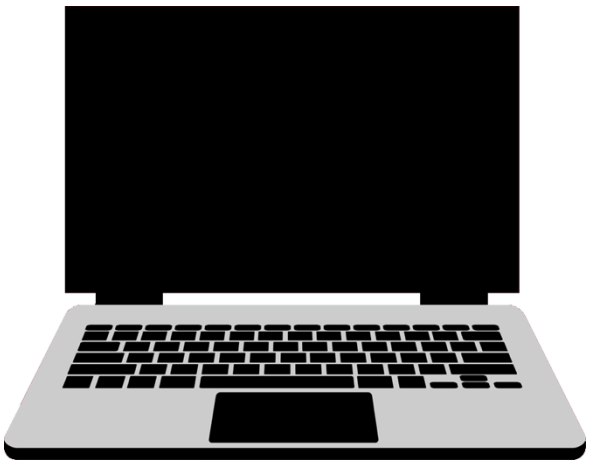
WannaCry

Buen día, gracias por confiar en DragonJAR para asesorarte gratuitamente sobre las recomendaciones a tener en cuenta al interior de tu organización en el caso del Ransomware WannaCry.

Este documento pretende ser una guía, paso a paso para que puedas reaccionar a equipos ya infectados con el WannaCry o evitar que equipos de tu organización se vean afectados.

Para esto dividimos el documento en 2, la primera parte para quien ya cuenta dentro de su infraestructura con equipos infectados y la segunda parte para quien desea evitar la infección y propagación de este ransomware en los equipos de cómputo que administra.

YA TENGO EQUIPOS INFECTADOS **QUIERO PREVENIR LA INFECCIÓN**



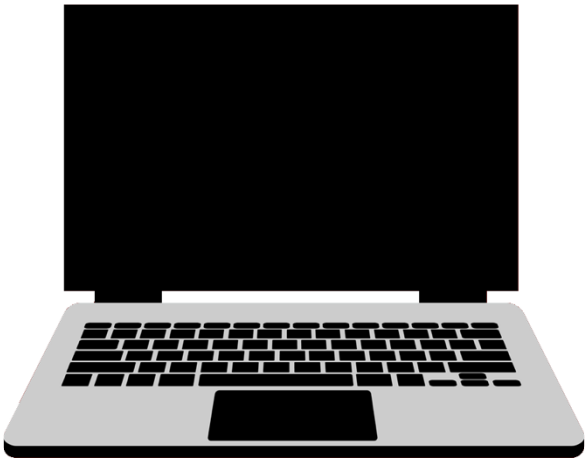
YA TENGO EQUIPOS INFECTADOS ¿QUÉ HAGO?

Si ya cuentas con equipos infectados en tu organización, seguramente ya los tienes identificados, es muy fácil hacerlo ya que este tipo de amenazas trata de llamar la atención del usuario para que pueda realizar el pago y descifrar sus archivos, en los equipos infectados encontraras una ventana roja similar a la que está en la imagen que tienes a la derecha, también el fondo de pantalla de los equipos ha cambiado a un mensaje con fondo negro similar a la imagen de la izquierda.

Pero también puede darse el caso que tengas infecciones no reportadas en equipos desatendidos como servidores o con sistemas embebidos, en esos casos es recomendable que hagas una búsqueda por toda la red de archivos con extensiones **.wncry** y archivos con extensiones **.wncry** si encuentras archivos con estas extensiones debes identificar inmediatamente el equipo donde se encuentran ya que posiblemente se encuentra infectado y puede ser un foco de propagación de esta amenaza en tu red.

Si tienes ya equipos identificados, lamento informarte que a día de hoy no hay forma de descifrar tus archivos, lo recomendable es que apagues el equipo y lo aísle de la red, si necesitas utilizar el hardware, guarda una copia de seguridad de los archivos afectados o cambia el disco duro para que cuando salga una forma de descifrar este ransomware, nosotros te comuniquemos la solución y puedas recuperar los archivos.

QUIERO PREVENIR LA INFECCIÓN ¿QUÉ HAGO?



Si quieres prevenir la infección de los equipos en tu organización, te recomendamos realizar varios procesos, iniciando por la instalación de las actualizaciones de seguridad en tu sistema operativo y software antivirus, pasando por la revisión (o implementación si no tienes) de las copias de seguridad y la concientización a tus usuarios para que notifiquen inmediatamente cualquier incidente relacionado con este ransomware.

Si cuentas con un Directorio Activo y utilizas el Windows Server Update Services (WSUS), lo primero que te recomendamos es revisar hasta qué punto los equipos Microsoft Windows asociados a tu Directorio Activo tienen parches instalados, el fallo en cuestión que utiliza WannaCry para propagarse fue parcheado por Microsoft el pasado 14 de Marzo y anunciado en el boletín MS17-010 y corresponde al parche KB4012598.

Si cuentas con un directorio Activo y no tienes implementado WSUS, es momento de plantearte la opción y gestionar de forma centralizada tus actualizaciones de seguridad, te dejo este enlace oficial para que sigas las instrucciones de Implementación de Windows Server Update Services en tu organización.

Si cuentas con equipos Windows fuera de tu Directorio Activo o directamente no cuentas con un directorio activo, la recomendación es que realices un escaneo de tu red en busca de equipos que no tengan instalado el parche anunciado en el boletín MS17-010 para eso te recomendamos seguir las instrucciones que verás a continuación.

Vamos a utilizar NMap con un script que nos permita detectar que equipos no tienen el parche instalado para eso necesitas descargar el instalador de https://nmap.org y sigue los siguientes pasos según el sistema operativo.

Para sistemas GNU/Linux

Necesitamos bajar el script NSE de nmap creado por Paulino Calderón que nos permite identificar los equipos sin el parche para el SMB, para eso utilizamos:

curl -0 https://raw.githubusercontent.com/cldrn/nmap-nse-scripts/master/scripts/smb-vuln-ms17-010.nse

Esperamos que descargue el archivo

```
root@Terminator:~# curl -O https://raw.githubusercontent.com/cldrn/nmap-nse-scripts/mas
ter/scripts/smb-vuln-ms17-010.nse
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6228  100  6228    0     0   9444      0 --:--:-- --:--:-- --:--:--  9450
```

Y luego lo copiamos en la carpeta de scripts de nmap, en este caso */usr/share/nmap/scrips:*

```
root@Terminator:~# cp smb-vuln-ms17-010.nse /usr/share/nmap/scripts/
```

Ingresamos a la carpeta de scripts de nmap usando:

- *cd /usr/share/nmap/scripts*

Y actualizamos la base de datos de scripts de nmap, para que detecte el script que acabamos de ingresar en la carpeta y poderlo utilizar:

- *nmap --scritp-updatedb*

```
root@Terminator:/usr/share/nmap/scripts# nmap --script-updatedb

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 17:38 -05
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 5.15 seconds
```

Ya con la base de datos de scripts actualizados, procedemos a identificar los equipos en la red que no cuenten con el parche soluciona el fallo de seguridad que utiliza WannaCry para su propagación, para esto utilizamos el parámetro:

- *nmap --p445 --script smb-vuln-ms17-010 (ip o rango de ips)*

Si encontramos un equipo vulnerable obtendremos una salida como esta:

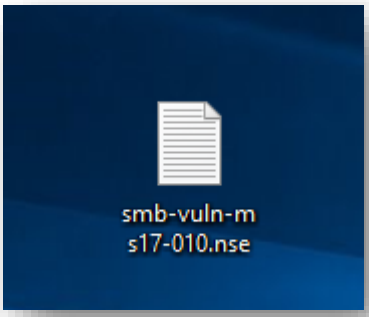
```
root@Terminator:/usr/share/nmap/scripts# nmap -p445 --script smb-vuln-ms17-010

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 18:51 -05
Nmap scan report for 192.168.1.13
Host is up (0.084s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 9C:D2:1E:F0:37:9B (Hon Hai Precision Ind.)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wanna
crypt-attacks/
```

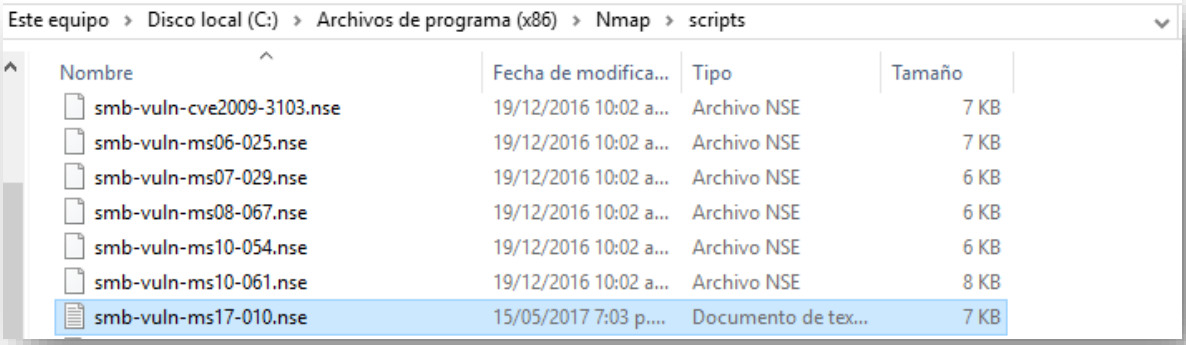
Para sistemas Windows

Para sistemas Windows, descargamos igual el nmap de la página oficial https://nmap.org ingresamos a a este link https://raw.githubusercontent.com/cldrn/nmap-nse-scripts/master/scripts/smb-vuln-ms17-010.nse
copiamos todo y lo guardamos en un bloc de notas con el nombre smb-vuln-ms17-010.nse



Abrimos el cmd (inicio, ejecutar, cmd.exe) y nos ubicamos donde está el archivo que acabamos de guardar (en este caso está guardado en el escritorio), luego lo movemos a la carpeta de scripts de nmap que en Windows seria:

C:\Program Files (x86)\Nmap\scripts



Debemos ir a la carpeta de Nmap así:

```
C:\WINDOWS\system32>cd C:\Program Files (x86)\Nmap
```

Luego debemos listar que debemos ejecutar así:

- *nmap -h*

```
C:\Program Files (x86)>Nmap -h
Nmap 7.40 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
```

Ahora si actualizamos la base de datos de script que es un proceso muy similar al realizado en sistemas GNU/Linux:

- nmap --script-updatedb

```
C:\Program Files (x86)>Nmap --script-updatedb

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 19:29 Hora est. PacÝfico, SudamÚrica
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 5.59 seconds
```

Ahora si podemos validar los equipos que se tienen vulnerabilidades con el siguiente comando:

- *nmap --p445 --script smb-vuln-ms17-010 (ip o rango de ips)*

```
C:\Windows\system32>nmap -sS -sV --script smb-vuln-ms17-010 [redacted]

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 19:39 Hora est. Pacífico, Sudamérica
NSE: Loaded 41 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:39
Completed NSE at 19:39, 0.00s elapsed
Initiating NSE at 19:39
Completed NSE at 19:39, 0.00s elapsed
Initiating ARP Ping Scan at 19:39
Scanning 192.168.1.13 [1 port]
Completed ARP Ping Scan at 19:39, 1.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:39
Completed Parallel DNS resolution of 1 host. at 19:39, 0.04s elapsed
Initiating SYN Stealth Scan at 19:39
Scanning 192.168.1.13 [1000 ports]
Discovered open port 139/tcp on [redacted]
Discovered open port 445/tcp on [redacted]
Discovered open port 135/tcp on [redacted]
SYN Stealth Scan Timing: About 41.53% done; ETC: 19:40 (0:00:44 remaining)
Completed SYN Stealth Scan at 19:40, 50.84s elapsed (1000 total ports)
Initiating Service scan at 19:40
Scanning 3 services on 192.168.1.13
Completed Service scan at 19:40, 6.48s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.1.13.
Initiating NSE at 19:40
Completed NSE at 19:40, 0.07s elapsed
Initiating NSE at 19:40
Completed NSE at 19:40, 0.00s elapsed
Nmap scan report for 192.168.1.13
Host is up (0.068s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 9C:D2:1E:F0:37:9B (Hon Hai Precision Ind.)
Service Info: Host: WINPWN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
```

Después de identificadas las maquinas vulnerables dentro de la organización, debes aplicar el parche correspondiente al sistema operativo *(es altamente recomendable que verifiques en un entorno controlado que todas las aplicaciones de tu negocio corran sin problemas después de aplicar el parche)* ya sea utilizando Windows Update o descargando y ejecutando el parche puntual para el sistema operativo de la página oficial.

Con esto estarías mitigando el riesgo de difusión de WannaCry o de cualquier código malicioso que quiera aprovechar este fallo de seguridad dentro de la red.

El siguiente paso es probar que la solución antivirus que tengas instalada este actualizada y funcione correctamente, para eso recomendamos realizar el EICAR Test File (clic aquí para ver cómo realizar el test).

Si realizas copias de seguridad en tu organización es el momento idóneo para revisar que el proceso esté funcionando correctamente, que las copias se realicen en un equipo diferente al que tiene la información a salvaguardar y que hagas pruebas de restauración para ver si las mismas funcionan como debe ser, no hay nada peor que enterarte en el momento más inoportuno (cuando requieres los backups) que estos no se estaban realizando adecuadamente o los datos están corruptos.

Si cuentas con algún canal de comunicación con tus usuarios, aprovéchalo para alertarles sobre la amenaza y que notifiquen al área encargada cuando se detecte alguna anomalía, actuar a tiempo puede salvar tu información, esta imagen generada para explicar la amenaza puede ser una forma simple de informar a tus usuarios sobre el WannaCry.

Muchas gracias por confiar en DragonJAR, hablaste con Pablo, recuerda que puedes contactarnos en www.DragonJAR.org/contacto