

Forum: [Hack Forums](#)

Thread: [\[TUT\] - How to Crypt a Turkojan Server Successfully...](#)

Carb0n F1ber - August 14, 2009, 5:34 am

This query has come up many times in this forum, "How to Crypt a Turkojan Server Successfully??" . It is very easy to crypt the server with any free crypters available in this forum, but many face the trouble when the server automatically extracts 2 DLL files, which then gets detected in the victims computer.

Here is a tutorial to show you how to extract, crypt, and re-join the DLL's back into the Turkojans server.

- 1) First of all, you will need your "server" created by Turkojan. Make sure you do not pack your server with UPX i.e., uncheck the option that says "Pack Server Using UPX" (you can find this option at the bottom of your Server Editor).
- 2) Next you will need "PE Explorer", download the 30-day evaluation from <http://www.heaventools.com/download-pe-explorer.htm>
- 3) Open PE Explorer, and open the server file created by Turkojan
- 4) Click on View - Resources
- 5) Right click on the DENEME resource and select "Save Resource As". Make sure you save as .DLL file
- 6) Repeat the same step with resource named ROOTKIT
- 7) Now, use your own methods to crypt the 2 extracted .DLL files. I personally use "asprotect". You can download a free trial from <http://www.aspack.com/downloads.aspx>
Note: asprotect does not make your .DLL files 100% FUD. Just use random key protection, and you might get as lucky as 95% UD. Else, use your own methods.
Do let me know if you find any other tool to crypt .DLL files. Even I'm searching for one
- 8) Now that you have crypted both .DLL files, time to pack it back with the server
- 9) Download "Resource Hacker" from <http://www.angusj.com/resourcehacker/>
- 10) Make sure you close PE Explorer, and open the same server file with Resource Hacker
- 11) Right click DENEME resource and select "Replace Resource". Click on "Open file with new resource" and select the crypted DENEME.DLL file. Under "Resource Type" type RCDATA, under "Resource Name" type DENEME, leave "Resource Language" empty. Repeat the same with ROOTKIT, typing ROOTKIT as "Resource Name".
- 12) "Save" or "Save As" the new server.
- 13) Now you can crypt the server file separately again.

14) Ready to go..!!

Credits: To RDG for teaching me this... ?

A simple thanks is always appreciated ? ...

Gr1ng - August 14, 2009, 5:40 am

Thank you, this helped me alot. :)

Zodiac - August 14, 2009, 5:44 am

Nice tut dude! ?

Xness - August 14, 2009, 5:59 am

Very well done indeed.

Carb0n F1ber - August 14, 2009, 6:48 am

Lolzzzz.....

Edit: If someone finds another method to crypt .DLL files, please post it here... Even I'm looking for one...

Thanks

markeli2 - August 14, 2009, 9:30 am

Sounds good, I'll try this and post my opinion

dover - August 14, 2009, 12:53 pm

Good tut but for noobs like me which options do we tick when crypting with the

<http://www.aspack.com/downloads.aspx>

Maybe you could add that into your guide^^

Apokz - August 16, 2009, 9:25 am

hmm followed this tut but now if i test the server after crypting with RDG's Tejon it wont connect to client. any ideas?

Carb0n F1ber - August 16, 2009, 12:10 pm

(Aug 16, 2009 09:25 AM)mancurian Wrote: [\[CITE\]](#) hmm followed this tut but now if i test the server after crypting with RDG's Tejon it wont connect to client. any ideas?Try again... You must have missed a thing ?

Apokz - August 16, 2009, 12:34 pm

(Aug 16, 2009 12:10 PM)Carb0n F1ber Wrote: [\[CITE\]](#) Try again... You must have missed a thing ? tried a number of times with the same result im guessing im missing somethin but really cant pin point what , ive been through it with RDG also

DarkZero - August 16, 2009, 3:35 pm

Thanks! This is exactly what I needed! Hopefully this will make my servers UD enough to not get deleted upon download.

Carb0n F1ber - September 3, 2009, 8:35 am

@ iBruteforce

Thanks for re-opening this thread... Anyone has any doubts, please post here...

Please do not PM me.. Thanks for understanding ?

PS: I also corrected the actual tutorial (first post) where there were lots of jumbled non-ascii characters

Feel No Pain - September 6, 2009, 12:15 pm

my anti virus thing blocked Turkojan from opening =[
Turkojan = This?

a-squared 4.5.0.24 2009.09.06 Backdoor.Win32.Turkojan.amr!IK
AhnLab-V3 5.0.0.2 2009.09.05 Win-Trojan/Turkojan.1527646
AntiVir 7.9.1.8 2009.09.06 TR/Drop.Age.1530279
Antiy-AVL 2.0.3.7 2009.09.04 Backdoor/Win32.Turkojan.gen
Authentium 5.1.2.4 2009.09.06 W32/BackdoorX.ACGA
Avast 4.8.1351.0 2009.09.05 Win32:Trojan-gen {Other}
AVG 8.5.0.409 2009.09.06 BackDoor.Delf.BUP
BitDefender 7.2 2009.09.06 Trojan.Generic.394500
CAT-QuickHeal 10.00 2009.09.05 Trojan.Agent.IRC
ClamAV 0.94.1 2009.09.06 -
Comodo 2203 2009.09.06 Backdoor.Win32.Turkojan.~EV
DrWeb 5.0.0.12182 2009.09.06 -
eSafe 7.0.17.0 2009.09.06 Win32.Turkojan.amr
eTrust-Vet 31.6.6721 2009.09.04 Win32/ASuspect.GFJLB
F-Prot 4.5.1.85 2009.09.06 W32/BackdoorX.ACGA
F-Secure 8.0.14470.0 2009.09.06 Backdoor:W32/Turkojan.Z
Fortinet 3.120.0.0 2009.09.06 PossibleThreat
GData 19 2009.09.06 Trojan.Generic.394500
Ikarus T3.1.1.72.0 2009.09.06 Backdoor.Win32.Turkojan.amr
Jiangmin 11.0.800 2009.09.06 -
K7AntiVirus 7.10.837 2009.09.05 Backdoor.Win32.Turkojan
Kaspersky 7.0.0.125 2009.09.06 Backdoor.Win32.Turkojan.amr
McAfee 5733 2009.09.06 BackDoor-CZP.dr
McAfee+Artemis 5733 2009.09.06 BackDoor-CZP.dr
McAfee-GW-Edition 6.8.5 2009.09.06 Trojan.Drop.Age.1530279
Microsoft 1.5005 2009.09.06 Backdoor:Win32/Turkojan.gen!A
NOD32 4401 2009.09.06 probably a variant of Win32/Agent
Norman 6.01.09 2009.09.04 -
nProtect 2009.1.8.0 2009.09.06 Trojan/W32.Agent.1527646
Panda 10.0.2.2 2009.09.06 Bck/Turkojan.J
PCTools 4.4.2.0 2009.09.06 Backdoor.Turkojan!sd6
Prevx 3.0 2009.09.06 High Risk System Back Door
Rising 21.45.14.00 2009.09.01 Backdoor.Agent.fbt
Sophos 4.45.0 2009.09.06 Troj/Turkoj-Gen
Sunbelt 3.2.1858.2 2009.09.06 Trojan.Win32.Generic!BT
Symantec 1.4.4.12 2009.09.06 Backdoor.Turkojan
TheHacker 6.3.4.3.396 2009.09.04 -
TrendMicro 8.950.0.1094 2009.09.05 BKDR_TURKOJAN.AL
VBA32 3.12.10.10 2009.09.05 Backdoor.Win32.Turkojan.amr
ViRobot 2009.9.4.1919 2009.09.04 Backdoor.Win32.Turkojan.1527646
VirusBuster 4.6.5.0 2009.09.06 Backdoor.Turkojan.AAJ

emzee - September 6, 2009, 1:19 pm

ehmmm i didnt get the crypting part ... 1st the GUI of the crypting program you provided us with is kinda complicated that i didnt know what to do !! :D can u give me more inscriptions !! & Thanks For Your Time =] <3

Toma - September 6, 2009, 2:39 pm

Nice tut,thanks.....

hivekiller - September 6, 2009, 4:19 pm

good tutorial...

i will try it when i finish creating a server...

chr0n1ck - September 6, 2009, 7:25 pm

Thanks!

Fantastic tutorial, very detailed and easy to follow.

+Rep for you

?

pal62 - September 6, 2009, 8:35 pm

outstanding tut...thanks for the information

Internet - September 6, 2009, 8:38 pm

Too bad this doesn't make your Turkojan server 100% FUD.. You'll be lucky to get it to 70% FUD..

larrystreet - September 8, 2009, 4:01 pm

Thanks for the great tutorial. My server is now undetected by my kaspersky. Great information. But something is up with that aspack crypter. I'm not accusing anyone of anything, but when i scanned it with kaspersky it had multiple detections of "aspack, prorat/backdoor".

I just opened it, and scanned it, i never used it to crypt anything. I expected something to show up, it is a public version. I didn't think prorat/backdoor would be used by kaspersky to identify a crypter. Just a heads up.

bhuvirebel - September 11, 2009, 7:37 am

Thanks for the post man!

Carb0n F1ber - September 11, 2009, 7:47 am

(Sep 6, 2009 01:19 PM)emzee Wrote: [\[CITE\]](#) ehmmm i didnt get the crypting part ... 1st the GUI of the crypting program you provided us with is kinda complicated that i didnt know what to do !! :D can u give me more inscriptions !! & Thanks For Your Time =] <3

Even if you get the crypting part..... It won't be FUD... So... Sorry, but find your own ways of crypting the .DLL files...

Post here if you find a crypter that could do .DLL files too

CyberCube - September 11, 2009, 7:52 am

nice tut. but it isn fud...

Carb0n F1ber - September 11, 2009, 7:53 am

(Sep 11, 2009 07:52 AM)CyberCube Wrote: [\[CITE\]](#) nice tut. but it isn fud...

The tutorial is focused on "How" to extract, crypt, and re-pack the .DLL files... ?

Post here if you find better ways to crypt .DLL files... Thanks ?

Honllyn - September 11, 2009, 7:57 am

" it's not a application win32 " Help me please.. ^^

Carb0n F1ber - September 11, 2009, 8:06 am

(Sep 11, 2009 07:57 AM)Honllyn Wrote: [\[CITE\]](#) " it's not a application win32 " Help me please.. ^^
Please elaborate when exactly you are receiving this error ?

Honllyn - September 11, 2009, 8:07 am

Just after compiling on resource Hacker
When I run the server

rajvid9 - September 11, 2009, 11:19 am

Nice tut dude.... good work.

Maxaber - September 11, 2009, 11:41 am

Thanks for the TUT man!!!

Internet - September 11, 2009, 11:46 am

Has anyone found a more effective way on crypting the .DLL files?

Honllyn - September 11, 2009, 11:52 am

Help me please...

SCFAdamVcG - September 11, 2009, 2:22 pm

Great tutorial ,thankyou ,I think what would put some more spark into this tutorial is if you could find the tutorial from Milw0rm on how to change a virus's signature ,Works a treat . :)

angel of death - September 11, 2009, 2:25 pm

well i saw this somewhere i dont remember so if you copy someone else work try to give credit to the main writer!!!!!!!!!!!!!!!!!!!!!!

Carb0n F1ber - September 11, 2009, 2:35 pm

(Sep 11, 2009 02:25 PM)angel of death Wrote: [\[CITE\]](#) well i saw this somewhere i dont remember so if you copy someone else work try to give credit to the main writer!!!!!!!!!!!!!!!!!!!!!!

Sorry dude, I typed this out myself... ?

Fuck shit ??

A quick google showed my exact tutorial using exact words, title, and even font color on another forum ...

The best part, even my asking for +Rep is posted there, and the point that I use RDG's Tejon.....
Lolzzzz..... Looserssssss

PS: He even stole it the same date I posted mine, some "senior member".... argggg

(Sep 11, 2009 02:22 PM)SCFAdamVcG Wrote: [\[CITE\]](#) Great tutorial ,thankyou ,I think what would put some more spark into this tutorial is if you could find the tutorial from Milw0rm on how to change a virus's signature ,Works a treat . :)

You got a link to it ?? Please post here..... Thanks ?

angel of death - September 11, 2009, 2:43 pm

well i saw this before yours somewhere else so this dont belong to you just say it lol dont be shy every one could do this lol

Carb0n F1ber - September 11, 2009, 2:47 pm

(Sep 11, 2009 02:43 PM)angel of death Wrote: [\[CITE\]](#) well i saw this before yours somewhere else so this dont belong to you just say it lol dont be shy every one could do this lol

#1 That forum does not have a +/- Rep system, yet he posted an exact replicate of my TUT asking for a +Rep

#2 I purchased RDG's Tejon from "this" forum, and RDG is the one who taught me the above stuff (I gave credit to him).. Yet, even that line is copied on in that forum...

So get back to your hole, and STFU if you don't know anything...

Since I can't post links to other forums here, I PM'd you the link to the forum, make a comparison yourself...

Honllyn - September 12, 2009, 12:35 am

Can you help me? ^^

Thx....

Carb0n F1ber - September 12, 2009, 12:44 am

(Sep 11, 2009 08:07 AM)Honllyn Wrote: [\[CITE\]](#) Just after compiling on resource Hacker When I run the server Did you follow #11 correctly ???

Quote:11) Right click DENEME resource and select "Replace Resource". Click on "Open file with new resource" and select the crypted DENEME.DLL file. Under "Resource Type" type RCDATA, under "Resource Name" type DENEME, leave "Resource Language" empty. Repeat the same with ROOTKIT, typing ROOTKIT as "Resource Name".

haxx0r - September 12, 2009, 12:44 am

great tut thx!!!

Spoiler ([Click to View](#))to short

Honllyn - September 12, 2009, 1:20 am

http://www.youtube.com/watch?v=FpWs_SNTIAg

...This is not good?

Carb0n F1ber - September 12, 2009, 1:27 am

(Sep 12, 2009 01:20 AM)Honllyn Wrote: [\[CITE\]](#) http://www.youtube.com/watch?v=FpWs_SNTIAg ...This is not good?

Try unchecking the "compress with UPX" option on Turkojan when creating the server.... Create a new server, and replace the .DLL's...

Try, and let me know....

Honllyn - September 12, 2009, 4:20 am

Ah ok....

Thank you very much ;)

Very nice tut

Carb0n F1ber - September 12, 2009, 4:24 am

(Sep 12, 2009 04:20 AM)Honllyn Wrote: [\[CITE\]](#) Ah ok....
Thank you very much ;)

Very nice tut
Worked ???

Anyways, I have updated the tutorial to state "Do not pack using UPX" ?

Honllyn - September 12, 2009, 5:20 am

Yes,
Thanks =)

BigG - September 12, 2009, 8:25 am

does this work with ardamax servers?

Internet - September 12, 2009, 8:41 am

(Sep 12, 2009 08:25 AM)slayerboy Wrote: [\[CITE\]](#) does this work with ardamax servers?
Nope.

Honllyn - September 13, 2009, 5:38 am

there other program that ASProtect?

xips - September 13, 2009, 6:15 am

thanks for the posting man.....

Carb0n F1ber - September 13, 2009, 6:59 am

(Sep 13, 2009 05:38 AM)Honllyn Wrote: [\[CITE\]](#) there other program that ASProtect?
I'm still searching for one... ?

Post here if you find... ?

Honllyn - September 13, 2009, 1:08 pm

Crypt Themida + Crypt ASProtect = FUD (I think)

Download Themida : <http://#.com/files/11421952/Themida.1.8.5.5.Full.zip.html>

[IMG]<http://nsa08.casimages.com/img/2009/06/23//090623012921671356.jpg>[IMG] Select your file
Go Protection Options ->

[IMG]<http://nsa08.casimages.com/img/2009/06/23//090623013131376135.gif>[IMG]
-> [IMG]<http://nsa07.casimages.com/img/2009/06/23//090623013250218535.gif>[IMG]

Sorry my very bad langage english xD

+my frist rep? :-)

Carb0n F1ber - September 13, 2009, 11:08 pm

(Sep 13, 2009 01:08 PM)Honllyn Wrote: [\[CITE\]](#) Crypt Themida + Crypt ASProtect = FUD (I think)
Download Themida : <http://#.com/files/11421952/Themida.1.8.5.5.Full.zip.html>

<http://nsa08.casimages.com/img/2009/06/23//090623012921671356.jpg> Select your file
Go Protection Options -> <http://nsa08.casimages.com/img/2009/06/23//090623013131376135.gif>

-> <http://nsa07.casimages.com/img/2009/06/23//090623013250218535.gif>

Sorry my very bad language english xD

+my frist rep? :-)#1 Please edit your posts and use the image tags around your hyperlinks... e.x.
[IMG]www.hyperlinkhere.com/test.jpg[/IMG]

#2 You could get a warning if you "ask" for +Reps ?

Honllyn - September 14, 2009, 12:21 am

File Info

Report generated: 14.9.2009 at 10.15.57 (GMT 1)
Filename: DENEME2.dll
File size: 464 KB
MD5 Hash: 9cb4c08538b59dc825a978e3a836fc0f
SHA1 Hash: E43C4553C4504601ACB309D26BBF622688455986
Self-Extract Archive: Nothing found
Binder Detector: Nothing found
Detection rate: 3 on 23

Detections

a-squared - Backdoor.Hupigon!!K
Avira AntiVir - -
Avast - -
AVG - -
BitDefender - -
ClamAV - -
Comodo - -
Dr.Web - -
Ewido - -
F-PROT6 - W32/Heuristic-210!Eldorado
Ikarus T3 - Backdoor.Hupigon
Kaspersky - -
McAfee - -
NOD32 v3 - -
Norman - -
Panda - -
QuickHeal - -
Solo Antivirus - -
Sophos - -
TrendMicro - -
VBA32 - -
VirusBuster - -
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

Good, no?

(+ BitDefender for rootkit :s)

Carb0n F1ber - September 14, 2009, 2:19 am

(Sep 14, 2009 12:21 AM)Honllyn Wrote: [\[CITE\]](#) Good, no?

Looks very very good... You have bypassed all the very-often-used AV's

Good job there ?

Can I borrow the file ? ???

Honllyn - September 14, 2009, 2:27 am

Yes, of course.

You have a good crypter for me? (PM)

Carb0n F1ber - September 14, 2009, 2:44 am

(Sep 14, 2009 02:27 AM)Honllyn Wrote: [\[CITE\]](#) Yes, of course.

You have a good crypter for me? (PM)

Don't you have RDG's ??? I use RDG too ... But all my stubs are highly detected...

Honllyn - September 14, 2009, 2:54 am

Can you send me? I have no encryption

I'll buy iCrypt 3.0 private (FUD) ^^

Carb0n F1ber - September 14, 2009, 4:02 am

(Sep 14, 2009 02:54 AM)Honllyn Wrote: [\[CITE\]](#) Can you send me? I have no encryption

I'll buy iCrypt 3.0 private (FUD) ^^

Sorry, cannot send it to you.... It is private version... Registered with serial number for unique computer only ?

Honllyn - September 14, 2009, 4:54 am

<https://hackforums.net/showthread.php?tid=126942>

I Go to buy^^

Honllyn - September 14, 2009, 10:08 am

Why when a victim run the server, Windows asks for confirmation at each startup?

Help me please :s

D3x73r - September 14, 2009, 11:03 am

thanks dude I like it !! Greate tut

Honllyn - September 14, 2009, 12:42 pm

Link RDG Tejon please

Honllyn - September 15, 2009, 2:38 am

Does anyone know how to bypass UAC?

If I found how to do

The server will work fine.

I can send you a encrypt only detected by Avira.

Thanks.

Lasagna - September 15, 2009, 9:53 pm

very nice tut man

TOO SHORTTTTTTTTTTTTTTTT

ken2003445 - September 19, 2009, 11:29 am

what is this for??

make anti virus undeteable or smoething??

hexxar - October 15, 2009, 7:04 am

bro ? you are the best xD :P toooo shooooooooooooorrrt

N1NJ4_N30 - October 17, 2009, 7:18 pm

I was just wondering but,
couldn't you use ResHack to extract the dll's instead of using PE Explorer?

Just a though (haven't tested it myself),
N1NJ4_N30

Carb0n F1ber - October 17, 2009, 9:52 pm

Nope, you cannot extract them as .DLL using ResHack... There is no such option...

r34p3r - October 18, 2009, 12:57 am

nice tut will have a go, thanks :)

wdildar - October 18, 2009, 1:32 am

nice post really liked it?

BeNoM - October 24, 2009, 2:44 am

tip: maybe give some credits to the site u copied it from. But its a good tut no doubt. thx for sharing

CyberDemon1337 - October 24, 2009, 2:47 am

Good job with this tut, thanks will be useful :D

Carb0n F1ber - October 24, 2009, 3:23 am

(Oct 24, 2009 02:44 AM)BeNoM Wrote: [\[CITE\]](#) tip: maybe give some credits to the site u copied it from. But its a good tut no doubt. thx for sharing
Please refer to post numbers 36 and 38 ... Thanks ?

Saki~chan - October 24, 2009, 11:08 am

Will this work on spynet servers too?

EDIT
NOPE!

encrypt - October 24, 2009, 11:51 am

Useful tutorial, thanks for sharing. I did try it at first then it didn't work then i went through it again and i missed a step out so make sure you read proper people.

ززز - October 29, 2009, 5:47 am

sorry.. when i try to save resource as.. it wont let me.. nothing happens, it just lags, im using vista atm

Xinapse - October 29, 2009, 6:43 am
thats a really good tut ! :)

Carb0n F1ber - October 29, 2009, 10:58 am
(Oct 29, 2009 05:47 AM)Royal Blue Wrote: [\[CITE\]](#) sorry.. when i try to save resource as.. it wont let me.. nothing happens, it just lags, im using vista atm
I'm not sure, never tried in Vista or Win7 Try running PE Explorer in XP mode ?

sweetspotted - November 5, 2009, 11:27 am
NICEEEEE Tut very helpful, now im gonna go try crypt some dll files 8D ty~

Fukushima - November 5, 2009, 11:35 am
Thank you, just what i needed!

-C0d3ak- - November 5, 2009, 1:11 pm
Nice tut dude! :D D D

NHILL - November 6, 2009, 8:30 pm
Hi great work man ?

really liked it

Thanks

\$weet - November 6, 2009, 11:00 pm
excellent tutorial man, helped me a lot as well as many others on here. thanks

Valour - November 7, 2009, 2:21 am
if i crypt the .dll file but th dll file changes to exe
will it still work ??
i m using redtube crypter

Carb0n F1ber - November 7, 2009, 5:22 am
(Nov 7, 2009 03:21 AM)Undefined Wrote: [\[CITE\]](#) if i crypt the .dll file but th dll file changes to exe
will it still work ??
i m using redtube crypter
You can replace resources with .EXE files as well.. I haven't tried it yet...

Perhaps you can try it and let us know ?? ? ??

NHILL - November 7, 2009, 5:50 am
Hi

1 - how can i use random key protection in asprotect option when protection dll

2 - Trial version of asprotect 1.5 or i need to buy this software too?

cause avast still dectecting dll ?

thanck for helping me ?

Carb0n F1ber - November 7, 2009, 6:07 am

(Nov 7, 2009 06:50 AM)NHILL Wrote: [\[CITE\]](#) HI

1 - how can i use random key protection in asprotect option when protection dll

2 - Trial version of asprotect 1.5 or i need to buy this software too?

cause avast still dectecting dll ?

thanck for helping me ?

Search google for the latest cracked version of asprotect.... Or try themida... they are both good to bring the detection rate down :)

silenthacker1 - December 25, 2009, 12:23 am

i am also using the turkojan its great for pc hacking

BaNNED - December 25, 2009, 3:42 pm

Today packed with public protector .

File Info

Report generated: 26.12.2009 at 0.38.11 (GMT 1)

Filename: RCData_ROOTKIT.DLL

File size: 346624

MD5 Hash: d44e50d99086256ce8ddd7359310bada

SHA1 Hash: EABA7795D1450FF1EBB15D6947B4D370375F55BA

Self-Extract Archive: Nothing found

Binder Detector: Nothing found

Detection rate: 1 on 24

Detections

a-squared - -

Avira AntiVir - -

Avast - -

AVG - -

BitDefender - -

ClamAV - -

Comodo - -

Dr.Web - -

Ewido - -

F-PROT6 - -

G-Data - -

Ikarus T3 - -

Kaspersky - -

McAfee - -

NOD32 v3 - -

Norman - -

Panda - -
QuickHeal - -
Solo Antivirus - -
Sophos - -
TrendMicro - -
VBA32 - Trojan-Downloader.Win32.Genome.yjt
VirusBuster - -
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

Good ? ?

Carb0n F1ber - December 25, 2009, 8:14 pm
(Dec 25, 2009 04:42 PM)Banned Wrote: [\[CITE\]](#) Good ? ?
Sexyyy... ?

Is that Themida ???

J0hn - December 26, 2009, 11:10 am
Excellent tut thanks

BaNNED - December 26, 2009, 11:37 am
(Dec 25, 2009 09:14 PM)Carb0n F1ber Wrote: [\[CITE\]](#) Sexyyy... ?

Is that Themida ???
No , Themida will get 2/24 or 3/24 (including Avira & AVG , depends on settings) at NVT ? .
And big pump file size . 30kb > 1.xx mb :(
But i got 1/24 at NVT with using WinLicense (same as Themida , but built in Registration System)
on my first scan protecting deneme.
Then i protected again rootkiti got 3/24 nvt :(. No Idea

shoaibbi - December 28, 2009, 5:13 am
thanks for the share brother

wb1066 - December 28, 2009, 7:01 am
thanks for the tut going to try

lorens13 - December 29, 2009, 8:56 pm
Nice,thanks for sharing it on HF^^

Project123 - January 10, 2010, 9:10 am
How do you use asprotect? ??

Carb0n F1ber - January 13, 2010, 5:11 am
(Jan 10, 2010 10:10 AM)Project123 Wrote: [\[CITE\]](#) How do you use asprotect? ??
Try to get a full (cracked) version...

lthasabika - January 20, 2010, 5:20 pm
Thanks For the post, I Thought turkojan was a lost cause with encryption untile today!

Skyro - January 20, 2010, 5:33 pm

Fantastic tutorial, thanks.

Matter - January 20, 2010, 7:45 pm

Very nice tut thanks

Gangstahpy - January 21, 2010, 12:23 pm

what do u mean in the end by crypting the file server seperatly?? i crypted the new server with fly crypter, am i supposed to crypt it with asprotect...? btw i did crypt it with asprotect but its still detectable...

Tattoo - March 3, 2010, 2:11 pm

Nice TuT have run through it a couple of times and am still getting detected with Avast but at least now I know how the process of Encrypting goes, Ill keep trying and hopefully crack it in the end. Thanks again for the time taken to help us Noobs

Carb0n F1ber - March 4, 2010, 7:54 am

(Mar 3, 2010 03:11 PM)Tattoo Wrote: [\[CITE\]](#) Nice TuT have run through it a couple of times and am still getting detected with Avast but at least now I know how the process of Encrypting goes, Ill keep trying and hopefully crack it in the end. Thanks again for the time taken to help us Noobs

Your welcome. Glad you got the point of this Tutorial. This does not help you crypt your .DLL files, it only explains you the "process" of crypting. You will have to find your own ways of crypting though.

PS: A guy in this thread suggested "Themida" to bring a huge difference in crypting .DLL files. Haven't tried it myself. I suggest you give it a go and post your findings here.

JUstj - March 8, 2010, 11:45 am

Hey guys i have a problem when i crypt the dll files with Themida and try to replace the original ones using Resource Hacker it stops responding and i cant replace the non-crypted dll files. Could this be because of wrong protecting options in themida or something? Iam pretty sure the problem is not in Resource Hacker but in Themida.

Help please.

Update i did it just had to wait more for Resource Hacker to replace the dll files cuz they were bigger... NOOBISH :P

But the crypted dll files get 4/21 on novirusthanks and the whole server gets 8/21 not so good... Maybe using more protection options in Themida?

blksith0 - March 17, 2010, 9:49 am

How do you use the ASProtect? PM me.

Thanks

Viraavy - March 20, 2010, 6:07 am

Very good tutorial.....

SYLDD - April 4, 2010, 2:31 pm

good tutorial but im afraid im to stupid to do all that lol

codepoet - April 6, 2010, 7:35 pm

this is very help full thank you

tipliedown - April 6, 2010, 7:42 pm

thanks dude i am looking for this :Smile:

Fuzzyhacker - July 1, 2010, 4:22 pm

Thank's man. Now i only have to worry about avast and avg

iDKxHiggins - July 10, 2010, 4:14 pm

wait... so do we bind the 2 .dll files to our server?

Fuzzyhacker - July 10, 2010, 5:13 pm

Quote:wait... so do we bind the 2 .dll files to our server?

No you 12 year old. read the directions

Mr.BTC - July 21, 2010, 11:53 pm

thanks dude gonna try this :D

but this rat is old tho :D

eastanbool - September 3, 2010, 3:54 pm

is there a new way to crypt the DLL files`???

XzatriX - September 26, 2010, 5:54 am

Great tuto Carb0n, as you can see, the dlls are 88% FUD, not so bad (:

Any proof :

[img]<http://nsa21.casimages.com/img/2010/09/26/100926024503625156.jpg>[/img]

File Info

Report date: 2010-09-26 14:51:59 (GMT 1)

File name: rc-data-rootkit-dll

File size: 166912 bytes

MD5 Hash: 4372ef902b68348ed003a3e8f0a0b691

SHA1 Hash: b99508b420d966f6ba94ef7e12a236f877120fab

Detection rate: 2 on 16 (12%)

Status: INFECTED

Detections

a-squared -

Avast -

AVG -

Avira AntiVir -

BitDefender -

ClamAV -

Comodo -

Dr.Web -

F-PROT6 -

Ikarus T3 - Backdoor.Win32.Poison

Kaspersky -

NOD32 -

Panda -

TrendMicro -
VBA32 - Trojan-Spy.Agent.41
VirusBuster -

Carb0n F1ber - September 26, 2010, 5:58 am

(Sep 26, 2010 05:54 AM)XzatriX Wrote: [\[CITE\]](#) Great tuto Carb0n, as you can see, the dlls are 88% FUD, not so bad (:

Wow nice. What method did you use to crypt the .dll files??

BTW, no one uses ikarus and VBA32 AV's anyways ?

4L1C4N - October 8, 2010, 8:31 pm

(Sep 6, 2009 12:15 PM)Feel No Pain Wrote: [\[CITE\]](#) my anti virus thing blocked Turkojan from opening =[

Turkojan = This?

a-squared 4.5.0.24 2009.09.06 Backdoor.Win32.Turkojan.amr!IK
AhnLab-V3 5.0.0.2 2009.09.05 Win-Trojan/Turkojan.1527646
AntiVir 7.9.1.8 2009.09.06 TR/Drop.Age.1530279
Antiy-AVL 2.0.3.7 2009.09.04 Backdoor/Win32.Turkojan.gen
Authentium 5.1.2.4 2009.09.06 W32/BackdoorX.ACGA
Avast 4.8.1351.0 2009.09.05 Win32:Trojan-gen {Other}
AVG 8.5.0.409 2009.09.06 BackDoor.Delf.BUP
BitDefender 7.2 2009.09.06 Trojan.Generic.394500
CAT-QuickHeal 10.00 2009.09.05 Trojan.Agent.IRC
ClamAV 0.94.1 2009.09.06 -
Comodo 2203 2009.09.06 Backdoor.Win32.Turkojan.~EV
DrWeb 5.0.0.12182 2009.09.06 -
eSafe 7.0.17.0 2009.09.06 Win32.Turkojan.amr
eTrust-Vet 31.6.6721 2009.09.04 Win32/ASuspect.GFJLB
F-Prot 4.5.1.85 2009.09.06 W32/BackdoorX.ACGA
F-Secure 8.0.14470.0 2009.09.06 Backdoor:W32/Turkojan.Z
Fortinet 3.120.0.0 2009.09.06 PossibleThreat
GData 19 2009.09.06 Trojan.Generic.394500
Ikarus T3.1.1.72.0 2009.09.06 Backdoor.Win32.Turkojan.amr
Jiangmin 11.0.800 2009.09.06 -
K7AntiVirus 7.10.837 2009.09.05 Backdoor.Win32.Turkojan
Kaspersky 7.0.0.125 2009.09.06 Backdoor.Win32.Turkojan.amr
McAfee 5733 2009.09.06 BackDoor-CZP.dr
McAfee+Artemis 5733 2009.09.06 BackDoor-CZP.dr
McAfee-GW-Edition 6.8.5 2009.09.06 Trojan.Drop.Age.1530279
Microsoft 1.5005 2009.09.06 Backdoor:Win32/Turkojan.gen!A
NOD32 4401 2009.09.06 probably a variant of Win32/Agent
Norman 6.01.09 2009.09.04 -
nProtect 2009.1.8.0 2009.09.06 Trojan/W32.Agent.1527646
Panda 10.0.2.2 2009.09.06 Bck/Turkojan.J
PCTools 4.4.2.0 2009.09.06 Backdoor.Turkojan!sd6
Prevx 3.0 2009.09.06 High Risk System Back Door
Rising 21.45.14.00 2009.09.01 Backdoor.Agent.fbt
Sophos 4.45.0 2009.09.06 Troj/Turkoj-Gen
Sunbelt 3.2.1858.2 2009.09.06 Trojan.Win32.Generic!BT
Symantec 1.4.4.12 2009.09.06 Backdoor.Turkojan
TheHacker 6.3.4.3.396 2009.09.04 -

TrendMicro 8.950.0.1094 2009.09.05 BKDR_TURKOJAN.AL
VBA32 3.12.10.10 2009.09.05 Backdoor.Win32.Turkojan.amr
ViRobot 2009.9.4.1919 2009.09.04 Backdoor.Win32.Turkojan.1527646
VirusBuster 4.6.5.0 2009.09.06 Backdoor.Turkojan.AAJ
That's gay and why I don't use AVs :DD

hacc - *October 8, 2010, 9:10 pm*

This is why I don't use Turkojan (actually I don't use RATs at all anymore)

misscute - *October 9, 2010, 1:48 pm*

is there any way to make our exe file into web browser

Carb0n F1ber - *October 10, 2010, 7:30 am*

(Oct 9, 2010 01:48 PM)misscute Wrote: [\[CITE\]](#) is there any way to make our exe file into web browser

Could you please re-phrase your question ?

hacc - *October 10, 2010, 8:24 am*

(Oct 9, 2010 01:48 PM)misscute Wrote: [\[CITE\]](#) is there any way to make our exe file into web browser

You can change the icon to the IE logo or Firefox or Chrome.

porney - *December 24, 2010, 7:28 am*

Thanks Carb0n F1ber, I've bin looking for this info. ?