madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

CONSEJERÍA DE ECONOMÍA, EMPLEO Y HACIENDA
Comunidad de Madrid

PROCEDIMIENTO TÉCNICO
ACTUACIÓN EN ENTORNO EDUCATIVO
RANSOMWARE WANNACRY
(Actualizado 26/05/2017)

Contenido

1 Introducción

Importante: este procedimiento sólo es necesario en equipos Windows, si usted tiene equipos con Linux no tiene que actuar sobre ellos y podría conectarlos a la red del centro y seguir utilizándolos normalmente. Si su equipo dispone de doble arranque (Linux – Windows) es necesario que siga este manual y actúe sobre la partición Windows

Tras la alarma generada el pasado día 12 de mayo por el ciberataque masivo lanzado a escala internacional mediante un malware de cifrado de datos y petición de rescate económico en equipos dotados con el **sistema operativo Windows** (únicamente), la Comunidad de Madrid, en coordinación con las directrices de los Centros nacionales especialistas en materia de seguridad de la información, ha tomado un conjunto de medidas planificadas y escalonadas para garantizar la seguridad de los puestos de trabajo y de los sistemas de información de la Administración, en línea con las recomendaciones del CCN-CERT e INCIBE.

Puesto que el éxito de la infección conlleva la inutilización plena del PC infectado y la pérdida de sus datos, así como que ese PC sea vehículo de la propagación de la infección a otros puntos de la red de forma exponencial, las medidas de prevención deben seguirse con cuidado.

La solución definitiva que neutraliza este malware es la instalación en los ordenadores con Windows de la actualización de seguridad para el sistema operativo puesta a disposición por Microsoft, así como una actualización del antivirus con que cuente el ordenador que contemple este malware de forma específica.

Si el sistema operativo Microsoft es de una versión inferior a Windows XP, NO existe parche de seguridad. Por ello, debe instalarse una versión de sistema operativo, desde cero, que sea Linux, Windows XP o superior.

Si ello no fuera posible es necesario contar con un antivirus que sea capaz de detectar la amenaza detenerla y eliminarla, o bien utilizar la herramienta NoMoreCry Tool V.0.4 o superior, suministrada por el CCN-CERT en su página https://www.ccn-cert.cni.es, que previene la infección.

La herramienta del CCN-CERT previene la infección en el caso de que no se haya producido. Por ello, previamente a la instalación de la herramienta, debe verificarse si el PC ha sido infectado ya o no (la pantalla de petición de rescate solo aparece cuando el proceso de infección del PC y cifrado de sus datos ha terminado totalmente).

Se recomienda actuar en primer lugar en aquellos equipos que contengan aplicaciones o datos importantes, desconectándolos de la red y llevando a cabo este procedimiento.

2 Protocolo de actuación

El proceso de instalación **requiere privilegios de administrador** para la ejecución de las herramientas e instalación de las actualizaciones. Existen casos en los que hay equipos de aula de informática que pueden tener instaladas aplicaciones que bloquean los cambios en la unidad C:, las cuales borran las últimas acciones realizadas cuando se reinicia el equipo. **Debe asegurarse que la ejecución de este procedimiento se realiza de forma que se guarden estas actuaciones.**

IMPORTANTE: Si dispone de algún PC que contenga información crítica y/o sensible, antes de iniciar los siguientes pasos **desconecte el equipo de la red** para evitar que quede infectado o si ya lo está pueda afectar a otros equipos de su red. Realice el protocolo según se describe a continuación.

En los equipos de titularidad privada de profesores y alumnos, confirme que se haya realizado el protocolo de actuación que se describe a continuación, **exceptuando la conexión a la red y antes de ser utilizado en el centro**.

El protocolo de actuación consiste en las siguientes etapas:

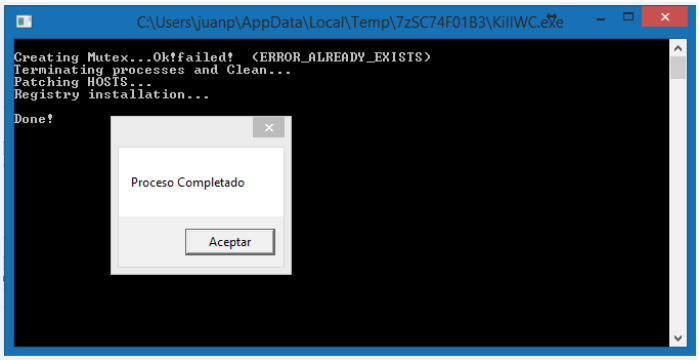
1. Desconecte el equipo de la red y enciéndalo.
2. Aplique la herramienta de detección y desinfección del ransomware de Panda WannaCry Fix.
3. **Si el equipo está infectado, apagarlo y desconectar de la red hasta nuevas instrucciones**, si no lo está continúe con el resto de pasos.
4. Identifique la versión del sistema operativo y la arquitectura del equipo.
5. Identifique si el equipo cumple los requisitos mínimos para para poder aplicar el parche de protección contra el ransomware wannacry.
6. Descargue las actualizaciones necesarias desde el equipo (en este momento puede conectarlo a la red). Si utiliza un pendrive USB para almacenar los parches necesarios y prefiere utilizarlo en lugar de descargar los parches en cada equipo, puede saltar este paso.
7. Aplique las actualizaciones en el equipo.
8. Si el equipo tiene instalado un antivirus debería actualizarlo, en caso contrario es muy recomendable que instale uno con capacidad de detección del ransomware wannacry.

2.1 Detección de posible infección con la herramienta Panda WannaCry Fix

El primer paso que deberá realizarse es garantizar que el equipo no se encuentra comprometido, para ello se utilizará una herramienta, que no requiere licencia para su uso, y cuyo objetivo es detectar si el equipo está infectado con el ransomware WannaCry. El programa se denomina "**panda-wannacryfix.exe**" y es compatible para sistemas operativos Windows XP o superior.

Esta aplicación debe descargarse siguiendo las instrucciones indicadas en el apartado 3 (ubicación de los recursos necesarios), guardarse en un pendrive USB y aplicarse en los equipos **asegurando que se encuentran desconectados de la red**.

La ejecución de esta herramienta consume unos minutos, entre 1 y 5, dependiendo de la capacidad del equipo e informa al usuario si el equipo se encuentra libre de esta amenaza mostrando la siguiente ventana informativa. Una vez ejecutada la aplicación se queda residente y protege contra la variante actual del virus. Si el equipo **no tiene el virus** presenta la siguiente pantalla.



Si el equipo está infectado, deberá apagarlo y desconectarlo de la red, hasta que se elabore alguna aplicación para eliminarlo y que pueda recuperar la información encriptada

NOTA: SI EL EQUIPO DISPONE DE ALGUN ANTIVIRUS ES POSIBLE QUE DEBA DETENERLO PARA PODER LANZAR CORRECTAMENTE ESTA UTILIDAD.

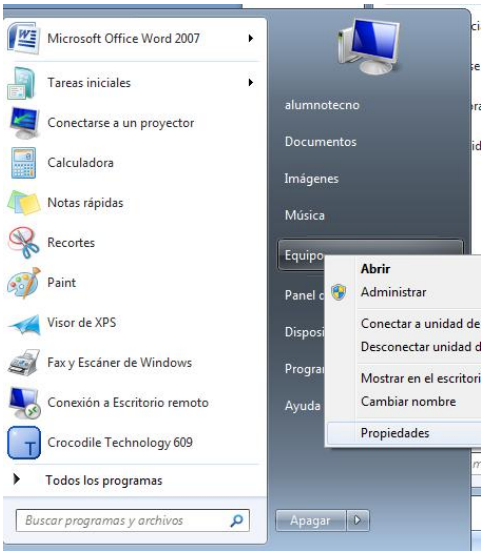
Si el antivirus del equipo impide la ejecución de esta aplicación y no es posible ejecutar la herramienta de detección y desinfección de Panda wannacry fix, puede saltar este paso y continuar con el procedimiento asegurando que el equipo **se encuentra desconectado de la red**. En estos casos se recomienda la actualización del antivirus, así como la comprobación de que dicho antivirus es capaz de detectar la amenaza wannacry.

NOTA: Se han detectado casos en los que una vez ejecutada la herramienta Panda wannacry fix, en los siguientes reinicios con usuarios no administradores se solicitan credenciales (usuario y contraseña) a los alumnos. Esta situación se produce porque el equipo tiene activado un sistema de protección que solicita permisos cuando el proceso de protección de Panda intenta ejecutarse. Para evitar este comportamiento puede desactivar este proceso ejecutando las instrucciones indicadas en el **ANEXO 1**.

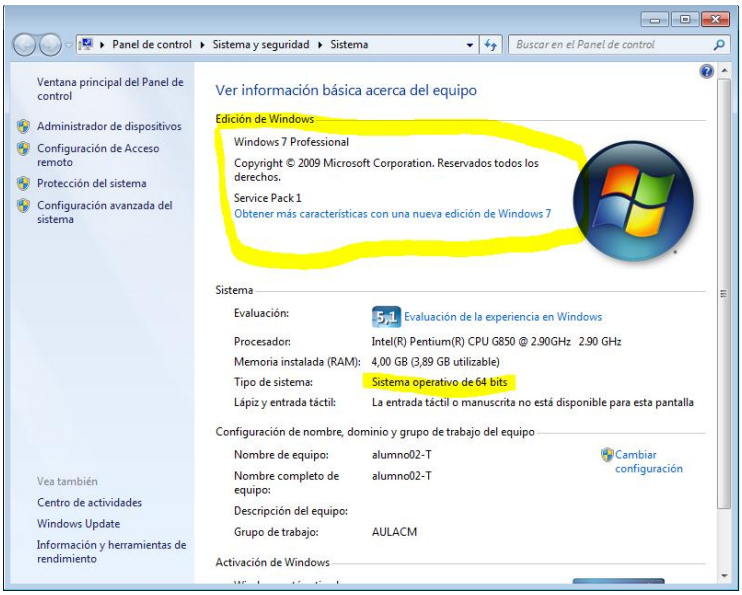
2.2 Identificación de la versión del sistema operativo y arquitectura del equipo

Para determinar si el equipo cumple los requisitos mínimos para aplicar las actualizaciones o cuál hay que descargar, es necesario conocer la versión del sistema operativo y la arquitectura del equipo.

1. Pinche en botón inicio, sobre Equipo pulse el botón derecho del ratón y elija la opción propiedades. (esta opción varia un poco dependiendo del SO). También puede hacer esta acción sobre el icono de Equipo/MI-PC en el escritorio.



2. Aparecerá una pantalla similar a la siguiente en la que deberá ver las opciones marcadas para identificar el SO y si es de 32 o 64 bits para aplicar el parche correspondiente.



3. Si se trata de Windows 10, para comprobar la versión (RTM, 1511,607, etc), se puede ejecutar el comando “winver” desde una consola de comandos (cmd) o desde la opción “ejecutar” (tecla Windows + “R”)”.

4. Si se trata de sistemas operativos Servidor Windows (Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2 o 2016), deberán seguirse las instrucciones indicadas en el **ANEXO 2**.

2.3 Identificación de los requisitos mínimos para aplicar los parches

Existen actualizaciones para las siguientes versiones de sistemas operativos con sus correspondientes services pack. Si la versión del sistema operativo que ha consultado en el punto anterior no se encuentra indicada en la siguiente tabla, puede aplicar previamente al parche de seguridad, la actualización que permita eliminar esta restricción.

Sistema Operativo
Windows Vista SP2 x86
Windows Vista SP2 x64
Windows 7 SP1 x86
Windows 7 SP1 x64
Windows 8.1 x86

Windows 8.1 x64
Windows 10 RTM x86
Windows 10 RTM x64
Windows 10 1511 x86
Windows 10 1511 x64
Windows 10 1607 x86
Windows 10 1607 x64
Windows XP SP3 x86
Windows XP SP2 x64
Windows 8 x86
Windows 8 x64
Windows Vista x86
Windows Vista x64

En función de la antigüedad del sistema operativo del equipo pueden ser necesarias actualizaciones para poder aplicar los parches de seguridad que protegen de la vulnerabilidad ante el ransomware wannacry. En todo caso se han considerado las más comunes indicadas en la siguiente tabla, y disponibles en los puntos de descarga (ftp de educamadrid y servidores web accesibles desde VLAN 100). Estas actualizaciones deberán aplicarse antes de los parches de seguridad.

Software Complementario
Windows XP SP3
Windows Vista SP2 x86
Windows Vista SP2 x64
Windows 7 SP1 x86
Windows 7 SP1 x64

Si el sistema operativo es Windows XP con un Service Pack inferior al SP3, será necesario primero instalar el Service Pack 3 que también se encuentra disponible en los puntos de descarga, y posteriormente el parche de seguridad correspondiente para Windows XP. En el caso de Windows 7 es necesario tener previamente instalado el Service Pack 1 por lo que si no lo tuviese sería necesaria su instalación como paso previo a la instalación del parche de seguridad. De manera similar sucede con Windows Vista y el Service Pack 2.

2.4 Descarga de las actualizaciones necesarias

Actualmente el acceso a Internet desde la Red Educativa se encuentra restringido, no obstante es posible el acceso a los siguientes recursos y descargar las actualizaciones necesarias.

Para la descarga de las actualizaciones necesarias se recomienda el uso del navegador Chrome o Firefox, ya que en ocasiones se han encontrado problemas en la descarga utilizando Internet Explorer.

Se han habilitado los siguientes puntos de descarga en función de la red en la que se encuentre el equipo desde el que se realice la conexión.

2.4.1 FTP Educamadrid

Se ha publicado en el portal de Educamadrid esta guía que detalla unas instrucciones generales necesarias para la actualización de los equipos, así como los parches y actualizaciones que deberán aplicarse. Los parches están identificados por sistema operativo, arquitectura (x86 32 bits o x64 64 bits) y en el caso de Windows 10 por compilación (RTM, 1511 o 1607).

Este recurso está accesible desde la red educativa, la red de gestión e Internet.

ftp://ftp.educa.madrid.org/MD

En la siguiente imagen se puede observar el aspecto de este recurso.

2.4.2 Servidores dedicados accesibles desde la red educativa (**solo VLAN 100**)

También es posible realizar las descargas necesarias desde un conjunto de cinco servidores, destinado cada uno de ellos a un Área Territorial, y cuyas direcciones web de acceso se indican a continuación:

- **DAT MADRID CENTRO: http://195.77.130.4 ➔ http://datcentro.madrid.org**
- **DAT MADRID NORTE: http://195.77.130.5 ➔ http://datnorte.madrid.org**
- **DAT MADRID SUR: http://195.77.130.6 ➔ http://datsur.madrid.org**
- **DAT MADRID ESTE: http://195.77.130.7 ➔ http://dateste.madrid.org**
- **DAT MADRID OESTE: http://195.77.130.8 ➔ http://datoeste.madrid.org**

En la siguiente imagen se muestra el aspecto aproximado de este recurso web.


madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

CONSEJERÍA DE ECONOMÍA, EMPLEO Y HACIENDA
Comunidad de Madrid

Parches de Seguridad para el Entorno Educativo

En esta página puede descargarse los parches de seguridad para la prevención del ataque del WannaCry

Parches Wannacry

Windows 8.1

windows8.1-kb4012213-x64.msu - Parche Windows 8.1 64 bits
windows8.1-kb4012213-x86.msu - Parche Windows 8.1 32 bits

Windows 7

windows7-kb4012212-x64.msu - Parche Windows 7 64 bits
windows7-kb4012212-x86.msu - Parche Windows 7 32 bits

Windows 10 1607

Windows10.0-kb4019472-x64.msu - Parche Windows 10 64 bits
Windows10.0-kb4019472-x86.msu - Parche Windows 10 32 bits

Windows XP

windowsxp_sp3-kb4012598-x86.exe - Parche Windows XP 32 bits

Agencia para la Administración Digital de la Comunidad de Madrid

2.4.3 Descarga directa desde Internet

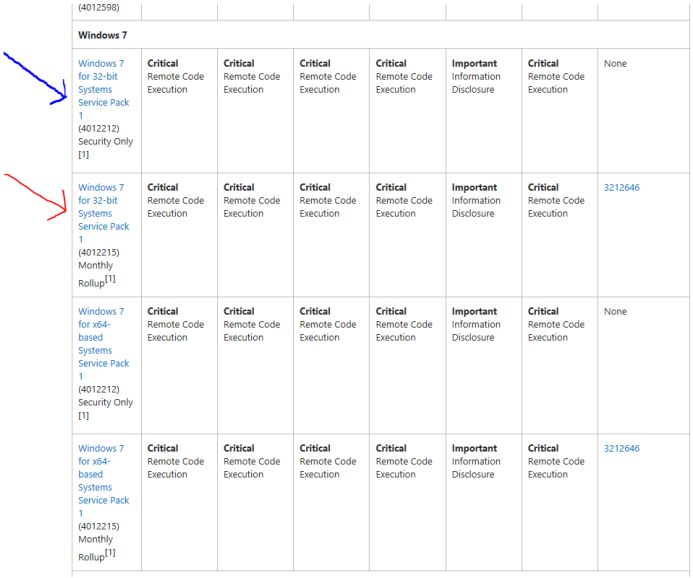
Además de los recursos indicados anteriormente, también es posible realizar la descarga de las actualizaciones necesarias a través de Internet en las direcciones que se indican a continuación. En el siguiente enlace se pueden descargar los parches por sistema operativo con soporte por parte de Microsoft.

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Existen parches para las siguientes versiones de Windows:

Sistema Operativo	Tipo de actualización
Windows Vista SP2 x86	
Windows Vista SP2 x64	
Windows 7 SP1 x86	Actualización de seguridad
Windows 7 SP1 x86	Acumulativo mensual
Windows 7 SP1 x64	Actualización de seguridad
Windows 7 SP1 x64	Acumulativo mensual
Windows 8.1 x86	Actualización de seguridad
Windows 8.1 x86	Acumulativo mensual
Windows 8.1 x64	Actualización de seguridad
Windows 8.1 x64	Acumulativo mensual
Windows 10 RTM x86	
Windows 10 RTM x64	
Windows 10 1511 x86	
Windows 10 1511 x64	
Windows 10 1607 x86	
Windows 10 1607 x64	

En la siguiente imagen se muestra el enlace que debe utilizarse para la descarga del parche correspondiente para el sistema operativo Windows 7 - 32 bits. Indicar que en algunos casos existen dos parches para el mismo sistema operativo, uno que protege ante la vulnerabilidad y otro que es acumulativo correspondiente al mes completo. Con el fin de reducir los tiempos de instalación se recomienda la descarga e instalación del parche de seguridad individual (marcado con la flecha azul) y que es el disponible en los repositorios indicados.



(4012598)							
Windows 7							
Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only [1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for 32-bit Systems Service Pack 1 (4012215) Monthly Rollup [1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows 7 for x64-based Systems Service Pack 1 (4012212) Security Only [1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for x64-based Systems Service Pack 1 (4012215) Monthly Rollup [1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646

Dada la gravedad del ciberataque, Microsoft ha publicado de manera excepcional actualizaciones para sistemas operativos no soportados. En la siguiente tabla se indica la lista de parches publicada.

Sistema Operativo
Windows XP SP3 x86
Windows XP SP2 x64
Windows 8 x86
Windows 8 x64
Windows Vista x86
Windows Vista x64

El enlace de descarga de estos parches es el siguiente:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

En el caso de la actualización de Windows 10 deberá tenerse en cuenta que de las cuatro versiones liberadas hasta ahora, necesitan el parche de seguridad las tres primeras:

- Windows 10 – RTM ➔ Necesita actualización kb4012606
- Windows 10 – 1511 ➔ Necesita actualización Kb4013198
- Windows 10 – 1607 ➔ Necesita actualización kb4019472
- Windows 10 – 1703 ➔ NO es necesario actualizar

En la siguiente imagen se pueden observar las opciones de descarga para las distintas versiones de Windows 10.

Windows 10							
Windows 10 for 32-bit Systems [3] (4012606)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210720
Windows 10 for x64-based Systems [3] (4012606)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210720
Windows 10 Version 1511 for 32-bit Systems [3] (4013198)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210721
Windows 10 Version 1511 for x64-based Systems [3] (4013198)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3210721
Windows 10 Version 1607 for 32-bit Systems [3] (4013429)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3213986
Windows 10 Version 1607 for x64-based Systems [3] (4013429)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3213986

NOTA: En algún caso se han presentado problemas de actualización con la versión Windows 10 – 1607 utilizando los de marzo (fecha en la que se publicó el boletín MS17-010), y se han solucionado instalando los parches correspondientes al mes de mayo, descargables desde el siguiente enlace:

https://support.microsoft.com/en-us/help/4000825

En dicho enlace será necesario elegir la versión correspondiente de Windows 10 que tengamos y descargar el último boletín disponible.

Importante: Si se trata de sistemas operativos anteriores: Windows 98, Windows Me, Windows 95, etc., entonces NO existe parche de seguridad. En estos casos no es posible proteger el sistema utilizando un parche y será necesario utilizar otra estrategia: instalar una versión de Windows más moderna, otro tipo de sistema operativo, por ejemplo Linux, etc.

2.4.4 Actualizaciones complementarias

Dado que pueden existir equipos que no dispongan de los requisitos mínimos necesarios para la instalación de los parches de seguridad, se han publicado en los puntos de descarga (ftp de Educamadrid, servidores de descarga por DAT) de las actualizaciones de los casos más comunes. Descarga de la herramienta de detección de infección Panda WannaCryFix.

Estas actualizaciones deberán aplicarse antes de los parches de seguridad (detallado en el punto 2.3 de identificación de requisitos mínimos para aplicar los parches).

Software Complementario
Windows XP SP3
Windows Vista SP2 x86
Windows Vista SP2 x64
Windows 7 SP1 x86
Windows 7 SP1 x64

Con el fin de detectar si un equipo está infectado se está utilizando una herramienta de Panda gratuita que puede descargarse en los recursos anteriormente indicados o en la siguiente url en Internet.

http://www.pandasecurity.com/spain/support/card?id=1689

2.5 Actualización del sistema operativo

El siguiente paso consiste en aplicar las actualizaciones. Como información se relacionan aquellas que se encuentran en los puntos de descarga con el código asignado por Microsoft (terminología KBXXXXXX) y el tamaño en MB.

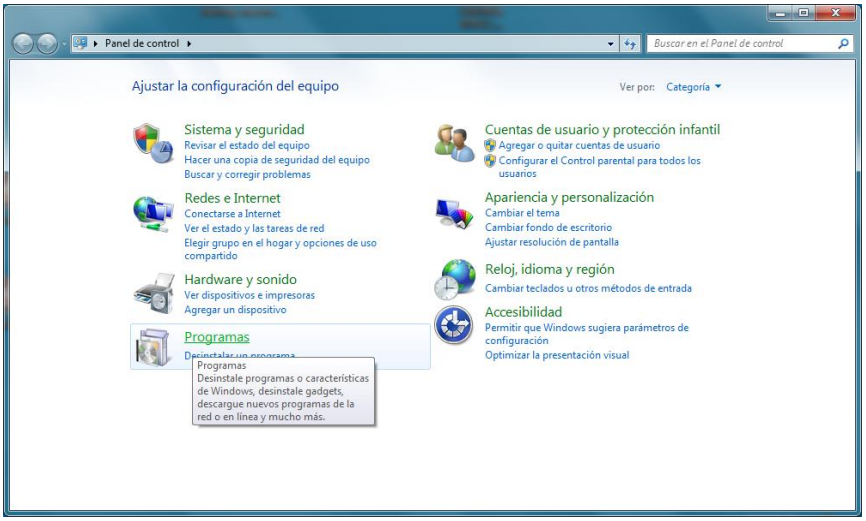
Las referencias y tamaños de las actualizaciones para los casos más comunes son las siguientes:

Sistema Operativo	KB	Tamaño
Windows Vista SP2 x86	KB4012598	1,2 MB
Windows Vista SP2 x64		1,3 MB
Windows 7 SP1 x86	KB4012212	19 MB
Windows 7 SP1 x64		33 MB
Windows 8.1 x86	KB4012213	24 MB
Windows 8.1 x64		37 MB
Windows 10 RTM x86	KB4012606	503 MB
Windows 10 RTM x64		1074 MB
Windows 10 1511 x86	KB4013198	569 MB
Windows 10 1511 x64		1079 MB
Windows 10 1607 x86	KB4019472	593 MB
Windows 10 1607 x64		1079 MB
Windows XP SP3 x86	KB4012598	672 KB
Windows XP SP2 x64		1,9 MB
Windows 8 x86	KB4012598	872 KB
Windows 8 x64		984 KB
Windows Vista x86	KB4012598	1,2 MB
Windows Vista x64		1,3 MB

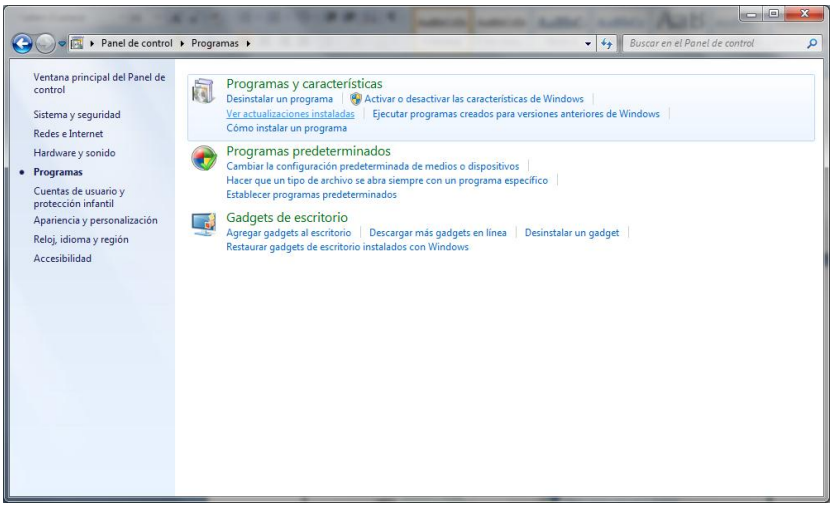
2.5.1 Verificación de que el equipo tiene instalada la actualización

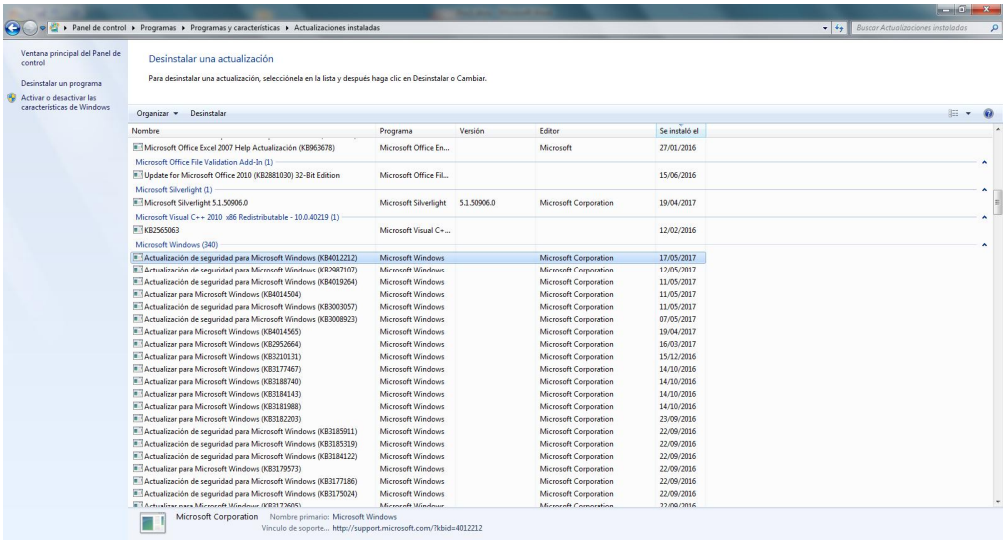
Una vez reiniciado el equipo se deben realizar las siguientes comprobaciones, siendo la más necesaria la verificación de que la actualización del sistema operativo se ha realizado.

Para verificar la actualización en los equipos con sistema operativo Windows 7 o superior, deberá acceder al panel de control y seleccionar Programas.

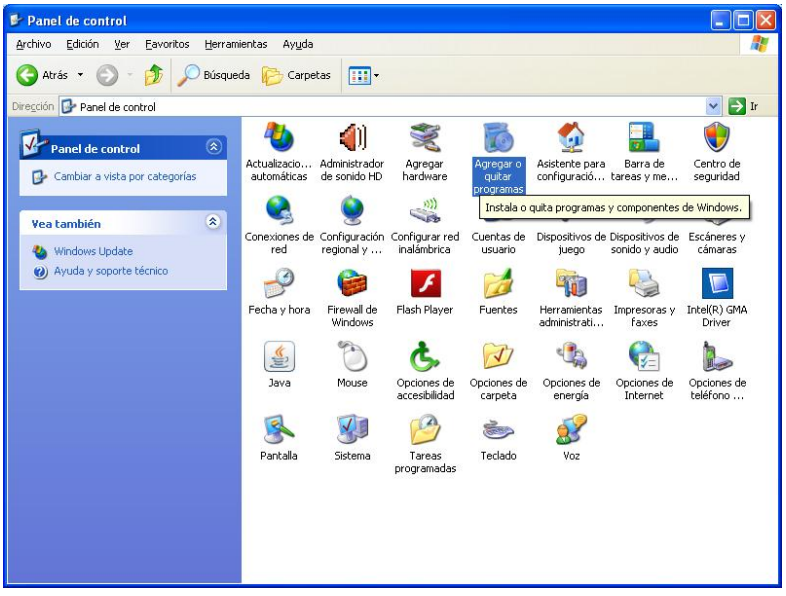


En la opción “Programas y características” Pulsar en “ver actualizaciones instaladas”, aparecerá la pantalla con todas las actualizaciones, deberá comprobar que se encuentra instalado el parche con la referencia que corresponda al sistema operativo y con la fecha de instalación del día de hoy.

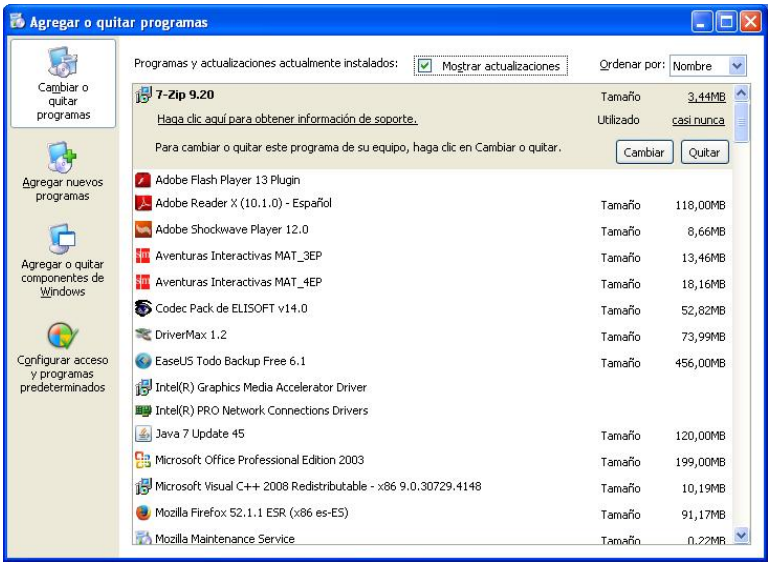




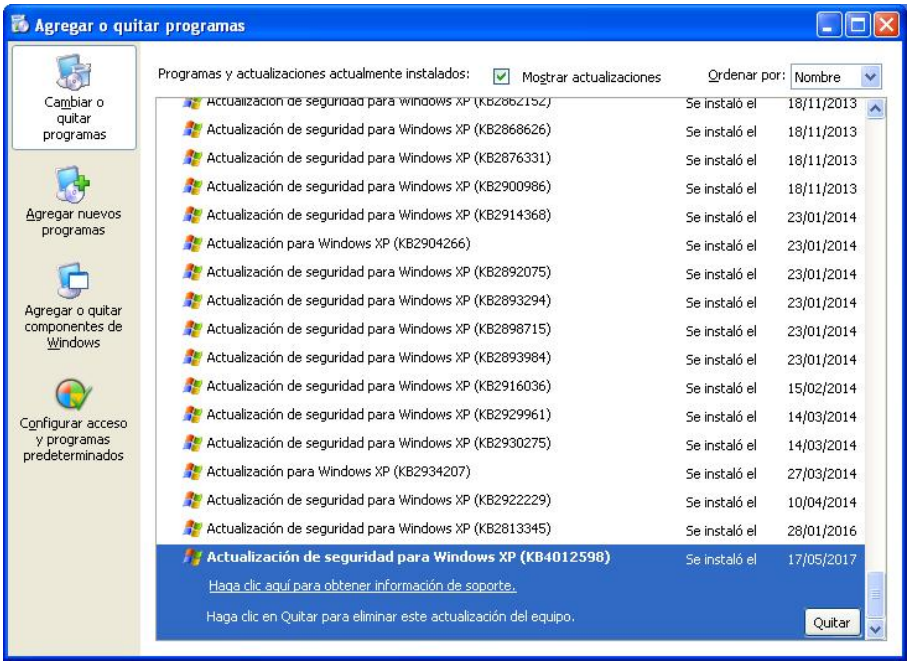
En Windows XP esta comprobación deberá realizarla en Panel de Control—Agregar o quitar programas



Una vez se abre la pantalla de “agregar quitar programas” marcamos la opción “Mostrar Actualizaciones”.



Al final del todo debería aparecer el parche instalado.



2.6 Mecanismos para impedir la infección local

2.6.1 Actualización del antivirus

Es muy recomendable actualizar el antivirus del equipo para garantizar que se detectan ejecuciones locales de ficheros infectados o posibles mutaciones de la amenaza que pudieran surgir en los próximos días. En caso de no contar con un antivirus se recomienda encarecidamente que se instale un producto que garantice la protección.

2.6.2 Herramienta NomoreCry

Si no se dispone de un antivirus con capacidad de detección de este malware se puede utilizar la herramienta publicada por el organismo CCN-CERT denominada NomoreCry Tool (Actualmente versión 0.4). Esta herramienta debe aplicarse si el equipo no está infectado y garantiza que el virus no podrá

atacar el equipo. No obstante no es una herramienta persistente por lo que si se quiere mantener su acción deberá ejecutarse en cada inicio de sesión.

A fecha de elaboración de este procedimiento se ha referenciado y publicado la última versión disponible 0.4, aunque sería conveniente visitar la página correspondiente al CCN-CERT para verificar que no existe una versión más actualizada.

https://www.ccn-cert.cni.es

3 Protocolos de actuación (Resumen)

3.1 Protocolo de actuación para equipos con información crítica y/o sensible

Se recomienda tratar estos equipos primero y dado que tienen información sensible, desconectarlos de la red para evitar que puedan infectarse.

Protocolo de actuación consistente en tres etapas:

1. Encender el equipo **sin conectar a la red** y detecte la posible infección, haciendo uso de un pendrive que contenga el programa "**panda-wannacryfix.exe**", compatible para sistemas operativos Windows XP o superior.
2. Actualizar el sistema operativo con los parches correspondientes, según se describe en el anterior apartado 2.2 y sucesivos.
3. Actualización del antivirus o instalación de herramientas que impidan la infección, según apartado 2.7.

3.2 Protocolo de actuación para el resto de equipos sin información sensible

Este resumen incluye los mismos pasos que el anterior, **pero al tratarse de equipos que no tienen información sensible**, ante cualquier problema o incidencia que pueda surgir (infección con otro tipo de virus, imposibilidad de concluir el proceso de análisis, o la instalación de parches o la actualización del antivirus, etc…), deberá considerarse su borrado y maquetado con una imagen limpia y confiable.

Protocolo de actuación consistente en tres etapas:

1. Encender el equipo. A continuación revisar si está infectado mediante el uso de la herramienta "panda-wannacryfix.exe".
2. Actualizar el sistema operativo con los parches correspondientes, según se describe en el anterior apartado 2.2 y sucesivos.
3. Actualización del antivirus o instalación de herramientas que impidan la infección, según apartado 2.7.

En ambos casos si el equipo está infectado, apagarlo y desconectar de la red hasta nuevas instrucciones.

4 ANEXO 1 – Desactivación de la persistencia Panda Wannacry Fix

En este apartado se muestra cómo desactivar la persistencia del proceso de detección de la herramienta Panda Wannacry Fix. Esta acción se deberá realizar cuando estén instalados los parches de seguridad para evitar el contagio en caso de que en la misma red se pudiera encontrar un equipo infectado. El programa Panda Wannacry Fix queda residente en el equipo, lo que significa que su acción permanece en los siguientes inicios de sesión del ordenador. Esta situación puede generar la petición de credenciales de usuario y contraseña de un usuario administrador del equipo en cada inicio de sesión. Para evitarlo se puede desactivar la característica de persistencia mediante el siguiente procedimiento.

Pulse el botón de inicio, y la opción “ejecutar”, (método abreviado pulse tecla Windows + R), escriba “msconfig” y aceptar, en la pantalla que se muestra seleccione la pestaña “Inicio de Windows”. **Deberá desactivar el check** en la entrada que ponga “Panda Technologies” asociada al comando **KillWC.exe** en Windows 10 puede ser necesario seleccionar dicha entrada, pulsar botón derecho y elegir la opción **“deshabilitar”.**

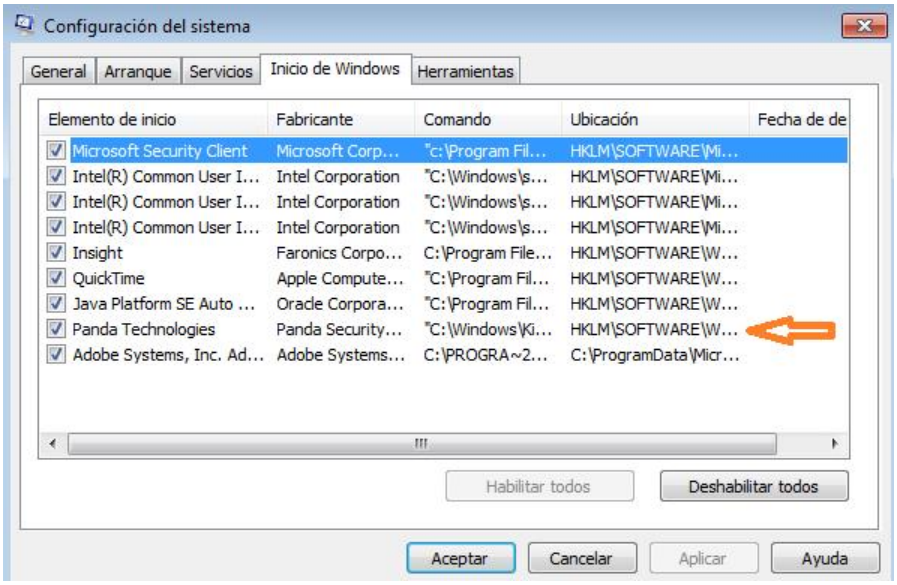


Imagen Windows 7 y superiores

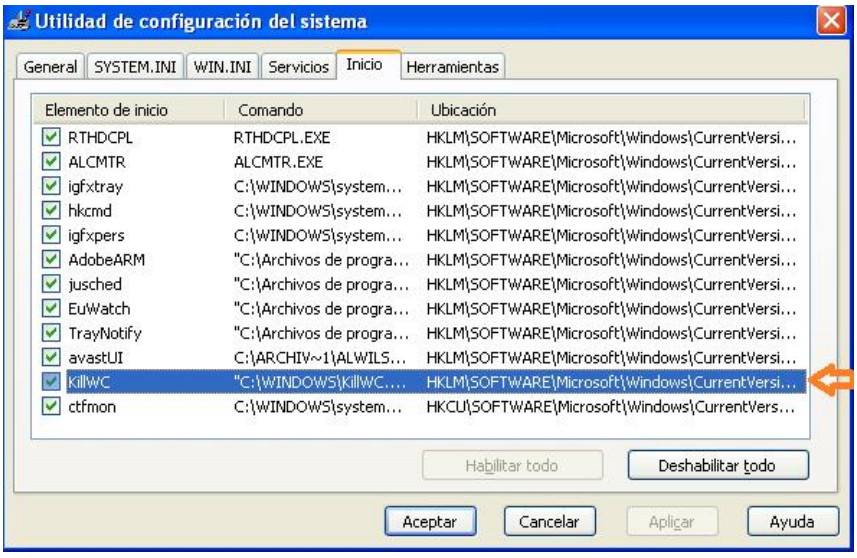


Imagen en Windows XP

5 ANEXO 2 – Parcheado de Servidores Windows

En algunos casos existen centros que cuentan con equipos con sistema operativo Windows Server. Estos equipos también son vulnerables a la amenaza y deben parchearse. Si se trata de equipos con sistemas Linux no es necesario ya que no están afectados por esta vulnerabilidad.

En la siguiente tabla se indican las referencias de los parches para los sistemas operativos de servidor más comunes.

Sistema Operativo	KB
Windows Server 2003 x86	KB4012598
Windows Server 2003 x64	
Windows Server 2008 x86	
Windows Server 2008 x64	
Windows Server 2008 con SP2 x86	
Windows Server 2008 con SP2 x64	
Windows Server 2008 R2 con SP1	KB4012212
Windows Server 2012	KB4012214
Windows Server 2012 R2	
Windows Server 2016	KB4013429

La descarga de estos parches se deberá realizar en la página web de Microsoft en la siguiente dirección url:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

En el caso de la descarga de los parches para Windows Server 2003 y Windows Server 2008 se utilizará el siguiente enlace:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

El procedimiento de instalación no difiere del realizado para los sistemas operativos cliente.