

Forum:[Hack Forums](#)

Thread: [RAT's, Crypters & Detections \(Discussion\)](#)

Oldylox1 - June 25, 2020, 9:34 pm

I have recently been getting a FUD runtime and scan via Windows Defender with RAZ Private stub alongside Hive Rat, Warzone Rat, BitRAT and AsyncRat.

Got my hands on a corporate edition of ESET trial, and also home edition but what is quite interesting is that scanning these files reveal nothing malicious, but ESET seems to be quite aggressive and does pickup on runtime that these are trojans/variants.

On runtime ESET is detecting: "MSIL/Agent.TWO Trojan"

On Password recovery in all RATS ESET detects: MSIL/Injector."UWL Trojan" & : "Generik.DVCZOHP Trojan" then with VNC it detects "Agent.CTE"

So to further my curiosity, has anyone/does any current crypter/RAT bypass ESET at all or have know of any methods to bypass this?

it seems they are doing a very good job in terms of detecting RATS/Malicious software which is a bonus for us - So I would be genuinely curious to figure if anything can bypass this.

(FOR MORE CONTEXT TO THIS QUESTION - READ

<https://hackforums.net/showthread.php?tid=6090295>)

VisualSoft - June 26, 2020, 4:17 am

ESET Has the best Memory scan module and Crypters on HF lake of Anti-Memory scan and in some case rat crash when implemented Anti-Memory scan.

So Only solution for this is to remove runtime detection from that particular AV and best rat to do this is having OpenSource Rat.

With Async and little modification you can easily pass most of all Av including Eset.

Mr. Atlas - July 9, 2020, 3:45 pm

(Jun 26, 2020 04:17 AM)VisualSoft Wrote: [\[CITE\]](#) ESET Has the best Memory scan module and Crypters on HF lake of Anti-Memory scan and in some case rat crash when implemented Anti-Memory scan.

So Only solution for this is to remove runtime detection from that particular AV and best rat to do this is having OpenSource Rat.

With Async and little modification you can easily pass most of all Av including Eset.

Have you tried out BitRAT ?

VisualSoft - July 9, 2020, 4:08 pm

(Jul 9, 2020 03:45 PM)Mr. Atlas Wrote: [\[CITE\]](#) Have you tried out BitRAT ?

no, but I wont trust any publicly sold rat when it comes to Hipe Bypass (Memory detection techinque of AV).

Cause they are used by hundreds of users and so High exposure to AV and so high runtime detection.

Mr. Atlas - July 9, 2020, 4:11 pm

(Jul 9, 2020 04:08 PM)VisualSoft Wrote: [\[CITE\]](#) no, but I wont trust any publicly sold rat when it

comes to Hipe Bypass (Memory detection technique of AV).

Cause they are used by hundreds of users and so High exposure to AV and so high runtime detection.

use private encryption to work around the problem, right?

VisualSoft - July 9, 2020, 4:16 pm

(Jul 9, 2020 04:11 PM)Mr. Atlas Wrote: [\[CITE\]](#) use private encryption to work around the problem, right?

Private encryption sold on HF dont protect from memory scan.

You need a combo of good Rat and Crypter then only it will both.

NYANxCAT - July 9, 2020, 5:10 pm

(Jun 25, 2020 09:34 PM)Oldylox1 Wrote: [\[CITE\]](#) On runtime ESET is detecting: "MSIL/Agent.TWO Trojan"

On Password recovery in all RATS ESET detects: MSIL/Injector."UWL Trojan" & :
"Generik.DVCZOHP Trojan" then with VNC it detects "Agent.CTE"

ESET latest new update engine + application

Windows 10 build 2004 (Latest)

So as you see it did bypass, yet it's not the corporate edition but I'm very sure it's the same thing but im too lazy to install it.

EDIT:

Quote:So to further my curiosity, has anyone/does any current crypter/RAT bypass ESET at all or have know of any methods to bypass this?

Nobody will tell you anything because it will kill the purpose of buying a crypter.

Oldylox1 - July 9, 2020, 5:47 pm

(Jul 9, 2020 05:10 PM)NYANxCAT Wrote: [\[CITE\]](#) ESET latest new update engine + application
Windows 10 build 2004 (Latest)

So as you see it did bypass, yet it's not the corporate edition but I'm very sure it's the same thing but im too lazy to install it.

EDIT:

Nobody will tell you anything because it will kill the purpose of buying a crypter.

At the end it was just my crypt. As I had it for over a month it wasn't bypassing it. When I renewed with RAZ he mentioned why it wasn't bypassing and he gave me a new crypt on renewal which resolved this issue.

Have it currently installed on 10 VM's with ESET Corp for a couple days now and still running great.

AsyncRAT is without a doubt the best free RAT out. BitRAT is great too.

UnknownProducts - July 9, 2020, 8:03 pm

(Jul 9, 2020 04:08 PM)VisualSoft Wrote: [\[CITE\]](#) no, but I wont trust any publicly sold rat when it comes to Hipe Bypass (Memory detection technique of AV).

Cause they are used by hundreds of users and so High exposure to AV and so high runtime detection.

Difference with BitRAT is source is fully obfuscated, based on USG and soon private editions will generate unique stubs with very high entropy, bypassing completely most AV runtime and scantime.

VisualSoft - July 9, 2020, 9:46 pm

(Jul 9, 2020 08:03 PM)UnknownProducts Wrote: [\[CITE\]](#) Difference with BitRAT is source is fully obfuscated, based on USG and soon private editions will generate unique stubs with very high entropy, bypassing completely most AV runtime and scantime.

true but what when you hit 1k users. The problem comes when its mass used.

I am not commenting on your quality, I am just telling the theory.

Fire_Star - July 10, 2020, 2:12 am

This is a very interesting conversation and a very useful thread.

Its nice to see the inputs from all of you People.

UnknownProducts - July 10, 2020, 6:48 am

(Jul 9, 2020 09:46 PM)VisualSoft Wrote: [\[CITE\]](#) true but what when you hit 1k users. The problem comes when its mass used.

I am not commenting on your quality, I am just telling the theory.

Everything mass used in big scale will be detected. Is a big cat and mouse game of course.