

Forum:[Hack Forums](#)

Thread: [Latest Windows 1909 with Latest Windows Defender](#)

Ren And Stimpy - March 27, 2020, 11:35 am

Latest Windows 1909 with Latest Windows Defender

You see how no public crpyter is bypassing!

Windows Defender killing the game. Damn I remember back in 2016 when they were the worse!

What you goes doing about bypassing now?

Some0ne.big - March 27, 2020, 11:43 am

(Mar 27, 2020 11:35 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Latest Windows 1909 with Latest Windows Defender

You see how no public crpyter is bypassing!

Windows Defender killing the game. Damn I remember back in 2016 when they were the worse!

What you goes doing about bypassing now?

Clean the stub by hand
use private malware

The only possible way to go

Ren And Stimpy - March 27, 2020, 11:49 am

(Mar 27, 2020 11:43 AM)Some0ne.big Wrote: [\[CITE\]](#) Clean the stub by hand
use private malware

The only possible way to go

I've done that. The latest win ver 1909 and the latest WD is NO joke,
Once stub is uploaded to internet and downloaded, still having issues bypassing

Also disablers no longer disabling REAL-TIME protection

Some0ne.big - March 27, 2020, 11:55 am

(Mar 27, 2020 11:49 AM)Ren And Stimpy Wrote: [\[CITE\]](#) I've done that. The latest win ver 1909 and the latest WD is NO joke,
Once stub is uploaded to internet and downloaded, still having issues bypassing

Also disablers no longer disabling REAL-TIME protection

Do you sign your executables?
where do you upload to?

Disablers don't work no more - thats a fact bro

Vuln - March 27, 2020, 12:01 pm

Interesting. So what exactly changed?

Ren And Stimpy - March 27, 2020, 12:05 pm

(Mar 27, 2020 12:01 PM)Vuln Wrote: [\[CITE\]](#) Interesting. So what exactly changed?

I see they added Tamper Protection, but not sure exactly what changed, as the earlier verisons can be bypassed easily.

This mother fucker is a beast. I've bypassed it a few times, but then once file is uploaded online then downloaded, it then get detected by WD and on mulitple machines, so it 100% is sharing it on their own database!

Maybe Nyan X Cat, can add some information or suggestions! <3

Mirakuru - March 27, 2020, 12:08 pm

(Mar 27, 2020 11:55 AM)SomeOne.big Wrote: [\[CITE\]](#) Disablers don't work no more - thats a fact bro
Add Exclusion instead of disabling.

You can use Remote Shell for it.

Example Powershell Command:

Code Add-MpPreference -ExclusionPath "C:\Temp"

Source:

<https://docs.microsoft.com/en-us/powershell/module/defender/Add-MpPreference?view=win10-ps>

Note: It is required Admin rights.

Vuln - March 27, 2020, 12:18 pm

(Mar 27, 2020 12:05 PM)Ren And Stimpy Wrote: [\[CITE\]](#) I see they added Tamper Protection, but not sure exactly what changed, as the earlier verisons can be bypassed easily.

This mother fugger is a beast. I've bypassed it a few times, but then once file is uploaded online then downloaded, it then get detected by WD and on mulitple machines, so it 100% is sharing it on their own database!

Maybe Nyan X Cat, can add some information or suggestions! <3

Thanks. I will dig into it some more.

Mirakuru - March 27, 2020, 12:45 pm

(Mar 27, 2020 12:05 PM)Ren And Stimpy Wrote: [\[CITE\]](#) I see they added Tamper Protection, but not sure exactly what changed, as the earlier verisons can be bypassed easily.

This mother fugger is a beast. I've bypassed it a few times, but then once file is uploaded online then downloaded, it then get detected by WD and on mulitple machines, so it 100% is sharing it on their own database!

Maybe Nyan X Cat, can add some information or suggestions! <3

[??` NYAN CAT `??](#) is already added something about it.

[<<<< Easy >>>> How to bypass Windows Defender for beginner in 5min](#)

-

Ren And Stimpy - March 27, 2020, 12:57 pm

LMAO Mirakuru!!!!

Thanks for the laughs hahahha

SIM-3717028 - March 27, 2020, 4:20 pm

I don't have a problem with win defender using my crypter, might be the actual payload you are using.

Ren And Stimpy - March 27, 2020, 4:52 pm

(Mar 27, 2020 04:20 PM)dsniqwixi Wrote: [\[CITE\]](#) I don't have a problem with win defender using my crypter, might be the actual payload you are using.

Yea HIGHLY doubt that mate. Def if your using a public crypter and a public RAT or your not on Windows 1909 with updated WD.

SIM-3717028 - March 27, 2020, 5:56 pm

<https://imgur.com/a/MODsron>

Would recommend you stay away from this user. Very unprofessional, user initiated a conversation with me first and then proceeded to harass me after I made the choice to decline a test stub based on the user's behavior.

CyberStrike - March 27, 2020, 7:27 pm

Windows Defender is rather robust, you have to figure the number of samples which they are getting is massive, not just from the usual providers but also from Outlook, as every attachment is run in a VM on Azure. I have found no documentation of this but my last engagement this happened (about 1 year ago).

NYANxCAT - March 27, 2020, 9:20 pm

(Mar 27, 2020 12:45 PM)Mirakuru Wrote: [\[CITE\]](#) [??` NYAN CAT `??](#) is already added something about it.

[<<<< Easy >>>> How to bypass Windows Defender for beginner in 5min](#)

-

Yup, I'm using Windows 1909 + Updated Windows Defender + Internet ON in all my tutorials and HF threads. The thread that you have mentioned is just a basic example yet bypassed WD, and as you see I UP&DW the file using the Edge browser.

Jean-Jacques Rousseau - March 29, 2020, 2:10 am

(Mar 27, 2020 07:27 PM)CyberStrike Wrote: [\[CITE\]](#) Windows Defender is rather robust, you have to figure the number of samples which they are getting is massive, not just from the usual providers but also from Outlook, as every attachment is run in a VM on Azure. I have found no documentation of this but my last engagement this happened (about 1 year ago).

This. The amount WD and WD cloud receive is huge, once your malware has made an action that is detected (for example download command), their engine will automatically create a sig for your binary and upload to cloud. The only solution is to use polymorphic binaries and/or wrappers that you can change easily. I am still experimenting with this.

CyberStrike - March 29, 2020, 3:32 am

(Mar 29, 2020 02:10 AM)Supercut Wrote: [\[CITE\]](#) This. The amount WD and WD cloud receive is huge, once your malware has made an action that is detected (for example download command), their engine will automatically create a sig for your binary and upload to cloud. The only solution is to use polymorphic binaries and/or wrappers that you can change easily. I am still experimenting with

this.

Something which I have seen though is that say they prevent one way of downloading a payload, for example in powershell using webclient, well they seem to use a regexp (regular expression) for detecting this. The Windows API has so much overlap I guess is the best way to say it, where multiple APIs have different functions which as in our example can allow a download. JA3 signatures are also something which AV products use, not to mention of course signing is crucial, even powershell scripts now should be signed.

SideNote: I remember a while back multiple AVs were caught uploading samples although the user had disabled that option, can't find anything on it this was circa 2017 I think.

Edit: Something I used to do was a quick enumeration of an environment, in my case I expected certain usernames or a specific AD domain name if this was not the case then payloads would not run, also I would have a timer on my payloads where in after say 1 day or 1 month they would expire.

Jean-Jacques Rousseau - March 29, 2020, 12:46 pm

(Mar 29, 2020 03:32 AM)CyberStrike Wrote: [\[CITE\]](#) Something which I have seen though is that say they prevent one way of downloading a payload, for example in powershell using webclient, well they seem to use a regexp (regular expression) for detecting this. The Windows API has so much overlap I guess is the best way to say it, where multiple APIs have different functions which as in our example can allow a download. JA3 signatures are also something which AV products use, not to mention of course signing is crucial, even powershell scripts now should be signed.

SideNote: I remember a while back multiple AVs were caught uploading samples although the user had disabled that option, can't find anything on it this was circa 2017 I think.

Edit: Something I used to do was a quick enumeration of an environment, in my case I expected certain usernames or a specific AD domain name if this was not the case then payloads would not run, also I would have a timer on my payloads where in after say 1 day or 1 month they would expire.

What I am currently doing is making my "crypter" as minimal as possible. What you are talking about is anti-emulation, this can be done by the fingerprinting methods that you are describing of course, however, that is not the most optimal way. What I am talking about is after emulation; when the payload is running and has been installed on target system.

Ren And Stimpy - March 30, 2020, 9:32 am

Thanks for all the responses. So is anyone bypassing?

rainbowlackjack - March 30, 2020, 5:01 pm

no i cant get anything to save to desktop

Ren And Stimpy - March 30, 2020, 6:29 pm

(Mar 30, 2020 05:01 PM)lackaff Wrote: [\[CITE\]](#) no i cant get anything to save to desktop

Yup, no exe will.

Lets see what people can think of how to bypass

Besides

Excludes or disabler, but that will work def if you have a Working UAC bypass.

Ramboll - March 30, 2020, 8:15 pm

windef + cloud and last update =====> done , bypassed

Ren And Stimpy - March 31, 2020, 6:04 am

(Mar 30, 2020 08:15 PM)Ramboll Wrote: [\[CITE\]](#) windef + cloud and last update ==> done , bypassed

Incorrect. As if it is a .exe it will not bypass. I also tested cloud. Detected on updated 1909 and WD

Ramboll - March 31, 2020, 7:04 am

(Mar 31, 2020 06:04 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Incorrect. As if it is a .exe it will not bypass. I also tested cloud. Detected on updated 1909 and WDs

bro better stop it . what s wrong with you ? lot of fake coders here just sucking ... last night i tested my crypter+ orcus vs windef + cloud with success.?

Ren And Stimpy - March 31, 2020, 8:03 am

(Mar 31, 2020 07:04 AM)Ramboll Wrote: [\[CITE\]](#) s

bro better stop it . what s wrong with you ? lot of fake coders here just sucking ... last night i tested my crypter+ orcus vs windef + cloud with success.?

100% it is not bypassing Windows Verison 1903 (updated) and Windows Defender.

You can start a HF convo, and send me your file I'll test, maybe yours is one of a kind....

Ramboll - March 31, 2020, 10:43 am

(Mar 31, 2020 08:03 AM)Ren And Stimpy Wrote: [\[CITE\]](#) 100% it is not bypassing Windows Verison 1903 (updated) and Windows Defender.

You can start a HF convo, and send me your file I'll test, maybe yours is one of a kind.... teamview ? pm me when ready

Ren And Stimpy - March 31, 2020, 11:09 am

(Mar 31, 2020 10:43 AM)Ramboll Wrote: [\[CITE\]](#) teamview ? pm me when ready

Respond in HF convo, mate. I been waiting on you!

Ramboll - March 31, 2020, 3:04 pm

(Mar 31, 2020 11:09 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Respond in HF convo, mate. I been waiting on you!

done, sent you the host link and pass rar...

Ren And Stimpy - March 31, 2020, 3:57 pm

(Mar 31, 2020 03:04 PM)Ramboll Wrote: [\[CITE\]](#) done, sent you the host link and pass rar... check the convso mate

Your site is not allowing download... resend

Ramboll - March 31, 2020, 4:17 pm

(Mar 31, 2020 03:57 PM)Ren And Stimpy Wrote: [\[CITE\]](#) check the convso mate

Your site is not allowing download... resend
resent on mediafire .

Ren And Stimpy - March 31, 2020, 4:39 pm

As proven. First execution will bypass and do an IT scan...
Then any other execution is detected

<https://prnt.sc/rqhl4n>

Windows 1909 is NO JOKE! (with exe files)

(Mar 31, 2020 04:17 PM)Ramboll Wrote: [\[CITE\]](#) resent on mediafire .
And again mate.
Detected, It will bypass ONCE, but after that never again

Trust me I've been in this since late 90s early 2000s

WD changed back in December 2017, and NOW this latest verison is a fucking BEAST!

A+ to Microsoft on this security!
And you wont be sending any executable scripts in a .zip

Ren And Stimpy - April 3, 2020, 11:16 am
Any suggestions, guys?

Still interested in this discussion

H4x10r - April 3, 2020, 11:37 am
use the first execute the right way
disbale transmission of samples via regs
reload new stub

__Digital__ - April 4, 2020, 7:37 am
Defender is really not that hard to interact with, i really don't understand why everyone has such a problem with it. As long as you have clean application run before your malicious file you be fine.

VisualSoft - April 4, 2020, 12:58 pm
(Apr 3, 2020 11:37 AM)H4x10r Wrote: [\[CITE\]](#) use the first execute the right way
disbale transmission of samples via regsl dont think it will be possible to disable it with regs?

Ren And Stimpy - April 6, 2020, 7:14 am
(Apr 4, 2020 12:58 PM)VisualSoft Wrote: [\[CITE\]](#) I dont think it will be possible to disable it with regs?
You can disable it with UAC bypass or if user has admin.

DestinySeekers - April 6, 2020, 7:54 am
(Apr 6, 2020 07:14 AM)Ren And Stimpy Wrote: [\[CITE\]](#) You can disable it with UAC bypass or if user has admin.
How would you disable WD with UAC Bypass / Admin?

Ren And Stimpy - April 6, 2020, 7:57 am
(Apr 6, 2020 07:54 AM)DestinySeekers Wrote: [\[CITE\]](#) How would you disable WD with UAC Bypass / Admin?

Edit the REG... but you need admin or a UAC bypass
(Apr 4, 2020 07:37 AM)__Digital__ Wrote: [\[CITE\]](#) Defender is really not that hard to interact with, i really don't understand why everyone has such a problem with it. As long as you have clean application run before your malicious file you be fine.
That may be true, but hte "clean" application has to disabled WD... or exlude your files

As 1909 detects executables and after first bypass it will NOT bypass again. Contact me on CONVO mate <3

Qismon - April 6, 2020, 8:05 am
Why is there still not a Powershell section on HF?

This is very easy with any scripting language as AMSI is worse than a drunk three legged dog.

Ren And Stimpy - April 6, 2020, 8:06 am

(Apr 6, 2020 08:05 AM)Qismon Wrote: [\[CITE\]](#) Why is there still not a Powershell section on HF?

This is very easy with any scripting language as AMSI is worse than a drunk three legged dog.
Bwhahahaha I 100% agree!

Deathy - April 6, 2020, 8:44 am

(Apr 6, 2020 07:57 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Edit the REG... but you need admin or a UAC bypass

That may be true, but hte "clean" application has to disabled WD... or exlude your files

As 1909 detects executables and after first bypass it will NOT bypass again. Contact me on CONVO mate <3

Whose to say Digital hasn't done just that with the clean application? ?

Ren And Stimpy - April 6, 2020, 10:09 am

(Apr 6, 2020 08:44 AM)Mos Eisley Wrote: [\[CITE\]](#) Whose to say Digital hasn't done just that with the clean application? ?

Then if he did, he can bypass it LOL

DestinySeekers - April 6, 2020, 10:41 am

(Apr 6, 2020 07:57 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Edit the REG... but you need admin or a UAC bypass

That may be true, but hte "clean" application has to disabled WD... or exlude your files

As 1909 detects executables and after first bypass it will NOT bypass again. Contact me on CONVO mate <3

Editing the reg doesn't even disable it due to tamper protection

Ren And Stimpy - April 6, 2020, 11:20 am

(Apr 6, 2020 10:41 AM)DestinySeekers Wrote: [\[CITE\]](#) Editing the reg doesn't even disable it due to tamper protection

Yes it does. You can disable and exclude files. You can turn off Tamper.. lol

VisualSoft - April 6, 2020, 2:51 pm

(Apr 6, 2020 07:14 AM)Ren And Stimpy Wrote: [\[CITE\]](#) You can disable it with UAC bypass or if user has admin.

No i mean to say, with the new Update its hard to disable WD

AuJesus - April 7, 2020, 1:11 am

I was wondering can you bind a wd disabler with exe converted to vbs(with like 30sec delay) would it bypass the wd? And if your exe bypasses scantime then you can maybe also bind a wd enabler and the victim will never notice? I am new please don't judge me.

Ren And Stimpy - April 7, 2020, 7:15 am

(Apr 7, 2020 01:11 AM)AuJesus Wrote: [\[CITE\]](#) I was wondering can you bind a wd disabler with exe converted to vbs(with like 30sec delay) would it bypass the wd? And if your exe bypasses scantime then you can maybe also bind a wd enabler and the victim will never notice? I am new please don't judge me.

you will need the disabler to have uac bypass or elevate admin
but 99% your vbs will be detected if you just convert your exe to vbs, unless you are using a private
or fud runpe

Moralitas - April 7, 2020, 1:33 pm

I've had some luck in the past changing some stuff but that no longer seems to be working.

Ren And Stimpy - April 8, 2020, 5:20 am

(Apr 7, 2020 01:33 PM)Moralitas Wrote: [\[CITE\]](#) I've had some luck in the past changing some stuff
but that no longer seems to be working.

Yea, MOST stuff will not work on this version mate!

FuzzyInteger - April 8, 2020, 9:00 am

(Mar 27, 2020 11:35 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Latest Windows 1009 with Latest Windows
Defender

You see how no public crypter is bypassing!

Windows Defender killing the game. Damn I remember back in 2016 when they were the worse!

What you goes doing about bypassing now?

ATM it's pretty easy to bypass, u need to archive a perfect structural entropy, as i see all crypter in
the market still put the payload in the same exe, that's make WD very hard to bypass, because the
STRUCTURAL ENTROPY of your exe is totally messed up ???

(Mar 31, 2020 04:39 PM)Ren And Stimpy Wrote: [\[CITE\]](#) As proven. First execution will bypass and
do an IT scan...

Then any other execution is detected

<https://prnt.sc/rqhl4n>

Windows 1009 is NO JOKE! (with exe files)

And again mate.

Detected, It will bypass ONCE, but after that never again

Trust me I've been in this since late 90s early 2000s

WD changed back in December 2017, and NOW this latest version is a fugging BEAST!

A+ to Microsoft on this security!

And you wont be sending any executable scripts in a .zip
as i sayd, your file have a really bad structural entropy that's why get flagged almost instantly

download this tool

<http://ntinfo.biz/index.html>

open the tool and choose your file, after that click on ENTROPY make a screenshot and post the
screen here ?

This is my stub + payload

as you see the entropy is almost perfect only few bytes have more to 5 value in entropy

Ren And Stimpy - April 8, 2020, 9:36 am

(Apr 8, 2020 09:00 AM)FuzzyInteger Wrote: [\[CITE\]](#) ATM it's pretty easy to bypass, u need to archive a perfect structural entropy, as i see all crypter in the market still put the payload in the same exe, that's make WD very hard to bypass, because the STRUCTURAL ENTROPY of your exe is totally messed up ???

as i said, your file have a really bad structural entropy that's why get flagged almost instantly

download this tool

<http://ntinfo.biz/index.html>

open the tool and choose your file, after that click on ENTROPY make a screenshot and post the screen here ?

This is my stub + payload

as you see the entropy is almost perfect only few bytes have more to 5 value in entropy

Not sure what that is showing.

I was ding sterography but the EXE is detected. Win Ver detects Applications easily

Send me your file via HF CONVO

Im not sure what the point of that tool even is lol

Send me your file in a .zip ill test it against WD runtime, as im not sure WTF your showing me hahahahah

Thanks for responding tho!

FuzzyInteger - April 8, 2020, 9:42 am

(Apr 8, 2020 09:36 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Not sure what that is showing.

I was ding sterography but the EXE is detected. Win Ver detects Applications easily

Send me your file via HF CONVO

Im not sure what the point of that tool even is lol

Send me your file in a .zip ill test it against WD runtime, as im not sure WTF your showing me hahahahah

Thanks for responding tho!

my stub are private, and bypass wd very easly, direct link exe too with edge all updated, as i told, download detect it easy (DIE TOOL) , and post here the entropy graph i will show you why WD pwn you ass fast

vendetta98 - April 8, 2020, 9:59 am

May be you can use private malware

Ren And Stimpy - April 8, 2020, 10:07 am

(Apr 8, 2020 09:42 AM)FuzzyInteger Wrote: [\[CITE\]](#) my stub are private, and bypass wd very easily, direct link exe too with edge all updated, as i told, download detect it easy (DIE TOOL) , and post here the entropy graph i will show you why WD pwn you ass fast
MSG me on HF convo

Win 1909 will detect the EXE, unless its PRIVATE malware with PRIVATE encrytion, but it will just bypass ONE time and not again.
Send me your file so i can confirm mate

FuzzyInteger - April 8, 2020, 12:27 pm

(Apr 8, 2020 10:07 AM)Ren And Stimpy Wrote: [\[CITE\]](#) MSG me on HF convo

Win 1909 will detect the EXE, unless its PRIVATE malware with PRIVATE encrytion, but it will just bypass ONE time and not again.

Send me your file so i can confirm mate

u are wrong, totally wrong, analyze your file with DIE

n0\$f3ratu\$ - April 9, 2020, 1:29 am

(Apr 8, 2020 09:00 AM)FuzzyInteger Wrote: [\[CITE\]](#) ATM it's pretty easy to bypass, u need to archive a perfect structural entropy, as i see all crypter in the market still put the payload in the same exe, that's make WD very hard to bypass, because the STRUCTURAL ENTROPY of your exe is totally messed up ???

as i sayd, your file have a really bad structural entropy that's why get flagged almost instantly

download this tool

<http://ntinfo.biz/index.html>

open the tool and choose your file, after that click on ENTROPY make a screenshoot and post the screen here ?

This is my stub + payload

as you see the entropy is almost perfect only few bytes have more to 5 value in entropy

Is that is your crypted file (stub + payload) then is sick.

Nice job.

Mine is 74! (not the public one)

opsplayer - April 9, 2020, 1:59 am

(Apr 9, 2020 01:40 AM)M0HX Wrote: [\[CITE\]](#) this is a fully functional working crypted file:

?

So reading the 2 posts about WD being hard to bypass, does this mean no crypter can bypass it therefore making ratting useless in this era of time?

Was thinking of starting my journey but really getting put off because of the threads I see now.

FuzzyInteger - April 9, 2020, 3:26 am

(Apr 9, 2020 01:40 AM)M0HX Wrote: [\[CITE\]](#) this is a fully functional working crypted file:

?

seems a bad entropy post a screen where the graphs are visible like the one i posted below

FuzzylInteger - April 9, 2020, 5:13 am

(Apr 9, 2020 03:59 AM)M0HX Wrote: [\[CITE\]](#) the graph shows high I guess. but no sections to see. could be a nice way to fool malware analysis :3

sections are visible when run in memory tho.
OMG the entropy is so so high !

as you see the graph show an HUGE amount of data with a very high entropy !!!

Windows defender, calculate the STRUCTURAL ENTROPY not the ENTROPY !!!

so wich difference is between structural and entropy ?

structural entropy is calculated every chunk (example 64 byte chunk)

so the file will be splitted into 64byte chunk and every chunk will be entropy calculated !

at the end of this task the AV will calculate how many block of data have an high entropy, if an high number of these block have an uncommon entropy the file will be flagged instant (machine learning work on this algo)

be carefull some ML algoritm use 16 byte chunk other 32byte chunk other 64 byte chunk ecc.....

|-----|

the base entropy (the whole entropy result of the entire file) it's just a calculation of the entire data (windows defender do not take care of this!)

FuzzylInteger - April 9, 2020, 5:38 am

(Apr 9, 2020 05:28 AM)M0HX Wrote: [\[CITE\]](#) Lol yea that's what I thought. thanks for the info. Structural entropy is used because u cannot bypass this algorithm with a padding or null bytes inserting inside a pe section ???

this is a little bit old paper, but still effective

<https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/download/16133/16383>

Ren And Stimpy - April 9, 2020, 7:42 am

Thanks for sharing Fuzzy! I wish you would respond on HF convo!

martigo333 - April 11, 2020, 7:40 am

So bye bye to Rat and crypters with this windows defender updates. I just paid 100\$ for a privet stub crypter If I had known I wouldn't have wasted my money at all. Who knows maybe a lot of people

don't know about this update yet.

__Digital__ - April 11, 2020, 7:43 am

(Apr 11, 2020 07:40 AM)martigo333 Wrote: [\[CITE\]](#) So bye bye to Rat and crypters with this windows defender updates. I just paid 100\$ for a privet stub crypter If I had known I wouldn't have wasted my money at all. Who knows maybe a lot of people don't know about this update yet.

Defender is easy to interact with i still do not understand why everyone has a problem with it. As long as you have a clean program which tells defender what to do first you will not have any problems.

H4x10r - April 13, 2020, 10:44 am

```
Code else if (line.StartsWith(@"SubmitSamplesConsent") && !line.EndsWith("2"))
    RunPS("Set-MpPreference -SubmitSamplesConsent 2"); //MAPSReporting

    else if (line.StartsWith(@"MAPSReporting") && !line.EndsWith("0"))
        RunPS("Set-MpPreference -MAPSReporting 0"); //MAPSReporting
NYANCAT !
```

FuzzylInteger - April 13, 2020, 12:04 pm

```
(Apr 13, 2020 10:44 AM)H4x10r Wrote: \[CITE\] Code else if
(line.StartsWith(@"SubmitSamplesConsent") && !line.EndsWith("2"))
    RunPS("Set-MpPreference -SubmitSamplesConsent 2"); //MAPSReporting

    else if (line.StartsWith(@"MAPSReporting") && !line.EndsWith("0"))
        RunPS("Set-MpPreference -MAPSReporting 0"); //MAPSReporting
NYANCAT !
```

This will not mitigate the Machine Learning problem, since your file is still spreaded on the web so, it will be analized quite shortly and Boom, u get flagged instantly, also u forgot about honeypot wich will pwn u very fast, the packer era it's almost over, we are into the cloud and IOT things so, why we do not use them ?

without a perfect structural entropy the ML and DEEP neural will always win, remember

Ren And Stimpy - April 13, 2020, 3:28 pm

Still have not seen a .exe bypass

__Digital__ - April 13, 2020, 5:43 pm

(Apr 13, 2020 03:28 PM)Ren And Stimpy Wrote: [\[CITE\]](#) Still have not seen a .exe bypass
Waiting for feedback since providing you the demo.

androexo - April 14, 2020, 1:57 am

I wish i could help you guys.. but im shit at this :(

Ren And Stimpy - April 14, 2020, 7:27 am

Digital exe did bypass. It interacted with WD once and had the IT scan, then tested on a diff machine to see if samples was sent and the EXE did bypass

Nice work brother!

__Digital__ - April 14, 2020, 7:49 am

(Apr 14, 2020 07:27 AM)Ren And Stimpy Wrote: [\[CITE\]](#) Digital exe did bypass. It interacted with WD once and had the IT scan, then tested on a diff machine to see if samples was sent and the EXE did bypass

Nice work brother!

Thanks or letting them know it is possible if everyone would quit thinking so hard about it

Jean-Jacques Rousseau - April 14, 2020, 8:28 am

(Apr 13, 2020 12:04 PM)FuzzylInteger Wrote: [\[CITE\]](#) This will not mitigate the Machine Learning problem, since your file is still spreaded on the web so, it will be analized quite shortly and Boom, u get flagged instantly, also u forgot about honeypot wich will pwn u very fast, the packer era it's almost over, we are into the cloud and IOT things so, why we do not use them ?

without a perfect structural entropy the ML and DEEP neural will always win, remember

I have extremely strong anti emulation and powerful runtime, the only issue is advanced machine learning that is breaking my stub shortly (WD Cloud after a few days of hard spread). We are back at beating scantime again, runtime is a piece of cake compared to scantime nowadays. Do you have ideas for breaking machine learning algorithms? I have some basic methods for breaking entropy based detections techniques, but these machine learning algorithms are getting better and better, it is only a question of time until every unknown executable is detected upon scan.

Do you have xmpp or discord where we can discuss this further? I have some ideas.

FuzzylInteger - April 14, 2020, 10:02 am

(Apr 14, 2020 08:28 AM)Supercut Wrote: [\[CITE\]](#) I have extremely strong anti emulation and powerful runtime, the only issue is advanced machine learning that is breaking my stub shortly (WD Cloud after a few days of hard spread). We are back at beating scantime again, runtime is a piece of cake compared to scantime nowadays. Do you have ideas for breaking machine learning algorithms? I have some basic methods for breaking entropy based detections techniques, but these machine learning algorithms are getting better and better, it is only a question of time until every unknown executable is detected upon scan.

Do you have xmpp or discord where we can discuss this further? I have some ideas.
there are only 2 way

1) archieve a perfect structural entropy

2) do not include your payload in the same exe

Jean-Jacques Rousseau - April 14, 2020, 11:04 am

(Apr 14, 2020 10:02 AM)FuzzylInteger Wrote: [\[CITE\]](#) there are only 2 way

1) archieve a perfect structural entropy

2) do not include your payload in the same exe

I have used both of them and had sucess. I have a third idea, but I dont have time or energy to code it myself yet. If you are interested, contact me, we can discuss.

Ren And Stimpy - April 21, 2020, 7:19 am

Thanks for all the assistance! Keep sharing guys!

VisualSoft - May 1, 2020, 8:46 am

Well I was making some test with WD and found Now they have Memory Scan inbuilt with the Newest Update.

Jean-Jacques Rousseau - May 1, 2020, 9:56 am

(May 1, 2020 08:46 AM)VisualSoft Wrote: [\[CITE\]](#) Well I was making some test with WD and found Now they have Memory Scan inbuilt with the Newest Update.

What tests did you run to come up with these results?

VisualSoft - May 1, 2020, 9:58 am

(May 1, 2020 09:56 AM)Supercut Wrote: [\[CITE\]](#) What tests did you run to come up with these results?If you Load any Rat in memory, WD Blocks it.
I found it when i was working with my project.

NYANxCAT - May 1, 2020, 10:01 am

(May 1, 2020 09:58 AM)VisualSoft Wrote: [\[CITE\]](#) If you Load any Rat in memory, WD Blocks it.
I found it when i was working with my project.
Don't use load.entrypoint, it's already blocked by wd.

Jean-Jacques Rousseau - May 1, 2020, 10:02 am

(May 1, 2020 09:58 AM)VisualSoft Wrote: [\[CITE\]](#) If you Load any Rat in memory, WD Blocks it.
I found it when i was working with my project.
You might be getting caught in WDs emulator. The emulator is sophisticated, however, you can write some WD-specific anti-emulation simply by reverse engineering it and checking some hardcoded values. How are you loading these RATs?
(May 1, 2020 10:01 AM)NYANxCAT Wrote: [\[CITE\]](#) Don't use load.entrypoint, it's already blocked by wd.
Well, if you are writing .NET malware, of course all actions will be blocked. Lol. I could only imagine using .NET as a first stage wrapper since it is easy to FUD and write USG for.

NYANxCAT - May 1, 2020, 10:10 am

(May 1, 2020 10:02 AM)Supercut Wrote: [\[CITE\]](#) You might be getting caught in WDs emulator. The emulator is sophisticated, however, you can write some WD-specific anti-emulation simply by reverse engineering it and checking some hardcoded values. How are you loading these RATs?

Well, if you are writing .NET malware, of course all actions will be blocked. Lol. I could only imagine using .NET as a first stage wrapper since it is easy to FUD and write USG for.
not really, but I can't share methods to bypass wd here. i just wanted to point out that load entry point is useless. gl

VisualSoft - May 1, 2020, 10:38 am

(May 1, 2020 10:10 AM)NYANxCAT Wrote: [\[CITE\]](#) not really, but I can't share methods to bypass wd here. i just wanted to point out that load entry point is useless. gl
Loading the Rat server under assembly.load or appdomain.currentdomain or threaddomain will instantly blocked by WD.
As soon as it gets Loaded, it will be blocked by WD and no further process will work.

__Digital__ - May 1, 2020, 11:00 am

Yes defender changed a few things however still can be bypassed, just have to understand the way defender works

VisualSoft - May 1, 2020, 11:01 am

(May 1, 2020 10:02 AM)Supercut Wrote: [\[CITE\]](#) You might be getting caught in WDs emulator. The emulator is sophisticated, however, you can write some WD-specific anti-emulation simply by reverse engineering it and checking some hardcoded values. How are you loading these RATs?
Can be, but from what I Can see its looks like a memory detection.

RHKD - May 3, 2020, 10:05 am

you can use a WD disable and execute your rat but for that you need admin privileges, i always change the exe manifest and make it open only with admin privileges and no need to bypass the

runtime

VisualSoft - May 3, 2020, 10:25 am

(May 3, 2020 10:05 AM)Shad2233 Wrote: [\[CITE\]](#) you can use a WD disable and execute your rat but for that you need admin privileges, i always change the exe manifest and make it open only with admin privileges and no need to bypass the runtime
WD got anti-Tamper Protection in the newest Update.

RHKD - May 3, 2020, 12:50 pm

(May 3, 2020 10:25 AM)VisualSoft Wrote: [\[CITE\]](#) WD got anti-Tamper Protection in the newest Update.

so after what you said i created a windows 1909 vm on azure and i tried to check for update in windows defender and everything was fully updated with anti-tamper on, after that i used nyanxcat's windows defender disable it was detected on scan time (if you use the codes on your stub and crypt it or just crypt the wd disable i don't think it'll get detected) i run it and the first thing it do is disabling tamper protection after that it'll disable everything, so yeah it worked, i opened a quasar rat client and fully scanned the hardware and nothing got detected.

Subliminal_ - May 3, 2020, 4:43 pm

Sorry accidentally posted in the wrong thread. Please delete.

VisualSoft - May 3, 2020, 8:59 pm

(May 3, 2020 12:50 PM)Shad2233 Wrote: [\[CITE\]](#) so after what you said i created a windows 1909 vm on azure and i tried to check for update in windows defender and everything was fully updated with anti-tamper on, after that i used nyanxcat's windows defender disable it was detected on scan time (if you use the codes on your stub and crypt it or just crypt the wd disable i don't think it'll get detected) i run it and the first thing it do is disabling tamper protection after that it'll disable everything, so yeah it worked, i opened a quasar rat client and fully scanned the hardware and nothing got detected.

What about after you restart the system?

RHKD - May 3, 2020, 11:13 pm

(May 3, 2020 08:59 PM)VisualSoft Wrote: [\[CITE\]](#) What about after you restart the system?
yea i also restarted it and still nothing happened everything works fine

VisualSoft - May 3, 2020, 11:16 pm

(May 3, 2020 11:13 PM)Shad2233 Wrote: [\[CITE\]](#) yea i also restarted it and still nothing happened everything works fine
thats good, good work with it.

s??!s? - May 23, 2020, 5:58 pm

Its bypassing.

My discord- HelpingHand#1111

VisualSoft - May 23, 2020, 11:26 pm

(May 23, 2020 05:58 PM)s??!s? Wrote: [\[CITE\]](#) Its bypassing.

My discord- HelpingHand#1111

Yap it is, Just need to use correct things.

ACCOUNT - May 25, 2020, 4:06 am

I can bypass everything, even add exclusions. Just can't disable tamper protection which is not a big

deal.... just know how to work windows ;)

Jean-Jacques Rousseau - May 25, 2020, 8:04 am

(May 25, 2020 04:06 AM)Pistachio Wrote: [\[CITE\]](#) I can bypass everything, even add exclusions. Just can't disable tamper protection which is not a big deal.... just know how to work windows ;) I believe this is a thread where we share and work on each others ideas.

cunninghamcunnimr - May 25, 2020, 12:12 pm

hackforums.net/showthread.php?tid=6078890

VisualSoft - May 26, 2020, 12:46 am

(May 25, 2020 12:12 PM)cunninghamcunnimr Wrote: [\[CITE\]](#)
hackforums.net/showthread.php?tid=6078890

Like the above user said, this thread is to discuss about new methods.

danny34 - May 27, 2020, 11:37 am

Cloud based ML is tricky to bypass.

Jean-Jacques Rousseau - May 27, 2020, 12:37 pm

(May 27, 2020 11:37 AM)danny34 Wrote: [\[CITE\]](#) Cloud based ML is tricky to bypass. ML is trained to detect goodware, and flag the rest.

Hide your shellcode deep into legitimate programs :)

danny34 - May 28, 2020, 1:57 pm

(May 27, 2020 12:37 PM)Supercut Wrote: [\[CITE\]](#) ML is trained to detect goodware, and flag the rest.

Hide your shellcode deep into legitimate programs :)

Yes shellter is good example, also asm anti-emu and high level anti-emu works too.

C, C++,Python,AutoIt too. As long as shell code is not executed in sandbox its all good.

Metamorphic or polymorphic shellcode without anti-emulation is detected easily.

And another bypass

****s://imgur.com/a/XE9P8WW