ensure proper process and file permissions are in place to prevent adversaries from disabling or interfering with security services. |
| | | **M1024 Restrict Registry Permissions:** Ensure proper Registry permissions are in place to prevent adversaries from disabling or interfering with security services. |
| | | **M1018 User Account Management:** Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services. |
| | T1140 Deobfuscate/Decode Files or Information | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1027 Obfuscated Files or Information | **M1049 Antivirus/Antimalware:** Anti-virus can be used to automatically detect and quarantine suspicious files. Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10+ to analyze commands after being processed/interpreted. |
| | | **M1047 Audit:** Consider periodic review of common fileless storage locations (such as the Registry or WMI repository) to potentially identify abnormal and malicious data. |

| | | |
|---|---|---|
| | | **M1040 Behavior Prevention on Endpoint:** On Windows 10+, enable Attack Surface Reduction (ASR) rules to prevent execution of potentially obfuscated payloads. |
| | | **M1017 User Training:** Ensure that a finite amount of ingress points to a software deployment system exist with restricted access for those required to allow and enable newly deployed software. |
| | T1027.002 Software Packing | **M1049 Antivirus/Antimalware:** Employ heuristic-based malware detection. Ensure updated virus definitions and create custom signatures for observed malware. |
| | T1548.002 Bypass User Account Control | **M1047 Audit:** Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate. |
| | | **M1026 Privileged Account Management:** Remove users from the local administrator group on systems. |
| | | **M1051 Update Software:** Consider updating Windows to the latest version and patch level to utilize the latest protective measures against UAC bypass. |
| | | **M1052 User Account Control:** Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking. |
| | T1036 Masquerading | **M1049 Antivirus/Antimalware:** Anti-virus can be used to automatically quarantine suspicious files. |
| | | **M1040 Behavior Prevention on Endpoint:** Implement security controls on the endpoint, such as a Host Intrusion Prevention System (HIPS), to identify and prevent execution of potentially malicious files (such as those with mismatching file signatures). |
| | | **M1045 Code Signing:** Require signed binaries. |
| | | **M1038 Execution Prevention:** Use tools that restrict program execution via application control by attributes other than file name for common operating system utilities that are needed. |
| | | **M1022 Restrict File and Directory Permissions:** Use file system access controls to protect folders such as C:\Windows\System32. |

| | | |
|---|---|---|
| | | **M1017 User Training:** Train users not to open email attachments or click unknown links (URLs). Such training fosters more secure habits within your organization and will limit many of the risks. |
| | T1497 Virtualization/Sandbox Evasion | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1134 Access Token Manipulation | **M1026 Privileged Account Management:** Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runas. |
| | | **M1018 User Account Management:** An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require. |
| | T1055 Process Injection | **M1040 Behavior Prevention on Endpoint:** Some endpoint security solutions can be configured to block some types of process injection based on common sequences of behavior that occur during the injection process. For example, on Windows 10, Attack Surface Reduction (ASR) rules may prevent Office applications from code injection. |
| | | **M1026 Privileged Account Management:** Utilize Yama (ex: /proc/sys/kernel/yama/ptrace_scope) to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced access control and process restrictions such as SELinux, grsecurity, and AppArmor. |

| | | |
|---|---|---|
| | | **M1015 Active Directory Configuration:** Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication. [18] [19] Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials. |
| | | **M1040 Behavior Prevention on Endpoint:** On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. |
| | | **M1043 Credential Access Protection:** With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping. |
| | | **M1041 Encrypt Sensitive Information:** Ensure Domain Controller backups are properly secured. |
| | | **M1028 Operating System Configuration:** Consider disabling or restricting NTLM. Consider disabling WDigest authentication. |
| | | **M1027 Password Policies:** Ensure that local administrator accounts have complex, unique passwords across all systems on the network. |
| | | **M1026 Privileged Account Management:** Windows:Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. Linux:Scraping the passwords from memory requires root privileges. Follow best practices in restricting access to privileged accounts to avoid hostile programs from accessing such sensitive regions of memory. |
| **TA0006 Credential Access** | T1003 OS Credential Dumping | **M1025 Privileged Process Integrity:** On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA. |

| | | |
|---|---|---|
| | | **M1017 User Training:** Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts. |
| | T1056 Input Capture | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1552.002 Credentials in Registry | **M1047 Audit:** Proactively search for credentials within the Registry and attempt to remediate the risk. |
| | | **M1027 Password Policies:** Do not store credentials within the Registry. |
| | | **M1026 Privileged Account Management:** If it is necessary that software must store credentials in the Registry, then ensure the associated accounts have limited permissions so they cannot be abused if obtained by an adversary. |
| | T1552.001 Credentials In Files | **M1047 Audit:** Preemptively search for files containing passwords and take actions to reduce the exposure risk when found. |
| | | **M1027 Password Policies:** Establish an organizational policy that prohibits password storage in files. |
| | | **M1022 Restrict File and Directory Permissions:** Restrict file shares to specific directories with access only to necessary users. |
| | | **M1017 User Training:** Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers. |
| **TA0007 Discovery** | T1124 System Time Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1087 Account Discovery | **M1028 Operating System Configuration:** Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located HKLM\ SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation. |

| | | |
|---|---|---|
| | T1007 System Service Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1083 File and Directory Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1082 System Information Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1518.001 Security Software Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1497 Virtualization/Sandbox Evasion | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1057 Process Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1010 Application Window Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1033 System Owner/User Discovery | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| **TA0009 Collection** | T1560 Archive Collected Data | **M1047 Audit:** System scans can be performed to identify unauthorized archival utilities. |
| | T1005 Data from Local System | **M1057 Data Loss Prevention:** Data loss prevention can restrict access to sensitive data and detect sensitive data that is unencrypted. |
| | T1114 Email Collection | **M1047 Audit:** Enterprise email solutions have monitoring mechanisms that may include the ability to audit auto-forwarding rules on a regular basis. In an Exchange environment, Administrators can use Get-InboxRule to discover and remove potentially malicious auto-forwarding rules.<br>**M1041 Encrypt Sensitive Information:** Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires |

| | | |
|---|---|---|
| | | the adversary to obtain the private certificate along with an encryption key to decrypt messages. |
| | | **M1032 Multi-factor Authentication:** Use of multi-factor authentication for public-facing webmail servers is a recommended best practice to minimize the usefulness of usernames and passwords to adversaries. |
| | T1056 Input Capture | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| | T1115 Clipboard Data | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |
| **TA0011 Command and Control** | T1105 Ingress Tool Transfer | **M1031 Network Intrusion Prevention:** Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. |
| | T1573 Encrypted Channel | **M1031 Network Intrusion Prevention:** Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. |
| | | **M1020 SSL/TLS Inspection:** SSL/TLS inspection can be used to see the contents of encrypted sessions to look for network-based indicators of malware communication protocols. |
| | T1571 Non-Standard Port | **M1031 Network Intrusion Prevention:** Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. |
| | | **M1030 Network Segmentation:** Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports for that particular network segment. |

| | | |
|---|---|---|
| | | **M1037 Filter Network Traffic:** Filter network traffic to prevent use of protocols across the network boundary that are unnecessary. |
| | | **M1031 Network Intrusion Prevention:** Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. |
| | T1095 Non-Application Layer Protocol | **M1030 Network Segmentation:** Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems. Also ensure hosts are only provisioned to communicate over authorized interfaces. |
| | T1071 Application Layer Protocol | **M1031 Network Intrusion Prevention:** Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. |
| **TA0040 Impact** | T1529 System Shutdown/Reboot | This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. |

## 4. Mitigación

Prevenir un ataque del malware Remcos requiere de una combinación de buenas prácticas, que incluyen:

- Utilizar un filtro de spam de correo electrónico efectivo y actualizado, para evitar de esta forma, la ejecución por parte de usuarios descuidados del malware Remcos.
- Proporcionar capacidad de detección de posibles ataques de ingeniería social y phishing a los empleados a través de campañas de concienciación, con el objetivo de disminuir la probabilidad de ataques exitosos en la organización.
- Verificar minuciosamente el contexto de documentos o archivos desconocidos antes de abrirlos.
- Configurar los clientes de correo electrónico para notificar a los usuarios cuando los correos electrónicos se originen fuera de la organización.
- Asegurar de que las aplicaciones de Office estén configuradas con “Desactivar todas las macros sin notificación” o “Desactivar todas las macros excepto las firmadas digitalmente”.
- Prestar especial atención a las notificaciones de advertencia en clientes de correo electrónico y aplicaciones de Office que pueden alertarle sobre contextos sospechosos, como archivos que contienen macros de VBA.
- Utilizar software antivirus y antimalware actualizado para detectar y eliminar amenazas.
- Mantener todos los sistemas operativos y software actualizados para protegerse contra vulnerabilidades explotables.
- Realizar copias de seguridad regulares de los datos importantes para recuperar información en caso de infección.
- Limitar los privilegios de usuario y controlar el acceso a archivos críticos para minimizar el impacto de una infección.
- Evitar el uso del gestor de contraseñas de los navegadores. En su lugar, se sugiere optar por aplicaciones específicas diseñadas para gestionar contraseñas de manera segura y confiable.

## 5. Indicadores de compromiso

**Hashes:**

- **Sha256**: 6c040340e398600d3f192f83b9cdb219171108c5d7d8ca14813fa48d326d1a8b
- **Sha1**: 336fc5bc0da79cdad2076ebb55393e3fb7456ac4
- **MD5**: 1eac408f61ea7a336c934476f8597c58

**Dominios e IPs:**

- top.noforabusers1.xyz
- 91.92.252.36

**Regla Yara:**

Estas reglas sirven para identificar las muestras del agente Remcos en sistemas Windows infectados.

```
rule agente_remcos {
        meta:
                description = "Deteccion de la ejecución de un agente del RAT Remcos"
                sharing = "TLP:WHITE"
        strings:
                $s1 = "Watchdog module activated" ascii
                $s2 = "Remcos restarted by watchdog!" ascii
                $s3 = " BreakingSecurity.net" ascii
        condition:
                //uint16(0) == 0x5a4d
                //and
                (all of ($s*))}
```

## 6. Referencias Adicionales


- https://www.zscaler.com/blogs/security-research/dbatloader-actively-distributing-malwares-targeting-european-businesses
- https://www.socinvestigation.com/remcos-rat-new-ttps-detection-response/
- https://perception-point.io/blog/behind-the-attack-remcos-rat/
- https://www.connectwise.com/resources/formbook-remcos-rat
- https://muha2xmad.github.io/mal-document/remcosdoc/
- https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing
- https://blog.morphisec.com/remcos-trojan-analyzing-attack-chain
- https://asec.ahnlab.com/en/32376/
- https://isc.sans.edu/diary/Remcos+RAT+Delivered+Through+Double+Compressed+Archive/28354
- https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Remcos/Remcos.md
- https://www.esentire.com/blog/remcos-rat
- https://www.splunk.com/en_us/blog/security/detecting-malware-script-loaders-using-remcos-threat-research-release-december-2021.html
- https://amgedwageh.medium.com/analysis-of-an-autoit-script-that-wraps-a-remcos-rat-6b5b66075b87
- https://www.malwarebytes.com/blog/threat-intelligence/2021/07/remcos-rat-delivered-via-visual-basic
- https://www.cybereason.com/blog/cybereason-exposes-malware-targeting-us-taxpayers
- https://www.bitdefender.com/files/News/CaseStudies/study/390/Bitdefender-PR-Whitepaper-Remcos-creat5080-en-EN-GenericUse.pdf
- https://github.com/1d8/analyses/blob/master/RemcosDocDropper.MD
- https://www.zscaler.com/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat
- https://news.sophos.com/en-us/2020/05/14/raticate/
- https://dissectingmalwa.re/malicious-ratatouille.html
- https://blog.checkpoint.com/2019/06/19/sandblast-agent-phishing-germany-campaign-security-hack-ransomware/

- https://blog.talosintelligence.com/picking-apart-remcos/
- https://malware-traffic-analysis.net/2017/12/22/index.html
- https://secrary.com/ReversingMalware/RemcosRAT/
- https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2
- https://www.quorumcyber.com/wp-content/uploads/2023/07/Quorum-Cyber-_-REMCOS-Malware-Report.pdf
- https://www.joesandbox.com/analysis/882699/0/pdf
- https://breakingsecurity.net/wp-content/uploads/dlm_uploads/2018/07/Remcos_Instructions_Manual_rev22.pdf

# Apéndice A: Mapa de técnicas de ATT&CK


cyber
zaintza
BASQUE CYBERSECURITY AGENCY