

Forum:[Hack Forums](#)

Thread: [White Hat Hardening Scripts \(BEGINNER FRIENDLY!!!\)](#)

BORA9 - May 22, 2025, 8:26 pm

I got some good white hat techniques if anyone wants them! PM me or Donate!!!

I've come across some emulators and botnets. ALL using remote desktop services.

I do not use remote desktop services to be honest. Never have. Come to find out I found some browser emulators using basic CPU analysis.

Add-Type @"

using System;

using System.Runtime.InteropServices;

using System.Text;

public class HiddenWindows {

[DllImport("user32.dll")]

public static extern int EnumWindows(EnumWindowsProc proc, int lParam);

public delegate bool EnumWindowsProc(IntPtr hWnd, int lParam);

[DllImport("user32.dll")]

public static extern bool IsWindowVisible(IntPtr hWnd);

[DllImport("user32.dll")]

public static extern int GetWindowText(IntPtr hWnd, StringBuilder lpString, int nMaxCount);

[DllImport("user32.dll")]

public static extern uint GetWindowThreadProcessId(IntPtr hWnd, out uint processId);

public static void ListHiddenWindows() {

EnumWindows((hWnd, lParam) => {

if (!IsWindowVisible(hWnd)) {

var title = new StringBuilder(256);

GetWindowText(hWnd, title, 256);

if (title.Length > 0) {

uint pid;

GetWindowThreadProcessId(hWnd, out pid);

Console.WriteLine(\$"Hidden Window: {title} | PID: {pid}");

}

}

return true;

}, 0);

}

}

"@

[HiddenWindows]::ListHiddenWindows()

Get file paths for PIDs

```
Get-Process | ForEach-Object {  
    $processPath = $_.Path  
    if ($processPath) {  
        Write-Output "PID: $($_.Id) | Executable Path: $processPath"  
    }  
}
```

For hidden windows!

dwm.exe a virus using a user service to emulate. It's complicated using four .exe's and a cert.
This was the beginning.

Rose_KALI - June 10, 2025, 3:37 am

thank you for this thread. I finally know where to start for my learning.