

Forum:[Hack Forums](#)

Thread: [Mortar Loader - Red teaming evasion technique to defeat and divert detection.](#)

DI?E - January 12, 2022, 6:49 am

Mortar Loader performs encryption and decryption of selected binary inside the memory streams and execute it directly with out writing any malicious indicator into the hard-drive. Mortar is able to bypass modern anti-virus products and advanced XDR solutions and it has been tested and confirmed bypass for the following:

Kaspersky ?
ESET ?
Malewarebytes ?
Mcafee ?
Cortex XDR ?
Windows defender ?
Cylance?
TrendMicro ?
Bitdefender ?
Norton Symantec ?

<https://github.com/0xsp-SRD/mortar>

Perplex - January 12, 2022, 9:18 am

Was just checking it out earlier, the research article on 0xsp is nicely written.

Good stuff

Perplex - January 12, 2022, 9:25 am

(Jan 12, 2022 10:20 AM)Incog Wrote: [\[CITE\]](#) Saw this on another forum, worth looking into, if people can link articles about it would be great

Based on the research of this talk> <https://www.youtube.com/watch?v=H7EMBz7GLMk>

Link is in the github, so you probably found already, but if not, then here

MeW11 - January 12, 2022, 5:17 pm

Thank you kind sir! ? good karma for you

H4x10r - January 13, 2022, 4:36 pm

wont even bypass defender mates need to be customized