

Forum:[Hack Forums](#)

Thread: [avcheck.net possibly distributing files](#)

.fn. - November 12, 2020, 7:54 pm

i am currently almost 42 hours awake so excuse me if there is a simple explanation that i missed but basically i compiled a bin of my project, scanned it on avcheck and a short time afterwards a bot appeared in my panel, as far as I'm aware avcheck is scantime only so no reason for the file to be ran

<https://avcheck.net/id/duseJE37SbOy> original scan
<https://avcheck.net/id/1cTFjJjvLs9O> same file an hour later with one extra detection from Emsisoft Anti-Malware (check the part of the hash you can see)

bot ip from russia, running windows 7 professional 64bit

note: antiscan.me (posted in many threads as proof of fud) uses avcheck api

R A Z - November 12, 2020, 8:43 pm

the scans are normal because the detection names are same "Gen:Variant.Zusy.328313", in my opinion on the first scan Emsisoft Anti-Malware was on old version and on the new scan the engine was updated .

Jacque Fresco - November 12, 2020, 9:04 pm

probably what RAZ said. curious about the bot. maybe a leak appeared making the scanner upload data to the cloud. but i highly doubt they scan with internet turned on. i dont use it so idk.

you could write up a simple script specifically uploading data to a server once online. if you find data on that server but you only uploaded it to avcheck and its not your own machine silently distributing then.. lol

Cyber Coder - November 12, 2020, 10:34 pm

it is possible to distribute unintentionally like my scanner cyberscan.org did in the 1st week till i figure out what was happening .

How i was handling it . All options to distribute OFF , internet OFF all the time except when they updated for few mins, turned out avast was still screwing me over in that little window time.

How i fixed it ? Made sure to always take a snapshot after update and revert back to that snapshot before updating again so that avs will never get the file they scanned before internet gets on.

Jacque Fresco - November 13, 2020, 7:26 am

(Nov 12, 2020 11:34 PM)Cyber Coder Wrote: [\[CITE\]](#) How i fixed it ? Made sure to always take a snapshot after update and revert back to that snapshot before updating again so that avs will never get the file they scanned before internet gets on.

Clever, these AV's seem to actually store their previous unknown files to have them uploaded once internet is back on. But by reverting right back to after the update, is defeating this technic

YAK CODER - November 16, 2020, 7:57 am

No sir

you are wrong

the case is that major av that give Gen:Variant.Zusy.328313 is Bitdefender Total Security 2020

Bitdefender share its signature database with many av
the issue that emsi soft update this signature on 1 hour or 2 relay
about Gen: detction family
its basic shit play with file resouce like icons or other resources will remove it

.fn. - November 16, 2020, 9:02 am

(Nov 16, 2020 08:57 AM)YAK_CODER Wrote: [\[CITE\]](#) No sir
you are wrong
the case is that major av that give Gen:Variant.Zusy.328313 is Bitdefender Total Security 2020
Bitdefender share its signature database with many av
the issue that emsi soft update this signature on 1 hour or 2 relay
about Gen: detction family
its basic shit play with file resouce like icons or other resources will remove it
detection is not the issue, the issue is my bin being executed on an apparent no distributing
scantime check

Jacque Fresco - November 16, 2020, 10:11 am

(Nov 16, 2020 10:02 AM).fn. Wrote: [\[CITE\]](#) detection is not the issue, the issue is my bin being
executed on an apparent no distributing scantime check
so will you create a small dedicated bin that only sends a ping to a certain server if executed? it
would help figuring out if something is up with avcheck.net

.fn. - November 16, 2020, 10:57 am

(Nov 16, 2020 11:11 AM)Jacque Fresco Wrote: [\[CITE\]](#) so will you create a small dedicated bin that
only sends a ping to a certain server if executed? it would help figuring out if something is up with
avcheck.net
that is literally what has happened and why i created this thread

stowalone - January 10, 2021, 4:00 pm

a friend told me about yoru crypter, how do i go about getting it, i need asap... kindly get back to me,
thanks for your time