

Forum:[Hack Forums](#)

Thread: [autopsy of payloads](#)

Bashir Durrani - December 12, 2019, 9:36 am

hi every one i m new

so i was busy working on different payloads as u will and thought what if we create some kind of strings from that exe put some junk code in front and behind

will that fud

any ideas

Sara - December 12, 2019, 10:59 am

your close, almost got the correct idea :p

MagicianMan32 - December 12, 2019, 12:27 pm

these ways would have worked in the past

but now not only signature based systems are being deployed by Avs

there are heuristic , ML and AI .

long sequence of strings or bytes actually triggers the heuristic to detect the file so they are a very bad choice

hosting your evil bytes online is a better option

but you still got the runtime security which is a pain to bypass

even if you do so you will be disappointed when you start spreading as your file might get caught by cloud based system or reputation systems like virustotal and so on , things gets different when done on larger scale so you need to widen your perspective and start looking at the situation from different angles , not just (get the file fud on spyral scanner)

Bashir Durrani - December 22, 2019, 8:10 am

you r right but i have seen many of them in action and non of them were detected by almost every antivirus especially java ones