

Forum:[Hack Forums](#)

Thread: [WINDOWS SECURITY/DEFENDER Detected FUD server](#)

duhduha - June 30, 2020, 1:57 am

Hi Guys, i have some problem about Windows Security detected my FUD server. I FUD my server using Crypter and i scan to all No Distribute site like kleenscan, antiscanme etc. and i update my Windows Security/ Defender with latest definition and My server was undetected and still FUD, but when i turn ON internet and Scan my server with Online Mode with Windows Defender detected as Malicious or Virus, remember my Windows Defender is latest update, but when internet turn off i scan again and Win Security not detected !! No execution problem too, run time FUD too. My question is : is Windows Defender Offline Scan and Online Scan difference! did they have two types of engine or definition? or did they use other Antivirus like Bitdefender to Kaspersky etc. to scan undetected Server online? My machine is latest Windows 10 and latest Windows Security with latest update. Plus, windows security submit unknown sample too quick and detect server sooner or later...Thanks in advance for your answer...

no one know.? Microsoft really improve their security software i think

Ren And Stimpy - June 30, 2020, 11:38 am

You simply crypt your file then use mLNK to bypass WD and SS

__Digital__ - June 30, 2020, 11:53 am

(Jun 30, 2020 01:57 AM)duhduha Wrote: [\[CITE\]](#) Hi Guys, i have some problem about Windows Security detected my FUD server. I FUD my server using Crypter and i scan to all No Distribute site like kleenscan, antiscanme etc. and i update my Windows Security/ Defender with latest definition and My server was undetected and still FUD, but when i turn ON internet and Scan my server with Online Mode with Windows Defender detected as Malicious or Virus, remember my Windows Defender is latest update, but when internet turn off i scan again and Win Security not detected !! No execution problem too, run time FUD too. My question is : is Windows Defender Offline Scan and Online Scan difference! did they have two types of engine or definition? or did they use other Antivirus like Bitdefender to Kaspersky etc. to scan undetected Server online? My machine is latest Windows 10 and latest Windows Security with latest update. Plus, windows security submit unknown sample too quick and detect server sooner or later...Thanks in advance for your answer...

no one know.? Microsoft really improve their security software i think

Use a program similar to a downloader or dropper which will get granted admin rights to interact with defender. Then execute your given payload.

duhduha - July 1, 2020, 7:50 am

(Jun 30, 2020 11:38 AM)Ren And Stimpy Wrote: [\[CITE\]](#) You simply crypt your file then use mLNK to bypass WD and SS

is this a new method and new tricks? or Old and everyone knew it?.....seem good and appealing for me