

Forum:[Hack Forums](#)

Thread: [*NEW* T-VIRUS \[1/53 DETECTION\] RELEASE](#)

tusharthegreat - September 20, 2014, 10:26 pm

Hi folks, i've been workin on this since.... well i dont know.

Actually it is not completely made by me.
I got help from many forums like hackforums.net

DETECTION RATIO = 1/53 ! (ONLY SOPHOS)
Currently this ratio without any crypter/obfuscator !

check it out.

WHAT IT DOES ?

start
blocks all input to the os
starts downlading some 1gb iso 8 times simultaneously
installs its service (bypass uac too)
starts another program which starts filling ur disk @ 1gb/min.
disables UAC
disables safemode
changes many IMPORTANT file assosiations
deletes,replaces,sets permission to nobody can access to

1. taskmanager
2. explorer
3. windows\boot
4. msconfig
5. ccleaner

strips permissions of USERS, ADMINISTRATORS, SYSTEM, TRUSTED INSTALLER AND USER
from WINDOWS directory thus making the os crash! trust me i've tried it and it worked !

tries to delete many keys from registry
disables taskmanager from registry
disables firewall
changes ie's homepage to pronos
some other batch hacks
deletes program files and program files (x86)
disables cmd

DETECTION RATIO = 1/53 ! (ONLY SOPHOS)

IF U want i can email it 2 u n u can use it on ur friends/enemies !

boobybay - September 20, 2014, 10:54 pm

Hello,

not a good start for my first message on this forums, though i hope you get it as constructive criticism ;)

How does your virus replicate? Because this is the main feat of a virus - most commonly file infection. If it would replicate itself through networks it would rather be a worm. What you're listing is more of a sabotage malware.

I'm replying because you posted in the .NET section and im interested in new file infections in .NET other then prependers. So if anyone has fresh ideas here, how to get classics to .NET like appenders oder cave infection, i'm workin on it myself atm.

And now to the constructive part: allthough i don't get the use yet (clearing the mbr would be much simpler if you just want to annoy) : i would refrain from downloading additional modules, because they could become detected aswell and you'd need to maintain a large codebase (even if you encrypt and memory inject). I'd think of some other ways like invoking deserialized and decrypted rpcs for example... if you wanna have additional tech to retrieve (much easier to implement then memory injection and no need for suspect APIs to alert AV.

RPC also has an advantage over using reflection in case youd recompile at runtime to achieve poly, because codedom still creates a physical image of the assembly, before executing it.

So props for your program and hope you evolve it to a usefull usage!

If you have any questions regarding ideas feel free to ask.

boobs

Mace - September 20, 2014, 11:04 pm

you could have written a loop instead to create 1 gb files in less than a second with nullbytes.

Cornflower Blue ???-? — September 21, 2014, 2:19 am

(Sep 20, 2014 11:04 PM)Mace Wrote: [\[CITE\]](#) you could have written a loop instead to create 1 gb files in less than a second with nullbytes.

What if my HDD speed is only 200 mbp/s, then you cant write 1gb/s.

NetMorph - September 21, 2014, 2:24 am

Why can't you share it here, and why must it be via Email?

tusharthegreat - September 24, 2014, 7:20 am

yes i 've uploaded it : <https://hackforums.net/showthread.php?tid=4460214>

actually exams are goin on and i had to do some changes.

And it CAN replicate using AUTORUN.INF

Marwix - September 24, 2014, 7:22 am

This is probably just a way for him to infect you without showing the actual code. I don't even think that he have made anything ?

TheBarret - September 24, 2014, 2:58 pm

this kid is full of shit, totally worthless.