Comprensión y creación de virus P2P (Agosto de 2020)

Jhon Eddi Malagon - 20151020021
Facultad de ingeniería Universidad Distrital Francisco José de Caldas
Bogotá D.C Colombia
jemalagong@correo.udistrital.edu.co

Resumen – Se presentarán diferentes virus para comprender el funcionamiento de estos, su propagación y como afectan al sistema, además de sus protocolos para funcionar o por los cuales se puede propagar, creando concia hacia el conocimiento y la debida programación e implementación de los protocolos dichos virus fueron usados con fines académicos.

Palabras Clave – Virus informático, malware, rasomware, gusano informático, backdoor, red P2P, protocolo SMTP, win32, troyano.

I. INTRODUCCIÓN

Día a día estamos constantemente expuestos a un ataque cibernético mientras navegamos por nuestros sitios favoritos de internet, descargando cantidades impresionantes de información y aplicaciones, muchos de estos resultan en malwares o también conocidos como virus informáticos, disfrazados de aplicaciones, anuncios publicitarios, videos, documentos, entre otros tantos. Para evitar que estos malware nos perjudiquen, desde haciendo la navegación molesta en nuestro dispositivo, hasta el completo fallo total de este.

Cabe mencionar que estos problemas no solo los vivimos usuarios independientes o "casuales" sino también empresas importantes, gobiernos, celebridades entre otros. Muchos de estos fallos se deben a la falta de conocimiento o conciencia al momento de navegar en la web o al configurar nuestro sistema de redes, creando vulnerabilidades las cuales llegan a ser sencillas de explotar, ocasionando problemas al acceso de nuestra información o información importante que nosotros tengamos.

II. MALWARE

Es un término general para referirse a cualquier tipo de "malicious software", diseñado para infiltrarse en un dispositivo sin el conocimiento de la persona. Hay muchos tipos de Malware y cada uno busca sus objetivos de un modo diferente.

Comportamiento:

Funcionamiento: el Malware es descargado o instalado involuntariamente por la persona, infectando el dispositivo. Usualmente la descarga es realizada involuntariamente al hacer click en un vínculo o a través de la visita a un sitio web malicioso.
Dependiendo del tipo de Malware, este puede tener un objetivo de ataque diferente. Se encuentra el ransomware, que funciona bloqueando o denegando acceso a su dispositivo y sus archivos hasta que pague un rescate al hacker. En segundo lugar, está el Spyware, el cual recaba información sobre un dispositivo o red para luego enviársela al atacante. En tercer lugar, están los gusanos, cuyo funcionamiento se basa en infectar un equipo para luego replicarse y extenderse a dispositivos adicionales, permaneciendo activo en todas las máquinas afectadas. En algunos casos son utilizados para instalar malwares adicionales. En cuarto lugar, están también los adwares, cuya función es crear ingresos para el desarrollador a través del uso de la publicidad. Adquieren información de la persona y después la utilizan para personalizar los anuncios mostrados. Otro tipo de Malware es el Troyano, este funciona al ser instalado en el dispositivo luego de que se ha infiltrado proyectándose como software legítimo, ya instalado procede a activarse y en ocasiones descarga malwares adicionales. [1]

¿Cómo se contrarresta?

Medidas de prevención: Algunas medidas de prevención son tener el sistema operativo y el navegador web actualizados, además, es pertinente tener instalado un antivirus y un firewall. Otra medida de prevención es utilizar una cuenta de usuario con privilegios limitados y tener precaución al ejecutar software procedente de internet o de medios extraíbles. Es importante evitar descargar software de redes P2P, ya que no se sabe su contenido ni su procedencia, se debe también desactivar la interpretación de Visual Basic Script y permitir JavaScript, ActiveX y cookies solo en páginas web de confianza. [4]

III. RANSOMWARE

Es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

Todos los virus fueron tomados de: https://gedzac.com

Comportamiento

Este malware funciona a través de la instalación no autorizada del ransomware, debido a que este se encuentra camuflado dentro de otro archivo o programa que pueda ser de interés para el usuario. Una vez que es instalado, se activa y provoca el bloqueo de todo el sistema operativo, presenta un mensaje de advertencia con la amenaza y el importe del rescate que se ha de pagar para recuperar el acceso a la información. [2]

¿Cómo se contrarresta?

Lo primero que se debe tener en cuenta para contrarrestar el ataque de un ransomware es no realizar el pago por el rescate de documentos. Es recomendable solicitar el apoyo de un especialista en seguridad informática para ejecutar un desencriptador adecuado. Otra manera de contrarrestar el ransomware es con la instalación de un producto de seguridad, a través de este se ejecuta un análisis completo para eliminar la amenaza, sin embargo, este método es útil para eliminar la amenaza, pero no asegura la recuperación de todos los productos.
El principal método de prevención contra un ransomware es la inversión en un buen programa antivirus, de manera que proporcione herramientas anti-exploits y anti-ransomware. Es recomendable crear copias de seguridad de los datos del dispositivo con regularidad. Es esencial mantener el sistema operativo y el navegador web actualizados. [5]

IV. Virus

Un virus informático es un programa o código malicioso y autorreplicante que se cuela en un dispositivo sin el conocimiento y/o permiso del administrador.

Comportamiento

Dependiendo de los tipos de virus, estos se clasifican en dos categorías según su funcionamiento: los activos y los inactivos. Los primeros corresponden a aquellos virus que, al momento de instalarse en el dispositivo, empiezan a infectar y a replicarse. Los segundos son los inactivos, estos son activados cuando el usuario ejecuta el código de forma inadvertida. Los virus presentan cuatro fases, siendo la primera la fase durmiente, seguida por la fase de propagación, luego la fase de activación y, por último, la fase de ejecución.

¿Cómo se contrarresta?

Dentro de las medidas de prevención contra los virus se encuentran medidas aplicables también con otros tipos de malwares. Mantener el sistema operativo y el navegador actualizados, instalar un programa de seguridad que realice análisis periódicos y sea capaz de eliminar amenazas. Evitar la instalación de software en sitios desconocidos. [3]

V. Red P2P

Forma coloquial de referirse a las denominadas redes entre iguales, redes entre pares o redes punto a punto. En estas redes no existen ni ordenadores cliente ni ordenadores que hagan de servidor. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. El hecho de que sirvan para compartir e intercambiar información de forma directa entre dos o más usuarios ha propiciado que hayan sido, y estén siendo, utilizadas para intercambiar archivos cuyo contenido está sujeto a las Leyes de copyright, lo que ha generado una gran polémica entre defensores y detractores de estos sistemas.

Las redes peer-to-peer aprovechan, administran y optimizan el uso del Ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, obteniendo más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.

Dichas redes son útiles para diversos propósitos. A menudo se usan para compartir Ficheros de cualquier tipo (por ejemplo, Audio, Vídeo o Software). Este tipo de red es también comúnmente usado en telefonía VoIP para hacer más eficiente la transmisión de datos en tiempo real. La eficacia de los nodos en el enlace y transmisión de datos puede variar según su configuración local (Cortafuegos, NAT, Enrutadores, etc.), velocidad de proceso, disponibilidad de ancho de banda de su conexión a la red y capacidad de almacenamiento en disco. [6]

Red o protocolo	Uso	Programas
ANts P2P	Intercambio de ficheros/Distribución de software/Distribución de multimedia	ANts P2P
Ares	Intercambio de ficheros	Ares Galaxy, Warez P2P, KCeasy, jAres P2P
BitTorrent	Intercambio de ficheros/Distribución de software/Distribución de multimedia	BitTorrent,eMule
DirectConnect	Intercambio de ficheros, chat	DC++, NeoModus Direct Connect, SababaDC, BCDC++, RevConnect, fulDC, LDC++, CzDC, McDC++, DCDM++, DDC++, iDC++, IceDC++, Zion++, R2++, rmDC++, LinuxDC++, LanDC++, ApexDC++, StrongDC++
eDonkey	Intercambio de ficheros	aMule, eDonkey2000 (extinguido), eMule, eMule Plus, FlashGet, iMesh, Jubster, lMule, MLDonkey, Morpheus, Pruna, Shareaza, xMule
FastTrack	Intercambio de ficheros	giFT, Grokster, iMesh (y sus variantes como iMesh Light), Kazaa (y sus variantes como

		Kazaa Lite), KCeasy, Mammoth, MLDonkey, Poisoned
Freenet	Almacenamiento distribuido	Freenet, Entropy (red separada de Freenet)
GNUnet	Intercambio de ficheros, chat	GNUnet, (GNUnet-gtk)
Gnutella	Intercambio de ficheros	BearShare, Cabos, FilesWire, FrostWire, Gnucleus, Grokster, gtk-gnutella, iMesh, Kiwi Alpha, LimeWire (extinguido), MLDonkey, Morpheus, MP3 Rocket, Poisoned, Shareaza, Swapper, XoloX, KCEasy
Gnutella2	Intercambio de ficheros	Adagio, Gnucleus, Kiwi Alpha, MLDonkey, Morpheus, Shareaza, TrustyFiles
JXTA	Aplicaciones distribuidas	Collanos Workplace (Software colaborativo), Sixearch
Kad	Intercambio de ficheros	aMule, eMule, MLDonkey
Napster	Intercambio de ficheros	Napigator, Napster
OpenNap	Intercambio de ficheros	WinMX, Utatane, XNap, Napster
Osiris sps	creación de portales web anónimos	Osiris (Serverless Portal System)
P2PTV	Streaming de video	TVUPlayer, Joost, CoolStreaming, Cybersky-TV, TVants, PPLive, LiveStation,Sopcast
Peercasting	Streaming	PeerCast, IceShare, FreeCast, Rawflow
Pichat	Chat e intercambio de información	Pichat, Pidgin, Moonchat, C4
Usenet	Grupos de noticias	
WPNP	Intercambio de ficheros	WinMX
Windows Peer-to-Peer	Desarrollo de aplicaciones distribuidas, colaboración	ncluido en el Advanced Networking Pack para Windows XP, Windows XP SP2, Windows Vista.

Tabla 1: Protocolos P2P y caracteísticas [6]

VI. Protocolo SMTP

Sus siglas corresponden a la traducción “Protocolo simple de transferencia de correo”. Una manera de describir dicho protocolo: es como la oficina de correos de la web: recoge el email del remitente y lo entrega en la oficina de correos local del destinatario, que es otro servidor SMTP

Cada vez que se envía un email mediante el protocolo SMTP, se abre una nueva sesión del servicio de retransmisión SMTP. A continuación, se llevan a cabo una serie de intercambios de información entre el cliente de email y el servidor SMTP de destino, como si de una conversación se tratara.

Entre los clientes más conocidos está el Outlook, que pertenece a Microsoft, y Thunderbird, que es gratuito y pertenece a Mozilla.[7]

Cuando se envía un email a través del protocolo de retransmisión SMTP, lo que se produce es la validación de una serie de comandos de texto (de la cadena de caracteres ASCII), que posteriormente son enviados a un servidor SMTP. Por lo general, se utilizan los puertos 25 o 587.

En este proceso no entra en juego el contenido del correo electrónico, sino que la atención del lenguaje SMTP define exclusivamente en la transmisión.

Cada vez que se envía un email mediante el protocolo SMTP, se abre una nueva sesión del servicio de retransmisión SMTP. A continuación, se llevan a cabo una serie de intercambios de información entre el cliente de email y el servidor SMTP de destino, como si de una conversación se tratara. [8]

VII. Win32

Es un tipo de aplicación que ofrece soporte para arquitecturas x86 y que hasta ahora han sido la moneda habitual a la hora de contar con cualquier utilidad en nuestros equipos. Tanta es su importancia que el esfuerzo radica ahora en permitir su uso en procesadores ARM y en las futuras versiones ligeras de Windows.[9]

Algunas de estas características son:

- Estas aplicaciones suelen contar con extensiones muy conocidas como .exe o .msi.
- A las mismas instaladas se accede desde Panel de control > Programas > Programas y características.
- Pensadas para ser usadas sobre todo con periféricos tradicionales como teclado y ratón.
- Aunque cuentan con permisos limitados, algunas se pueden ampliar y el usuario puede darles permisos de administrador.
- Se puede abrir la misma aplicación en un mismo equipo varias veces.
- Son compatibles con las versiones de Windows XP, Windows Vista, Windows Vista, Windows 7, Windows 8.1 y Windows 10.
- Se pueden instalar desde distintas fuentes: página web del desarrollador, discos USB, desde la nube...
- Las aplicaciones Win32 pueden distribuirse por cualquier medio y se pueden instalar desde cualquier fuente: sitios web, medios ópticos, redes, etc.
- Las aplicaciones de escritorio pueden tener cualquier tipo de modelo de licencia.
- Escapan del control de Microsoft a menos que sean descargadas desde la Tienda de Microsoft. Los desarrolladores establecen las bases de cada aplicación.
- Las aplicaciones Win32 sólo funcionan en procesadores Intel y AMD con arquitectura x86 y de forma normal no pueden por ahora funcionar en procesadores ARM.

VIII. VIRUS WIN.32REDES

Este virus es una adaptación propia del virus win32.LinkinPark del autor Khronos. [10]

Es un malware tipo gusano, el cual su método de infección consiste en transmitirse por medio de dispositivos extraíbles como lo son discos duros externos, USB y por medio del protocolo de red P2P. Infectando programas de descarga como ares, emule entre otros, donde creara ficheros que se abrirán ante el usuario en forma de html, en este caso dentro de las carpetas y el programa emule:

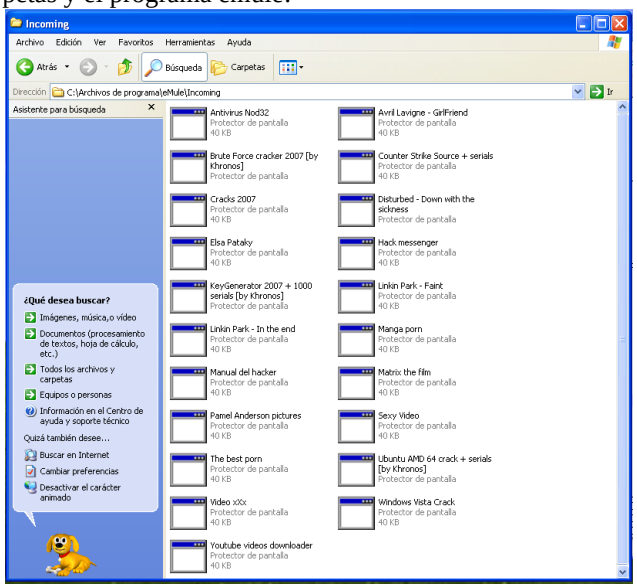

Imagen 1: Captura de los archivos generados por el virus

Este virus se puede catalogar como "inofensivo" ya que no altera archivos importantes dentro del computador, además que es sencillo de eliminar, permitiendo experimentar con este para comprender la lógica de programación detrás de este y de otros virus y como se pueden propagar mediante que secuencias.

IX. VIRUS NJ1.3

También conocido como virus NetJoe [10], este es un virus de espionaje cuya estructura es la de un backdoor, permitiendo disfrazarse de alguna aplicación para pasar desapercibido.

El virus Backdoor, comúnmente suele ser un troyano que abre una puerta trasera en el sistema de tu computadora y permite que un hacker remoto tome el control de tu equipo sin que lo sepas. El virus Backdoor puede copiarse a sí mismo e instalar nuevas actualizaciones usando Internet. [11]

Consta de dos ejecutables, uno el cual funciona como servidor que será el que envía información, es decir la "víctima", el segundo ejecutable es el que recibe información además de poder interactuar de manera remota con el sistema de la "víctima", accediendo a información y diversos aspectos del sistema.

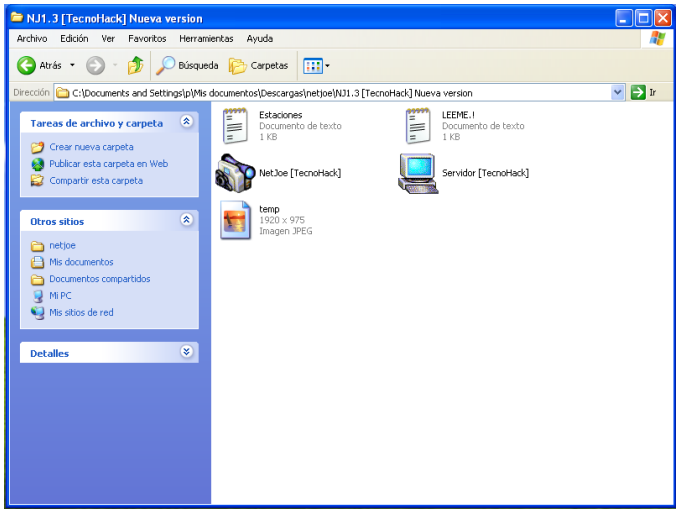

Imagen 2: Captura de los ejecutables NJ1.3

Además, puede tener acceso a la cámara del dispositivo, a la información del sistema, los programas ejecutándose y poder interactuar con ellos como cerrarlos abrirlos, bloquearlos, desbloquearlos.

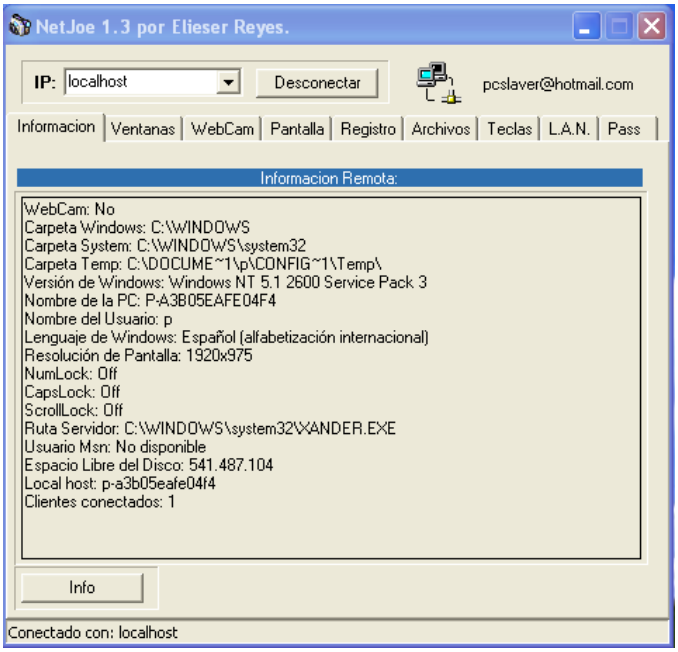

Imagen 3: Información del PC "víctima"

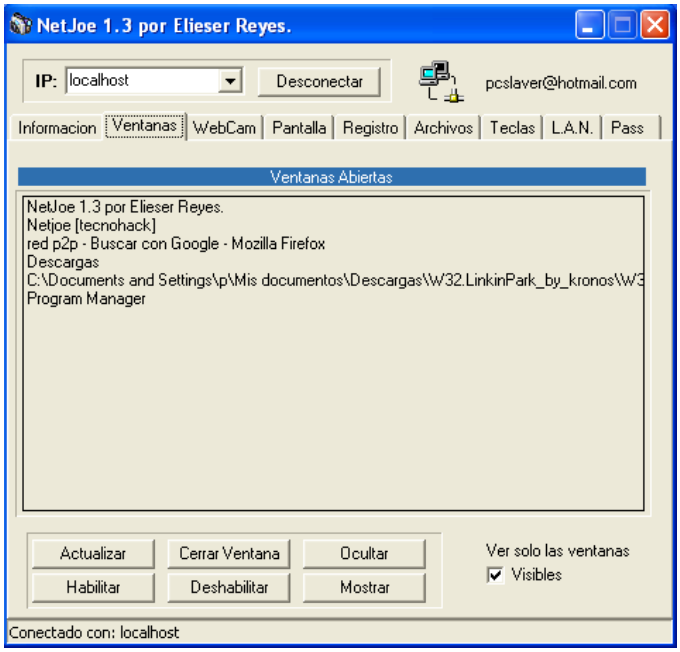

Imagen 4: Información de los programas abiertos

El virus también cuenta con la capacidad de poder tomar capturas de pantalla para conocer la vista y el estado de la "víctima", además de acceder y manipular los diferentes archivos dentro del dispositivo

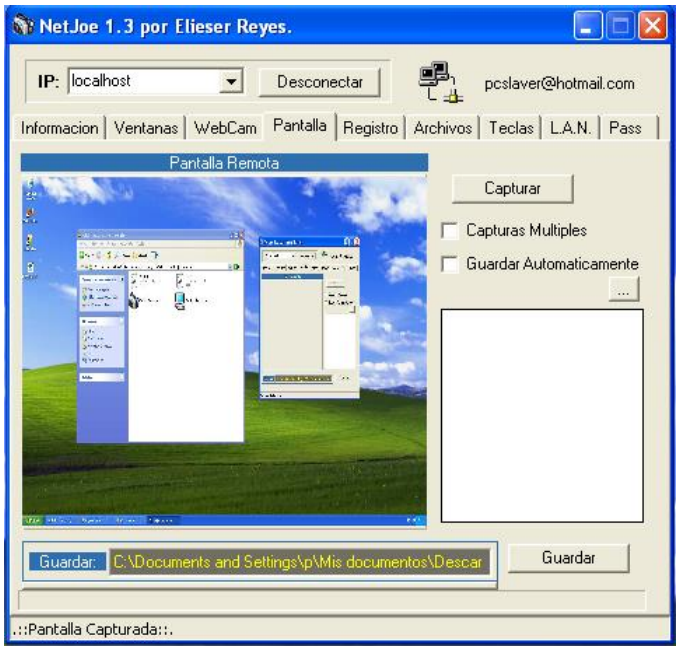

Imagen 5: Captura hecha por el software

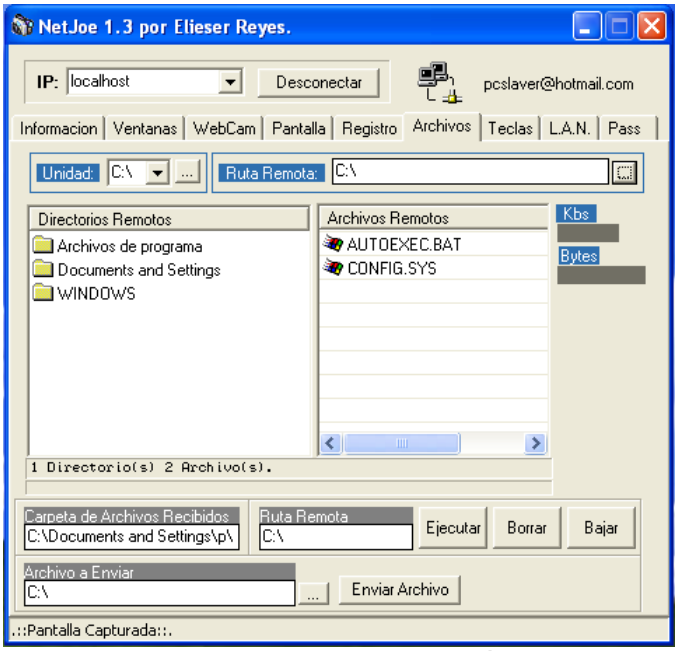

Imagen 6: Vista de los archivos de la "víctima"

X. VIRUS KAY.A

Es un virus del tipo troyano, el cual es mucho más agresivo que los anteriores expuestos, teniendo la capacidad de infectar cualquier ejecutable, pudiendo replicarse en todas las unidades disponibles e infectándolas a la vez, es decir teniendo la capacidad de ser un virus retroviral. [10]

Al momento de infectar el dispositivo, este quedará residente dentro de la memoria RAM, siendo un poco más complicado el rastrearlo, dejando programas basura instalados dentro del disco local del sistema operativo junto con la carpeta System32, recordemos que esta carpeta es donde se encuentran los programas fundamentales para el buen funcionamiento de Windows.

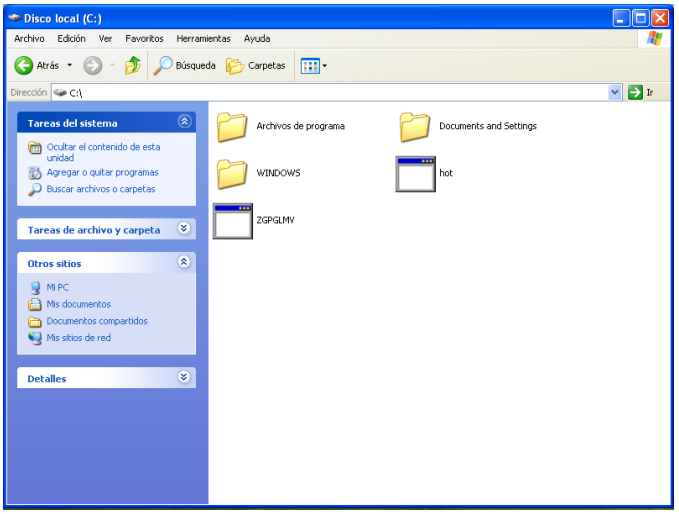

Imagen 7: Archivos creados por el virus

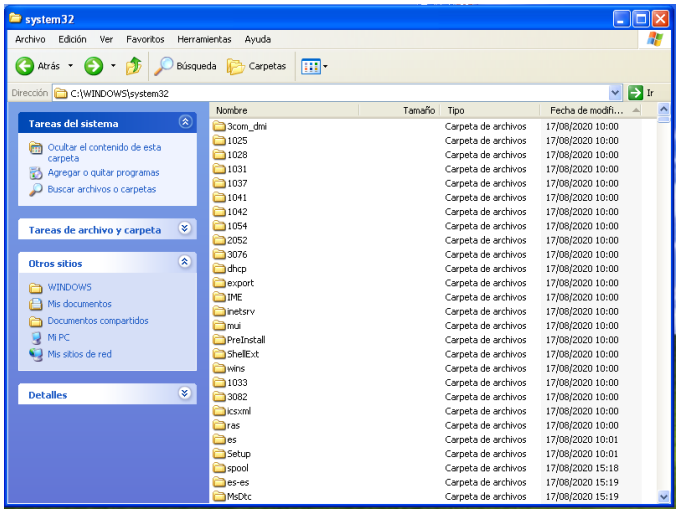

Imagen 8: Archivos creados o modififcados por el virus

Este virus puede llegar a incapacitar el acceso a aplicaciones como lo sería el administrador de tareas, aplicaciones de búsqueda web, entre otras, además de impedir en ocasiones que el sistema operativo inicie adecuadamente.

XI. Virus Memz

Es un virus extremadamente agresivo y peligroso, ya que posee la capacidad de inutilizar el sistema operativo en cuestión de minutos, afectando el funcionamiento de aplicaciones, impidiendo que se logren abrir correctamente o de lo contrario que estén abriendo y cerrándose automáticamente sin que el usuario haya interactuado con ellas, además de cambiar aspectos como el color de la pantalla, la velocidad y precisión del mouse, creando ventanas emergentes de advertencia o peligro, junto con su sonido de advertencia en el sistema, ejecutándose de manera indiscriminada, este virus es obra de Leurak.

Imagen 9: Ejemplo del funcionamiento del virus Memz

Al intentar desactivar este virus, creará una reacción aún peor, el sistema se descontrolará de manera veloz y en cuestión de segundos el sistema operativo quedará completamente inutilizado.

XII. Conclusión

Los virus expuestos en este documento y trabajo tienen un grado un poco menor a los que solemos encontrar en nuestro día a día, pero eso no significa que sean inofensivos o que estén obsoletos, muchos de estos virus funcionan en máquinas con sistemas operativos recientes, además que con un poco más de tiempo y esfuerzo estos virus pueden presentar un gran problema en los diferentes computadores si no se tiene las debidas precauciones para hacer frente a estas amenazas.

Cabe mencionar que los virus expuestos se aprovechan de no solo de las vulnerabilidades de un computador mal protegido sino también de una red con debilidades en sistemas de protocolos y firewall, permitiendo la libre infección de los diferentes dispositivos y dando a conocer la importancia de la debida configuración pertinente en los protocolos de red junto con sus cuidados.

References

[1] Belcic, I. (2019). “La guía esencial del Malware:detección, prevención y eliminación.” [Interntet]. Disponible en: https://www.avast.com/es-es/c-malware

[2] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. En: Almgren, M., Gulisano, V., & Maggi, F. (2015). Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, 3-24. DOI: 10.1007/978-3-319-20550-2_1

[3] Latto, N. (2020). “La guía esencial sobre virus informáticos. Sitio web: Avast-Academy.” [Internet]. Disponible en: https://www.avast.com/es-es/c-computer-virus

[4] Malwarebytes, (2020) “¿Qué es el malware?” [Internet]. Disponible en: https://es.malwarebytes.com/malware/

[5] Malwarebytes, (2020). “Ransomware: qué es y cómo eliminarlo.” [Internet] Disponible en: https://es.malwarebytes.com/ransomware/

[6] EcuRed. “Red Peer to Peer” [Internet]. Disponible en: https://www.ecured.cu/Red_Peer_to_Peer#Redes.2C_protocolos_y_aplicaciones

[7] M Gonzalez, (2011). “Protocolo SMTP: cómo se envían y reciben los emails a través de internet” [Internet]. Disponible en: https://www.xatakamovil.com/conectividad/protocolo-smtp-como-se-envian-y-reciben-los-emails-a-traves-de-internet#:~:text=Para%20la%20transferencia%20de%20estos,de%20normas%20para%20el%20envío

[8] . Redondo, (2020). “¿Qué es un servidor SMTP y por qué se usa?” [Internet] Disponible en: https://es.mailjet.com/blog/news/servidor-smtp/#significado

[9] J. Antonio (2019) “¿Conoces las diferencias entre una aplicación Win32 y una descargada sólo desde la Tienda de Microsoft? Las repasamos en 11 puntos” [Internet] Disponible en: https://www.xatakawindows.com/aplicaciones-windows/conoces-diferencias-aplicacion-win32-descargada-solo-tienda-microsoft-repasamos-11-puntos

[10] Repositorio de virus Gedzac [Internet] Disponible en: https://gedzac.com

[11] Techlandia. [Internet]. Disponible en: https://techlandia.com/informacion-virus-backdoor-hechos_163844/

[12]