

Forum:[Hack Forums](#)

Thread: [IDP.Alexa.51 Detection by Avast Behaviour Shield](#)

Dark.Shadow - July 22, 2017, 11:53 am

I am using a .Net RAT, but recently faced a new detection by Avast Behaviour Shield.
IDP.ALEXA.51.

Stub has bypassed avast deep Screen also but get detected by behavior.

Any idea what this detection really is, as according to web, its false positive many time, but it represents backdoor Trojan.

faced this detection with native crypter of C++ for Netwire also.

alaintenaho - July 22, 2017, 12:32 pm

since 2 months now.. Welcome to AVAST

DeluxeSoftware - July 22, 2017, 12:57 pm

That's a detection of the AVG engine. I guess, it's mainly triggered by injections.

moufmouf - July 22, 2017, 1:07 pm

did u tried darkeye

because i wanna buy it and i dont want to get IDP.ALEXA.51

Dark.Shadow - July 22, 2017, 2:23 pm

(Jul 22, 2017 01:07 PM)moufmouf Wrote: [\[CITE\]](#) did u tried darkeye

because i wanna buy it and i dont want to get IDP.ALEXA.51

I have used DarkEye in Past, found it best crypter for Netwire, as it gave FUD without any error.

but haven't used it for past few months, don't know if it bypass avast or not

Cyber Coder - July 22, 2017, 11:51 pm

this detection needs native rat + anti memory scanner

xcrafter245 - July 23, 2017, 2:21 am

(Jul 22, 2017 11:51 PM)Cyber Coder Wrote: [\[CITE\]](#) this detection needs native rat + anti memory scanner

want do you mean?

DeluxeSoftware - July 23, 2017, 2:53 am

(Jul 22, 2017 11:51 PM)Cyber Coder Wrote: [\[CITE\]](#) this detection needs native rat + anti memory scanner

Bullshit. It's not triggered by the file being .NET or native... ???

Cyber Coder - July 23, 2017, 3:46 am

(Jul 23, 2017 02:53 AM)DeluxeSoftware Wrote: [\[CITE\]](#) Bullshit. It's not triggered by the file being .NET or native... ???

huh?anti memory scanner works only with native files so you need a native rat and an anti memory scanner to bypass it;) heard it might work with .net by using reflection instead of runpe but never tried

Tsukiri - July 23, 2017, 3:49 am

I'd take Cyber Coders advice, he atleast seems to know what he is talking about.

Grab yourself netwire and (code) a crypter with an anti mem scan function and you should be good.

I'd still say that even if you crypt a file beyond recognition, if it is some shitty malware then this behaviour shield will still pick it up as malicious because

certain hooks / actions it performs, which are recognized by Avast.

Dark.Shadow - July 23, 2017, 4:28 am

(Jul 23, 2017 03:49 AM)Tsukiri Wrote: [\[CITE\]](#) I'd take Cyber Coders advice, he atleast seems to know what he is talking about.

Grab yourself netwire and (code) a crypter with an anti mem scan function and you should be good.

I'd still say that even if you crypt a file beyond recognition, if it is some shitty malware then this behaviour shield will still pick it up as malicious because

certain hooks / actions it performs, which are recognized by Avast.

anyway to bypass this shield, when am using Netwire Rat?

Tsukiri - July 23, 2017, 6:35 am

(Jul 23, 2017 04:28 AM)Dark.Shadow Wrote: [\[CITE\]](#) anyway to bypass this shield, when am using Netwire Rat?

Get a good crypter with antimem scan or an undetected injection method. Aka, a private runPE which bypasses Avast.

Dark.Shadow - July 23, 2017, 7:38 am

(Jul 23, 2017 06:35 AM)Tsukiri Wrote: [\[CITE\]](#) Get a good crypter with antimem scan or an undetected injection method. Aka, a private runPE which bypasses Avast.

antimemory scan will bypass the behavior shield?

DeluxeSoftware - July 23, 2017, 11:02 am

(Jul 23, 2017 07:38 AM)Dark.Shadow Wrote: [\[CITE\]](#) antimemory scan will bypass the behavior shield?

Don't listen to the other guys. Like yes, it is your crypters fault but it has nothing to do with anti memory scan.

I just tested that by loading netwire into memory without any anti mem scan and I got no detection.

Tsukiri - July 23, 2017, 1:19 pm

(Jul 23, 2017 11:02 AM)DeluxeSoftware Wrote: [\[CITE\]](#) Don't listen to the other guys. Like yes, it is your crypters fault but it has nothing to do with anti memory scan.

I just tested that by loading netwire into memory without any anti mem scan and I got no detection.

Obviously it's his crypters fault.. If he uses a crypter that bypasses it then no anti mem scan is needed, but making it impossible for scanner to scan it will also bypaass it

DeluxeSoftware - July 23, 2017, 1:37 pm

(Jul 23, 2017 01:19 PM)Tsukiri Wrote: [\[CITE\]](#) Obviously it's his crypters fault.. If he uses a crypter that bypasses it then no anti mem scan is needed, but making it impossible for scanner to scan it will also bypaass it

Stop, just stop. Like you have no idea what you are talking about and you posted 32 posts today.. Jesus, you are posthunting as hell.

Miss_intengible - July 23, 2017, 2:16 pm

(Jul 23, 2017 11:02 AM)DeluxeSoftware Wrote: [\[CITE\]](#) Don't listen to the other guys. Like yes, it is your crypters fault but it has nothing to do with anti memory scan.

I just tested that by loading netwire into memory without any anti mem scan and I got no detection. You loaded the netwire into memory only? or you started execution of netwire in memory too ?

DeluxeSoftware - July 23, 2017, 2:32 pm

(Jul 23, 2017 02:16 PM)Miss_intengible Wrote: [\[CITE\]](#) You loaded the netwire into memory only? or you started execution of netwire in memory too ?
haha, I injected it and ran it of course

Miss_intengible - July 23, 2017, 2:41 pm

Itself? or in another process ?

moufmouf - July 23, 2017, 9:57 pm

(Jul 22, 2017 02:23 PM)Dark.Shadow Wrote: [\[CITE\]](#) I have used DarkEye in Past, found it best crypter for Netwire, as it gave FUD without any error.

but haven't used it for past few months, don't know if it bypass avast or not
im trying to buy it and use it with my netwire but the support always answer me that the crypter not builded for this things
is it can bypass avast and not detected as alexa or samthing like that
and is it fud or i have to do samthing else to get it fully fud

Dark.Shadow - July 24, 2017, 2:48 am

(Jul 23, 2017 02:32 PM)DeluxeSoftware Wrote: [\[CITE\]](#) haha, I injected it and ran it of course
Inject itself or in some other process?

I have seen reputed softwares bypassing Avast behavior shield, and doesn't even trigger any detection. so will it work if injected into some other process or?

Dark.Shadow - July 26, 2017, 1:25 am

How does Certified apps bypass this Shield? like I have downloaded basic apps from Filehippo or Cnet, and They aren't detected by Avast.

Is it because of certificate or signature?

Tsukiri - July 26, 2017, 9:50 am

(Jul 26, 2017 01:25 AM)Dark.Shadow Wrote: [\[CITE\]](#) How does Certified apps bypass this Shield? like I have downloaded basic apps from Filehippo or Cnet, and They aren't detected by Avast.

Is it because of certificate or signature?
Because they arent malicious?

Dark.Shadow - July 27, 2017, 9:40 am

(Jul 26, 2017 09:50 AM)Tsukiri Wrote: [\[CITE\]](#) Because they arent malicious?
How they know its not malicious? due to signature or?

Because both requires net connectivity and open port to download the data for further installation

Tsukiri - July 29, 2017, 8:46 am

(Jul 27, 2017 09:40 AM)Dark.Shadow Wrote: [\[CITE\]](#) How they know its not malicious? due to

signature or?

Because both requires net connectivity and open port to download the data for further installation
You dont seem to get it. An Anti-Virus analyzes the program from malicious content and checks whether it tries malicious things (for example if it keeps writing to a .txt file then it's probably a keylogger and an anti-virus can recognize that).

If a program doesn't try anything sketchy which can trigger the anti-virus as malicious, nor does it contain any code that could be flagged as malicious, then why would the AV want to remove it?

Heresys32 - August 5, 2017, 3:24 pm

Inject itself or in some other process?

I have seen reputed softwares bypassing Avast behavior shield, and doesn't even trigger any detection. so will it work if injected into some other process or?

kevy42 - August 5, 2017, 4:11 pm

(Aug 5, 2017 03:24 PM)Heresys32 Wrote: [\[CITE\]](#) Inject itself or in some other process?

I have seen reputed softwares bypassing Avast behavior shield, and doesn't even trigger any detection. so will it work if injected into some other process or?

nope, its scanning the memory, to avade avast ud need a private Runpe + native payload encryption + anti-memroy scanner.

nathanmark - February 12, 2021, 2:49 am

IDP.ALEXA.51 is indeed a detection which is generally associated with "SeaMonkey", "Plants vs. Zombies" or other video games. It is confirmed that the observed object originates from .tmp or .exe files in separate Windows directories, such as percent AppData percent and percent temp percent. Given researchers' false-positive findings, it is normally recognized as ransomware by AVG and confirmed to be potentially harmful to infected computers.