



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Detección automática temprana y actuaciones correctivas contra
virus de tipo ransomware en redes corporativas*

Grado en Ingeniería Mecánica

ALUMNO: Javier Montenegro Portela

DIRECTORES: Guillermo Rey González
Pedro Orgeira Crespo

CURSO ACADÉMICO: 2018-2019

Universida_deVigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Detección automática temprana y actuaciones correctivas contra
virus de tipo ransomware en redes corporativas*

Grado en Ingeniería Mecánica
Intensificación en Tecnología Naval
Cuerpo General / Infantería de Marina

UniversidadeVigo

RESUMEN

El presente Trabajo de Fin de Grado busca la validación de un programa presentado por los tutores del mismo para la detección automática temprana y actuaciones correctivas contra virus de tipo ransomware en redes corporativas. Más adelante se desarrollará la problemática que hace necesaria dicha solución, se probará la misma a nivel local y se plantearán unas conclusiones de acuerdo con las pruebas realizadas.

Se destaca que el autor del TFG no es el autor del programa que se está validando, sino que se limita a probarlo y a comprobar el correcto funcionamiento del mismo, explicando sus ventajas respecto a lo utilizado normalmente a día de hoy.

PALABRAS CLAVE

Ransomware, Ciberseguridad, Virus, Informática

AGRADECIMIENTOS

Primeramente, quería agradecer con completa sinceridad la realización de este trabajo a mi familia, amigos y tutores. Sin su muy estimada ayuda nunca hubiera sido capaz de cumplir con la exigencia de un proyecto y una carrera como estos. Es también digno de mención el apoyo de todos mis camaradas, los que han estado junto a mí a lo largo de los años o sólo durante unos días, compartiendo mis aventuras y desgracias. Si soy nada es gracias a ellos.

Estos cinco años me han proporcionado una oportunidad de crecer como persona. Han sido alegrías, han sido presión y han sido recuperación. Doy mi agradecimiento a quien haya formado parte de ellos.

CONTENIDO

Contenido	1
Índice de Figuras	3
1 Introducción.....	5
1.1 Planteamiento del problema.....	5
1.2 Solución a evaluar	5
1.3 Requerimientos	6
2 Estado del Arte	7
2.1 Evolución vírica	7
2.1.1 Descripción	7
2.2 Ransomware.....	10
2.2.1 El concepto	10
2.2.2 Historia	10
2.3 Esquemas de redes corporativas	15
2.3.1 Principales tipos de redes.....	15
2.3.2 Seguridad corporativa	18
2.3.3 Servidores y almacenamiento	21
2.4 Redes en el entorno Microsoft	22
2.4.1 Estructura genérica	22
2.4.2 Directorio Activo	24
2.4.3 CIFS	24
2.4.4 El registro de Windows	25
2.4.5 WMI.....	27
2.5 Entorno de desarrollo	28
2.5.1 Visual Studio 2017	28
2.5.2 C#.....	30
2.5.3 Refactorización de código	30
2.6 La ciberseguridad y el ransomware en las Fuerzas Armadas Españolas	31
3 Desarrollo del TFG.....	34
3.1 Esquema de bloques de funcionamiento	34
3.1.1 Modo Normal.....	35
3.1.2 Modo Paranoico	39
3.2 Comparativa entre modos	39
4 Validación del sistema.....	40

4.1 Prueba del programa	40
5 Conclusiones y líneas futuras	45
6 Bibliografía.....	47

ÍNDICE DE FIGURAS

Figura 2-1 Mensaje ejecutado por el programa Elk Cloner, obtenido de [4]	8
Figura 2-2 Mensaje programado en <i>Brain</i> , según imagen obtenida de [7]	9
Figura 2-3 Instalación del programa AIDS Information, donde se aloja el virus, obtenida de [8] ..	10
Figura 2-4 Aviso emitido por el virus una vez activado, obtenida de [8]	11
Figura 2-5 Aviso para realizar el pago, obtenido de [13]	12
Figura 2-6 Mensaje del virus WannaCry proporcionando instrucciones para el pago. Obtenida de [23]	14
Figura 2-7 Ejemplo de una LAN, obtenida de [30]	16
Figura 2-8 Dos redes LAN conectadas por una red WAN, obtenida de [29]	17
Figura 2-9 Funcionamiento de un DMZ con dos firewalls de apoyo, obtenido de [32]	17
Figura 2-10 Capas de seguridad de una red, obtenida de [33]	18
Figura 2-11 Esquema simplificado de un cortafuegos, obtenida de [33]	18
Figura 2-12 Conexión entre dos equipos según modelo OSI, de elaboración propia	19
Figura 2-13 Red de equipos con un <i>switch</i> que utiliza un <i>router</i> para conectarse a Internet [38] ...	20
Figura 2-14 El bosque de dominios α está formado por los árboles 1 y 2, que a su vez aglutinan los dominios A-B y C-D (respectivamente). A su vez, cada dominio tendría diversos equipos. Elaboración propia	23
Figura 2-15 Relación unilateral entre dos dominios representados por un equipo, de elaboración propia.	23
Figura 2-16 Relaciones de confianza entre dominios individuales, árboles y bosques. Cada dominio, representado por un equipo, puede estar compuesto de múltiples dispositivos. Elaboración propia.	24
Figura 2-17 Captura de pantalla del Editor del Registro, de obtención propia.	25
Figura 2-18 El registro permite tanto la administración local como la remota. Imagen obtenida de [45]	26
Figura 2-19 Diagrama con la arquitectura del WMI, obtenido de [48]	28
Figura 2-20 Cuadro de diálogo “Nuevo Proyecto” donde se está creando una solución, obtenida de [50]	30
Figura 2-21 Boletín informativo enviado por el MCCD, obtenido de [59]	32
Figura 3-1 Captura del Explorador de soluciones de VS2017.	34
Figura 3-2 Captura del Editor de Registro de Windows con las entradas que se evalúan en el cuadro rojo.	35
Figura 3-3 Captura del código, donde se ven las extensiones a comprobar en el caso de ficheros Office.	36
Figura 3-4 Parte del proyecto en la que se evalúan los bytes iniciales del archivo “.dwg”.	36
Figura 3-5 Código de ejecución para archivos de imagen.	37

Figura 3-6 Código con las direcciones de comprobación del registro.	37
Figura 3-7 Código para notificación por correo. La dirección está tapada por protección de datos.	38
Figura 4-1 Interfaz del programa. Presentación en equipo administrador de red.	40
Figura 4-2 Modificación del registro añadiendo la entrada “Prueba” (en azul).....	41
Figura 4-3 Monitor de registro cuando se detecta una clave no autorizada.	41
Figura 4-4 Fichero “clavesregistro.txt” con la entrada “probando” al final, de forma que queda validada.	41
Figura 4-5 Señal de error en caso de no localizarse el fichero que debe ser monitorizado.....	42
Figura 4-6 Ventana de monitorización al detectar un posible fichero de petición de rescate.	42
Figura 4-7 Ventana de comprobación de ficheros, informando de los que deben comprobarse.....	43
Figura 4-8 Elementos cifrados detectados: Imagen, PDF y fichero de ofimática.	43

1 INTRODUCCIÓN

1.1 Planteamiento del problema

Cada vez es más patente la integración de la sociedad en el mundo digital. En cierto modo, podría llegar a decirse que la gente nace conectada a la red. Sin embargo, esta conexión cibernética puede considerarse un serio riesgo, más aún conociendo los ataques que ya han tenido lugar. Empresas paralizadas, servicios públicos neutralizados, pérdidas millonarias de información... El avance de la sociedad la hace más vulnerable de lo que se cree frente a los ataques de aquellos con el conocimiento y los recursos necesarios para llevarlos a cabo.

Uno de estos métodos de ataque es el conocido como ataque de ransomware, el cual se explicará más adelante. Existente desde hace más de 30 años, sigue siendo una amenaza presente en los principales foros de seguridad informática. Sin embargo, poco o nada puede hacerse contra un ataque que a veces llega a niveles de cifrado dignos de inteligencia militar, llegándose a acusar a gobiernos de estar detrás de ellos en algunos casos.

La necesidad de defenderse de este tipo de ataques es algo innegable en caso de grandes empresas y organismos, pues pueden acarrear enfrentarse a pérdidas millonarias tanto directa como indirectamente, siendo los gastos directos los utilizados para pagar el rescate y los indirectos los ocasionados por la negación del acceso a la información necesaria para el ejercicio de las funciones de la empresa.

Las redes de los grandes organismos, como podrían ser las redes corporativas de las FAS, son susceptibles de este tipo de ataques. Un ordenador infectado puede comprometer toda la red a la que se encuentra conectado gracias a conceptos que se explicarán más adelante como los dominios o las relaciones de confianza en el entorno de Microsoft.

1.2 Solución a evaluar

Las medidas de actuación frente al ransomware son muy limitadas a día de hoy, por lo que en este TFG se presenta un software proporcionado por los tutores del mismo, capaz de proporcionar una alarma temprana y unas reacciones iniciales rápidas para poder mitigar los efectos del ataque, cuando no evitarlo completamente.

La mentalidad detrás de esta solución, tal y como se explicará más adelante, suponen apartarse del planteamiento tradicional en materia de defensa contra ransomware, ofreciendo una alternativa nueva que se presenta como más eficiente.

Se destaca que el objetivo del presente proyecto no es la programación de software de detección de ransomware, sino la evaluación y validación de la solución propuesta por los tutores ante el problema planteado.

1.3 Requerimientos

Para poder utilizar correctamente el sistema de detección hace falta un equipo con el sistema operativo Windows 10 Pro instalado y una cuenta con permisos de administrador. Para un uso real del programa haría falta un dominio con las IP de los equipos pertenecientes a ellos conocidas (lo cual tiene sentido en un entorno corporativo, donde personal de seguridad informática estaría supervisando la consola de alarmas, entre sus otras tareas), pero la evaluación se realizará en el propio equipo, por lo que la creación de la red no es algo necesario.

Para la implementación de la solución en una red corporativa, aparte de la lista de IP de los equipos, es necesario el control como administrador del dominio, para garantizar el acceso a los diferentes equipos y sus archivos de forma remota.

2 ESTADO DEL ARTE

2.1 Evolución vírica

2.1.1 Descripción

Cuando se habla de los virus informáticos, es importante conocer varios aspectos sobre ellos: qué son, cómo funcionan, qué motivo puede haber detrás de ellos, etc. Y no siempre es fácil responder a estas preguntas.

En general, cuando se habla de virus en el ámbito de la tecnología, uno se refiere a un programa que cumple una característica concluyente: es capaz de replicarse a sí mismo y modificar el software del ordenador sin el consentimiento del usuario [1]. No debe olvidarse que un virus puede alcanzar la simplicidad de apenas un par de líneas de código. Sin embargo, a medida que avanzan los sistemas de seguridad de los ordenadores y la complejidad de sus defensas, también debe avanzar la complejidad los agentes que intentan modificar los equipos.

La cada vez mayor dependencia de la sociedad moderna ha hecho a ésta cada vez más vulnerable frente a ataques informáticos. Por esto es primordial concienciar a la sociedad sobre ciberseguridad, así como establecer unas pautas mínimas de seguridad informática que estén al alcance de la mayoría de los usuarios.

Antes de continuar, debe analizarse la principal característica de un virus: debe ser ejecutado. El virus no puede inventarse a sí mismo, sino que el usuario debe darle el poder de actuar. La mayoría de las veces, esto se logra a través de engaños, haciendo que el usuario crea que está ejecutando un programa inocente o abriendo un archivo que necesita (véase el caso de CryptoLocker, sin ir más lejos). Esta acción inocente, fruto del engaño del que se es víctima, hace que el ordenador otorgue los permisos de ejecución al programa malicioso, dándole al virus el poder que necesita para cumplir su función.

Dicha función puede ser tan variada como a uno se le ocurra. Hay virus prácticamente inofensivos, creados normalmente a modo de prueba o como una broma, limitándose a presentarle al usuario un mensaje ofensivo o ejecutar otros programas del ordenador. Sin embargo, también los hay capaces de eliminar archivos, bloquearlos, borrarlos o directamente formatear todo el ordenador.

Ya en 1949 el matemático húngaro John von Neumann propuso la posibilidad de crear programas de ordenador capaces de autorreproducirse, en lo que entonces parecía una idea futurista. Una idea que se adelantaba por poco más de 20 años al que se considera como primer virus informático: *Creeper*.

El *Creeper* aparece en 1971 como un experimento informático. Este programa se limitaba a pasar de un ordenador a otro a través de la red ARPANET (*Advanced Research Projects Agency Network*, o

Red de la Agencia de Proyectos de Investigación Avanzada). La peculiaridad de este virus es que, después de replicarse en el siguiente ordenador, se borra a sí mismo en el equipo del que sale, dando una sensación de que es un único programa que salta de un lado a otro más que un virus autorreplicante. Aunque no estaba programado para afectar a los archivos del usuario, sí que se cree que provocó la pérdida de ficheros al reproducirse demasiado rápido, desbordando la memoria del sistema y llevando a la destrucción involuntaria de información almacenada. [2]

Como no podía ser de otra forma, la aparición del primer virus llevó directamente a la creación del primer antivirus. Así, en 1972 nace el *Reaper*, un virus cuya función consiste en replicarse por la red para encontrar el virus objetivo que pretende destruir. Debido a su comportamiento vírico y su función, este tipo de programas reciben el nombre de *nematodes* [3] en honor a los nemátodos, un tipo de gusanos utilizados en control de plagas. Sin embargo, el uso de virus para acabar con otros virus es una práctica poco aceptada por muchas de las principales empresas de antivirus, que lo ven como un método poco eficiente de solucionar el problema. [1]

No sería hasta 1982 cuando aparecería el primer virus fuera de un laboratorio. En este año, un joven estudiante de secundaria desarrolló un programa capaz de autorreplicarse para el sistema operativo Apple DOS. Ofreciendo un disquete a sus amigos cercanos con una versión pirata de algún juego, éstos infectaban sus ordenadores con el código escondido junto al juego. A partir de ese momento, cada vez que se iniciaba el juego se activaba un contador que, al llegar a los 50 inicios del juego, bloqueaba el ordenador y mostraba el mensaje de la figura 2-1. Tras infectar un equipo, el programa se replicaría en los disquetes que se introdujeran en él para posteriormente infectar los diferentes ordenadores en los que se usaran, expandiéndose de esta forma. Una simple broma infantil que no llegó demasiado lejos antes de ser detectado y eliminado. [4]

A screenshot of a text message displayed in a monospaced font, likely from a terminal or a simple text editor. The text is green on a black background. It reads: "Elk Cloner: The program with a personality. It will get on all your disks. It will infiltrate your chips. Yes it's Cloner! It will stick to you like glue. It will modify ram too. Send in the Cloner!"

Figura 2-1 Mensaje ejecutado por el programa Elk Cloner, obtenido de [4]

Pese a todo lo dicho, lo cierto es que el término virus no sería aplicado a la informática hasta que en 1984 Frederick B. Cohen publicara un documento titulado “Virus de ordenadores – Teoría y Experimentos” [5]. En él, desarrolla el concepto de esta amenaza a la seguridad tanto individual como colectiva a la que los usuarios de equipos informáticos se exponen continuamente. En ese mismo trabajo, se plantea la posibilidad de un virus creado para automatizar la compresión de archivos en el ordenador. Sin embargo, como se ha mencionado anteriormente, este uso de los virus no es considerado aceptable por los profesionales en el desarrollo de antivirus, ya que todo virus de este estilo implica realizar cambios no autorizados en el software del ordenador. Aceptar programas que sobrepasen las limitaciones del ordenador y el control del usuario es una debilidad de seguridad que debe ser activada, en cualquier caso.

Pero para hablar del primer virus verdaderamente en libertad se debe avanzar todavía un par de años, hasta 1986. En enero de este año se libera a la red el *malware* conocido como *Brain*. Pese a lo tedioso del proceso de infección, ya que no se llega a propagar por la red, sí que supuso un grave problema a ambos lados del Atlántico, causando auténticos estragos en Europa y América. El código del virus se limitaba a modificar el sector de arranque del disquete, mostrando el mensaje que se puede observar en la figura 2-2 y renombrando el arranque como ©*Brain*. Si bien no modificaba los archivos localizados en los equipos infectados, el espacio que ocupaba en la memoria del disco duro del ordenador o del disquete correspondiente podía suponer una importante pérdida de información, siendo este el mayor problema que supuso. Los programadores incluyeron su número de contacto para que los dueños de equipos infectados pudieran encontrar una solución, pero no se esperaban la repercusión que tuvieron: miles de llamadas colapsaban la línea continuamente. [6]

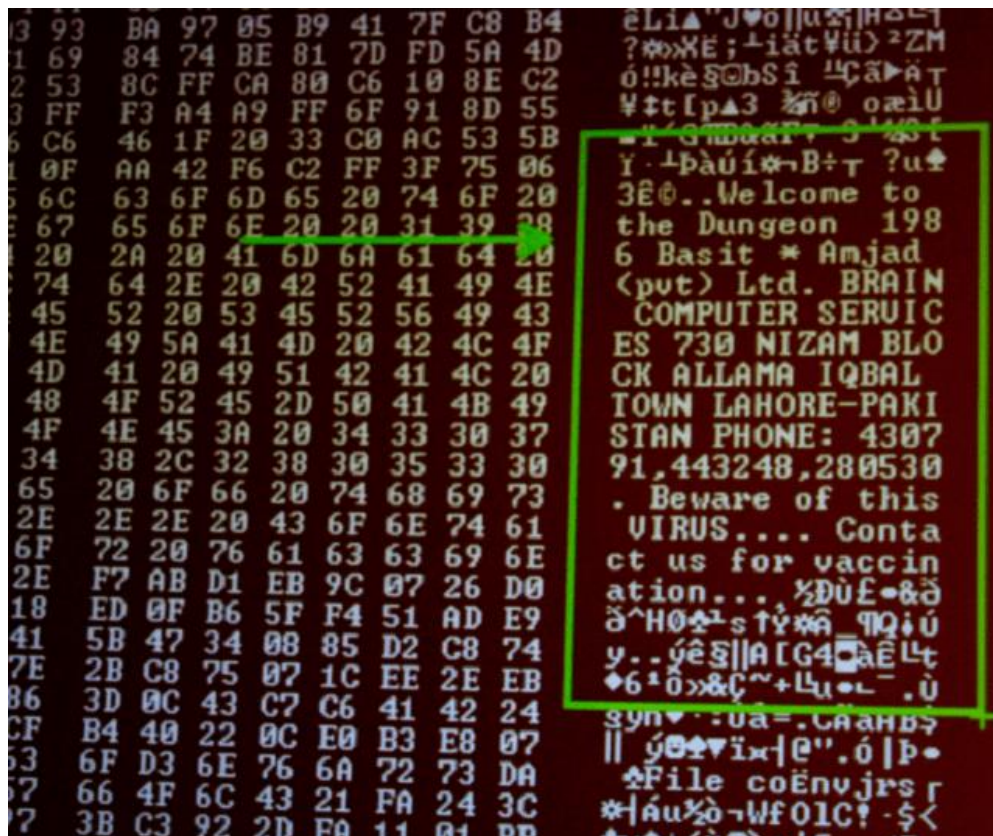


Figura 2-2 Mensaje programado en *Brain*, según imagen obtenida de [7]

En los años siguientes, muchos serían los *softwares* maliciosos que surgirían, incluso llegando a causar auténticos desastres a nivel global. Robos de información, bloqueo de cuentas o ficheros, chantajes, filtraciones y muchas más acciones ilegales son sólo algunas de las posibilidades que ofrecen los virus. Y, al igual que las vacunas, también son utilizados con la intención de probar los más modernos antivirus. En muchos casos, los mayores hackers acaban trabajando para empresas de seguridad después de haber sido capaces de burlar sus defensas, siempre con la intención de mejorar el sistema de protección. Igualmente, son muchas las empresas (especialmente agencias gubernamentales por funciones de recopilación de información) que intentan detectar los fallos de seguridad de los principales sistemas operativos con la intención de explotarlos en su propio beneficio.

2.2 Ransomware

2.2.1 El concepto

Ransomware (acrónimo de “*ransom software*” traducido literalmente como software de rescate) es una amenaza surgida a finales del siglo XX cuya intención es, a grandes rasgos, secuestrar los archivos de un usuario mediante el uso de software malicioso, exigiéndosele posteriormente el pago de un rescate para recuperarlos.

Este bloqueo de la información, si bien a veces tan simple en cuanto a programación y desarrollo que los usuarios no se han visto obligados ni a pagar el rescate, ha llevado al desarrollo de un concepto relativamente reciente debido a sus vertientes más agresivas y peligrosas: la criptovirología (“*cryptovirology*”, en inglés). Esta rama de la informática se dedica al estudio de la criptología para el desarrollo de malware, con la intención de ser capaces de burlar los cada vez más poderosos antivirus. Al fin y al cabo, no se debe olvidar que la rama vírica de la ciberseguridad es una guerra de evolución constante entre los creadores de virus y los que los combaten.

A modo de resumen, se podría decir que el ransomware se limita a provocar que el usuario habitual de una computadora sea incapaz de acceder a sus propios archivos, proporcionando además las instrucciones necesarias para completar el pago correspondiente (o los pasos a seguir, según las intenciones del creador) y recuperar el acceso a los archivos.

2.2.2 Historia

Como se ha mencionado en el apartado anterior, el concepto de *ransomware* surge a finales del siglo XX. Pero en los escasos treinta años que han pasado desde el primer uso de un software malicioso con el fin de extorsionar a un usuario, son muchas las variaciones que han sido desarrolladas, algunas de forma más efectivas que otras. Aquí se realizará un rápido repaso a esta evolución.

2.2.2.1 AIDS Information Trojan

El primer virus de ransomware conocido es el llamado Troyano del AIDS Information, o *PC Cyborg Trojan*. Creado por Joseph Popp en 1989, este virus se aloja en el ordenador objetivo mediante la instalación de un falso programa dirigido a una lista concreta de destinatarios. Cerca de 20 000 personas recibieron por correo el disquete de instalación del programa *AIDS Information*, el cual garantizaba proporcionar información para ayudar en la prevención de contraer el SIDA (figura 2-3).

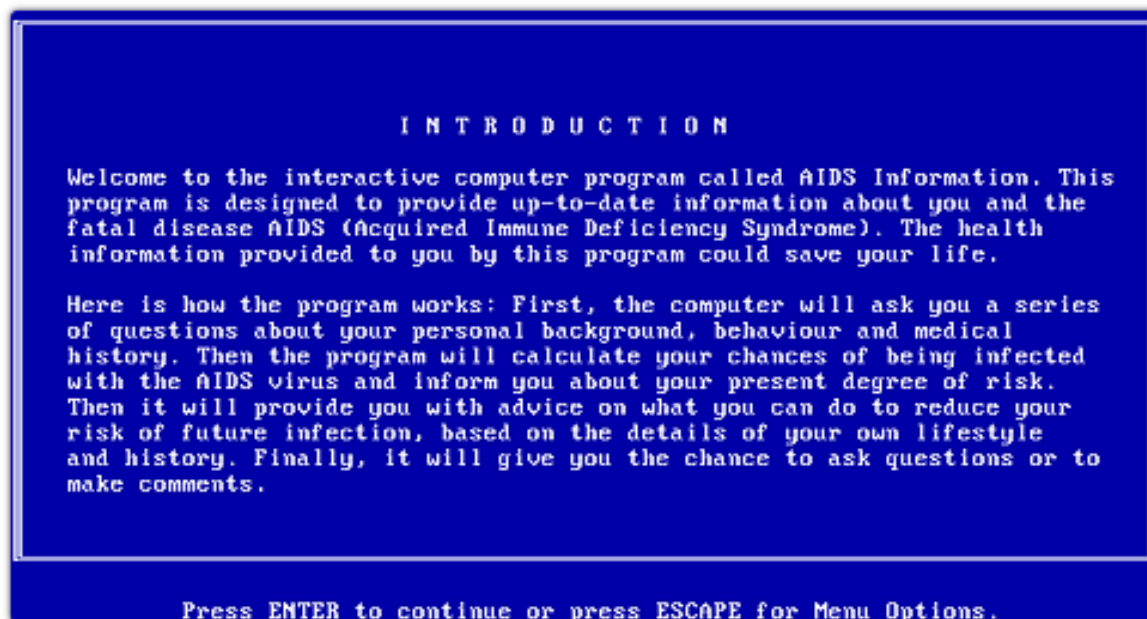


Figura 2-3 Instalación del programa AIDS Information, donde se aloja el virus, obtenida de [8]

Una vez instalado, el virus arranca un contador, sumando una unidad cada vez que el usuario inicia su equipo. Una vez la cuenta llega a 90, el virus oculta los directorios y cambia el nombre de los archivos del disco local C: haciendo que el equipo se vuelva inutilizable. En este momento, el virus le hace saber a la víctima que su licencia ha expirado y que debe “renovarla”, realizando un pago de 189\$ anuales (o 378\$ por una licencia a perpetuidad) a una dirección en Panamá [9], tal como se puede observar en la figura 2-4.

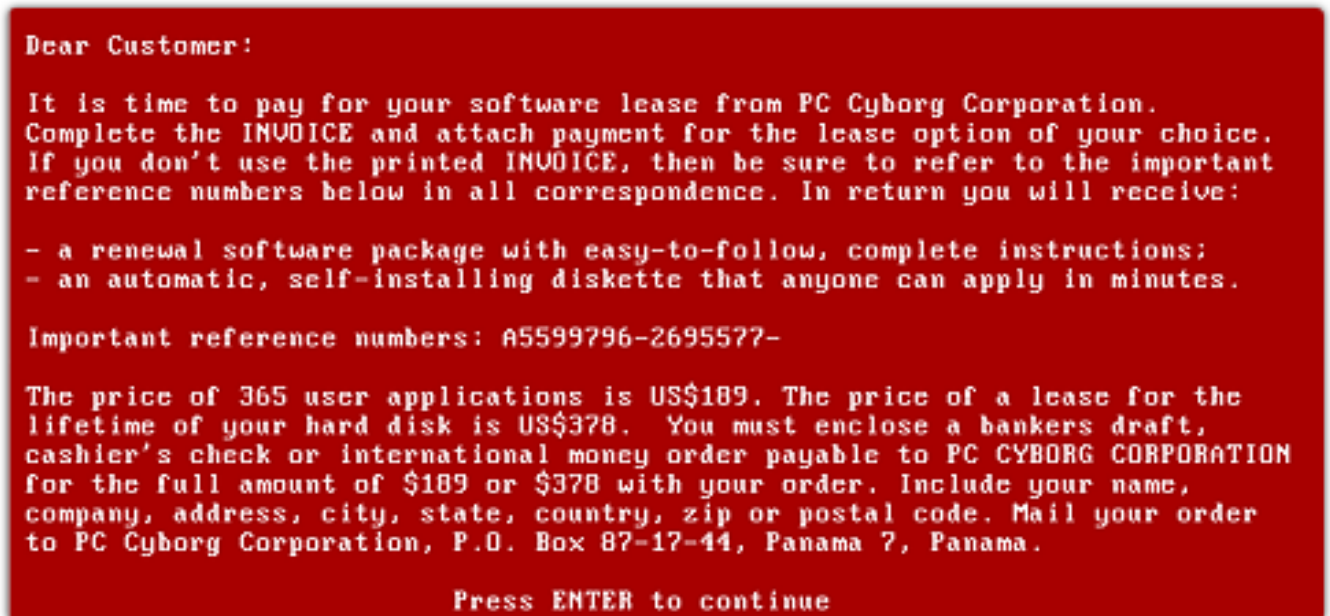


Figura 2-4 Aviso emitido por el virus una vez activado, obtenida de [8]

El doctor Joseph Popp fue finalmente detenido por el FBI después de que en Inglaterra se promulgara una orden de arresto con su nombre. Fue descubierto gracias a un equipo de ciberseguridad británico, que fue capaz de relacionarle con el software después de analizar el código. Durante el juicio, Popp afirmó que el dinero obtenido mediante la extorsión era utilizado para apoyar la investigación contra el SIDA. [10]

Según la investigación policial, el software fue instalado por cerca del 5% de usuarios que lo recibieron. Esto supuso un alcance de cerca de 1 000 equipos infectados sólo por este virus. [11]

2.2.2.2 CryptoLocker

En un ejemplo mucho más reciente, aparecido a finales de 2013, se tiene el caso del virus conocido como *CryptoLocker*. Coincidiendo con un rápido crecimiento del bitcoin, la moneda virtual más exitosa en la última década hasta su reciente caída bursátil, los creadores de este virus fueron capaces de hacerse con millones de dólares en apenas unos meses. Este malware bloquea el acceso a los archivos mediante el uso de una clave privada, conocida sólo para el creador del virus y alojada en un servidor oculto hasta que la víctima pague el rescate, añadiendo la presión de que el mensaje de aviso amenaza con destruir dicha clave si no se paga en un plazo de 72 horas, volviendo definitivamente inaccesibles todos los archivos infectados. [12]



Figura 2-5 Aviso para realizar el pago, obtenido de [13]

El rescate necesario alcanzaría los 300\$ o los 300€, como se refleja en la figura 2-5, aunque podía ser menor dependiendo del método de pago. El primer método se realiza mediante un sistema de tarjetas prepago-recargables (*MoneyPak*) en múltiples partes de los EEUU, donde se encontraban los principales objetivos de este ataque. Si no, como alternativa, el programa dejaba realizar el pago mediante la transferencia de bitcoins.

El bitcoin (฿) es una criptomoneda, una forma de divisa electrónica que permite el pago anónimo entre usuarios de Internet. No está centralizada, encontrándose todos los movimientos comerciales grabados en una suerte de registro público distribuido llamado *blockchain* (cadena de bloques). En este registro se incluyen todas las transacciones confirmadas. Usando criptología se garantiza la integridad y el orden cronológico de dicho registro. [14]

Esta moneda, surgida en 2009, tuvo su primer gran crecimiento precisamente a finales del 2013, y mientras que a mediados de septiembre de ese año un bitcoin podía equivaler a 120\$ con escasas fluctuaciones, el 28 de noviembre se alcanzó un pico de más de 1 000\$ por cada bitcoin. Esto provocó que este método de rescate tuviese que modificarse, pasando de unos dos bitcoins en principio a menos de 0,3฿ durante el punto álgido de esta criptomoneda. A los chantajistas les interesaba que el cliente buscara el pago mediante bitcoin, ya que ofrece un mayor anonimato y una menor trazabilidad debido a la gestión de las transacciones, que evitan que ninguna de las partes se conozca realmente. Por ello debían procurar que el pago mediante bitcoin saliera siempre más rentable que el pago a través de *MoneyPak*. [15]

La instalación del virus se realizaba de la misma manera que se ha realizado durante este último tercio de siglo: la víctima lo instalaba voluntariamente. En lo que parecía un correo electrónico inocente [16] se añadía un archivo adjunto disimulado como PDF, el cual resultaba ser el ejecutable del propio programa. Gracias a la previsualización de los nombres de los archivos de Windows que hace que la extensión de los mismos permanezca invisible durante la mayor parte del tiempo, la extensión .EXE quedaba oculta y la víctima ejecutaba el virus. Esto provocaba que el software malicioso se guardara a sí mismo en la carpeta de aplicaciones locales, creando a continuación una entrada en el registro del ordenador que le permitía autoejecutarse al iniciar sesión.

Aparte, el equipo infectado sufría también modificaciones en los archivos .EXE para que, en cuanto se ejecutara cualquier otro programa, el ordenador intentara eliminar todas las *Shadow Copies*

guardadas en el ordenador. Estas “copias sombra” son un servicio adicional de Windows que permite crear copias de seguridad de diferentes archivos, ya sea automática o manualmente. Teniendo en cuenta que el objetivo del *CryptoLocker* era impedir el acceso de la víctima a sus propios archivos, poder recuperar estas copias no cifradas supondría un fallo en su programa. Al finalizar la eliminación de dichos archivos de recuperación, el ejecutable regresaría a su forma habitual de Windows. El virus también era capaz de trasladarse por redes corporativas para hacer el máximo daño posible, inutilizando empresas u organismos enteros por culpa de un error cometido por un equipo.

Un dato destacable del funcionamiento de este malware es la modificación del registro de Windows del ordenador. Mientras que el *AIDS Information Trojan* no alteraba el registro del ordenador por no existir éste todavía en el momento de su liberación, este nuevo virus lo modifica para poder ejecutarse de forma automática con el arranque del ordenador. El registro, como se explica más adelante, es una base de datos de Windows que el sistema operativo usa de referencia continuamente, ya que se va actualizando con la información de los usuarios, los programas instalados, los elementos de hardware que forman parte del sistema, etc. [17]

Este virus utiliza la clave de registro “HKEY_CURRENT_USER\Software\CryptoLocker_????” (donde ???? identifica la versión del virus utilizada) para guardar la información de configuración. Dentro crea un directorio llamado “Files” (archivos) donde almacena la información de todos los archivos cifrados por él. Una vez pagado el rescate, esta lista es procesada por la herramienta de descifrado para liberar los archivos. Al dar un nombre a los valores de los archivos cifrados, *CryptoLocker* se limita a coger la ruta del archivo y sustituye todos los valores “\” por “?”. En un ejemplo, este mismo documento pasaría de ser “C:\Users\Media\Documents\TFG.docx” a “C:?Users?Media?Documents?TFG.docx”.

Finalmente, en junio de 2014, el Departamento de Justicia de los Estados Unidos anunció oficialmente que una operación multinacional contra el botnet *Gameover Zeus*, utilizado para la distribución de este malware y otros similares, así como la obtención de los servidores centrales de *CryptoLocker*. Se estima que para abril de 2014 este virus habría infectado más de 234 000 ordenadores, y que más de 27 millones de dólares fueron obtenidos sólo en los dos primeros meses a partir de este chantaje. [18] [19]

Poco después de los primeros ataques de *CryptoLocker*, los creadores notaron que mucha gente no pagaba no por falta de voluntad o desapego a sus archivos, sino por falta de tiempo. Por ello, se empezó a ofrecer la posibilidad de comprar la clave una vez pasados los tres días. El usuario afectado debería subir un archivo cifrado para poder cotejarlo con la base de datos de los servidores. Una vez encontrada el cifrado exacto, se le ofrecería la clave de descifrado. Por supuesto, esta segunda oportunidad tenía un sobrecoste que llegó a alcanzar los 10 bitcoins, en el momento de los primeros pagos. Huelga decir que esto sirvió para que la gente pagara más rápido en cuanto le llegaba el aviso. [20]

2.2.2.3 WannaCry

Como caso más reciente de ataque de ransomware a nivel internacional se analizará el caso del virus *WannaCry*. Surgido en mayo de 2017, este ataque estaba dirigido a ordenadores con el sistema operativo Windows aprovechando un *exploit* conocido como *EternalBlue*. Este ataque de ransomware, a diferencia de los anteriores, no se prolongó en el tiempo, durando apenas unos días.

EternalBlue es un *exploit* desarrollado por la NSA (Agencia de Seguridad Nacional de los Estados Unidos), según reconocerían algunos empleados de esta dicha agencia [21]. Este fallo de seguridad se basa en un fallo en el protocolo *Server Message Block* (Servicio de Bloqueo de Mensajes). El *SMB* funciona en la capa de aplicación del modelo OSI, permitiendo la interconexión de diferentes equipos que pertenezcan a una misma red LAN o a una red corporativa. Si bien el objetivo inicial de este protocolo era poder compartir archivos o conectarse a impresoras locales para facilitar el trabajo de los

operadores, se demostró que podía ser utilizado para producir grandes daños si no se tomaban las medidas de protección necesarias.

Gracias al *EternalBlue*, se podrían mandar órdenes a ordenadores pertenecientes a una misma red. Esto es lo que aprovecha el *WannaCry* para propagarse por toda una red de equipos en cuanto uno ejecuta el virus. El *malware* utiliza este fallo para enviarse a sí mismo a todos los equipos disponibles, ejecutarse y cifrar los archivos que encontrara para posteriormente exigir un rescate como se observa en la figura 2-6. [22]



Figura 2-6 Mensaje del virus WannaCry proporcionando instrucciones para el pago. Obtenida de [23]

El ataque se produjo apenas un mes después de que un grupo de hackers conocido como *Shadow Brokers* filtraran el *EternalBlue*, en una serie de filtraciones de *malware* creado por la NSA y que supuso un gran escándalo para el gobierno de los Estados Unidos. Según especulaciones anteriores a la propia filtración, se podría tratar de un movimiento llevado a cabo desde dentro, por alguien perteneciente a la misma NSA. [24]

En una rapidísima reacción, Microsoft desarrolló un parche en apenas un par de días que solucionaba el problema del *EternalBlue*, protegiendo a los usuarios del programa malicioso. Debido a que había una gran cantidad de usuarios con sistemas ya fuera del ciclo de soporte (como Windows XP, para el que dejaron de publicarse actualizaciones de seguridad en 2014), Microsoft se vio obligado a crear también parches concretos para este sistema operativo, especialmente vulnerable y desprotegido, en una acción sin precedentes. [25]

Si bien el ataque fue enfrentado con una gran velocidad, debido a la importancia de las redes locales en entornos empresariales y corporativos, cientos de sistemas sufrieron el bloqueo de sus archivos, viéndose obligados a pagar el rescate correspondiente. Según estimaciones, en las primeras 24 horas el virus habría entrado en más de 75 000 equipos a lo largo de no menos de 99 países, provocando diversos problemas en grandes empresas de todo el mundo. En Francia, la producción de Renault tuvo que ser detenida. Del mismo modo, en España, importantes agencias como Telefónica o Iberdrola sufrieron el ataque y vieron buena parte de sus archivos bloqueados. El Ministerio de Interior ruso informó que 1 000 de sus sistemas fueron infectados. Sin embargo, algunas de las peores

consecuencias se vieron en el Reino Unido, donde hasta 48 centros del *National Health System* (Sistema Nacional de Salud) se vieron incapaces de acceder a los historiales de sus pacientes, así como a las agendas informatizadas que tuvieran en sus equipos. Esto provocó que miles de citas se tuvieran que cancelar, llegando a aplazarse importantes intervenciones quirúrgicas. [26]

Sin embargo, el ataque podría haber sido mucho peor. Algo que realmente ayudó a evitar que el virus se propagara increíblemente más rápido fue el descubrimiento accidental por parte de un analista informático de un *kill switch* (herramienta de apagado forzoso) en el código del programa. Este método de autodestrucción incorporado en el propio virus fue descubierto mientras realizaba ingeniería inversa en el código del *malware* con la intención de encontrar algún tipo de información sobre el ataque. Sobra decir que nunca imaginó encontrar algo así. [27]

En diciembre de 2017, países como Estados Unidos o Reino Unido afirmaron oficialmente que el ataque había sido orquestado por Corea del Norte. Por supuesto, el gobierno de este país negó cualquier implicación en el ataque. Lo cierto es que a día de hoy no se sabe a ciencia cierta quién o quiénes están detrás de la creación de este *ransomware*. [28]

2.3 Esquemas de redes corporativas

2.3.1 Principales tipos de redes

Cuando se habla de redes de ordenadores se puede recurrir a conceptos tan genéricos y amplios como el propio Internet, también conocido como la “red de redes”. Sin embargo, reduciéndolo al uso de redes corporativas, será tratado como el sistema que regula y facilita la interconexión entre diferentes equipos, pertenecientes a un mismo entorno donde la comunicación es importante para el buen funcionamiento de la empresa u organización que los posee. Sin embargo, no todas las redes se organizan igual, distinguiéndose diversas estructuras que más adelante serán estudiadas. [29]

Para que una red pueda funcionar correctamente, es necesaria una conexión de los equipos, ya sea por cable o inalámbrica. En las conexiones por cable, además, se diferencian las conexiones por cable de cobre (donde se transmiten señales eléctricas) o las conexiones por fibra óptica (donde se transmiten señales de luz).

Al analizar las redes, se deben analizar los cuatro elementos que, entre otras cosas, la definen al definir la comunicación entre los equipos pertenecientes a la red. Estos elementos son: reglas, medios, mensajes y dispositivos.

Las reglas son el nombre que reciben los diferentes protocolos que permiten la comunicación entre dos equipos de una misma red. De este modo, así como el servicio WWW (*World Wide Web*) utiliza el protocolo HTTP (*HiperText Transport Protocol*), la telefonía IP utiliza el protocolo SIP (*Session Initiation Protocol*). Es el lenguaje utilizado para enviar y recibir la información necesaria.

Los medios no son más que la forma física de establecimiento de la red. Y, como se ha señalado anteriormente, estos se subdividen en dos categorías principales: los medios por cable o los inalámbricos. Las redes por cable suelen permitir una red más fiable y más rápida, mientras que usar un medio inalámbrico permite la creación de redes muy rápidamente, con un crecimiento también más rápido gracias al uso de repetidores de señal.

Los mensajes son los paquetes de información que deben transmitirse, el conjunto de datos cuyo acceso desde diferentes dispositivos se encuentra detrás de la creación de la red. Para que la transmisión de este tipo de información entre sistemas informáticos sea posible, es primordial convertir el mensaje a bits antes de procesarlo. Este proceso de convertirlo a bits se hace independientemente de la naturaleza del mensaje, lo que significa que pasará por ello ya sea un archivo de texto, una imagen, un audio, un vídeo o cualquier otro tipo de datos.

Finalmente, se habla de los dispositivos, que no son sino aquellos elementos que conforman la red. Esto incluye los denominados como “dispositivos de fin” (ordenadores, consolas, teléfonos, impresoras), que son aquellos que se usan para transmitir o para recibir la información, así como los “dispositivos intermedios” (módems, switches, routers, servidores de comunicación, dispositivos de seguridad, ...), que son los que posibilitan la comunicación entre los diferentes dispositivos de fin y facilitan el correcto funcionamiento y la eficiencia de la red.

A continuación, se realizará un breve análisis de los principales tipos de red que se usan a nivel corporativo hoy en día:

2.3.1.1 LAN

LAN (*Local-Area Networks*, o Redes de Área Local), es la denominación que tradicionalmente recibían las agrupaciones de dispositivos bajo una administración común que se encuentran en un área geográficamente reducida y que persiguen el mismo objetivo en una organización (figura 2-7). Sin embargo, una LAN puede ser tanto un grupo de usuarios en una planta concreta de un edificio, como también puede utilizarse para describir a todos los usuarios de un campus con múltiples edificios. Esto se debe a que la palabra “Local” del nombre ha evolucionado junto a la tecnología, perdiendo la necesidad de la cercanía geográfica a medida que la conexión informática facilita la superación de este tipo de barreras.

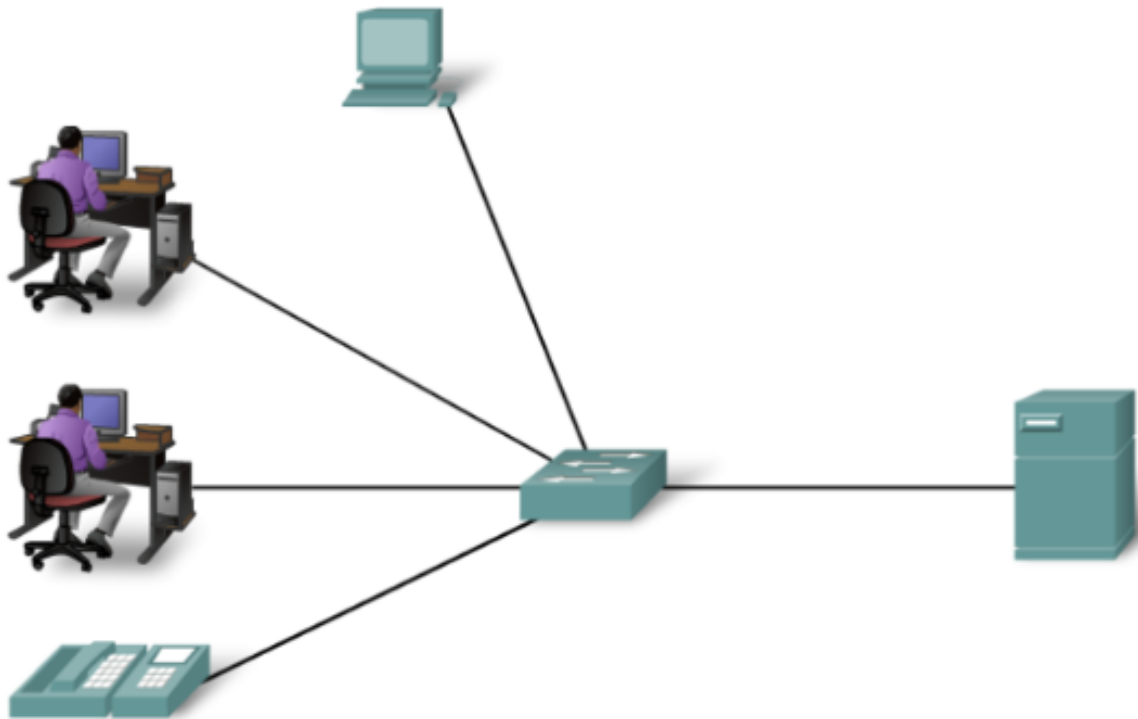


Figura 2-7 Ejemplo de una LAN, obtenida de [30]

2.3.1.2 WAN

WAN (*Wide-Area Networks*, o Redes de Área Amplia) es el nombre que recibe una red utilizada para conectar dos redes LAN muy separadas geográficamente. Si una compañía dispone de oficinas en diferentes ciudades, ésta deberá contratar un Proveedor de Servicios de Telecomunicaciones (TSP) que proporcione líneas de comunicación entre las LAN. El TSP controla todos los dispositivos intermedios de la red WAN que transporta los mensajes, mientras que las redes LAN de ambos extremos están controladas por la compañía contratante del TSP. Una red WAN sólo tiene por propósito conectar LAN, y no suele disponer de dispositivos de fin. La relación entre ambas redes se puede ver gráficamente en la figura 2-8.

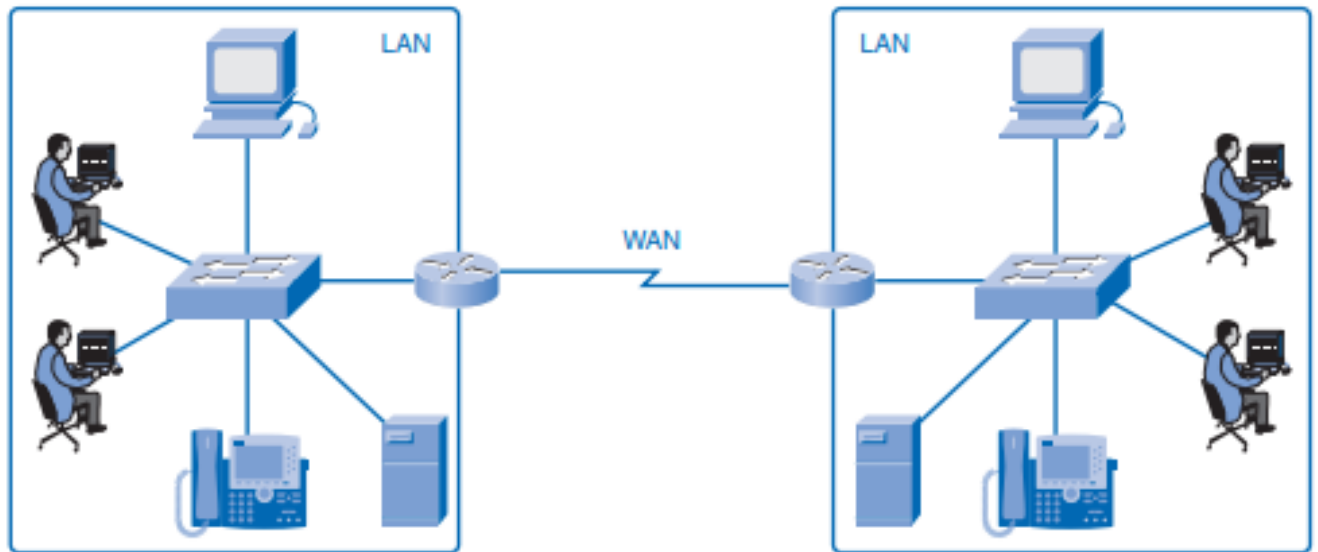


Figura 2-8 Dos redes LAN conectadas por una red WAN, obtenida de [29]

2.3.1.3 DMZ

DMZ (*DeMilitarized Zone*, o Zona Desmilitarizada) es un término utilizado en las redes informáticas para referirse a una configuración de red local diseñada para mejorar la seguridad mediante la separación de equipos a ambos lados de un *firewall*. Una DMZ puede ser establecida tanto en centros de trabajo como en hogares, aunque su utilidad es menor en estos últimos. [31]

La máxima utilidad de este tipo de configuraciones se da en centros de trabajo corporativos, donde las empresas pueden usar una DMZ para que el equipo que aloja un servidor quede de cara al público, mientras que los equipos de trabajo propios de la empresa quedan a salvo detrás del *firewall* frente a un ataque.

Un auténtico DMZ establece una subred completamente nueva fuera de la protección del firewall. Estos equipos desprotegidos suponen una capa extra de protección para los ordenadores detrás del cortafuegos, ya que todas las solicitudes entrantes son interceptadas y deben pasar a través de un equipo de la DMZ antes de llegar siquiera al *firewall*. Los DMZ más avanzados también restringen las comunicaciones de los ordenadores tras el firewall para evitar que se comuniquen directamente con los dispositivos del DMZ, haciendo que sus mensajes salgan a través de la red pública.

Los DMZ se pueden crear con diversas capas de apoyo de *firewall* para proteger grandes redes corporativas.

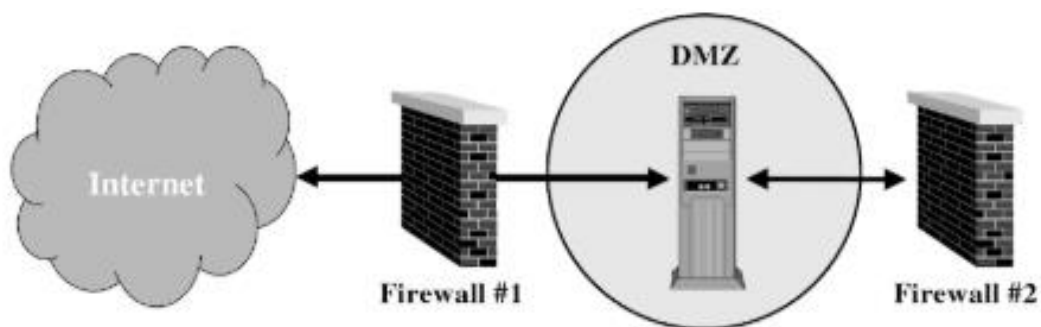


Figura 2-9 Funcionamiento de un DMZ con dos firewalls de apoyo, obtenido de [32]

2.3.2 Seguridad corporativa

Entre los diferentes elementos que ofrecen seguridad a las redes corporativas, se van a destacar los siguientes tres: *firewall*, *router* y *switch*. Como el título de este subapartado indica, estos elementos a analizar son algunos de los diferentes sistemas que se utilizan por las empresas para controlar el tipo de paquetes que entran y salen de sus redes, así como para gestionar las comunicaciones entre los diferentes equipos y evitar la intrusión de programa maligno en las redes.

2.3.2.1 Firewall

Debido a la falta de soluciones que proporcionen seguridad absoluta, una red debe ser construida con una serie de capas que formen una barrera frente a acciones externas. El fin de esta barrera debe ser proteger la información almacenada en los equipos de la red, especialmente en los servidores. Como se puede ver en la figura 2-10, el *firewall* sería la más externa de esta serie de capas.

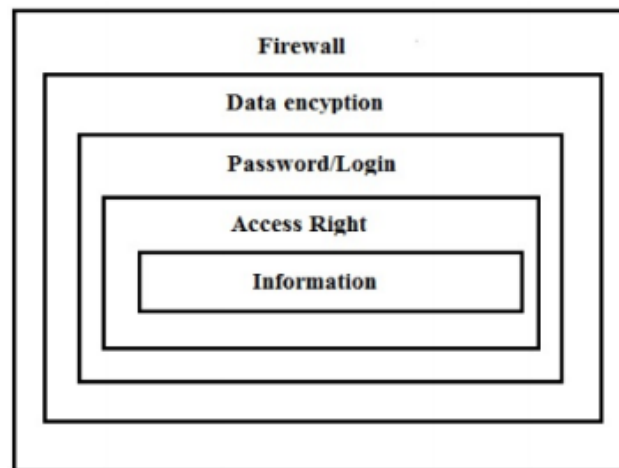


Figura 2-10 Capas de seguridad de una red, obtenida de [33]

Los *firewalls* (en español, cortafuegos) pueden encontrarse en un *hardware* especializado o vía software en un equipo anfitrión. Los primeros suelen ser más complicados, más caros y más difíciles de instalar; son equipos físicos que protegen redes LAN completas ocupando un lugar fuera de la conexión e impide los accesos indeseados. Los localizados en equipos anfitriones, por otro lado, no son más que un software ejecutado por un ordenador individual, por lo que no tiene la misma capacidad de recursos que los de *hardware* especializado. Son utilizados por pequeñas empresas o por equipos individuales, y simplemente permite o restringe la transmisión de información en una red siguiendo una serie de reglas básicas. La idea general, de una forma muy básica, se puede observar en la figura 2-11.

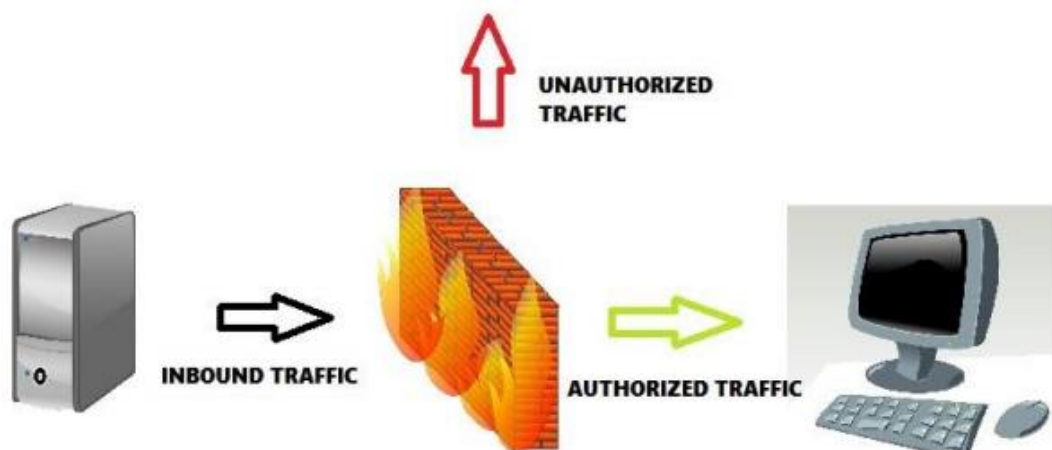


Figura 2-11 Esquema simplificado de un cortafuegos, obtenida de [33]

Las funciones básicas de un cortafuegos moderno son gestionar y controlar el tráfico en la red, autenticar los accesos, proteger los recursos de los equipos conectados, grabar e informar de los eventos que puedan suceder y actuar como intermediario entre los diferentes dispositivos. Sin embargo, esto no es aplicable a los cortafuegos tradicionales, que apenas son una capa exterior de protección que no puede realizarlo todo.

Un cortafuegos tradicional no es sino una máquina artificial, incapaz de clasificar la información como “buena” o “mala”. Sólo puede bloquear el tráfico siguiendo unos parámetros claramente definidos por un operario. Aún más, un cortafuegos tradicional no puede evitar un ataque si el ataque no va a través de él. Básicamente, no puede evitar la filtración o el robo de información cuando ésta se realiza mediante una copia física (mediante acceso físico al equipo donde se almacena la información). Esto se debe a que ese robo se realiza mediante un acceso a un dispositivo de fin en la propia red LAN, y el cortafuegos se encuentra posicionado fuera de dicha red, protegiéndola frente a amenazas de carácter informático.

Finalmente, un cortafuegos tradicional no puede actuar como un antivirus continuamente debido a la velocidad de procesamiento, la aparición continua de virus y la encriptación de datos que se utiliza para ocultar los virus que debe ser enfrentada con antivirus específicos. Sin embargo, sigue siendo uno de los métodos de protección más comunes. Además, la (no tan) nueva generación de firewalls, bajo el paradigma UTM, sí cubre las carencias históricas de los firewalls tradicionales, ofreciendo entre otros filtrado basado no sólo en capa 3-4, sino en capa 7, autenticación de usuarios con integración en AD, análisis vírico en tiempo real, y un largo etcétera. [33]

2.3.2.2 Router

Un *router* es un dispositivo electrónico capaz de enlazar múltiples redes en principio independientes mediante el uso de medios inalámbricos o físicos. En términos técnicos, un *router* es una puerta de enlace que funciona en el nivel tres del modelo OSI, lo que significa que se encuentra en la capa de red. Es en esta capa donde el *router* va a gestionar la conexión entre ambos equipos, tal como se puede observar en la figura 2-12. Como ejemplo en usos domésticos, un router básico facilita una conexión genérica a Internet, de donde se redirigirá el paquete de información al destino mediante el uso de otros *router* o dispositivos similares. [34]

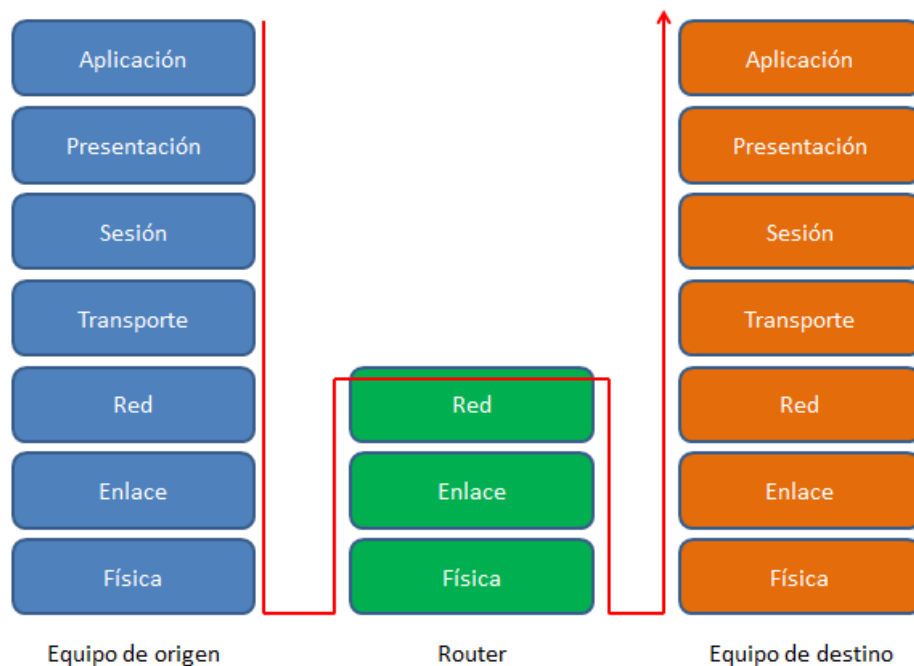


Figura 2-12 Conexión entre dos equipos según modelo OSI, de elaboración propia

La arquitectura de un router se compone de dos partes principales. Estos componentes, aunque interrelacionados físicamente, realizan funciones mayormente independientes la una de la otra. Estas partes son el “plano de control” y el “plano de conmutación”.

El plano de control es la parte encargada de estudiar la topología de la red. Mediante algoritmos de encaminamiento cada vez más sofisticados, en esta sección se registra y se almacena una suerte de mapa con los diferentes puntos de encaminamiento que debe seguir un paquete para alcanzar su destino de la forma más eficiente posible. Debido al funcionamiento de dichos algoritmos, lo normal es que este planeo de la red sea más fiable cuantas más transferencias de paquetes se hayan realizado. [35]

El plano de conmutación, por otra parte, define a la parte del *router* que decide qué hacer con los paquetes. En la mayoría de los casos, se trata de una base de datos en la que el *router* comprueba la dirección de destino de los paquetes entrantes y recupera la información necesaria para determinar el camino por el que ha venido. Tras este análisis, en ciertos casos se da que el *router* debe deshacerse del paquete entrante por cuestiones de seguridad informática, tras lo que es posible que envíe un mensaje de error al remitente para informarle de que la transmisión no ha completado su recorrido. Sin embargo, debido a ciertas políticas de seguridad, son muchos los *router* que los eliminan sin enviar dicha notificación, por el simple hecho de no informar a un posible atacante de que el sistema cuenta con este tipo de defensas. [36]

2.3.2.3 Switch

Un *switch* es un dispositivo de red utilizado para enlazar diferentes equipos en una red. Funciona de forma similar al *router*, con la principal diferencia de que uno se utiliza para conectar equipos y el otro se utiliza para conectar redes. Sin embargo, esto no impide que un dispositivo pueda llegar a ser utilizado en sustitución del otro, ya que hoy en día son muchas las marcas comerciales que ofrecen switches capa 3, con capacidades avanzadas de routing. [37]

En una red diseñada apropiadamente, los *switch* son los responsables de dirigir y controlar el flujo de información a nivel local. Otra diferencia con los *router* es que, mientras estos últimos trabajan normalmente en la capa 3 del sistema OSI, los *switch* suelen llevar a cabo sus acciones en el nivel 2, aunque tienen funciones que afectan a varios niveles de dicho sistema.

De forma parecida a los *router*, son capaces de descartar paquetes considerados peligrosos de acuerdo con unos parámetros introducidos manualmente. Sin embargo, esta es una funcionalidad que no se suele utilizar, ya que los *switch*, por lo general, se utilizan en redes donde el acceso ya es limitado y no se encuentran tan expuestas. De todas formas, siempre se pueden usar para proporcionar una capa extra de protección.

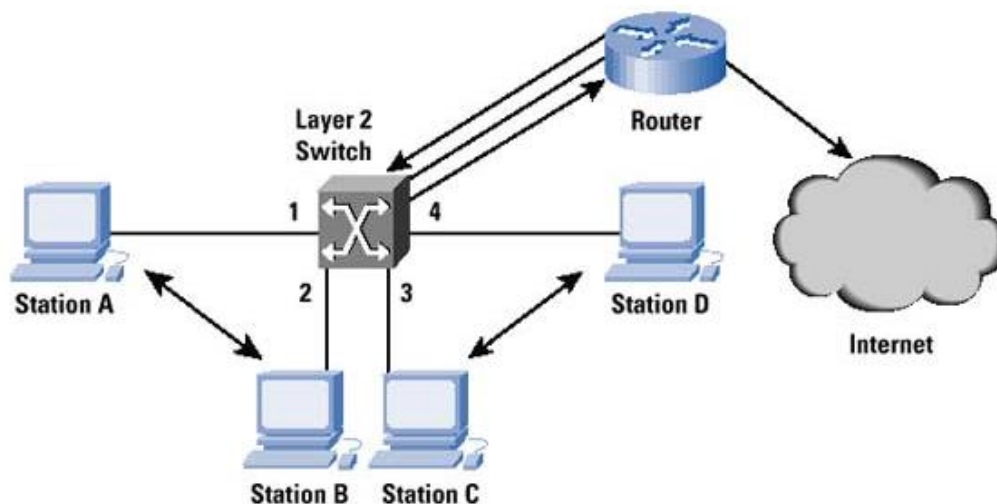


Figura 2-13 Red de equipos con un switch que utiliza un router para conectarse a Internet [38]

2.3.3 Servidores y almacenamiento

La información se almacena en unidades de disco duro, desde los cuales puede ser leída o sobrescrita. Dependiendo de los métodos utilizados para realizar estas tareas y la tecnología con la que se construyeron dichas unidades, la función de lectura/escritura puede ser más o menos rápida. Sin embargo, el almacenamiento de información en un único lugar puede suponer un peligro, pues no son pocas las causas que conllevan la pérdida del acceso a dicha información o, peor aún, la eliminación del mismo. Por ello, lo normal es disponer de varias de estas unidades con el fin de asegurar la buena gestión de nuestra información. Independientemente de las copias de seguridad que se haga de dicha información.

En las redes, estas unidades de almacenamiento normalmente son recursos de ordenador compartidos, en los que un equipo anfitrión permite al resto de equipos de la red el acceso a la información. En este punto, se estudiarán dos conceptos: el NAS y el SAN.

2.3.3.1 Network-Attached Storage (NAS)

El NAS, conocido en español como almacenamiento conectado en red, es la tecnología dedicada a facilitar el acceso de diferentes equipos a la información almacenada en otro equipo con el que estén conectados. En lugar de utilizar un equipo genérico y configurarlo o eliminar contenido para dedicarlo al almacenamiento, se utiliza una computadora cuya única función es el almacenamiento y la transferencia de archivos. [39]

Una unidad NAS es un ordenador conectado a una red que proporciona servicios de almacenamiento de información al resto de equipos de la red. Aunque es posible hacer que una unidad NAS ejecute algún tipo de software, lo normal es limitar estos equipos a almacenamiento en red. Por ejemplo, lo habitual es que no dispongan de teclado ni interfaz, sino que sean controladas a través de la red por otro equipo de la misma a través de un navegador.

Los clientes generalmente acceden al NAS con una conexión Ethernet. El NAS aparece en la red como un único nodo que es la dirección IP de la unidad (conocida como caja o cabeza NAS). Un NAS puede almacenar cualquier tipo de información que aparezca en la forma de archivos, como carpetas de correo, contenido web, copias de seguridad del sistema, etc. La comunicación con una unidad NAS se hace a sobre TCP/IP.

Un servidor NAS proporciona la forma más fácil de añadir un sistema de almacenamiento a una red. Se puede incrementar el tamaño de almacenamiento sin afectar al resto de equipos en la red o a la red misma. Esto hace de los NAS ideales para bases de datos locales o copias de seguridad, aparte de ser relativamente baratos.

El servidor NAS es un aparato de red completamente integrado. Funciona independientemente, funcionando incluso cuando el servidor de red se encuentra fuera de servicio, y proporciona un excelente servicio a todos sus usuarios.

Los que se encuentran a favor del NAS afirman que esta tecnología proporciona una serie de ventajas sobre los servidores de archivos tradicionales, tales como un inferior coste, mejor seguridad, mayor disponibilidad y una menor dificultad para el uso y administración de los mismos.

2.3.3.2 Storage Area Network (SAN)

SAN, traducido al español como red de área de almacenamiento, es una red cuyo principal propósito es el almacenamiento de información, y que a su vez se encuentra en comunicación con la red principal de una empresa.

Una SAN se diferencia de un NAS en diferentes aspectos, si bien la confusión entre ambas es habitual por poseer características similares y servir para el mismo fin: proporcionar capacidad de almacenamiento de información a otros dispositivos.

Las SAN convencionales difieren de los NAS en múltiples aspectos. Las SAN normalmente utilizan conexiones Fiberchannel en lugar de Ethernet, y una SAN a menudo incorpora múltiples dispositivos de red en una LAN privada, mientras que un NAS depende de dispositivos individuales conectados directamente a una red LAN preexistente. El sistema tradicional NAS es una solución de almacenamiento en red más simple, y efectivamente suple a una implementación completa de una SAN.

La distinción entre NAS y SAN ha ido difuminándose en los últimos tiempos, a medida que las compañías tecnológicas continúan inventando y poniendo a la venta nuevos productos de almacenamiento en red. Las SAN actuales pueden llegar a utilizar Ethernet, igual que los sistemas NAS utilizan o no canal de fibra. Algunos sistemas NAS llegan a incorporar redes privadas con múltiples dispositivos de fin.

2.4 Redes en el entorno Microsoft

2.4.1 Estructura genérica

2.4.1.1 Dominios

Un dominio de Windows es una red de ordenadores en la que todos los ordenadores, usuarios, impresoras, etc. se encuentran registrados en una base de datos central localizada en uno o más núcleos de ordenadores centrales conocidos como controladores de dominio. Es en estos controladores donde tiene lugar la autenticación de los usuarios y se autoriza el acceso a los recursos compartidos.

Cuando se crea un nuevo dominio, esto se hace implementando las características de Directorio Activo, catálogo global y FSMO en un servidor. Esto procede a convertir dicho servidor en el primer controlador de dominio de este nuevo dominio. En una organización de reducido tamaño se puede tener un solo dominio. Sin embargo, en grandes organizaciones es muy común utilizar múltiples dominios para separar departamentos, secciones o recursos de usuarios. [40]

Los dominios se estructuran en árboles y bosques. Un árbol de dominios es una colección de dominios relacionados. Un bosque de dominios es una colección de árboles relacionados. De esta forma, se organiza por bloques el conjunto de dominios que conforman todo el servicio de una empresa. Es en este momento, en el que es necesario acceder a otros dominios, en el que entran en juego las relaciones de confianza.

Cuando un usuario no autorizado solicita acceso a los recursos compartidos de un servidor, éste solicita al controlador de dominio que compruebe los permisos de acceso. En caso de estarlo, se establece la conexión apropiada permitiéndose así la transferencia de información. En el caso contrario, se cancela la conexión inmediatamente.

2.4.1.2 Bosques

Un bosque, como se ha indicado anteriormente, es un conjunto de árboles de dominios. De esta forma, en la figura 2-14 se observa un bosque de dominios (α) formado por los árboles 1 y 2. Cada árbol de la figura, a su vez, aglutina dos dominios (representados por el servidor), siendo los dominios A y B en el caso del árbol 1 y los dominios C y D en el caso del árbol 2.

Este tipo de organización en bosques y árboles, si bien innecesaria en organizaciones de menor porte, puede llegar a ser imprescindible en redes corporativas más complejas donde, por cuestiones de organización, se pueden tener decenas de árboles, cada uno con docenas de dominios, cada uno a su vez con cientos de equipos y usuarios.

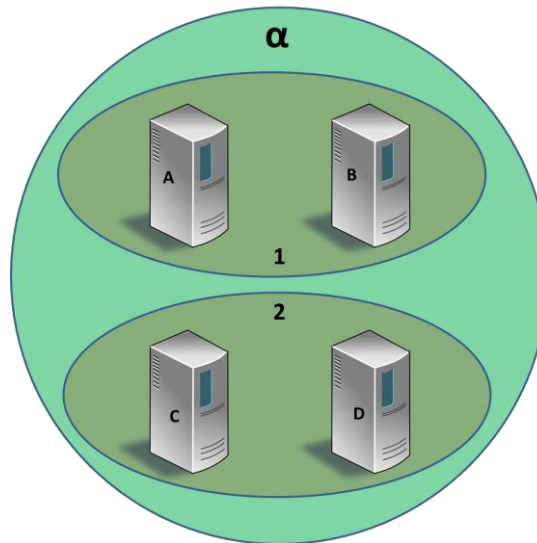


Figura 2-14 El bosque de dominios α está formado por los árboles 1 y 2, que a su vez aglutinan los dominios A-B y C-D (respectivamente). A su vez, cada dominio tendría diversos equipos. Elaboración propia

2.4.1.3 Relaciones de confianza

Las relaciones de confianza son las relaciones que se dan entre dos dominios en cuanto al acceso a los recursos compartidos. Si un usuario del dominio A confía en otro usuario del dominio B, podrá proporcionarle acceso a la información de su dominio. Esto será así, aunque el dominio B decida no confiar en el A, creándose una relación unilateral tal como se ve en la figura 2-15.



Figura 2-15 Relación unilateral entre dos dominios representados por un equipo, de elaboración propia.

Siguiendo la lógica detrás de la confianza, si el dominio A confía en el dominio B y éste confía a su vez en el equipo C, se establece una relación de confianza automática en la que A concede permisos de acceso a C, aunque no haya sido explícitamente establecida. Esto posee la ventaja de que simplifica la concesión de permisos en una empresa grande, pero también puede llevar a la vulnerabilidad de accesos no planeados a dominios que se prefería mantuvieran más protegidos si no se tiene cuidado con dichos permisos.

También se pueden establecer estas relaciones de confianza entre bosques de dominios. Al fin y al cabo, recuérdese que un bosque no es más que una agrupación de dominios. Se pueden crear relaciones de confianza entre dichos bosques para permitir a los dominios de uno el acceso al otro bosque y viceversa. Esta relación por bosques ofrece diversos beneficios en grandes organizaciones, donde administrativamente es más fácil establecer estas relaciones de confianza entre departamentos enteros organizados en bosques que ir estableciéndolas dominio a dominio.

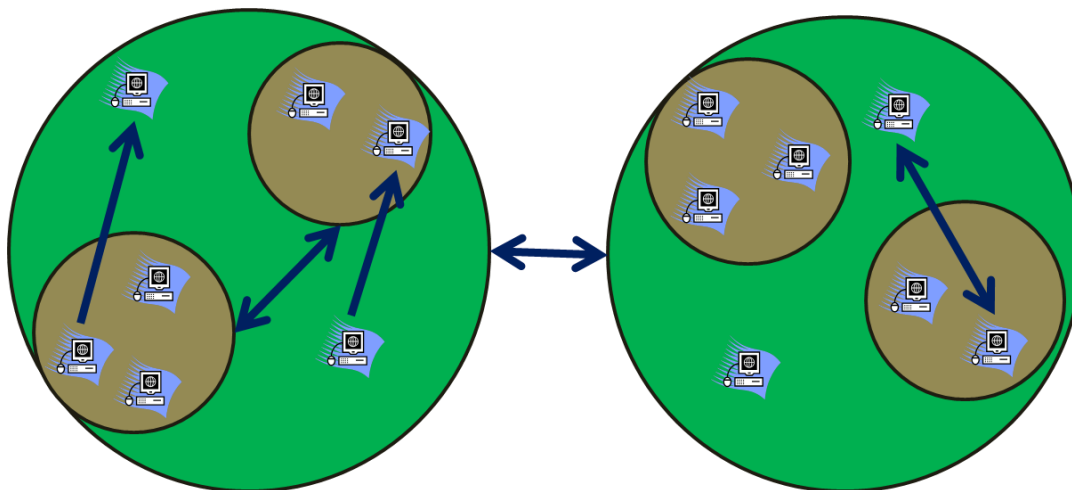


Figura 2-16 Relaciones de confianza entre dominios individuales, árboles y bosques. Cada dominio, representado por un equipo, puede estar compuesto de múltiples dispositivos. Elaboración propia.

2.4.2 Directorio Activo

El Directorio Activo (AD, por sus siglas en inglés) es un servicio de directorios que Microsoft desarrolló para las redes de dominio. Introducida por primera vez en Windows 2000 Server, el AD ha servido como un repositorio central para cantidades significantes de información en todas las versiones de Windows desde ese momento. Hay una importante información almacenada en el Directorio Activo, incluyendo dato de usuarios, grupos, zonas DNS, equipos compartidos, dominios, relaciones de confianzas, etc.

El directorio es una estructura jerárquica que almacena información sobre los objetos en la red, tales como usuarios y equipos. Un servicio de directorio proporciona los métodos para almacenar este tipo de información y hacer que esté disponible para los usuarios y administradores de la red. El controlador de dominio en redes Windows no es sino el equipo de la red que utiliza la herramienta AD DS (*Active Directory Domain Services*). [41]

El directorio activo no es una herramienta para compartir la información, sino una herramienta de autenticación. Cuando se habla de guardar la información de los usuarios, se trata principalmente de las credenciales que les dan acceso a ciertos tipos de información o aspectos de la red, así como de los límites que dichas credenciales les conceden al iniciar sesión. Esta herramienta también sirve para cambiar los permisos de los usuarios, manteniendo dicha estructura jerarquizada, de forma que no sólo es una herramienta de autenticación, sino también una de autorización. Por último, sirve para llevar un registro de los diferentes accesos que los usuarios realizan sobre cierto dominio o recurso. De esta forma, se habla de que el Directorio Activo sirve para reforzar el protocolo AAA: *Authentication, Authorization and Accounting* (Autenticación, Autorización y Registro, en español). [42]

2.4.3 CIFS

CIFS (*Common Internet File System*) es el nombre que recibe el SMB después de ser reinventado en 1996, viéndose ampliado por Microsoft. Esta nueva versión del protocolo incluye, entre otras, las siguientes funciones: acceso a archivos, bloqueo de archivos y registros, almacenamiento en caché, notificación en la modificación de archivos, negociación entre dialectos del protocolo. [43]

- Acceso a archivos: El protocolo permite las operaciones habituales con archivos, como abrir, cerrar, leer, escribir y buscar.
- Bloqueo de archivos y registros: El protocolo da la posibilidad de bloquear archivos y registros, así como el acceso sin claves a archivos. Sin embargo, las solicitudes de bloqueo de archivo no prevalecerán sobre las de acceso sin clave, por lo que estas últimas serán denegadas en caso de intentar acceder a un archivo bloqueado.

- Almacenamiento en caché: El protocolo admite almacenamiento en caché, así como la previsualización de archivos y la escritura diferida online. Esta última optimización es segura siempre que no más de un usuario acceda a un archivo, mientras que la previsualización de archivos es segura mientras nadie modifique el archivo. En caso de que varios clientes accedan a la vez a un archivo para modificarlo, el servidor les notifica de los cambios en el número y el modo de acceso al archivo de estos usuarios, de modo que se pueda seleccionar la forma más apropiada de acceso seguro.
- Notificación en la modificación de archivos: Diferentes aplicaciones pueden llevar un registro con el servidor para ser notificadas en caso de que un archivo sea modificado. Esto sirve para saber cuándo una presentación debe ser actualizada sin tener que estar comprobando el servidor continuamente.
- Negociación entre dialectos del protocolo: Existen múltiples versiones de este protocolo, siendo conocida cada una como “dialecto”. Cuando se conectan por primera vez entre ellos dentro de una red, se negocia el dialecto que van a utilizar.

En su punto álgido, CIFS llegó a ser un protocolo utilizado no sólo en Windows, sin también en Linux y Unix. Esto hizo de él una herramienta muy extendida, pero al mismo tiempo dejó abierta la posibilidad de alcanzar a más equipos y redes con un ataque bien enfocado. [44]

2.4.4 El registro de Windows

El registro tiene una sutil pero importante función en los sistemas operativos basados en Windows. Por una parte, es una herramienta pasiva, siendo mayoritariamente una librería de ajustes y configuración localizada en el disco duro. Por otra, dicha librería es una herramienta fundamental en actividades como editar documentos, sobrescribir archivos o navegar por Internet. La configuración establecida en el registro determina cómo se muestra y se comporta el entorno de Windows, incluidas las aplicaciones que funcionan en él. [45]

Windows guarda la información de configuración en el registro. Éste es una base de datos jerárquica (tal como se puede observar en la figura 2-17), que puede ser descrita como un repositorio central para dicha información. La característica de una base de datos jerárquica lo hacen especialmente eficiente para el almacenamiento de información de configuración. No hay nada en Windows que no afecte directa o indirectamente al registro. Tanto en gran parte de las acciones de usuario final, como en casi todas las que se realiza a nivel sistema, el sistema operativo consulta el registro. Y lo mismo para cada aplicación ejecutada, cada operación realizada.

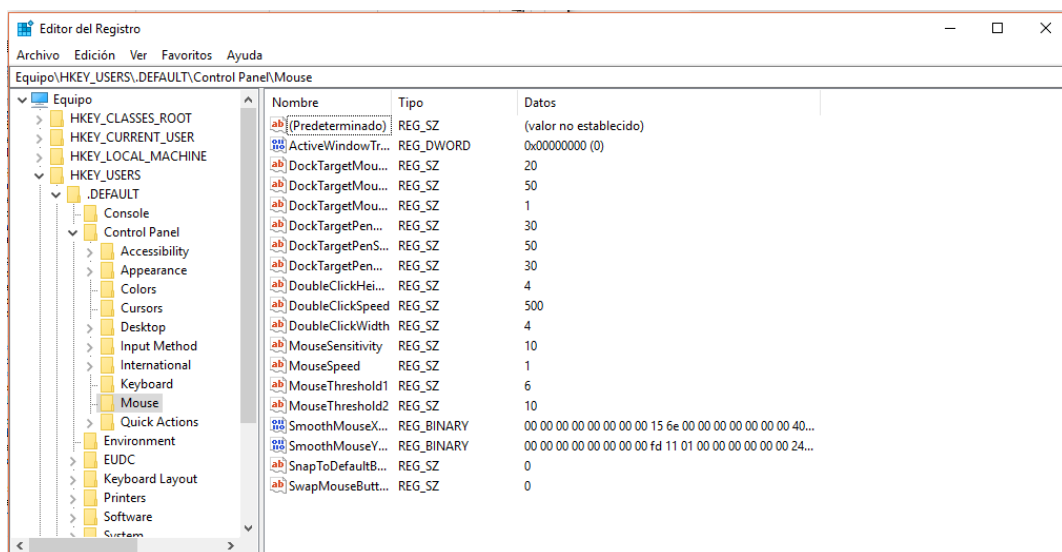


Figura 2-17 Captura de pantalla del Editor del Registro, de obtención propia.

Aparte de ser un lugar de almacenamiento central para ajustes, el registro permite las complejas relaciones entre diferentes partes de Windows, las aplicaciones y la interfaz del usuario. Por ejemplo, el que salgan diferentes menús de acciones según el archivo en el que se haga clic con el botón derecho del ratón se debe asimismo al registro. Los ajustes para cada usuario que inicia sesión en Windows están separados de aquellos de otros usuarios, también gracias al registro.

El conocimiento del registro permite el acceso a diferentes funcionalidades, como la gestión de políticas. Los administradores de red utilizan políticas para configurar ajustes de usuarios y equipos de acuerdo a ciertos estándares, y los usuarios no son capaces de modificar dichos ajustes. Por ejemplo, una política establecida podría ser bloquear el escritorio tras 15 minutos de inactividad, lo cual serviría para proteger el equipo en caso de que el operador abandonara su puesto sin cerrar sesión. La gestión de políticas puede llegar a abaratar costes e impulsar la productividad.

Un beneficio indirecto pero importante es la compatibilidad de aplicaciones. Microsoft define estándares para las localizaciones a las que pertenecen los diferentes tipos de ajustes en el registro. La compañía tiene estándares para las asociaciones de archivos, ajustes de impresoras, ajustes de aplicaciones, etc. Las aplicaciones que siguen dichos estándares es más probable que funcionen bien con el sistema operativo y con otras aplicaciones, ya que todas estarán siguiendo los mismos ajustes en los mismos lugares. De hecho, la mayoría de las aplicaciones que funcionan bien en Windows 2000 son compatibles con Windows XP y los sistemas operativos posteriores, dado que la estructura general del registro no cambia excesivamente entre los sistemas operativos.

El registro capacita otras muchas funcionalidades de gestión, tales como

- Redirección de carpetas
- Perfiles de hardware
- Archivos offline
- Supervisión del rendimiento
- Alternancia entre perfiles de usuario
- Administración local o remota (figura 2-18)
- Windows Management Instrumentation (WMI)

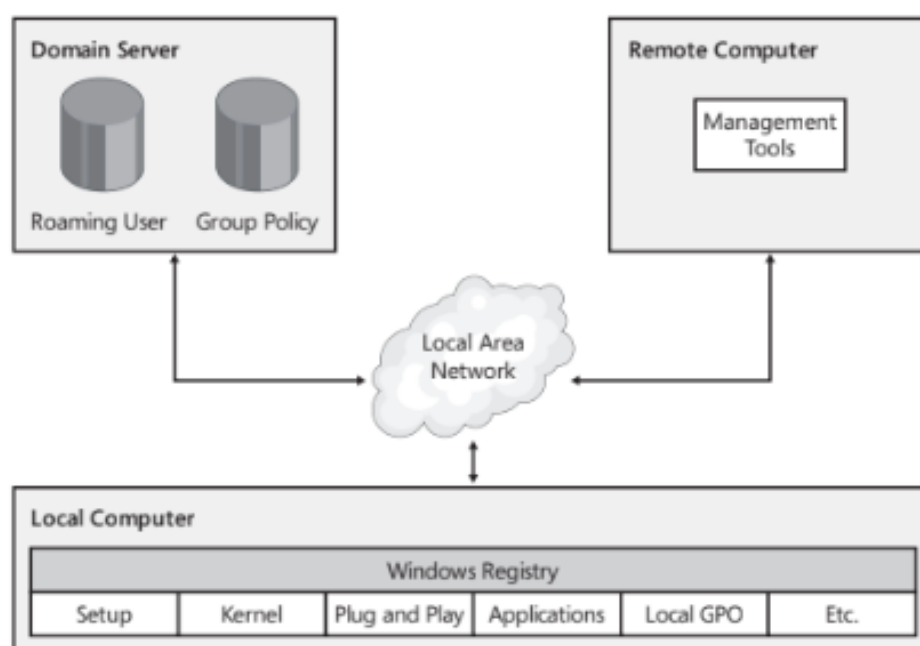


Figura 2-18 El registro permite tanto la administración local como la remota. Imagen obtenida de [45]

Pese a todos sus beneficios, el registro plantea un dilema. Por una parte, es el núcleo central de toda la información de configuración de Windows, la piedra angular. Por otra parte, el hecho de que el

registro sea tan crítico lo convierte en una de las debilidades del sistema operativo. Si el registro falla, Windows falla con él.

2.4.5 WMI

Windows Management Instrumentation (WMI) es el nombre por el que se conoce la infraestructura para la gestión de información y operaciones en sistemas operativos basados en Windows. Se pueden escribir código de WMI para automatizar tareas en equipos remotos, pero WMI también proporciona gestión de la información a otras partes del sistema operativo y sus productos. [46]

WIM es la implementación en Windows de la Gestión Empresarial Basada en la Red (WBEM, por sus siglas en inglés) el cual es una iniciativa industrial para desarrollar una tecnología estándar para acceder a la información de la gestión en un entorno empresarial. WMI utiliza el estándar industrial Modelo de Información Común (CMI, por sus siglas en inglés) para representar sistemas, aplicaciones, redes, dispositivos y otros componentes gestionados. El CMI está gestionado y mantenido por la Fuerza Operativa de Gestión Distribuida (DMTF). [47]

La habilidad para obtener datos de gestión desde equipos remotos, y la capacidad para actuar sobre ellos, es lo que hace útil al WMI. Las conexiones remotas de WMI se realizan a través del Modelo de Objetos de Componentes Distribuidos (DCOM). Una alternativa es utilizar la Gestión Remota de Windows (WinRM).

Las aplicaciones de gestión pueden obtener datos o realizar operaciones a través de WMI en una gran variedad de lenguajes. WMI puede ser utilizado en todas las aplicaciones basadas en Windows, y su mayor utilidad se da en aplicaciones de empresa y scripts administrativos. Está diseñado para programadores que utilicen lenguajes de programación basado en Windows (C++/C#/VB.NET, ...), y capaz de utilizar los recursos del Microsoft ActiveX.

WMI proporciona una interfaz uniforme para cualquier aplicación (local o remota) que pretendan obtener datos de gestión de un equipo, una red o una empresa. Esta interfaz uniforme está diseñada de forma que las aplicaciones clientes de WMI no necesitan recurrir a una amplia variedad de sistemas de Interfaz de Programación de Aplicaciones (API) en funcionamiento. Muchas API no pueden ser llamadas por clientes automatizados como las aplicaciones de Visual Basic, mientras que otras directamente no acceden a equipos remotos.

En la figura 2-19 se puede ver la relación entre la infraestructura del WMI, los proveedores y los objetos gestionados, así como la relación entre la infraestructura WMI y sus clientes. [48]

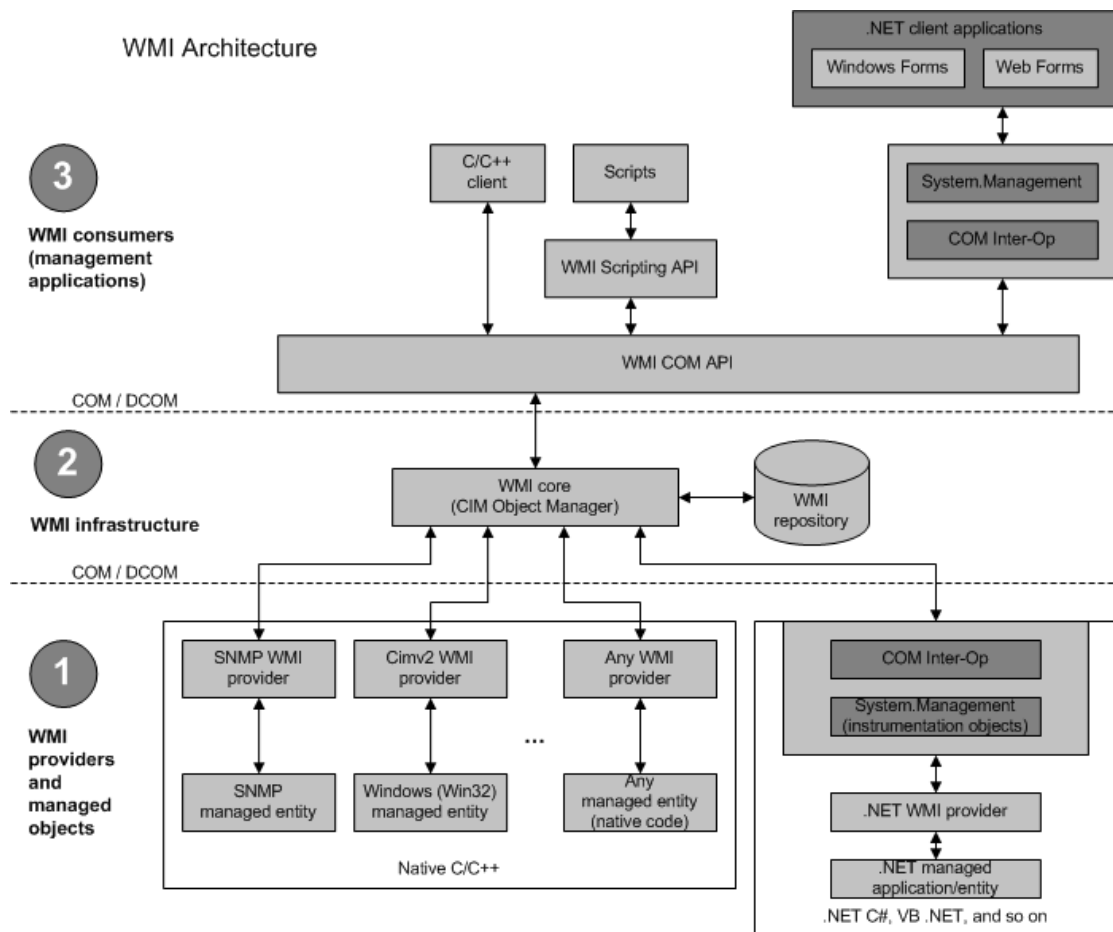


Figura 2-19 Diagrama con la arquitectura del WMI, obtenido de [48]

Un proveedor WMI es un objeto Component Model Object (COM) que supervisa uno o más objetos del WMI. Un objeto es un componente lógico o físico de la empresa, como un controlador de disco duro, un adaptador de red, una base de datos, un sistema operativo, un proceso o un servicio. De forma similar a un controlador, un proveedor proporciona al WMI información de un objeto y maneja mensajes del WMI al objeto controlado. Un ejemplo del proveedor es el proveedor de registro, que accede a los datos en el registro del sistema.

Un cliente de WMI es una aplicación de gestión o programa que interacciona con la infraestructura del WMI. Una aplicación de gestión puede realizar preguntar, enumerar datos, ejecutar métodos del proveedor o subscribirse a eventos mediante el COM API para WMI. Ésta es una herramienta utilizada para escribir aplicaciones cliente de WMI o para crear un nuevo proveedor WMI. La referencia COM API proporciona información para administradores de sistemas avanzados, así como desarrolladores que están creando aplicaciones de proveedor o cliente. [49]

2.5 Entorno de desarrollo

2.5.1 Visual Studio 2017

Microsoft Visual Studio es un popular entorno de desarrollo integrado (IDE) para construir aplicaciones modernas y de gran calidad para una gran variedad de plataformas tales como Windows, la red, la nube y dispositivos móviles. Esta familia de entornos nace en 1997 con la presentación del Visual Studio original, en un compendio nuevo de herramientas de programación en el que se aunaba Visual C++ y Visual Basic. El Visual Studio se vendía en dos ediciones diferentes, el Visual Studio Profesional y Visual Studio Empresa, siendo este último el más completo de los dos. Una diferencia que se mantiene hasta el día de hoy, existiendo en la actualidad más versiones.

La versión de 2017 es similar a la de 2013 y 2015 en cuanto a cómo se centra en aumentar la productividad del desarrollador mediante mejoras del editor de código y herramientas de detección de errores. [50]

Visual Studio 2013 dio a los desarrolladores la oportunidad de registrarse en Visual Studio con su cuenta de Microsoft. Si bien esto no era obligatorio, proporcionaba una serie de ventajas, tales como obtener Visual Studio por ser parte de la Red de Desarrolladores Microsoft (MSDN), desbloquear permanentemente ediciones de *Visual Studio Express* (conocido ahora como *Visual Studio Community*) y aumentar el periodo de prueba. Pero más importante era que los desarrolladores podían aprovecharse de ajustes sincronizados, aplicándolos en múltiples instalaciones de Visual Studio, lo cual implicaba poseer automáticamente el mismo grupo de ajustes en todos los equipos utilizados por la misma cuenta de Microsoft. Aún más allá, Visual Studio 2017 desarrolla aún más posibilidades adicionales registrándose con una cuenta de Microsoft.

Visual Studio 2017 extiende la experiencia de registro permitiendo que múltiples cuentas de Microsoft se registren en el entorno de desarrollo. Tener múltiples cuentas accediendo a Visual Studio es común por las siguientes razones:

- Cuentas separadas para desarrollar y probar aplicaciones.
- Cuentas separadas para trabajo y para casa.
- Cuentas separadas para múltiples desarrolladores trabajando con el mismo equipo.

Todos estos servicios requieren el acceso con una cuenta Microsoft. En Visual Studio 2017, cuando se inicia sesión, el IDE automáticamente conectará la cuenta actual a cualquier servicio Microsoft asociado, no siendo necesario volver a introducir las credenciales cada vez. Además, Visual Studio 2017 simplifica el seleccionar una cuenta cuando se crean servicios en línea o se están estableciendo controles de aplicación.

Una de las funcionalidades más esperadas por los desarrolladores es la habilidad de escribir código una vez y compartir dicho código a través de múltiples tipos de aplicaciones. Visual Studio 2017 simplifica el proceso de compartir código introduciendo la herramienta *Shared Projects* (Proyectos Compartidos). Esta herramienta permite la compartición de código, utilidades y recursos entre múltiples tipos de proyectos. Si bien este concepto aparece por primera vez en la segunda actualización de Visual Studio 2013, en VS2017 dichos proyectos compartidos están disponibles tanto para C# y Visual Basic.

Los proyectos compartidos están disponibles a través de específicos modelos de proyecto en el cuadro de diálogo “Nuevo Proyecto”. En esta ventana también se pueden crear nuevas soluciones y programas para compartir en línea, tal como se puede observar en la figura 2-20.

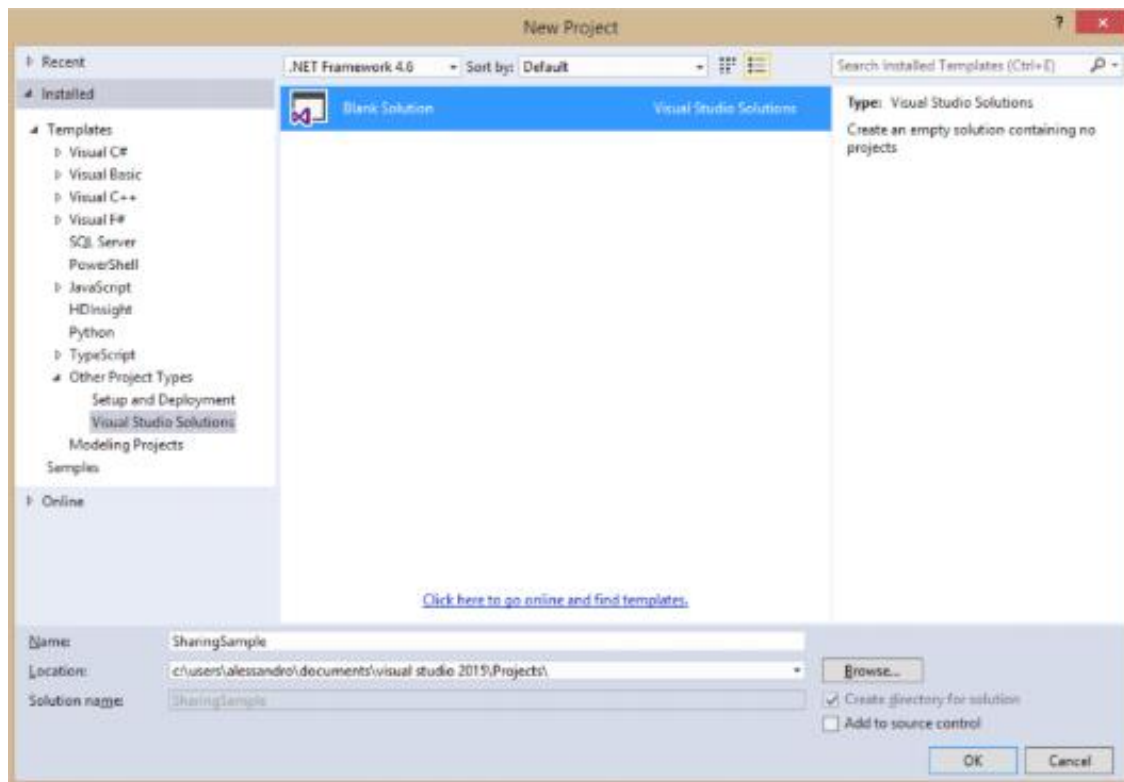


Figura 2-20 Cuadro de diálogo “Nuevo Proyecto” donde se está creando una solución, obtenida de [50]

A nivel corporativo se vuelve una herramienta indispensable, pues facilita la colaboración en proyectos de programación, así como el trabajo de un mismo usuario desde diferentes equipos, enlazándolos todos en una red de acceso a través de la cuenta de Microsoft.

2.5.2 C#

C# es un lenguaje de programación de propósito general, orientado a los objetos y basado en componentes. El que sea de propósito general implica que existe una gran variedad de formas de uso para alcanzar múltiples objetivos. El que sea orientado a los objetos significa que funciona con el concepto de “objeto”, un elemento que posee diferentes tipos de información, conocidos como “atributos” y procedimientos, conocidos como “métodos”. Una funcionalidad de los objetos es que los métodos son capaces de modificar los campos de los atributos asociados a un objeto según lo que se haya programado. [51]

El que sea basado en componentes, por otra parte, da a entender que se encuentra estructurado siguiendo una separación de elementos. Un componente es un servicio predefinido que, a su vez, es capaz de comunicarse con otros componentes.

Otra característica de este lenguaje de programación es que maneja tipos explícitos en lugar de implícitos, a diferencia de otros lenguajes como Python. Esto significa que toda variable debe estar definida antes de compilar el código, devolviéndose un mensaje de error en caso de no hacerse así. En Python, sin embargo, las variables pueden ser creadas en cualquier momento, asumiéndose un valor igual a 0 para ellas en caso de no haber sido declaradas antes. Por supuesto, este último caso puede parecer más cómodo para trabajar más rápidamente, pero puede inducir a fallos innecesarios y muy difíciles de detectar en caso de cometer un error al teclear. Como se dice en el Zen del Python: “Explícito es mejor que implícito”. [52]

2.5.3 Refactorización de código

Una de las principales ventajas que ofrece Visual Studio, trabajando con cualquiera de los lenguajes para los que está diseñado, es la refactorización. Este es un proceso que permite optimizar o

mejorar el código una vez ya escrito, modificando su estructura sin que su comportamiento externo se vea afectado. Gracias a la agrupación de proyectos en soluciones, también es posible realizar la refactorización a todo el conjunto en lugar de tener que realizarla proyecto a proyecto. En esta línea, Visual Studio ofrece la posibilidad de previsualizar los cambios a realizar, primero revisando los cambios sugeridos en cuanto a las referencias del código. Una vez se han aceptado dichos cambios, se muestran las modificaciones al código. En ambas fases de la refactorización se puede cancelar el proceso para volver atrás, siendo necesario aceptar manualmente las propuestas del programa. [53]

Algunas de las funcionalidades que ofrece la opción de refactorización son:

2.5.3.1 Extracción de método

Proporciona una forma rápida de crear una función que se va a utilizar de forma recurrente a partir del código que ya hemos implementado. De esta forma, al codificarlo por primera vez se puede volver a utilizar de forma recurrente de una forma más rápida, al asignarle un nombre durante la refactorización. Además, al utilizar un método en lugar de copiar y pegar las diferentes líneas de código se evitan duplicidades y se ofrece la posibilidad de modificar el método una única vez para que se produzca el cambio en todo el programa, en lugar de tener que realizar los cambios necesarios una y otra vez. [54]

2.5.3.2 Eliminación de código inútil

Cuando el programa encuentra una línea de código que no se va a ejecutar en ningún momento o una función o método al que no lleva ningún camino, se ofrece la opción del epígrafe. Esta funcionalidad sirve principalmente para depurar el código una vez se han realizado diferentes modificaciones sobre un proyecto original, el caso más normal en el que quedan funciones descolgadas o situaciones sin resolver. [55]

2.5.3.3 Cambio de nombre de un símbolo de código

Una de las funcionalidades más utilizada, sobre todo en el caso de necesitar renombrar una variable. Al cambiar el nombre de una variable en el código, el programa cambia automáticamente todas las líneas de código en las que dicha variable es llamada, de forma que no hace falta revisarlo minuciosamente después de realizar este tipo de modificaciones. Además, en casos de programar códigos demasiado voluminosos, el hacerlo manualmente suele llevar a error en demasiadas ocasiones, viéndose eliminado dicho error al hacerlo manualmente. [56]

2.5.3.4 Acercamiento de la declaración a la referencia

Esta funcionalidad permite mover las declaraciones de las variables más cerca de su uso. Al igual que las funcionalidades anteriores, ésta está enfocada a la prevención de errores, haciendo que la cercanía entre la declaración de la variable a la zona de código donde se va a ejecutar permita evitar los fallos humanos derivados, precisamente, de las declaraciones vacías o el uso equívoco de una variable al estar mal declarada. [57]

2.6 La ciberseguridad y el ransomware en las Fuerzas Armadas Españolas

Durante los últimos años, es innegable la cada vez más avanzada integración del Ministerio de Defensa y su compromiso con el mundo digital. Si bien no es un cambio que se haga en pocos años, el fruto del esfuerzo realizado en este campo es cada vez más palpable, siendo necesaria una concienciación del personal para garantizar la seguridad de los sistemas utilizados.

En este aspecto, la fundación del Mando Conjunto de Ciberdefensa (MCCD) en 2013 supuso un gran progreso. Respondiendo a la cada vez más apremiante necesidad de defensa de los sistemas informáticos, este órgano dependiente del Estado Mayor de la Defensa cumple, entre muchas otras funciones, con la obtención, el análisis y la explotación de la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad. Asimismo, son los responsables de definir,

dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa. [58]

BOLETÍN DE CONCIENCIACIÓN EN CIBERDEFENSA

CONSEJOS CONTRA EL RANSOMWARE



El **ransomware** es un tipo de malware que secuestra datos mediante cifrado. El atacante cifra los datos del ordenador o del dispositivo móvil y exige un pago por la clave de descifrado.

Como cualquier otro malware, la **infección** se suele dar por tres vías: enlaces o archivos adjuntos en **correos electrónicos**; acceder a **páginas web comprometidas**; o la instalación de **programas infectados**, normalmente descargados a través de páginas no oficiales.

Tras su instalación, el ransomware procede a cifrar todos los archivos comenzando por los que estima más importantes o sensibles. El usuario suele ser informado cuando el proceso ya ha terminado y es irreversible.

Otra posible aproximación de los atacantes es extorsionar a la víctima tras convencerla de que han accedido al dispositivo o a su cámara y han conseguido información comprometida. Por ejemplo, que simulen una investigación policial que ha encontrado software o contenido ilegal y lo que exigen es el pago de una falsa multa.

Con carácter general, tratan de provocar o simular una situación en la que la única salida parece ser hacer lo que el atacante pide, ya sea pagar u otro tipo de extorsión.

Ante estos ataques la solución con mejores garantías es **prevenir, proteger y recuperar** adecuadamente nuestros datos.

PREVENIR

PROTEGER

RECUPERAR

El ataque puede ser indiscriminado o estar dirigido a nuestro colectivo. Limita el uso del correo electrónico y los equipos corporativos a las necesidades del servicio, **evita la descarga ilegal** de contenidos y **desconfía** de los correos electrónicos con adjuntos o enlaces que no hayas solicitado.

La mejor protección de tus datos implica tener **copias de seguridad** frecuentes. Los archivos que son accesibles a través de USB o de la red wifi también pueden ser cifrados por el malware. Las copias de seguridad se deben almacenar desconectadas del equipo. Ten actualizado el Sistema Operativo. Instalar y mantener al día un buen antivirus puede también ayudar a detectar a tiempo las versiones más comunes de ransomware.

Si, a pesar de todo, somos afectados por el ransomware la mejor recomendación es borrar y limpiar completamente el equipo afectado. Pide **ayuda profesional** si es necesario. Sólo entonces debemos restaurar la copia de nuestros datos. Precipitarnos al conectar nuestra copia de seguridad al equipo puede exponerla al malware.

Y SOBRE TODO: NUNCA PAGUES EL RESCATE

Nada garantiza que una vez pagado el rescate vayamos a recuperar los datos o a superar la extorsión. De hecho, los atacantes suelen aumentar la presión sobre los usuarios que responden a su mensaje.

Estos incidentes se deben poner en conocimiento de los administradores de seguridad de la red implicada y, en función de la gravedad o de los daños causados, también podemos trasladar la correspondiente denuncia a las autoridades competentes.



DELANTE DEL TECLADO, TODOS SOMOS COMBATIENTES



GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA



MANDO CONJUNTO DE CIBERDEFENSA


Figura 2-21 Boletín informativo enviado por el MCCD, obtenido de [59]

Cumpliendo con esta última función, son comunes los correos enviados por dicho órgano a todo el personal del Ministerio de Defensa de manera divulgativa con información sobre las posibles amenazas informáticas a las que se enfrentan los usuarios de los sistemas del Ministerio de Defensa. En esta línea, se destaca un correo enviado el 20 de febrero de 2019 (figura 2-21), titulado “Consejos contra el ransomware”. En dicho correo, se adjunta un boletín de concienciación en ciberdefensa que proporciona una serie de consejos contra el ransomware. Estos consejos son: prevenir, proteger, recuperar y no pagar. [59]

- Prevenir: Debe limitarse el uso del correo electrónico y los equipos corporativos a las necesidades del servicio, evitar la descarga ilegal de contenidos y desconfiar de correos electrónicos con adjuntos o enlaces no solicitados.

- Proteger: Es preferible crear copias de seguridad de todos los archivos con frecuencia, almacenándolas en zonas aisladas de los equipos desde los que se hayan hecho, así como tener actualizado el sistema operativo y el antivirus.
- Recuperar: Lo mejor en caso de ser afectados es borrar y limpiar el equipo infectado, pidiendo ayuda profesional si es necesario. Una vez hecho esto, restaurar las copias de seguridad realizadas.
- Nunca pagar el rescate: Nada garantiza la recuperación de archivos o el fin de la extorsión tras realizar el pago. De hecho, lo normal es que la presión aumente tras realizar contacto. Lo mejor es poner estos incidentes en conocimiento de los administradores de seguridad de la red implicada y, según la gravedad de los daños, también trasladar la correspondiente denuncia a las autoridades competentes.

Estas líneas generales de respuesta ante ataque de ransomware se prueban especialmente efectivas a nivel individual si son seguidas de forma sistemática, especialmente la creación de copias de seguridad de archivos. Sin embargo, al hablar de redes corporativas un virus de ransomware no controlado a tiempo sigue siendo capaz de causar daños que, en muchos casos, se vuelven irreparables. Estas medidas sirven para proteger a individuos en sus equipos locales, pero no son realmente útiles cuando se habla de proteger una red, pues no son capaces de impedir la rápida propagación de un virus de estas características por la red.

3 DESARROLLO DEL TFG

3.1 Esquema de bloques de funcionamiento

El programa a evaluar en este TFG ha sido desarrollado con el lenguaje de programación C# en el entorno de Visual Studio 2017. La solución completa, “ComprobadorRegistro.sln”, se encuentra formada por tres proyectos y una carpeta de recursos, como se puede observar en la figura 3-1.

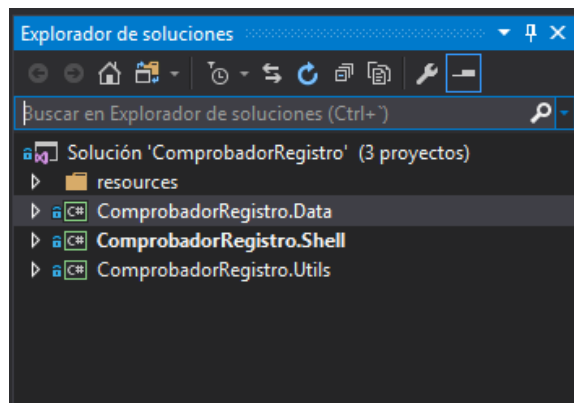


Figura 3-1Captura del Explorador de soluciones de VS2017.

Por los ataques conocidos de ransomware y la mecánica de todo ataque de este estilo, se observa que en todos estos intentos de extorsión el denominador común está compuesto de tres partes: la modificación del registro de Windows del equipo objetivo, la incapacidad de la víctima para acceder a sus ficheros por encontrarse estos cifrados y la aparición de un archivo de rescate. El software de este trabajo, proporcionado por los tutores, se centra en el primer y tercer punto para la detección temprana de posibles ataques de ransomware, usando el segundo para realizar una confirmación más detallada sobre la naturaleza del propio ataque.

A día de hoy, la principal forma de luchar contra el ransomware al nivel de las grandes redes corporativas consiste en prevenir los errores humanos que suelen provocar la entrada de virus en el sistema, ya que se considera muy poco eficiente la revisión de todos los archivos en busca de aquellos que puedan estar bloqueados. Sin embargo, el programa a validar en este TFG se basa en la idea de que no hace falta controlar todos los archivos existentes, sino que basta con revisar ciertas entradas concretas del registro de Windows y aquellos archivos que se modifican (por la aparición necesaria del archivo de solicitud de rescate), habiendo dos alternativas (la de revisar todos los archivos que se crean nuevos o se modifican, aplicable a cabinas de almacenamiento y redes muy rápidas, o sólo donde surge un archivo de petición de rescate, para ámbitos más modestos).

El primer archivo de interés es una lista con todas las direcciones IP (C:\Users\Media\Desktop\TFG\ComprobadorRegistro.Shell\bin\Debug\ips.txt) de los equipos donde se va a llevar a cabo la comprobación. Por hacerse la validación en el propio equipo en este entorno demo que se está utilizando a falta de una red real, la única dirección que se va a utilizar es la 127.0.0.1, conocida como dirección de *localhost*. En el entorno real de producción, se incluirían bien la lista de las IPs de los equipos activos en el dominio, o se consultaría por WMI al DHCP que realiza las entregas de las mismas.

El siguiente archivo es el de las carpetas a supervisar en los equipos incluidos en la lista anterior (C:\Users\Media\Desktop\TFG\ComprobadorRegistro.Shell\bin\Debug\carpetas.txt). La ventaja de poner la ruta completa es que de esta forma se pueden especificar no sólo los discos duros de los equipos finales, sino también las carpetas de archivos compartidos que se deseen. Se hablará más adelante sobre ello, pero es importante destacar que el programa no va a evaluar los archivos que se encontraran en esa carpeta previamente a la ejecución del mismo, sino que se centra sólo en los que se crean o introducen en el directorio a partir de ese momento. Para realizar una sencilla demostración del sistema, se trabajará con la carpeta C:\temp.

Por último, se tiene una lista de entradas de registro de Windows válidas, de confianza, para que la señal de alarma no salte con la entrada de ejecución de programas que se conocen y se espera que funcionen (C:\Users\Media\Desktop\TFG\ComprobadorRegistro.Shell\bin\Debug\clavesregistro.txt). Al comprobarse las entradas correspondientes a Run y RunOnce (figura 3-2) se están evaluando los diferentes programas que el sistema ejecuta automáticamente en el arranque del sistema operativo, ocasión que los virus de este estilo utilizan para funcionar sin el permiso explícito del usuario.

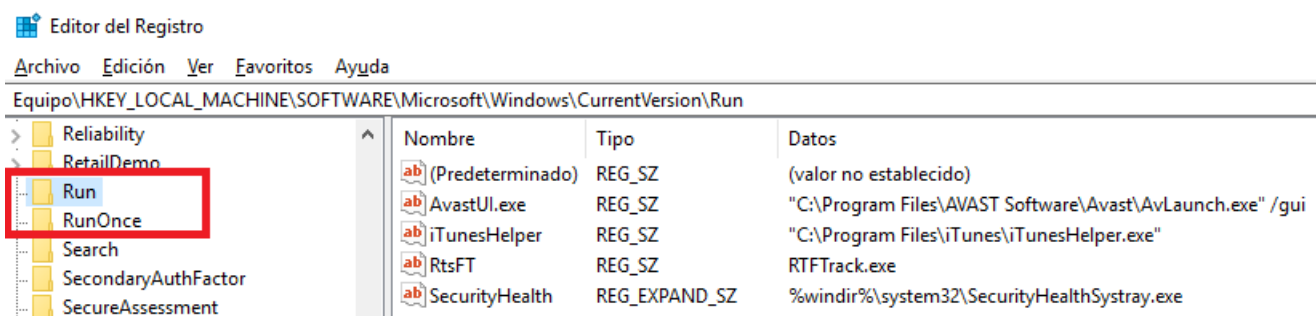


Figura 3-2 Captura del Editor de Registro de Windows con las entradas que se evalúan en el cuadro rojo.

Se ofrecen dos formas de funcionamiento, el modo “Normal” y el modo “Paranoico”:

3.1.1 Modo Normal

Cuando se genera un archivo en una carpeta perteneciente a un equipo de la lista, el programa se limita a comprobar si el nuevo fichero tiene una estructura similar a un fichero de petición de rescate, lo cual suele ser simplemente llamarse “Crypto” o tener algún nombre similar (patrones que están recogidos en el software, en función de todos los ransom aparecidos hasta la fecha). En caso de no tener dicha estructura la comprobación finaliza, dándose por bueno el archivo recién creado. Sin embargo, en caso de dar positivo, se recorre la ubicación donde se ha localizado (incluidos los subdirectorios) y se comprueba la legibilidad de todos los ficheros que se encuentren ahí con la finalidad de detectar cualquier tipo de fichero cifrado, pues si hay petición de rescate, hay cifrado. En esta comprobación de la legibilidad de cada fichero se evalúa de una forma diferente según su tipo, siendo estos algunos ejemplos:

- Documentos de ofimática. En estos casos se utiliza un FileReader hecho a medida para comprobar si el documento se puede abrir. Este FileReader está preparado para detectar archivos tipo ".doc", ".docx", ".xls", ".xlsx", ".ppt" y ".pptx" (Figura 3-3), los principales ficheros realizados con Microsoft Office (correspondientes a Word, Excel y PowerPoint).

```
namespace ComprobadorRegistro.Utils.Files
{
    public class OfficeEncryptedFileChecker : IEncryptedFileChecker
    {
        private static List<string> _handledExtensions = new List<string>() { ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx" };
    }
}
```

Figura 3-3 Captura del código, donde se ven las extensiones a comprobar en el caso de ficheros Office.

- Ejecutables. Para estos ficheros se comprueba el número mágico. Éste es una serie de caracteres alfanuméricos que identifican al archivo. Estos caracteres suelen estar situados al comienzo del propio archivo, lo que hace que su identificación se pueda realizar con relativa velocidad. El número mágico podría ser comparado posteriormente con una biblioteca para garantizar la seguridad de dicho ejecutable.
- DraWinG (DWG). Con los archivos de dibujo computerizado, como los generados por los programas de AutoDesk, se usa una metodología similar a la anterior, ya que no se abre el archivo directamente, sino que se comprueban los primeros bytes para confirmar que se corresponden con lo esperado (figura 3-4). Comprobando esos seis bytes iniciales se puede comprobar si es un archivo real o no, ya que sirven para identificar la versión del programa de AutoDesk con el que ha sido realizado, pero en un virus o programa malicioso en general los bytes indicados no se corresponden con nada parecido.

```
public FileInfo CheckEncrypted(string file)
{
    if (IsHandled(file))
    {
        FileInfo output = null;
        try
        {
            using (FileStream fs = File.OpenRead(file))
            {
                byte[] first6bytes = new byte[6];
                if (fs.Read(first6bytes, 0, 6) > 0)
                {
                    var txt = System.Text.Encoding.Default.GetString(first6bytes);
                    var rgx = new System.Text.RegularExpressions.Regex("AC\\d{4}", System.Text.RegularExpressions.RegexOptions.IgnoreCase);

                    if (!rgx.IsMatch(txt))
                        output = new FileInfo(file);
                }
            }
        }
        catch (Exception)
        {
            output = new FileInfo(file);
        }

        return output;
    }
    else
    {
        return (Next != null) ? Next.CheckEncrypted(file) : null;
    }
}
```

Figura 3-4 Parte del proyecto en la que se evalúan los bytes iniciales del archivo “.dwg”.

- Imágenes. Llamando imágenes a los formatos ".jpg", ".bmp", ".png" e ".ico", se intentan abrir como mapas de bits para después evaluar sus valores altura y ancho (figura 3-5).

```
private static List<string> _handledExtensions = new List<string>() { ".jpg", ".bmp", ".png", ".ico" };  
private IEncryptedFileChecker _next = null;  
public IEncryptedFileChecker Next  
{  
    get { return _next; }  
    set { _next = value; }  
}  
  
public bool IsHandled(string file)  
{  
    return _handledExtensions.Contains(Path.GetExtension(file).ToLower());  
}  
  
public FileInfo CheckEncrypted(string file)  
{  
    if (IsHandled(file))  
    {  
        try  
        {  
            using (Bitmap bmp = new Bitmap(file))  
            {  
                var h = bmp.Height;  
                var w = bmp.Width;  
            }  
        }  
    }  
}
```

Figura 3-5 Código de ejecución para archivos de imagen.

Al mismo tiempo que realiza la comprobación de los archivos creados a tiempo real, se lleva a cabo una revisión del registro cada quince minutos. En esta comprobación, el programa busca las claves de registro Run y Runonce (figura 3-6), ambas localizadas en la misma entrada del registro (Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion). Éstas son las que determinan los programas a ejecutar durante tras el arranque del ordenador, quedando funcionando en un segundo plano una vez que el sistema operativo ya está en funcionamiento. De esta forma, un programa malicioso podría recibir permisos para ejecutarse automáticamente al insertarse aquí. Toda entrada que se encuentre es comprobada con la lista de claves de registro permitidas, saltando la alarma sólo en caso de que no haya ninguna coincidencia.

```
namespace ComprobadorRegistro.Utils.Registry  
{  
    public class Constants  
    {  
        public const uint HKEY_CLASSES_ROOT = 0x80000000;  
        public const uint HKEY_CURRENT_USER = 0x80000001;  
        public const uint HKEY_LOCAL_MACHINE = 0x80000002;  
        public const uint HKEY_USERS = 0x80000003;  
        public const string RUN_KEY = @"SOFTWARE\Microsoft\Windows\CurrentVersion\Run";  
        public const string RUN_ONCE_KEY = @"SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce";  
        public const string WMI_ROOT_NAMESPACE = "root\\default";  
    }  
}
```

Figura 3-6 Código con las direcciones de comprobación del registro.

Una vez localizada una amenaza, el programa lleva a cabo una serie de pasos:

- Se registra la incidencia para poder llevar un control de la situación. Esto incluye hora, localización de la amenaza y los archivos que se consideran cifrados.

```

{
    public class MailService
    {
        public void SendMail(string to, string subject, string body)
        {
            if (!Properties.Settings.Default.SendEmailAlerts) return;

            #if DEBUG
            to = "p[REDACTED]";
            #endif

            //Envio por correo externo
            try
            {
                var mail = new System.Net.Mail.MailMessage();
                mail.To.Add(to);
                mail.From = new System.Net.Mail.MailAddress(Properties.Settings.Default.MailSender);
                mail.Subject = subject;
                mail.Body = body;
                mail.IsBodyHtml = true;
                var smtp = new System.Net.Mail.SmtpClient();
                smtp.Send(mail);
            }
            catch (Exception ex)
            {
                //Envio por correo interno
                try
                {
                    var mail = new System.Net.Mail.MailMessage();
                    mail.To.Add(to);
                    mail.From = new System.Net.Mail.MailAddress(Properties.Settings.Default.MailSender);
                    mail.Subject = subject;
                    mail.Body = body;
                    mail.IsBodyHtml = true;
                }
            }
        }
    }
}

```

Figura 3-7 Código para notificación por correo. La dirección está tapada por protección de datos.

- Notificación por correo (figura 3-7). Se envía un correo electrónico a la dirección especificada con la información registrada.
- Presentación en consola de administración. En la consola desde la que se ejecuta el programa, la cual debe tener acceso de administrador a la red, sale una ventana emergente mostrando al operador la información de la amenaza detectada para poder reaccionar lo más rápido posible.
- Grupos de notificación. En primera instancia, se realizan de 10 en 10 y, posteriormente, pasan a ser de 100 en 100. Esto sirve para no inundar de notificaciones al sistema, así como para asegurar que durante la primera alerta la red ni el sistema se vean sobrecargados.
- Reacciones al sistema:
 - Apagado de tarjeta de red. Con esto se pretende aislar al equipo para evitar la propagación del malware. Así se protege al resto de equipos de la red de la amenaza.
 - Apagado remoto del equipo. En caso de que el apagado de la tarjeta de red no se realice correctamente, lo más seguro es apagar el equipo y, conociendo la amenaza gracias al registro, no volverlo a conectar a la red corporativa hasta haber solucionado la incidencia.
 - Inhabilitación de la boca de switch en la pila del rack correspondiente. Si bien está deshabilitado para esta versión local del programa, la última posibilidad es forzar una expulsión del equipo de la red mediante la inhabilitación de su conexión al switch. De esta forma, aunque se haya perdido acceso al equipo debido al propio ataque, éste podría quedar igualmente aislado al no ser capaz de comunicarse con el switch de la red, anulándose por tanto la posibilidad de expandir la infección y continuar cifrando archivos de recursos compartidos de red.

3.1.2 Modo Paranoico

El modo paranoico, si bien idéntico al normal en la etapa de reacción, supone un mayor consumo medio de recursos a lo largo del tiempo. Como su nombre indica, este modo es para cuando se espera un ataque, lo cual hace que los periodos de comprobación del registro estén menos espaciados y que el análisis de los archivos creados sean más exhaustivos.

Para empezar, mientras el modo normal se limitaba a comprobar la estructura del nombre de los archivos generados en las carpetas de estudio, el modo paranoico va a intentar abrirlos directamente. El análisis de legibilidad que en el modo normal se realiza únicamente tras detectar un archivo de petición de rescate es la constante en este caso. Cada vez que se genera un archivo en las carpetas evaluadas se comprueba para determinar si es legible o se encuentra cifrado. Sin embargo, esto no quita que sólo se evalúen los ficheros de nueva creación.

La otra gran diferencia respecto al modo normal es que en el modo paranoico se reduce el tiempo entre comprobaciones del registro de Windows, pasando de ser cada quince minutos a realizarse una comprobación cada minuto.

En un equipo único esta operación es una tarea sencilla, pero cuantas más carpetas y más direcciones IP deban ser monitorizadas la carga de trabajo del modo paranoico será mayor. Aumentando considerablemente con cada equipo, en una red demasiado grande podría llegar a consumir tantos recursos que hicieran impracticable el funcionamiento de este modo.

3.2 Comparativa entre modos

Para poder gestionar eficientemente la red en modo paranoico, lo más recomendable sería utilizar una serie de administradores repartidos de una forma concreta, supervisando cada uno unas direcciones IP determinadas. De esta forma, si bien se vuelve necesario un mayor número de equipos de administrador para poder gestionar toda la red corporativa, se observa que el riesgo de fallos en el equipo administrador de la red por sobreconsumo de recursos es mucho menor.

En el caso de que el equipo administrador se viera sobrepasado por la demanda de procesamiento necesaria para llevar a cabo la monitorización objeto de este sistema supondría la inutilidad del mismo, dejando la red sin protección. Es por ello que, en caso general, es más recomendable usar el modo normal para la monitorización de la red durante periodos largos de tiempo, para garantizar la continuidad de la protección.

Sin embargo, esta última afirmación no quita que el modo paranoico posea la ventaja de recibir una alerta aún más temprana frente a las diferentes amenazas. Esto puede suponer hasta 14 minutos de antelación en el caso de las modificaciones al registro de Windows, y la diferencia completa entre la detección o no en caso de que la estructura del archivo de petición de rescate no se corresponda a la esperada.

Es por ello que la recomendación final es utilizar el modo normal para monitorización genérica de la red, utilizando el modo paranoico para la monitorización de los equipos sólo en caso de que se espere un ataque o una amenaza. Y, en ese caso, se recomienda tener preparados una serie de equipos para hacer de administradores y controladores de la red a nivel local, para evitar la sobredemanda de recursos.

4 VALIDACIÓN DEL SISTEMA

4.1 Prueba del programa

Para ejecutar el programa, el primer paso es localizar el ejecutable del Shell. Éste se encuentra en [...]ComprobadorRegistro\ComprobadorRegistro.Shell\bin\Debug\ComprobadorRegistro.Shell.exe, y es necesario ejecutarlo con permisos de administrador para garantizar el correcto funcionamiento del programa. Antes de ejecutarlo, sin embargo, es necesario comprobar los tres ficheros mencionados anteriormente: “carpetas.txt”, “clavesregistro.txt” e “ips.txt”. Los tres se encuentran en la misma carpeta que el ejecutable.

Una vez se ejecuta, se abre una ventana con la interfaz de este programa de monitorización de registro, tal y como puede verse en la figura 4-1. En esta imagen se observa que no detecta ninguna entrada sospechosa en el registro en la última comprobación, así como que el estado de los ficheros en la carpeta objetivo está siendo comprobado. Al ser una comprobación en tiempo real, es decir, de forma continuada, dicha señal de comprobación sólo desaparece cuando es sustituida por una señal de aviso o de error. Aquí se puede comprobar que las direcciones IP de los equipos, así como las carpetas, sean los que se definen en los ficheros correspondientes.

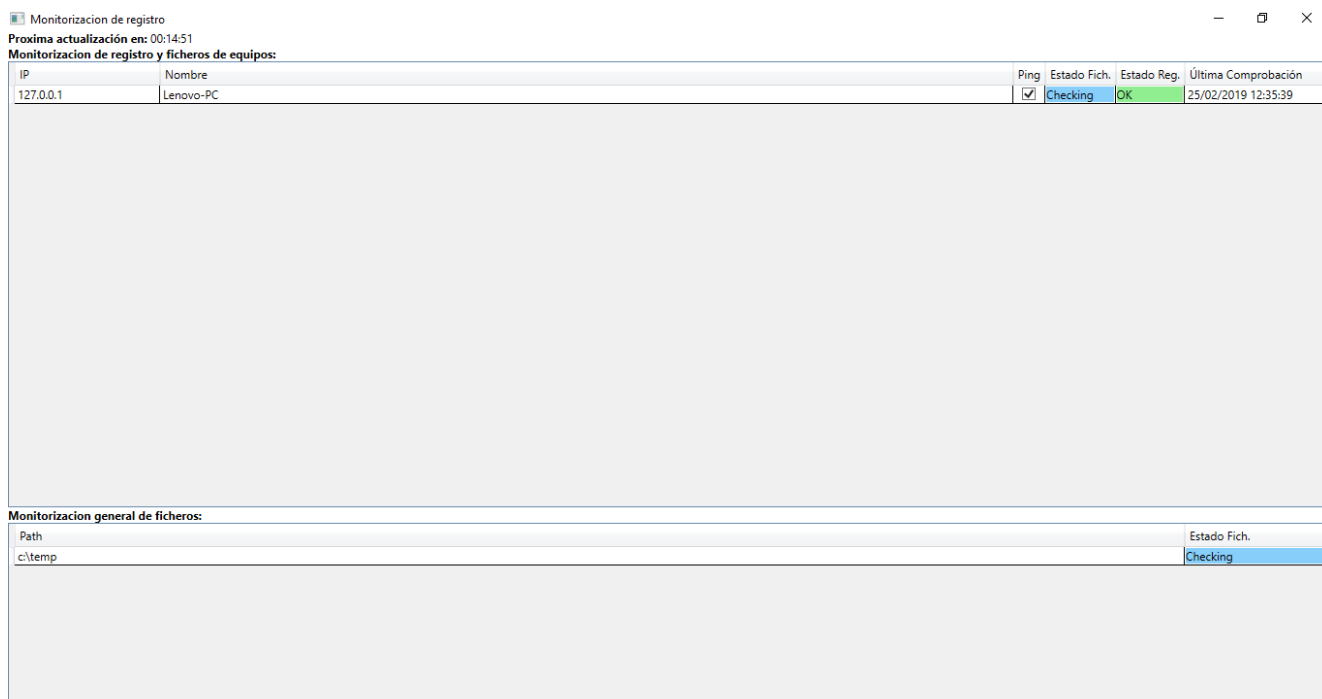


Figura 4-1 Interfaz del programa. Presentación en equipo administrador de red.

Para forzar la detección de entradas no autorizadas, se procede a abrir el Editor de Registro de Windows. Para ello se escribe “regedit” en la ventana de ejecutar del ordenador. A continuación, se crea una entrada falsa, un conjunto de números y letras aleatorios, en cualquiera de las dos direcciones del registro a evaluar (figura 4-2).

Microsoft\Windows\CurrentVersion\Run		
Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
AvastUI.exe	REG_SZ	"C:\Program Files\AVAST Software\Avast\AvLaunch.exe" /gui
iTunesHelper	REG_SZ	"C:\Program Files\iTunes\iTunesHelper.exe"
RtsFT	REG_SZ	RTFTrack.exe
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
Prueba	REG_SZ	Probando

Figura 4-2 Modificación del registro añadiendo la entrada “Prueba” (en azul).

Posteriormente, se fuerza el reinicio del programa de monitorización de registro, abriendo el Shell con permisos de administrador de nuevo o actualizando mediante la tecla de función F5, obteniendo el resultado que se puede observar en la figura 4-3:

Monitorización de registro					
Proxima actualización en: 00:14:33					
Monitorización de registro y ficheros de equipos:					
IP	Nombre	Ping	Estado Fich.	Estado Reg.	Última Comprobación
127.0.0.1	Lenovo-PC	☒	Checking	Warning	25/02/2019 16:00:20
Fecha	Cambio	Fichero	Valor de Clave del Registro		
			probando		
			Validar		

Figura 4-3 Monitor de registro cuando se detecta una clave no autorizada.

Al detectar una clave de registro no incluida en el fichero “clavesregistro.txt” da la señal de aviso que se puede ver en “Warning”, donde se indica a su vez el valor que no se encuentra en la lista de claves autorizadas. A su vez, el programa permite validar dicha clave, lo cual supone incluirla de forma automática en el documento especificado, de forma que no vuelva a saltar en futuras ejecuciones del programa (figura 4-4).

```

clavesregistro.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
asdfasd
"c:\program files\itunes\ituneshelper.exe"
rtftrack.exe
c:\windows\system32\securityhealthsystray.exe
"c:\program files (x86)\common files\java\java update\jusched.exe"
"c:\program files\avast software\avast\avlaunch.exe" /gui
probando
  
```

Figura 4-4 Fichero “clavesregistro.txt” con la entrada “probando” al final, de forma que queda validada.

A continuación, para probar el programa al completo, se centrará la atención en la evaluación de ficheros. Para empezar, se comprueba qué pasa en el caso de que la carpeta especificada en el fichero “carpetas.txt” no esté en el equipo indicado en “ips.txt”. Para esta situación, se obtiene el resultado de la Figura 4-5:

Monitorización general de ficheros:	
Path	Estado Fich.
c:\temp	Error

Figura 4-5 Señal de error en caso de no localizarse el fichero que debe ser monitorizado.

De esta forma se llega a la conclusión de que el programa no sólo es válido para la detección de ransomware, sino también para la comprobación de la existencia de las carpetas de interés para la organización. No es extraña la pérdida de ficheros debida a errores humanos al trabajar con recursos compartidos, y este sistema puede servir para que la administración sepa si hay algún problema con ellos.

Creada la carpeta y funcionando el programa en modo normal, se crea un archivo no ejecutable por el programa. En este caso, y conociendo el método de evaluación, se ha creado una hoja de cálculo de Microsoft Excel, pero se ha modificado el código abriéndolo con un editor de texto para que el FileReader no sea capaz de abrirlo y salte la alarma. Sin embargo, al estar funcionando en modo normal, aún no detecta nada pues no posee la estructura de fichero de petición de rescate. Es al crear un documento de texto y ponerle el nombre “crypto” que se realiza la comprobación, devolviendo el resultado obtenido en la figura 4-6:


Monitorizacion de registro

Proxima actualización en: 00:14:53

Monitorizacion de registro y ficheros de equipos:

IP	Nombre	Ping	Estado Fich.	Estado Reg.	Última Comprobación
127.0.0.1	Lenovo-PC	☒	Checking	OK	25/02/2019 17:15:25

Monitorizacion general de ficheros:

Path	Estado Fich.
c:\temp	Checking

Fecha	Cambio	Fichero
25/02/2019 17:14:29	Created	c:\temp\Crypto1.txt

Figura 4-6 Ventana de monitorización al detectar un posible fichero de petición de rescate.

En la figura 4-6 se ve que el aviso se da por el cambio “Created” (creación) del fichero de texto mencionado antes, habiéndole sido asignado el nombre “Crypto1”. Éste es el tipo de estructura que busca el programa como ejemplo de petición de rescate. Además, informa de la fecha, hora y ruta hasta el fichero con cada amenaza detectada.

Aparte, sale una ventana emergente informando de los ficheros determinados como cifrados en la carpeta donde se ha encontrado la posible petición de rescate, tal y como se puede observar en la figura 4-7.

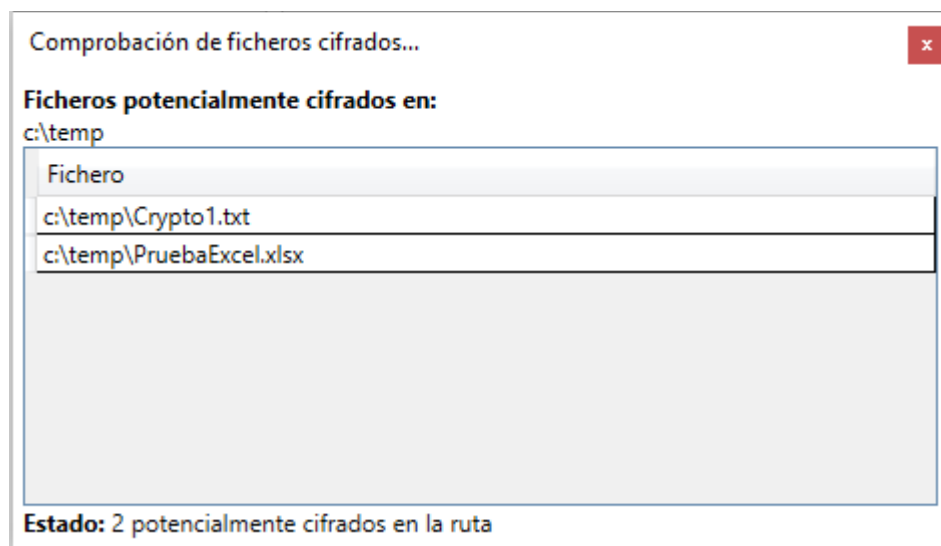


Figura 4-7 Ventana de comprobación de ficheros, informando de los que deben comprobarse.

El experimento se repite probando con otros tipos de archivos, como documentos tipo “.jpg” o “.pdf” para comprobar la correcta detección de todos los documentos ilegibles. El resultado se puede observar en la figura 4-8.

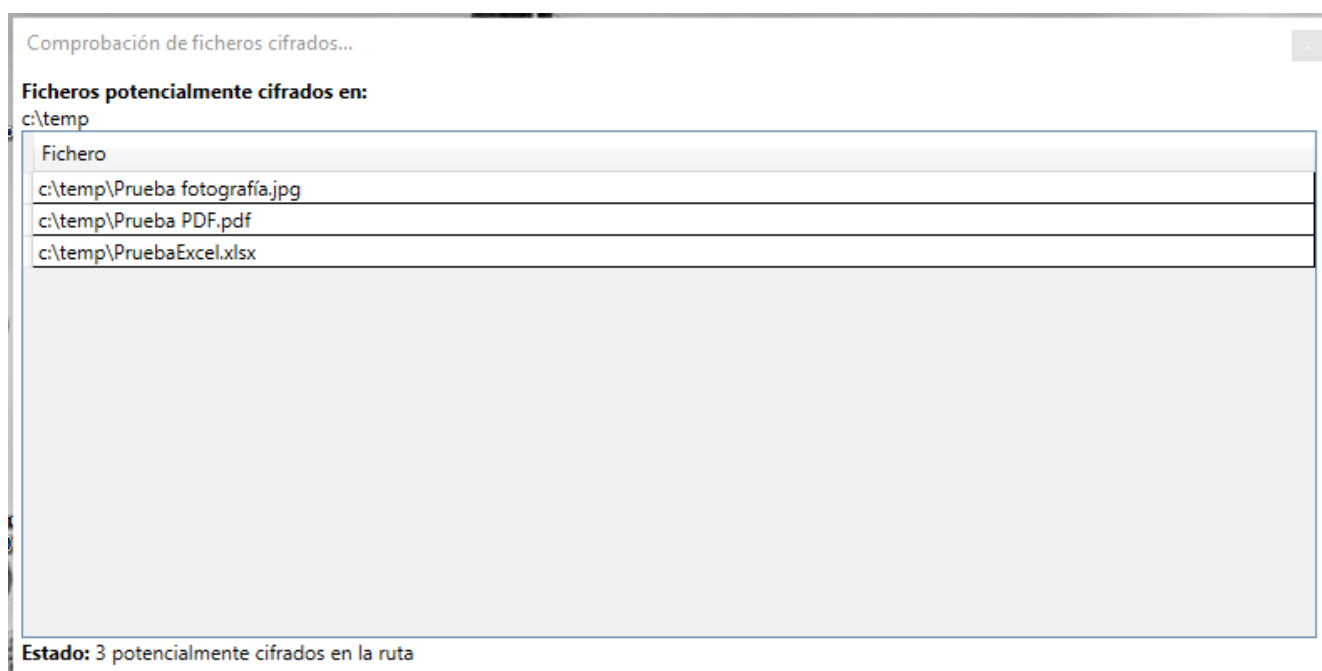


Figura 4-8 Elementos cifrados detectados: Imagen, PDF y fichero de ofimática.

A falta de una red de equipos disponible, se valida en un ordenador individual la solución propuesta, confirmando que es eficiente y funciona correctamente en el sistema de prueba. La alerta se

demuestra inmediata en el caso de aparición de fichero de petición de rescate, exactamente como se esperaba.

Del mismo modo, la detección de entradas no previstas en el registro es igualmente efectiva, pudiendo ocurrir al finalizar el contador o al forzar la revisión del sistema según se desee. La función de validación de las entradas del registro funciona correctamente, siendo ésta muy útil para la creación de una lista común de entradas de registro autorizadas. En caso de instalación genérica de un software nuevo en todos los equipos de una red corporativa, el incluir la entrada de registro correspondiente en la lista a tiempo evita la aparición de cientos de alarmas sin comprometer en ningún momento la seguridad de la red.

5 CONCLUSIONES Y LÍNEAS FUTURAS

El programa propuesto por los tutores se demuestra especialmente efectivo contra ataques de ransomware. Tradicionalmente, la política de enfrentamiento contra los programas maliciosos de rescate supone o bien comprobar uno a uno los archivos de la red en busca del archivo cifrado correspondiente o bien asumir que es más efectivo concienciar al personal en el uso correcto de los ordenadores y los peligros del malware que tratar de enfrentarlo. Este programa se sale de ambas líneas de pensamiento, ofreciendo una solución válida y eficiente contra los ataques de cifrado de ficheros.

Su implementación puede ser beneficiosa en una red corporativa, pues ayuda a la monitorización de los archivos peligrosos que se generen en la red, llevando un registro completo de todos éstos. Supone reducir la posibilidad del fallo humano, reduciendo las posibilidades de que el usuario cometa un error al tratar con los ficheros de la red o ejecutarlos. No sólo la posibilidad de error, sino también la posibilidad de ataque deliberado.

Si bien es necesario un equipo administrador de dominio capaz de estar encendido todo el día (o más, como se ha discutido anteriormente, por asunto de demanda de recursos), se puede observar que es la opción más eficiente para el control de este tipo de amenazas, y un aumento moderado en cuanto al consumo de estos recursos es un irrisorio precio a pagar comparado con la posibilidad de que alguien secuestre los archivos de una red.

En el caso de la Armada, esta herramienta podría ser igual de útil que en cualquier otra red de corporativa. Si bien se trata de una red inmensa con cientos de equipos a lo largo de todo el país, este programa podría ser la única forma de defensa real y practicable contra ataques de ransomware a día de hoy.

Sin embargo, no es perfecto. Como ya se ha especificado, este programa monitoriza sólo los archivos nuevos en las carpetas objetivo (sólo en el caso de los archivos, el registro lo comprueba entero), por lo que cualquier fichero infectado previamente no será detectado por el programa. Por mucho que parezca una vulnerabilidad, no debe ser considerada como tal. El programa se ejecuta en un entorno que se considera limpio y se encuentra centrado en la eficiencia, por lo que la asunción de la integridad de la red es un comienzo lógico para este tipo de amenazas. Al fin y al cabo, una red que ya haya sido infectada por este tipo de malware y ya tenga sus archivos cifrados no necesita ningún tipo de software para identificar el ataque.

En el futuro es de esperar que se encuentren soluciones más eficientes si cabe, capaces de gestionar hasta la monitorización del registro a tiempo real. Sin embargo, habrá que esperar hasta el desarrollo de procesadores más potentes y complejos que los actuales para poder ver una solución de ese nivel.

Llegados a este caso, se podrían implementar otras formas de detección simultáneas, como el análisis a tiempo real de los procesos que realiza cada equipo con una lista de procesos autorizados en la red, con la posibilidad añadida de detener automáticamente aquellos que consuman una cantidad desmesurada de recursos, pues es sabido que los procesos víricos de cifrado llegan a consumir hasta el 99% de la capacidad de la CPU.

La lucha contra la criptovirología seguirá avanzando, desarrollándose cada vez sistemas más eficaces para enfrentar los ataques de ransomware que surgan en el futuro. Pero la conclusión final de este trabajo es que en materia de prevención de ataques y alerta temprana este programa es lo más avanzado que se puede encontrar a día de hoy gracias a su planteamiento alejado de la idea tradicional de defensa frente a este tipo de ataques.

6 BIBLIOGRAFÍA

- [1] A. Solomon, «All About Viruses,» 17 Enero 2012. [En línea]. Available: <https://web.archive.org/web/20120117091338/http://vx.netlux.org/lib/aas10.html>. [Último acceso: 30 Enero 2019].
- [2] T. Meltzer y S. Phillips, «From the first email to the first YouTube video: a definitive internet history,» The Guardian, 23 Octubre 2009. [En línea]. Available: <https://www.theguardian.com/technology/2009/oct/23/internet-history>. [Último acceso: 30 Enero 2019].
- [3] SecurityFocus, «Good worms back on the agenda,» The Register, 30 Enero 2006. [En línea]. Available: https://www.theregister.co.uk/2006/01/30/good_worms_nematodes_blackhatconference/. [Último acceso: 30 Enero 2019].
- [4] Seguridad Apple, «Elk Cloner: El primer virus para el hogar fue de Apple II,» Eleven Paths, 17 Mayo 2011. [En línea]. Available: <https://www.seguridadapple.com/2011/05/elk-cloner-el-primer-virus-para-el.html>. [Último acceso: 30 Enero 2019].
- [5] F. B. Cohen, «Computer Viruses - Theory and Experiments,» 1984. [En línea]. Available: <https://web.archive.org/web/20070218125016/http://www.all.net/books/virus/index.html>. [Último acceso: 30 Enero 2019].
- [6] F. Secure, «Brain: Searching for the first PC virus in Pakistan,» 9 Marzo 2011. [En línea]. Available: <https://www.youtube.com/watch?v=lnedOWfPKT0>. [Último acceso: 30 Enero 2019].
- [7] PC-Solución, «Brain : El Primer virus lanzado libremente,» PC-Solución, 26 Julio 2018. [En línea]. Available: <https://pc-solucion.es/2018/07/26/brain-el-primer-virus-lanzado-libremente/>. [Último acceso: 30 Enero 2019].
- [8] P. Ducklin, «Naked Security,» Sophos, 25 Septiembre 2012. [En línea]. Available: <https://nakedsecurity.sophos.com/2012/09/25/ransomware-would-you-pay-up/>. [Último acceso: 20 Enero 2019].
- [9] J. Bates, «Virus Bulletin,» Enero 1990. [En línea]. Available: <https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf>. [Último acceso: 18 Enero 2019].

Enero 2019].

- [10] M. Alexander, «Suspect arrested in AIDS disk fraud case,» *Computerworld*, vol. XXIV, n° 6, p. 8, 1990.
- [11] H. Gierow, «Golem,» 7 Julio 2016. [En línea]. Available: <https://www.golem.de/news/die-erste-ransomware-der-virus-des-wunderlichen-dr-popp-1607-121809.html>.
- [12] V. Blue, «Zero Day,» 22 Diciembre 2013. [En línea]. Available: <https://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/>. [Último acceso: 21 Enero 2019].
- [13] D. Goodin, «ArsTechnica,» 17 Octubre 2013. [En línea]. Available: <https://arstechnica.com/information-technology/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/>. [Último acceso: 20 Diciembre 2019].
- [14] Bitcoin, «Bitcoin,» 2009. [En línea]. Available: <https://bitcoin.org/en/how-it-works>. [Último acceso: 22 Enero 2019].
- [15] Blockchain, «Blockchain Luxembourg,» [En línea]. Available: <https://www.blockchain.com/es/charts/market-price?timespan=all>. [Último acceso: 21 Enero 2019].
- [16] D. Ferguson, «CryptoLocker attacks that hold your computer to ransom,» *The Guardian*, 19 Octubre 2013.
- [17] Bleeping Computer, «Bleeping Computer,» 14 Octubre 2013. [En línea]. Available: <https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information>. [Último acceso: 22 Enero 2019].
- [18] United States Computer Emergency Readiness Team, «United States CERT,» Gobierno de los Estados Unidos, 2 Junio 2014. [En línea]. Available: <https://www.us-cert.gov/ncas/alerts/TA14-150A>. [Último acceso: 24 Enero 2019].
- [19] Office of Public Affairs, «The United States Department of Justice,» Department of Justice, 2 Junio 2014. [En línea]. Available: <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>. [Último acceso: 2019 Enero 24].
- [20] M. Smith, «CSO from IDG,» 4 Noviembre 2013. [En línea]. Available: <https://www.csoonline.com/article/2225714/microsoft-subnet/cryptolocker-crooks-charge-10-bitcoins-for-second-chance-decryption-service.html>. [Último acceso: 24 Enero 2019].
- [21] E. N. y. C. Timberg, «The Wall Street Journal,» 16 Mayo 2017. [En línea]. Available: https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html. [Último acceso: 25 Enero 2019].
- [22] E. C. Advisory, «ESET,» ESET, 15 Mayo 2017. [En línea]. Available: https://support.eset.com/ca6443/?locale=en_US&viewlocale=en_US. [Último acceso: 25 Enero 2019].
- [23] J. C. M. Llano, «Juan Carlos Mejía Llano Consultor de Marketing Digital y Transformación Digital,» 14 Mayo 2017. [En línea]. Available: <https://www.juancmejia.com/temas-varios/solucion-para-el-virus-wanna-cry-conozca-que-es>.

- y-como-limpiar-el-malware-tipo-ransomware/. [Último acceso: 27 Enero 2019].
- [24] J. Banford, «Reuters,» 22 Agosto 2016. [En línea]. Available: <https://www.reuters.com/article/us-intelligence-nsa-commentary/commentary-evidence-points-to-another-snowden-at-the-nsa-idUSKCN10X01P>. [Último acceso: 25 Enero 2019].
- [25] D. Cameron, «Gizmodo Australia,» Gizmodo, 13 Mayo 2017. [En línea]. Available: <https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/>. [Último acceso: 25 Enero 2019].
- [26] BBC News, «BBC,» 13 Mayo 2017. [En línea]. Available: <https://www.bbc.com/news/world-europe-39907965>. [Último acceso: 26 Enero 2019].
- [27] MalwareTech, «MalwareTech,» 13 Mayo 2017. [En línea]. Available: <https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html>. [Último acceso: 27 Enero 2019].
- [28] T. P. Bossert, «The Wall Street Journal,» 18 Diciembre 2017. [En línea]. Available: <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537>. [Último acceso: 25 Enero 2019].
- [29] M. A. Dye, R. McDonald y A. W. Rufi, Network Fundamentals, CCNA Exploration Companion Guide, Indianápolis, Indiana: Cisco Press, 2007.
- [30] M. A. Dye, R. McDonald y A. W. Rufi, CISCO CCNA EXPLORATION 4.0 Aspectos Básico de Interworking, Indianápolis: Cisco Press, 2009.
- [31] B. Mitchell, «Demilitarized Zone in Computer Networking,» LifeWire, 30 Noviembre 2003. [En línea]. Available: <https://www.lifewire.com/demilitarized-zone-computer-networking-816407>. [Último acceso: 1 Febrero 2019].
- [32] S. Splaine, Testing Web Security: Assessing the Security of Web Sites and Applications, Indianápolis: Wiley Publishing, Inc., 2002.
- [33] B. Nguyen, «Network Security and Firewall,» 29 Abril 2016. [En línea]. Available: https://www.theseus.fi/bitstream/handle/10024/105907/Nguyen_Binh.pdf?sequence=1&isAllowed=y. [Último acceso: 31 Enero 2019].
- [34] B. Mitchell, «Learn the Meaning of a Network Gateway,» LifeWire, 1 Junio 2008. [En línea]. Available: <https://www.lifewire.com/definition-of-gateway-817891>. [Último acceso: 1 Febrero 2019].
- [35] L. Yang, R. Dantu, T. A. Anderson y R. Gopal, «Forwarding and Control Element Separation (ForCES) Framework,» The Internet Society, Hillsboro, 2004.
- [36] T. Fisher, «What Is a Router and How Does it Work?,» LifeWire, 19 Diciembre 2018. [En línea]. Available: <https://www.lifewire.com/what-is-a-router-2618162>. [Último acceso: 1 Febrero 2019].
- [37] P. Christensson, «What is the difference between a switch and a router?,» PC Helper, 20 Febrero 2014. [En línea]. Available: https://pc.net/helpcenter/answers/difference_between_switch_and_router. [Último acceso: 2 Febrero 2019].
- [38] T. Sridhar, «Layer 2 and Layer 3 Switch Evolution,» *The Internet Protocol Journal*, vol.

- 1, nº 2, 1998.
- [39] D. Suresh, «An Introduction to Network Attached Storage,» *HWM*, pp. 90-92, 2003.
- [40] S. Lowe, «An overview of the Active Directory Domains And Trusts,» TechRepublic, 22 Junio 2009. [En línea]. Available: <https://www.techrepublic.com/blog/the-enterprise-cloud/an-overview-of-the-active-directory-domains-and-trusts-console/>. [Último acceso: 4 Febrero 2019].
- [41] Windows IT Pro Center, «Core Network Guide,» Microsoft, 10 Abril 2018. [En línea]. Available: <https://docs.microsoft.com/es-es/windows-server/networking/core-network-guide/core-network-guide>. [Último acceso: 5 Febrero 2019].
- [42] Zappytech, «Active Directory basics – explaining AD to IT beginners,» 19 Marzo 2013. [En línea]. Available: <https://zappytech.wordpress.com/2013/03/19/active-directory-basics/>. [Último acceso: 5 Febrero 2019].
- [43] SNIA CIFS Technical Work Group, Common Internet File System (CIFS) Technical Reference Revision: 1.0, Storage Networking Industry Association, 2002.
- [44] M. Rouse, «CIFS (Common Internet File System),» TechTarget, 23 Marzo 2017. [En línea]. Available: <https://searchstorage.techtarget.com/definition/Common-Internet-File-System-CIFS>. [Último acceso: 8 Febrero 2019].
- [45] J. Honeycutt, Microsoft Windows Registry Guide, Redmond: Microsoft Press, 2005.
- [46] Windows Dev Center, «Windows Management Instrumentation,» Microsoft, 31 Mayo 2018. [En línea]. Available: <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmi-start-page>. [Último acceso: 9 Febrero 2019].
- [47] Windows Dev Center, «About WMI,» Microsoft, 31 Mayo 2018. [En línea]. Available: <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/about-wmi>. [Último acceso: 10 Febrero 2019].
- [48] Windows Dev Center, «WMI Architecture,» Microsoft, 31 Mayo 2018. [En línea]. Available: <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmi-architecture>. [Último acceso: 10 Febrero 2019].
- [49] Windows Dev Center, «COM API for WMI,» Microsoft, 31 Mayo 2018. [En línea]. Available: <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/com-api-for-wmi>. [Último acceso: 10 Febrero 2019].
- [50] A. Del Sole, Visual Studio 2015 Succintly, Morrisville: Syncfusion, 2015.
- [51] J. Mayo, C# Succintly, Morrisville: Syncfusion, 2015.
- [52] T. Peters, «PEP 20 -- The Zen of Python,» Python, 19 Agosto 2004. [En línea]. Available: <https://www.python.org/dev/peps/pep-0020/>. [Último acceso: 19 Febrero 2019].
- [53] Microsoft Developer Network, «Refactorización (C#),» Microsoft, 10 Enero 2018. [En línea]. Available: <https://msdn.microsoft.com/es-es/library/719exd8s.aspx>. [Último acceso: 20 Febrero 2019].
- [54] G. Warren y G. Hogenson, «Extract a method refactoring,» Microsoft, 26 Enero 2018. [En línea]. Available: <https://docs.microsoft.com/en-gb/visualstudio/ide/reference/extract-method?view=vs-2017>. [Último acceso: 20 Febrero 2019].

- [55] G. Warren y G. Hogenson, «Remove unreachable code refactoring,» Microsoft, 26 Enero 2018. [En línea]. Available: <https://docs.microsoft.com/en-gb/visualstudio/ide/reference/remove-unreachable-code?view=vs-2017>. [Último acceso: 21 Febrero 2019].
- [56] G. Warren, «Rename a code symbol refactoring,» Microsoft, 26 Enero 2018. [En línea]. Available: <https://docs.microsoft.com/en-gb/visualstudio/ide/reference/rename?view=vs-2017>. [Último acceso: 21 Febrero 2019].
- [57] G. Warren y G. Hogenson, «Move declaration near reference refactoring,» Microsoft, 26 Enero 2018. [En línea]. Available: <https://docs.microsoft.com/en-gb/visualstudio/ide/reference/move-declaration-near-reference?view=vs-2017>. [Último acceso: 21 Febrero 2019].
- [58] «Mando Conjunto de Ciberdefensa - Cometidos,» Estado Mayor de la Defensa, [En línea]. Available: <http://www.emad.mde.es/CIBERDEFENSA/cometidos/>. [Último acceso: 20 Febrero 2019].
- [59] Mando Conjunto de Ciberdefensa, «Consejos contra el ransomware,» Mando Conjunto de Ciberdefensa, Madrid, 2019.