



# Análisis Forense

Adan Avilés

Junio 2020

# Índice

<b>1. Presentación del problema</b>	<b>3</b>
1.1. Sede de Australia . . . . .	3
1.2. Sede en Italia . . . . .	3
1.3. Sede en España . . . . .	3
1.3.1. Evidencias Facilitadas . . . . .	3
<b>2. Resolución:</b>	<b>5</b>
2.1. Australia . . . . .	5
2.2. Italia . . . . .	7
2.3. España . . . . .	8

# 1. Presentación del problema

La empresa Invent S.L, que dispone de sedes en Australia, Italia y España, ha sufrido un incidente de seguridad en cada una de ellas.

## 1.1. Sede de Australia

Por una parte, en la sede de Australia, se ha detectado la fuga de información sensible de varios de sus empleados (direcciones de correo y contraseñas). El conjunto de afectados indica haber recibido una campaña de correos sospechosos con adjuntos HTML similares al portal de Office 365 durante los últimos días. Esta empresa no tiene (2FA) factor de autenticación en dos pasos, por lo que un atacante podría acceder al correo corporativo y otro tipo de aplicativos públicos en Internet alojados en Microsoft. Puesto que hay más de 10.000 empleados en la empresa, no es posible el reseteo y bloqueo de todas las cuentas por motivos de continuidad de negocio, por lo que es necesario localizar únicamente a los afectados.

## 1.2. Sede en Italia

Por otra parte, en Italia se ha producido un acceso no autorizado a uno de sus servidores de contabilidad. Dicho acceso ha sido detectado mediante una revisión periódica por el equipo de IT. En este caso, el equipo planea contratar a un proveedor externo para que se haga cargo de este incidente

## 1.3. Sede en España

Finalmente, en la sede de España, se ha detectado un ataque en uno de los servidores de su fábrica de textiles. Todos los archivos del servidor han sido cifrados con la extensión “.NM4”. Estos equipos estaban parcheados contra MS17-010.

### 1.3.1. Evidencias Facilitadas

Puesto que formamos parte del equipo de respuesta ante incidentes de la compañía, nuestra misión consiste en descubrir qué ha pasado en cada una de las situaciones que se plantean.

Para ello el equipo de IT nos ha facilitado las siguientes evidencias:

- Australia: logs de tráfico del proxy de navegación en el intervalo de fechas en el que se produjo el incidente.
- Italia: ninguna puesto que se encargará un proveedor externo.
- España: estado de los puertos abiertos en el sistema y parte del mensaje de rescate.

## 2. Resolución:

Resolveremos ahora las cuestiones planteadas para cada país.

### 2.1. Australia

#### ¿Qué tipo de amenaza ha impactado?

La sede australiana ha sufrido un ataque de Ingeniería Social, que es conocido como “Phising”.

Los atacantes han suplantado el login de *Outlook* mediante una web falsa, para así poder conseguir las credenciales de los empleados que caigan en el ataque, pudiendo acceder al contenido que tengan almacenado en *Office 365* y su información, además de de la empresa.

Para conseguir esto lo único que tuvieron que hacer es enviar un correo de forma masiva a los empleados, pidiendo que abran el archivo HTML y se logeen en él, después esos datos se enviarían a los atacantes.

#### ¿Qué direcciones de correo de usuario se han visto afectadas?

Abrimos el archivo facilitado en WireShark.

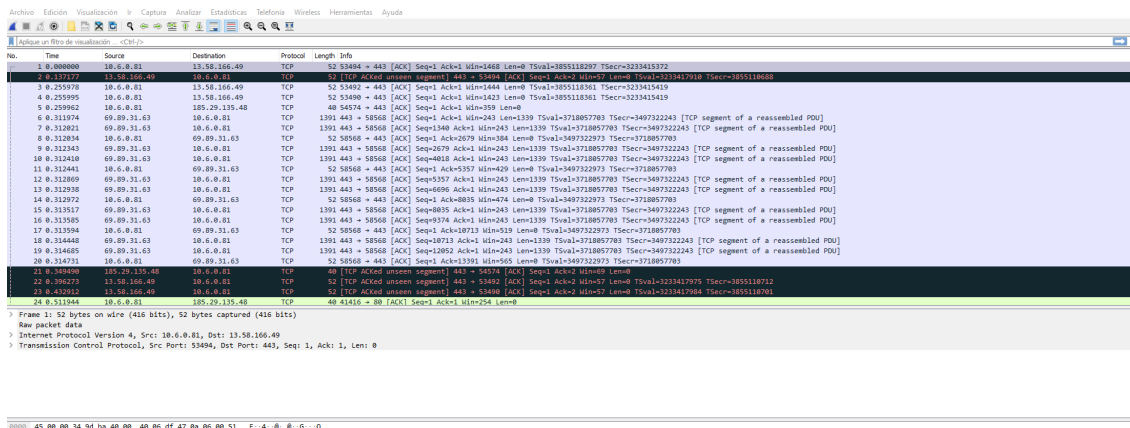


Figura 1: Wireshark Pcap

Haciendo un filtrado en wireshark para peticiones GET (`http.request.method == "GET"`), y revisándolo, encontramos uno que en la info contiene *user*, lo cual puede ser porque es un inicio de sesión.

**Decode from Base64 format**  
Simply enter your data then push the decode button.

bWdhcmNpYUBpbmZlbnQuY29rOm1hbnphbmExMjMK==&aHR0cHM6Ly9wYXN0ZWJpb20vMmVhRmVtM0MK==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

mgarcia@invent.com:manzana123  
https://pastebin.com/2R0Fem3C

**Figura 2:** *Parámetros decodificados*

Decodificamos los parámetros de la url, que aparecen en base64 obteniendo: Así, si nos dirigimos al pastebien y sacamos los datos, vemos que tenemos los siguientes pares de usuario:contraseña:

- mgarcia@invent.com:manzana123
- hifid@invent.com:123dmr
- hjerfs@invent.com:applepup
- jdarwin@invent.com:redcar#

Imagínese que tiene que analizar el fichero .pcap facilitado en las evidencias en un entorno linux/windows por línea de comando sin entorno gráfico. Realice un script para parsear el fichero .pcap, de forma que se muestre el resultado final (los correos electrónicos afectados ) por línea de comando.

## 2.2. Italia

Para enviar las evidencias al proveedor externo se va a realizar una captura de información y clonado del servidor comprometido. ¿Qué parte hardware del servidor se debería clonar antes de apagar el equipo?

La parte del hardware que deberíamos clonar sería la memoria RAM para su posterior análisis, pues al apagarlo se perderán los datos.

¿Qué comando utilizaría para realizar el clonado del disco?

El comando que utilizaremos será **dd**, *data duplicator*.

La sintaxis general de este comando es

```
dd if =$input_data of =$output_data
```

En nuestro caso, la duplicación de disco a disco sería:

```
dd if =/dev/sda1 of=/dev/sdb1 bs=4096
```

¿Qué y cómo habría que calcular después del clonado del disco para verificar la integridad del mismo?

Tras el clonado, y habiendo tenido en cuenta que no hemos usado herramientas intrusivas que puedan alterar los datos, sino que sean conocidas o estén documentadas además de ser reproducibles, habremos de calcular el **HASH**.

Si el hash de ambos discos coincide, sabremos que tenemos una copia exacta del disco original. Hemos de tener en cuenta que herramientas como *CAINE* calculan automáticamente el hash de la copia para poder compararlo.

También se puede hacer en línea de comandos con Linux. Con el comando **fdisk -l**, obtendría la lista de discos y con el comando (por ejemplo) **md5sum nombre\_de\_\_disco** obtendría el hash md5.

## Encrypted files!

All your files are encrypted. Using AES256-bit encryption and RSA-2048-bit encryption.  
 Making it impossible to recover files without the correct private key.  
 If you are interested in getting the key and recover your files  
 You should proceed with the following steps.

The only way to decrypt your files safely is to buy the Decrypt and Private Key software.  
 Any attempts to restore your files with the third-party software will be fatal for your files!

To proceed with the purchase you must access one of the link below

- <https://3fprihycwetwk2m7.onion.to/>
- <https://3fprihycwetwk2m7.onion.link/>

If neither of the links is online for a long period of time, there is another way to open it, you should install the Tor Browser

```
If your personal page is not available for a long period there is another way to open your personal page - installation and use of Tor Browser:

1. run your Internet browser (if you do not know what it is run the Internet Explorer);
2. enter or copy the address https://www.torproject.org/download/download-easy.html.en into the address bar of your browser and press ENTER;
3. wait for the site loading;
4. on the site you will be offered to download Tor Browser; download and run it, follow the installation instructions, wait until the installation is completed;
5. run Tor Browser;
6. connect with the button 'Connect' (if you use the English version);
7. a normal Internet browser window will be opened after the initialization;
8. type or copy the address

https://3fprihycwetwk2m7.onion

in this browser address bar;
```

**Figura 3:** Mensaje de los atacantes

## 2.3. España

### ¿Qué tipo de amenaza ha impactado?

La sede de España ha sufrido un ataque, mediante un ransomware que encripta los archivos con la extensión *NM4*. Es probable que sea un ransomware que se distribuya a través de mails o de descargar programas ilícitos.

El objetivo de este tipo de malware es obtener beneficio económico tras solicitar de dinero para desencriptar los ficheros encriptados o "secuestrados", como podemos ver en la imagen 3.

### ¿Cómo funciona este tipo de amenaza?

Este tipo de amenaza se basa en la infección de los ficheros por un malware que se centra en encriptar los archivos de los usuarios con una combinación de algoritmos que no sea posible de desencriptar.

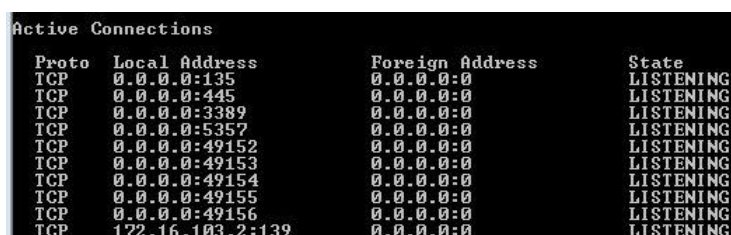


En particular, el virus *NM4* pertenece a la familia de variantes de ransomware que emplean los algoritmos de *AES* y *RSA* para su encriptación, complicando el proceso de desencriptación de los datos.

Seguidamente al haber infectado la maquina del usuario, la convierte en un bot para replicarse por la red interna del ordenador infectado, pivotando entre los puertos abiertos. Finalmente, deja en el equipo la nota o imagen que hemos visto con anterioridad, en la que están escritas las indicaciones a seguir si queremos recuperar los archivos.

### ¿Cuál ha sido el vector de entrada más probable utilizado?

Nos fijamos en las evidencias de los puertos, Sabemos que a través del puerto SMB,



Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	172.16.103.2:139	0.0.0.0:0	LISTENING

Figura 4: Puertos

como hacía *EternalBlue* no es probable al estar los equipos parcheados con MS17-010, como se nos indica, así que a través de los puertos 139 o 445 no es posible haber accedido. Un posible vector de estrada es a través del puerto 5357, pues este permite acceder usando el protocolo **Remote Desktop Protocol** (RDP) sumado a fuerza bruta de contraseñas.

### Indique 3-5 medidas imprescindibles que hubiesen evitado el ataque.

- Tener en cuenta qué puertos dejamos abiertos y sus posibles vulnerabilidades.
- Hacer que los empleados tengan el mínimo acceso posible a otras máquinas, para así evitar que el ransomware pivote. Para esto podemos tener la red compartimentada, no una única red con todos los equipos en ella.
- Tener una copia de seguridad (a ser posible diaria) de todos los archivos, para en caso de que algo así ocurra, tener siempre los archivos disponibles y solo tener que preocuparnos de recuperar los ordenadores infectados.
- Deshabilitar, como norma general, el Remote Desktop a no ser que sea extrictamente necesario.

- Filtrar los archivos ejecutables que se descargan o envían por correo.
- Tener instalado un antimalware actualizado.