

Forum:[Hack Forums](#)

Thread: [How to bypass Gen.variant / HEUR detections on your RAT](#)

BTCZeus - January 19, 2019, 4:19 pm

These detections are known as Generic or Heuristic, meaning that the file LOOKS like malware, but exact malicious code has not been found itself. There are many ways to bypass this. 80% of the time, it is not due to the stub itself (though extremely HQ crypters / private stubs generally negate this).

They are both treated the same, here is the solution:

1) Change assembly information. (Product version, description, product name, company, copy write etc.) If your crypter doesn't support this, try using resource hacker:

<http://www.angusj.com/resourcehacker/>

2) FUD icon. Using an overused icon can result in these detections. Instead of using a site that gives free .ICO files (Which is likely to be used by a lot of other people, thereby saturating the icon), it is advisable to find an image and convert it to an icon using ICO converter:

<https://www.icoconverter.com/> or even create your own icon.

3) Change the name of installed folders/files. Often, RATs / crypters will drop files in Appdata, Temp, or many other places in order to store logs and install the software. If given the chance, change the name of these files within the RAT/crypter. If # / DarkEyE by default drop a folder in Appdata named #, AVs will understand this signature process and will be more likely to detect files with the same process. Change the names to something random.

4) Pump the file. This is self explanatory. A smaller file is ideal, but if the only way to bypass these detections is to have a larger file, then go for it.

5) Startup / process injection methods. Once again, self explanatory. Experiment with different settings.

6) Delay the execution. Unrelated, but also helpful, add a 30+ second delay to the execution. This will help your runtime execution rate.

If you have tried all of these and you are still getting generic (gen.variant) or heuristic (HEUR) detections, it is your malware or simply the quality of the crypter you are using. If you are target spreading (spreading privately to a small amount of individuals) then consider buying a private stub or writing your own malware (ideal).

It's said everywhere, but people still scan their files on Virustotal or other mainstream web scanners. You are not only fucking yourself over, but anybody else who is using a shared stub on your crypter. For a paid scanner, consider Viruscheckmate and for free, take a look at <http://spyralscanner.net> (Spyral has given me false positives before but it's rare).

If there is incorrect / missing information you feel should be posted, let me know below and I'll try and keep this updated and bumped so that we can save everyone some time and effort. Cheers

Alles auf Rot - January 19, 2019, 4:23 pm

Thank you for your detailed description. Especially this helps me a lot to improve my projects, most of it I already got together, but nice that I got it confirmed. Please keep your post quality. Keep it up & welcome to Hackforums! Take my + rep, getting your profile a little more green :p

BTCZeus - January 19, 2019, 4:54 pm

(Jan 19, 2019 05:23 PM)Alles auf Rot Wrote: [\[CITE\]](#) Thank you for your detailed description. Especially this helps me a lot to improve my projects, most of it I already got together, but nice that I got it confirmed. Please keep your post quality. Keep it up & welcome to Hackforums! Take my + rep, getting your profile a little more green :p

I appreciate the kind words my man! I have a lot of experience with this sort of thing, so feel free to shoot me a PM if you are ever having issues =)

Vytrex - January 20, 2019, 12:04 am

(Jan 19, 2019 05:19 PM)LeoCrypto Wrote: [\[CITE\]](#) These detections are known as Generic or Heuristic, meaning that the file LOOKS like malware, but exact malicious code has not been found itself. There are many ways to bypass this. 80% of the time, it is not due to the stub itself (though extremely HQ crypters / private stubs generally negate this).

They are both treated the same, here is the solution:

1) Change assembly information. (Product version, description, product name, company, copy write etc.) If your crypter doesn't support this, try using resource hacker:

[hp://.angusj./resourcehacker/](http://.angusj./resourcehacker/)

2) FUD icon. Using an overused icon can result in these detections. Instead of using a site that gives free .ICO files (Which is likely to be used by a lot of other people, thereby saturating the icon), it is advisable to find an image and convert it to an icon using ICO converter: hs://.icoconverter.c/ or even create your own icon.

3) Change the name of installed folders/files. Often, RATs / crypters will drop files in Appdata, Temp, or many other places in order to store logs and install the software. If given the chance, change the name of these files within the RAT/crypter. If # / DarkEyE by default drop a folder in Appdata named #, AVs will understand this signature process and will be more likely to detect files with the same process. Change the names to something random.

4) Pump the file. This is self explanatory. A smaller file is ideal, but if the only way to bypass these detections is to have a larger file, then go for it.

5) Startup / process injection methods. Once again, self explanatory. Experiment with different settings.

6) Delay the execution. Unrelated, but also helpful, add a 30+ second delay to the execution. This will help your runtime execution rate.

If you have tried all of these and you are still getting generic (gen.variant) or heuristic (HEUR) detections, it is your malware or simply the quality of the crypter you are using. If you are target spreading (spreading privately to a small amount of individuals) then consider buying a private stub or writing your own malware (ideal).

It's said everywhere, but people still scan their files on Virustotal or other mainstream web scanners. You are not only fucking yourself over, but anybody else who is using a shared stub on your crypter. For a paid scanner, consider Viruscheckmate and for free, take a look at [hp://spyralscanner](http://spyralscanner). (Spyral has given me false positives before but it's rare).

If there is incorrect / missing information you feel should be posted, let me know below and I'll try and keep this updated and bumped so that we can save everyone some time and effort. Cheers
This is really good!

Most important thing is Write your own Malware. That's what I keep telling people all the time! It's the best way to get around all the security features...

Keep up the good work!

NYANxCAT - January 20, 2019, 3:40 am

Thanks for sharing these well-written steps, just remember these steps will only avoid scan-time detections and not run-time but I guess you are sharing this for newcomers.

mehtevs - January 20, 2019, 4:06 am

viruscheckmate is dead, take a look at dyncheck.com

Angelis - January 20, 2019, 4:09 am

Heh....

This is a surprisingly great write up @OP.

I find it ironic that people overlook #'s 2,3, and 4 in specific.

- So obvious, but so effective, and yet so overlooked by many.

QU?CKSILVER - January 20, 2019, 4:48 am

Heuristics are not that easy to bypass. Even when cloning legit file assemblies, version info and icons, antiviruses with heuristic engines such as Avira Cloud, Norton's SONAR, WinDef cloud protection will be triggered. And yes, file packers (a.k.a. Crypters) will MOST of the time give you a "heuristically dirty" output even if undetected by the file antivirus and it's simply because AV vendors have already found other malicious samples containing the same file structure.

One of the ways to make these engines ignore file heuristics is by adding a valid digital signature to the file, which is really expensive. Another way you can get around heuristics is by crypting using NSIS silent installers, self extracting archives (which will most of the time seem heuristically correct to antiviruses)... Sometimes, even adding junk data to the PE info can help, but not effective against all engines.

Another thing to note is that, if you get to bypass heuristic scanners once, it will not last for long... Especially if you are crypting malware.

As soon as your file is caught doing something suspicious during runtime, it will be submitted to the cloud for further scanning and will eventually get scan-time detected (as well as any other PE containing the same, or similar info).

Angelis - January 20, 2019, 5:09 am

(Jan 20, 2019 05:48 AM)QU?CKSILVER Wrote: [\[CITE\]](#) Heuristics are not that easy to bypass. Even when cloning legit file assemblies, version info and icons, antiviruses with heuristic engines such as Avira Cloud, Norton's SONAR, WinDef cloud protection will be triggered. And yes, file packers (a.k.a. Crypters) will MOST of the time give you a "heuristically dirty" output even if undetected by the file antivirus and it's simply because AV vendors have already found other malicious samples containing the same file structure.

One of the ways to make these engines ignore file heuristics is by adding a valid digital signature to

the file, which is really expensive. Another way you can get around heuristics is by crypting using NSIS silent installers, self extracting archives (which will most of the time seem heuristically correct to antiviruses)... Sometimes, even adding junk data to the PE info can help, but not effective against all engines.

Another thing to note is that, if you get to bypass heuristic scanners once, it will not last for long... Especially if you are crypting malware.

As soon as your file is caught doing something suspicious during runtime, it will be submit to the cloud for further scanning and will eventually get scantime detected (as well as any other PE containing the same, or similar info).

Although I agree...

Its funny how the simplest of shit can work sometimes.

AVFucker, for example... its just a file pumper, basically. but it fucking works, sometimes. ?

QU?CKSILVER - January 20, 2019, 5:17 am

(Jan 20, 2019 06:09 AM)Angelis Wrote: [\[CITE\]](#) Although I agree...

Its funny how the simplest of shit can work sometimes.

AVFucker, for example... its just a file pumper, basically. but it fucking works, sometimes. ?

Definetely,

Avira, for example, got a REALLY sensitive heuristic scanner. Chances are, 99% of the crypted files (even if you crypt a harmless app) will be caught by this thing... It's insane but luckily not so many people have that antivirus anymore, but then there is Windows Defender's cloud protection + MS SmartScreen which has always been a pain in the ass to bypass recently ?

Takehito Morokuzu - January 20, 2019, 6:32 am

(Jan 20, 2019 06:17 AM)QU?CKSILVER Wrote: [\[CITE\]](#) Definetely,

Avira, for example, got a REALLY sensitive heuristic scanner. Chances are, 99% of the crypted files (even if you crypt a harmless app) will be caught by this thing... It's insane but luckily not so many people have that antivirus anymore, but then there is Windows Defender's cloud protection + MS SmartScreen which has always been a pain in the ass to bypass recently ?

Would you recommend Avira as a daily AV for me to use, or should I stick with Defender? Just in case I get infected with a crypted malware.

Alles auf Rot - January 20, 2019, 6:35 am

(Jan 20, 2019 07:32 AM)-yuno gasai- Wrote: [\[CITE\]](#) Would you recommend Avira as a daily AV for me to use, or should I stick with Defender? Just in case I get infected with a crypted malware.

ESET is the golden answer.

QU?CKSILVER - January 20, 2019, 7:12 am

(Jan 20, 2019 07:32 AM)-yuno gasai- Wrote: [\[CITE\]](#) Would you recommend Avira as a daily AV for me to use, or should I stick with Defender? Just in case I get infected with a crypted malware.

Definetely not, it does not have a decent behavioral shield and virus signature updates are not as quick as other competitors like ESET.

If I were to recommend something, I'd go with Kaspersky because of its' System Watcher (defeats most if not all types of ransomware on runtime, checks for unknown startup programs, submits unknown samples, monitors network activity and blocks whatever it finds suspicious). It also has a rollback feature in case of malware damage. Amazing.

Vytrex - January 20, 2019, 11:27 am

(Jan 20, 2019 08:12 AM)QU?CKSILVER Wrote: [\[CITE\]](#) Definetely not, it does not have a decent behavioral shield and virus signature updates are not as quick as other competitors like ESET.

If I were to recommend something, I'd go with Kaspersky because of its' System Watcher (defeats most if not all types of ransomware on runtime, checks for unknown startup programs, submits

unknown samples, monitors network activity and blocks whatever it finds suspicious). It also has a rollback feature in case of malware damage. Amazing.

I don't know about recent product but back in the day Stinger Anti-Virus was the best! Which is now bought by McAfee... you might wanna look into that too?

Please enlighten me with your thoughts on Stinger!

Takehito Morokuzu - January 20, 2019, 1:16 pm

(Jan 20, 2019 12:27 PM)walkerdavila Wrote: [\[CITE\]](#) I don't know about recent product but back in the day Stinger Anti-Virus was the best! Which is now bought by McAfee... you might wanna look into that too?

Please enlighten me with your thoughts on Stinger!

McAfee is complete junk, even John McAfee himself hates it. Stinger is just a free tool now, I doubt it is any good anymore TBH.

BTCZeus - January 20, 2019, 8:59 pm

Bumping this to help members with questions.

foxtrott50 - January 21, 2019, 3:22 am

(Jan 20, 2019 04:40 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Thanks for sharing these well-written steps, just remember these steps will only avoid scan-time detections and not run-time but I guess you are sharing this for newcomers.

So what added features or things must be done to avoid runtime detection???

BTCZeus - January 22, 2019, 9:28 am

(Jan 21, 2019 04:22 AM)foxtrott50 Wrote: [\[CITE\]](#) So what added features or things must be done to avoid runtime detection???

Runtime is more so related to actual functions of the file itself. Scantime of course is related to the actual code, but many scantime detections can be bypassed by changing surface stuff. Runtime, on the other hand, can only be changed by functional differences, such as installation methods, startup methods, etc etc. The best way to bypass runtime is generally just having a high quality stub.

foxtrott50 - January 22, 2019, 3:57 pm

(Jan 22, 2019 10:28 AM)LeoCrypto Wrote: [\[CITE\]](#) Runtime is more so related to actual functions of the file itself. Scantime of course is related to the actual code, but many scantime detections can be bypassed by changing surface stuff. Runtime, on the other hand, can only be changed by functional differences, such as installation methods, startup methods, etc etc. The best way to bypass runtime is generally just having a high quality stub.

Could you please give some examples.

BTCZeus - January 22, 2019, 4:06 pm

(Jan 22, 2019 04:57 PM)foxtrott50 Wrote: [\[CITE\]](#) Could you please give some examples.

As I said, changing installation methods, process injections (ie instead of injecting into msixec inject into self if that helps) just functional stuff.

Labbepierre94 - January 24, 2019, 1:22 pm

Thank you for this invaluable information