

Forum:[Hack Forums](#)

Thread: [Thantos IRC C# \[5 DDoS funcs\] \[DL+X\] \[40kb stub\] \[Ring3rookt\] \[Great stability\] \[25\\$\]](#)

N3Cr0M0rPh - November 22, 2015, 12:02 am

Hello HF, I am here with my IRC bot, THANATOS, it is a part of my new slew of thanatos products.

Features:UDP Flood

TCP Flood

HTTP GET Flood

HTTP POST Flood

TCP Connect/SYN Flood

Download and execute

Visit website

Powerful install

Switch chan

Say message

Great Stability

~18kb stub

FULL ring3 rootkit, wipes process name completely from memory.

8/35 <http://nodistribute.com/result/mgDYk6HVEjaJB>

I only accept BTC payments my address is: 1PhzY3oowgCE2wK46zqi4ZTScLdB6qmGK8

The cost is 25\$.

This is a very HQ product. ?

?????? - November 22, 2015, 12:04 am

I would like a vouch copy

Reserving this place for the vouch

T7Amaazee - November 22, 2015, 12:06 am

seems like a decent bot will wait to see vouches.

N3Cr0M0rPh - December 7, 2015, 5:39 am

UPDATES: I added UAC bypass and a Ring3 rootkit :)

Lugina - December 7, 2015, 6:59 am

If you need a vouch i would love to try it out man. Shoot me a PM if you're interested in a review of the product.

tweety - December 7, 2015, 8:03 pm

This is the guy that posted this; <https://hackforums.net/showthread.php?tid=5085017>

jujuger - December 10, 2015, 1:23 pm

I can already tell this is fake.

You claim TCP SYN flood capabilities.

Windows computers can not do a syn flood. Raw sockets have been removed! Not in C# OR even in C++, asm, C or any other low lvl lang. Maybe it is possible with hardcore hacking, which i seriously doubt.

N3Cr0M0rPh - December 10, 2015, 3:05 pm

(Dec 10, 2015 02:23 PM)jujuger Wrote: [\[CITE\]](#) I can already tell this is fake.

You claim TCP SYN flood capabilities.

Windows computers can not do a syn flood. Raw sockets have been removed! Not in C# OR even in C++, asm, C or any other low lvl lang. Maybe it is possible with hardcore hacking, which i seriously doubt.

Its not fake, lmao. It uses normal TCP connect sockets and leaves them open.

N3Cr0M0rPh - December 14, 2015, 2:44 am

Updated the rootkit, it now hides the process and wipes it completely from memory.

#RockY - December 14, 2015, 4:54 am

if there is a vouch copy , I would interested in writing a review :)

G?Nj? - December 14, 2015, 6:29 am

any vouch copies left i would like one vouch after if working and as good as he claims it to be!

N3Cr0M0rPh - December 16, 2015, 3:28 am

Just updated, stub is now 40kb and is now NEARLY FUD
6/35 AV

<http://v2.scan.majyx.net/?page=results&sid=926087>

Filename: Windows Logon Application.exe

Type: File

Filesize: 44544 bytes

Date: 16/12/2015 - 12:25 GMT+2

MD5: 8d726d14cb9b0447b250e849ce226b50

SHA1: dfaeec517b0f5935da9b978dc9e9ca33ca240dd0

Status: Infected

Result: 6/35

AVG Free - OK
Avast - OK
AntiVir (Avira) - BDS/Backdoor.Gen
BitDefender - Gen:Heur.MSIL.Krypt.2
Clam Antivirus - OK
COMODO Internet Security - OK
Dr.Web - OK
eTrust-Vet - OK
F-PROT Antivirus - OK
F-Secure Internet Security - Gen:Heur.MSIL.Krypt.2
G Data - Gen:Heur.MSIL.Krypt.2
IKARUS Security - OK
Kaspersky Antivirus - OK
McAfee - OK
MS Security Essentials - OK
ESET NOD32 - OK
Norman - OK
Norton Antivirus - OK
Panda Security - OK
A-Squared - OK
Quick Heal Antivirus - OK
Solo Antivirus - OK
Sophos - OK
Trend Micro Internet Security - OK
VBA32 Antivirus - OK
Zoner AntiVirus - OK
Ad-Aware - Gen:Heur.MSIL.Krypt.2
BullGuard - Gen:Variant.Symmi.38296
FortiClient - OK
K7 Ultimate - OK
NANO Antivirus - OK
Panda CommandLine - OK
SUPERAntiSpyware - OK
Twister Antivirus - OK
VIPRE - OK

Scan Result: <http://v2.scan.majyx.net/?page=results&sid=926087>
[Scan by MaJyx Scanner](#)

N3Cr0M0rPh - December 20, 2015, 11:16 am

I have just upgraded to l33t. I am a very trustworthy member. And this is a very HQ product.

jujuger - December 22, 2015, 5:55 pm

(Dec 10, 2015 04:05 PM)N3Cr0M0rPh Wrote: [\[CITE\]](#) Its not fake, lmao. It uses normal TCP connect sockets and leaves them open.

I just remembered this thread, dude, leaving a tcp stream open is not a syn flood. Please remove the false advertising!

(Dec 14, 2015 03:44 AM)N3Cr0M0rPh Wrote: [\[CITE\]](#) Updated the rootkit, it now hides the process and wipes it completely from memory.

How do you wipe a process from memory? You mean you terminated it? If you 'wipe it from memory', it gets terminated.

N3Cr0M0rPh - December 22, 2015, 11:32 pm

(Dec 22, 2015 06:55 PM)jujuger Wrote: [\[CITE\]](#) I just remembered this thread, dude, leaving a tcp stream open is not a syn flood. Please remove the false advertising!

How do you wipe a process from memory? You mean you terminated it? If you 'wipe it from memory', it gets terminated.

Not it replaces the process name using WriteProcessMemory() and also scans through processes