

Forum:[Hack Forums](#)

Thread: [Dark Sadow Crypter**FUD Scan-Time & Run Time**No \\$hitC@sh**](#)

dark_sasddow - April 21, 2011, 8:36 am

Important : This is my first crypter if you have any idea please give me Thanks to nathan for source code

[img]http://img810.imageshack.us/img810/6039/darkcrypter2.jpg[/img]

File Info

Report date: 2011-04-21 17:16:30 (GMT 1)

File name: stub-exe

File size: 187904 bytes

MD5 Hash: 4ece2035d35e65bd8805301e70328c86

SHA1 Hash: 0d7ed632e5efbcfd3d79e027c79159605180d539

Detection rate: 0 on 10 (0%)

Status: CLEAN

Detections

Avast -

AVG -

Avira AntiVir -

ClamAV -

Comodo -

Emsisoft -

F-Prot -

Ikarus -

TrendMicro -

Zoner -

Scan report generated by

[NoVirusThanks.org](#)

[b]Please scan your server on novirusthanks.org and do remember to checkmark do not distribute the sample. works with any Cybergate configuration.Enjoy !

Let me know when the stub gets detected. Will update the stub and make it FUD.

Password encrypted

Atom 128>>GILA7 >>Hazz-15>> ZONG22>> Base - 64

Code

b2ZTb2Fma2NVbkxPcE9JTIhyWUIhcmwIM0RMT2loZG5sZVhGTjR4Y2xMUFCxb1BXSEE1eFJPWU
Z4Vw==

[Download](#)

Blix - April 21, 2011, 9:07 am

I dont think this is legit. 37 posts and neg rep? No thank you.

dark_sasddow - April 21, 2011, 9:50 am

lol without cheak u can not say any thing

imthavibe - April 21, 2011, 9:51 am

looks a little bit to simple to be legit soo uhhh HELL NO... not to mention no Download Link?

dark_sasddow - April 21, 2011, 9:53 am

(Apr 21, 2011 09:51 AM)imthavibe Wrote: [\[CITE\]](#) looks a little bit to simple to be legit soo uhhh HELL NO... not to mention no Download Link?
there is download link bro

Billy Cornpipe - April 21, 2011, 10:23 am

Both files in the .rar package came out clean on novirusthanks.org

HOWEVER the checksums for the stub.exe file that he listed in his scan data are not the same.

dark-crypter-exeSpoiler ([Click to View](#))File Info

Report date: 2011-04-21 19:13:31 (GMT 1)

File name: dark-crypter-exe

File size: 114042 bytes

MD5 Hash: 285489dbecf1caabce9ed3a3b3edf343

SHA1 Hash: e6b3c1615bb27fb1777f3dff962088985de85d9

Detection rate: 0 on 10 (0%)

Status: CLEAN

Detections

Avast -

AVG -

Avira AntiVir -

ClamAV -

Comodo -

Emsisoft -

F-Prot -

Ikarus -

TrendMicro -

Zoner -

Scan report generated by

NoVirusThanks.org

stub-exeSpoiler ([Click to View](#))File Info

Report date: 2011-04-21 19:14:53 (GMT 1)

File name: stub-exe

File size: 1482 bytes

MD5 Hash: 315598c8d7e60ee8e45ea6bc8e8a1f96

SHA1 Hash: 92a581281c3785684ceeb060818384d6b9b1bde7

Detection rate: 0 on 10 (0%)

Status: CLEAN

Detections

Avast -
AVG -
Avira AntiVir -
ClamAV -
Comodo -
Emsisoft -
F-Prot -
Ikarus -
TrendMicro -
Zoner -

Scan report generated by
NoVirusThanks.org

His OP scan of stub-exeSpoiler ([Click to View](#))File Info

Report date: 2011-04-21 17:16:30 (GMT 1)
File name: stub-exe
File size: 187904 bytes
MD5 Hash: 4ece2035d35e65bd8805301e70328c86
SHA1 Hash: 0d7ed632e5efbcfd3d79e027c79159605180d539
Detection rate: 0 on 10 (0%)
Status: CLEAN

Detections

Avast -
AVG -
Avira AntiVir -
ClamAV -
Comodo -
Emsisoft -
F-Prot -
Ikarus -
TrendMicro -
Zoner -

Scan report generated by
NoVirusThanks.org

Makes sense if he is scanning a crypted and binded server or keylogger. But he makes no mention of that and doesn't change the name.

dark_sasddow - April 21, 2011, 10:39 am

@billy you can use sandboxie and hex editor bro

Billy Cornpipe - April 21, 2011, 10:51 am

(Apr 21, 2011 10:39 AM)dark_sasddow Wrote: [\[CITE\]](#) @billy you can use sandboxie and hex editor bro Chill out man. I'm not saying it is or isn't infected. I simply provided an online scan result for the main executable since you did not. And it came out clean. I did notice a discrepancy in your

stub.exe scan and gave a possible explanation. Care to address that instead of getting defensive?

dark_sasddow - April 21, 2011, 10:53 am

@sorry bro thanks for your comment
166 views and only 8 comments

Desiderius?? - April 21, 2011, 10:02 pm

This is great FUD and it works and its not infected! thanks alot m8

No_Fear - April 21, 2011, 10:22 pm

Going to check it out

thx dude

\\message it short//

ÇdnîS Lu?i? - April 21, 2011, 10:56 pm

One good review on this is almost enough for me to try it, he should work on the rep though if he wants the slightest bit of trust from members.

dark_sasddow - April 21, 2011, 11:22 pm

(Apr 21, 2011 10:56 PM)IntellectualParadox Wrote: [\[CITE\]](#) One good review on this is almost enough for me to try it, he should work on the rep though if he wants the slightest bit of trust from members.
Thank you bro...

i got -rep in mistake

Sweby - April 22, 2011, 12:13 am

Thx bro, this work good. I crypt My DarkComet server. It is not FUD, it's detected by AVIRA like dropper. Anyway, good job.

cr4ck3rz - April 22, 2011, 1:33 am

Thx bro I go try with my server darkcomet ^^

dark_sasddow - April 22, 2011, 2:28 am

(Apr 22, 2011 12:13 AM)Sweby Wrote: [\[CITE\]](#) Thx bro, this work good. I crypt My DarkComet server. It is not FUD, it's detected by AVIRA like dropper. Anyway, good job.
May Be you need to change icon

i will re-fud stub soon

-mothered- - April 22, 2011, 3:06 am

Please provide a direct link to the virus scan report, and I'll take It from there.

Thanks.

aagibcheat - April 22, 2011, 3:23 am

I dont get it.

Whats the RAR password?

dark_sasddow - April 22, 2011, 3:50 am

(Apr 22, 2011 03:06 AM)mothered Wrote: [\[CITE\]](#) Please provide a direct link to the virus scan report, and I'll take it from there.

Thanks.Here It Is Bro...

http://vscan.novirusthanks.org/analysis/4ece2035d35e65bd8805301e70328c86/c3R1Yi1leGU=

(Apr 22, 2011 03:23 AM)aagibcheat Wrote: [\[CITE\]](#) I dont get it.

Whats the RAR password?You have to decrypt password

Bro....

superboy132 - April 22, 2011, 11:22 pm

Is this any good? Does it even work? Is it safe to download? And what is the detection rate?

daniels - April 22, 2011, 11:38 pm

people my eset smart security tells me that this is a trojan dropper....

use it on your own risk...

reyn45 - April 22, 2011, 11:47 pm

Thanks for this, works great. Truly needed something like this.

dark_sasddow - April 22, 2011, 11:53 pm

(Apr 22, 2011 11:38 PM)daniels Wrote: [\[CITE\]](#) people my eset smart security tells me that this is a trojan dropper....

use it on your own risk...

Lol it is crypter and trojan use sandboxie if you want

(Apr 22, 2011 11:47 PM)reyn45 Wrote: [\[CITE\]](#) Thanks for this, works great. Truly needed something like this.

Happy to help you?

princeshama - April 23, 2011, 2:02 am

wrong password infected post

dark_sasddow - April 23, 2011, 3:08 am

(Apr 23, 2011 02:02 AM)princeshama Wrote: [\[CITE\]](#) wrong password infected post

I do not think so lol..?

felicixus - April 23, 2011, 4:12 am

Hey, man =)

This is a good crypter, however is only scantime and the stub is detected 2/33

Here for you a free anonymous scan:

File Info

Report date: 2011-04-23.

Scan Occured: http://my-avscan.com/result_time.php?t=i&w=MjA0Nzg=

Link to scan: <http://my-avscan.com/result.php?scan=MjA0Nzg=>

File name: stub.exe

File size: 187904 bytes

MD5 Hash: 4ece2035d35e65bd8805301e70328c86

SHA1 Hash: 0d7ed632e5efbcfd3d79e027c79159605180d539

Detection rate: 2 out of 33
Status: INFECTED

Detections

AVG - Trojan horse Dropper.Generic3.BHLD.
Acavir - Clean.
Avast 5 -Clean.
Avast -Clean.
Avira -Clean.
BitDefender -Clean.
VirusBuster Internet Security -Clean.
Clam Antivirus -Clean.
COMODO Internet Security -Clean.
DrWeb -Clean.
eTrust-Vet -Clean.
F-PROT Antivirus -Clean.
F-Secure Internet Security -Clean.
G Data -Clean.
IKARUS Security-Clean.
Kaspersky Antivirus -Clean.
McAfee -Clean.
MS Security Essentials -Clean.
ESET NOD32 -Trojan.MSIL/TrojanDropper.Agent.AXMNHTrojan.MSIL/TrojanDropper.Agent.AXEN.
Norman -Clean.
Norton -Clean.
Panda Security -Clean.
A-Squared Security -Clean.
Quick Heal Antivirus -Clean.
Rising Antivirus -Clean.
Solo Antivirus -Clean.
Sophos -Clean.
Trend Micro Internet Security -Clean.
VBA32 Antivirus -Clean.
Vexira Antivirus -Clean.
Webroot Internet Security -Clean.
Zoner AntiVirus -Clean.
AhnLab V3 Internet Security -Clean.

Scan report generated by
my-avscan.com

Crypter file become 6/33 .-.

You need to rename strings, and add junk code. Also a assembly changer and an icon changer will be great and will remove after crypting detection:

File Info

Report date: 2011-04-23.

Scan Occured: [\[img\]](http://my-avscan.com/result_time.php?t=i&w=MjA0ODE=)

Link to scan: <http://my-avscan.com/result.php?scan=MjA0ODE=>

File name: crypted.exe

File size: 469016 bytes

MD5 Hash: ffdb60f3d4afa3963443d06f1dfd04d7

SHA1 Hash: 1bf850b5577d96c5845253376d71551101e85a32

Detection rate: 6 out of 33
Status: INFECTED

Detections

AVG - Trojan horse Dropper.Generic3.BHLD.
Acavir - Clean.
Avast 5 -Clean.
Avast -Clean.
Avira -TR/Dropper.Gen.
BitDefender -Clean.
VirusBuster Internet Security -Clean.
Clam Antivirus -Clean.
COMODO Internet Security -Clean.
DrWeb -Clean.
eTrust-Vet -Clean.
F-PROT Antivirus -Clean.
F-Secure Internet Security -Gen:Heur.MSIL.Krypt.2.
G Data -Gen:Heur.MSIL.Krypt.2 (Engine-A).
IKARUS Security-Clean.
Kaspersky Antivirus -Clean.
McAfee -Clean.
MS Security Essentials -Clean.
ESET NOD32 -Trojan.MSIL/TrojanDropper.Agent.AXMNHTrojan.MSIL/TrojanDropper.Agent.AXEN.
Norman -Clean.
Norton -Clean.
Panda Security -Suspicious.
A-Squared Security -Clean.
Quick Heal Antivirus -Clean.
Rising Antivirus -Clean.
Solo Antivirus -Clean.
Sophos -Clean.
Trend Micro Internet Security -Clean.
VBA32 Antivirus -Clean.
Vexira Antivirus -Clean.
Webroot Internet Security -Clean.
Zoner AntiVirus -Clean.
AhnLab V3 Internet Security -Clean.

Scan report generated by
my-avscan.com

dark_sasddow - April 23, 2011, 5:24 am

@ felicinox
what
my-avscan.com will send file simple to av company??

Harsh Gupta - April 23, 2011, 5:50 am

Is it supports all type of RAT including dark comet?

bigit1029 - April 23, 2011, 5:57 am

if its not infected would you mind scanning on virustotal?

dark_sasddow - April 23, 2011, 5:58 am

(Apr 23, 2011 05:57 AM)bigit1029 Wrote: [\[CITE\]](#) if its not infected would you mind scanning on virustotal?

Idiot Do not scan on virus total or it will be no longer fud

(Apr 23, 2011 05:50 AM)Harsh Gupta Wrote: [\[CITE\]](#) Is it supports all type of RAT including dark comet?

I have not check it on all but you can try and tell us..

x-elio789 - April 23, 2011, 10:27 am

..we have to decrypt password oo'

dark_sasddow - April 23, 2011, 9:22 pm

(Apr 23, 2011 10:27 AM)x-elio789 Wrote: [\[CITE\]](#) ..we have to decrypt password oo'
it is very easy just use crypto.com will take 1 minute

stealtre - April 26, 2011, 10:02 am

Uhm this file is not FUD anymore.

Could you please make it FUD again?

File Info

Report date: 2011-04-26 19:04:15 (GMT 1)

File name: server-2-crypted

File size: 475672 bytes

MD5 Hash: c48613356c641fc7c9b33b193951e3b1

SHA1 Hash: c0cdaceb8a1bdf5f95c034edc689636833ffd6d9

Detection rate: 3 on 10 (30%)

Status: INFECTED

Detections

Avast - MSIL:Dropper-IM [Drp]

AVG - Dropper.Generic3.BHLD

Avira AntiVir - TR/Dropper.Gen

ClamAV -

Comodo -

Emsisoft -

F-Prot -

Ikarus -

TrendMicro -

Zoner -

Scan report generated by

NoVirusThanks.org

Stenography - April 26, 2011, 10:35 am

56 posts,

-3 rep ..

who the fuck you trolling huh ?

gtfo asshole i am reporting

Darky - April 26, 2011, 10:44 am

Joke, No Download... Neg rep -3

djkilla - *April 26, 2011, 12:33 pm*

it don't work.

Avast says : MSIL:Dropper-IM (Drp)