

Forum:[Hack Forums](#)

Thread: [My Crypter + Binder \(Still Beta Need Help with Hexing Stubs\)](#)

xSilent - October 7, 2009, 9:37 pm

Ok, with tutorials I made this crypter and binder in vb6. Now they are detected, but I tried to Hex it and I always screw up. If someone could help me that would be awesome. Well here they are

And I suck at GUI so I don't want to hear how bad it looks

If any of you want to help me then please add me

My yahoo messenger: killerxcrypter

Crypter:

[img]http://i416.photobucket.com/albums/pp241/4thkyutest/pic1.jpg[/img]

Binder:

[img]http://i416.photobucket.com/albums/pp241/4thkyutest/pic2.jpg[/img]

Virus Scans:

Note bstub is for the binder and Stub is for the crypter

File Info

Report generated: 8.10.2009 at 5.34.39 (GMT 1)

Filename: bstub.exe

File size: 20 KB

MD5 Hash: Removed

SHA1 Hash: Removed

Self-Extract Archive: Yes => RarSFX Archive

Binder Detector: Nothing found

Detection rate: 5 on 23

Detections

a-squared - Trojan-Dropper.Win32.VB!IK

Avira AntiVir - -

Avast - -

AVG - -

BitDefender - -

ClamAV - -

Comodo - -

Dr.Web - -

Ewido - -

F-PROT6 - -

Ikarus T3 - Trojan-Dropper.Win32.VB

Kaspersky - HEUR:Trojan.Win32.Generic

McAfee - Generic VB.i trojan
NOD32 v3 - -
Norman - New unknown virus W32/Obfuscated.BQ!genr
Panda - -
QuickHeal - -
Solo Antivirus - -
Sophos - -
TrendMicro - -
VBA32 - -
VirusBuster - -
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

Crypter Stub:

File Info

Report generated: 8.10.2009 at 5.34.39 (GMT 1)
Filename: Stub.exe
File size: 16 KB
MD5 Hash: Removed
SHA1 Hash: Removed
Self-Extract Archive: Nothing found
Binder Detector: Nothing found
Detection rate: 9 on 23

Detections

a-squared - Trojan.Inject!IK
Avira AntiVir - TR/Dropper.Gen
Avast - -
AVG - Dropper.Heliosb.N
BitDefender - Trojan.Dropper.VB.1
ClamAV - -
Comodo - -
Dr.Web - Trojan.PWS.Multi.76
Ewido - -
F-PROT6 - -
Ikarus T3 - Trojan.Inject
Kaspersky - -
McAfee - Generic VB.i trojan
NOD32 v3 - Win32/Injector.WZ
Norman - -
Panda - -
QuickHeal - -
Solo Antivirus - -
Sophos - -
TrendMicro - -
VBA32 - Trojan.VB.Motil
VirusBuster - -
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

Client:

File Info

Report generated: 8.10.2009 at 6.54.39 (GMT 1)
Filename: Client.exe
File size: 52 KB
MD5 Hash: Removed
SHA1 Hash: Removed
Self-Extract Archive: Yes => RarSFX Archive
Binder Detector: Nothing found
Detection rate: 0 on 23

Detections

a-squared - -
Avira AntiVir - -
Avast - -
AVG - -
BitDefender - -
ClamAV - -
Comodo - -
Dr.Web - -
Ewido - -
F-PROT6 - -
Ikarus T3 - -
Kaspersky - -
McAfee - -
NOD32 v3 - -
Norman - -
Panda - -
QuickHeal - -
Solo Antivirus - -
Sophos - -
TrendMicro - -
VBA32 - -
VirusBuster - -
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

[Download Link Here](#)

If anyone can help me Hex the stubs, it would be awesome

I hope you guys like it ?

Binder:

Shapes = Add
Truck = Remove
Drill = Bind

Crypter:

Binoculars = Find
Safe = Crypt

Gizmo - October 8, 2009, 7:32 am

I'm going to test this.

<short>>>>>>>>>>>>>>>>

Crypter is not fud anymore :p And as second, I can't find the binder.

File Info

Report generated: 8.10.2009 at 16.40.44 (GMT 1)
Filename: crypterll.exe
File size: 25 KB
MD5 Hash: db7a3fe0724fd475f7b21f6f428abcba
SHA1 Hash: BB497BC9B90A94DC39ADA0093509895054148575
Self-Extract Archive: Nothing found
Binder Detector: Nothing found
Detection rate: 11 on 23

Detections

a-squared - Trojan.Inject!!K
Avira AntiVir - TR/Crypt.XDR.Gen
Avast - Win32:VB-LTZ [Trj]
AVG - Dropper.Heliosb.N
BitDefender - Trojan.Dropper.VB.1
ClamAV - -
Comodo - -
Dr.Web - Trojan.PWS.Multi.76
Ewido - -
F-PROT6 - -
Ikarus T3 - Trojan.Inject
Kaspersky - -
McAfee - Generic VB.i trojan
NOD32 v3 - Win32/Injector.WZ
Norman - -
Panda - -
QuickHeal - -
Solo Antivirus - -
Sophos - Mal/VB-AB
TrendMicro - -
VBA32 - Trojan.VB.Motil
VirusBuster - -
ZonerAntivirus - -

Scan report generated by
[NoVirusThanks.org](https://www.novirusthanks.org)

xSilent - October 8, 2009, 7:40 am

(Oct 8, 2009 07:32 AM)Gizmo Wrote: [CITE](#) I'm going to test this.

<short>>>>>>>>>>>>>>>>

Crypter is not fud anymore :p And as second, I can't find the binder.

File Info

Report generated: 8.10.2009 at 16.40.44 (GMT 1)

Filename: crypterll.exe

File size: 25 KB

MD5 Hash: db7a3fe0724fd475f7b21f6f428abcba

SHA1 Hash: BB497BC9B90A94DC39ADA0093509895054148575

Self-Extract Archive: Nothing found

Binder Detector: Nothing found

Detection rate: 11 on 23

Detections

a-squared - Trojan.Inject!IK

Avira AntiVir - TR/Crypt.XDR.Gen

Avast - Win32:VB-LTZ [Trj]

AVG - Dropper.Heliosb.N

BitDefender - Trojan.Dropper.VB.1

ClamAV - -

Comodo - -

Dr.Web - Trojan.PWS.Multi.76

Ewido - -

F-PROT6 - -

Ikarus T3 - Trojan.Inject

Kaspersky - -

McAfee - Generic VB.i trojan

NOD32 v3 - Win32/Injector.WZ

Norman - -

Panda - -

QuickHeal - -

Solo Antivirus - -

Sophos - Mal/VB-AB

TrendMicro - -

VBA32 - Trojan.VB.Motil

VirusBuster - -

ZonerAntivirus - -

Scan report generated by
[NoVirusThanks.org](https://www.novirusthanks.org)

I know its not FUD, thats why I need help Hexing the Stubs..I always screw up lol and go to File and Binder

carnagez71 - October 8, 2009, 8:04 am

could u fud my metus bot for free

Gizmo - October 8, 2009, 8:31 am

(Oct 8, 2009 08:04 AM)carnagez71 Wrote: [\[CITE\]](#) could u fud my metus bot for free
Dude, why SPAM here? Read the thread first before posting anything dude.

xSilent - October 8, 2009, 9:11 am

(Oct 8, 2009 08:31 AM)Gizmo Wrote: [\[CITE\]](#) (Oct 8, 2009 08:04 AM)carnagez71 Wrote: [\[CITE\]](#) could u fud my metus bot for free
Dude, why SPAM here? Read the thread first before posting anything dude.
carnage failed lol

xSilent - October 8, 2009, 6:13 pm

Any help with hexing?

Frag_Bag - October 9, 2009, 3:51 pm

Sorry dont know hexing, did you try a video tutorial?

xSilent - October 9, 2009, 10:19 pm

Most of the video tuts, dont deal with crypter stubs, thats why I need help

Ryxa - October 9, 2009, 10:29 pm

What method are you using to hex edit the stub?

xSilent - October 10, 2009, 7:20 am

(Oct 9, 2009 10:29 PM)HaruhiSuzumiya Wrote: [\[CITE\]](#) What method are you using to hex edit the stub?

uh, ok the video tutorial he was filling most of the stub with 00 and I tried doing that, but I screwed up my stub

and I dont understand file splitting

I'm using the HxD hex editor

Ryxa - October 10, 2009, 10:09 am

Well, I don't know about filling it in with zero's, but you're suppose to split the file, and scan then split the infected part, then scan, and so on, until you find the hex that's tagged by the antivirus. It should be something like "52". Just overwrite the 2 numbers with 2 zeros.

xSilent - October 10, 2009, 1:12 pm

(Oct 10, 2009 10:09 AM)HaruhiSuzumiya Wrote: [\[CITE\]](#) Well, I don't know about filling it in with zero's, but you're suppose to split the file, and scan then split the infected part, then scan, and so on, until you find the hex that's tagged by the antivirus. It should be something like "52". Just overwrite the 2 numbers with 2 zeros.

My AV sucks at just scanning files, but what AV do you suggest?

Ryxa - October 10, 2009, 1:12 pm

(Oct 10, 2009 01:12 PM)xKillerxPanther Wrote: [\[CITE\]](#) (Oct 10, 2009 10:09 AM)HaruhiSuzumiya Wrote: [\[CITE\]](#) Well, I don't know about filling it in with zero's, but you're suppose to split the file, and scan then split the infected part, then scan, and so on, until you find the hex that's tagged by the antivirus. It should be something like "52". Just overwrite the 2 numbers with 2 zeros.

My AV sucks at just scanning files, but what AV do you suggest?

Use MultiAV scanner when hexediting.

xSilent - October 10, 2009, 4:07 pm

(Oct 10, 2009 01:12 PM)HaruhiSuzumiya Wrote: [\[CITE\]](#) (Oct 10, 2009 01:12 PM)xKillerxPanther Wrote: [\[CITE\]](#) (Oct 10, 2009 10:09 AM)HaruhiSuzumiya Wrote: [\[CITE\]](#) Well, I don't know about filling it in with zero's, but you're suppose to split the file, and scan then split the infected part, then scan, and so on, until you find the hex that's tagged by the antivirus. It should be something like "52". Just overwrite the 2 numbers with 2 zeros.

My AV sucks at just scanning files, but what AV do you suggest?

Use MultiAV scanner when hexediting.

Do you have a link for a one that works? the one I have cant open files

If you do, thanks

Ryxa - October 10, 2009, 5:24 pm

I believe there's one on HackHound. I used to have it, but not anymore.

xSilent - October 10, 2009, 8:16 pm

(Oct 10, 2009 05:24 PM)HaruhiSuzumiya Wrote: [\[CITE\]](#) I believe there's one on HackHound. I used to have it, but not anymore.

yeah, that one is screwed up lol

xSilent - October 12, 2009, 9:01 am

I got it to 5/23, but I screwed the stub up

xSilent - October 13, 2009, 11:29 am

I'm updating the program with a well update button, so when I do fully release it, once I re-FUD the public version you all can check for updates

msuper28 - October 13, 2009, 11:53 am

Did you try to hex edit the stub? i have edited my stub for the first time and was 9/23 then 5/23 because i have added 00's byte to not useful things...

xSilent - October 13, 2009, 12:22 pm

(Oct 13, 2009 11:53 AM)msuper28 Wrote: [\[CITE\]](#) Did you try to hex edit the stub? i have edited my stub for the first time and was 9/23 then 5/23 because i have added 00's byte to not useful things...

I got it to 5/23, but I screwed the stub up

newbie223 - October 14, 2009, 8:48 pm

hey bro can u teach me make crypter A:D

xSilent - October 14, 2009, 9:18 pm

(Oct 14, 2009 08:48 PM)newbie223 Wrote: [\[CITE\]](#) hey bro can u teach me make crypter A:D

I guess, but i suck and someone still needs to help me with the stubs

LittleFighter™ - October 14, 2009, 9:27 pm

it crypted the file but file is not opening

xSilent - October 14, 2009, 9:32 pm

(Oct 14, 2009 09:27 PM)LittleFighter Wrote: [\[CITE\]](#) it crypted the file but file is not opening what did you try and crypt?

LittleFighter™ - October 14, 2009, 9:33 pm

(Oct 14, 2009 09:32 PM)xKillerxPanther Wrote: [\[CITE\]](#) what did you try and crypt?setup of adramax

xSilent - October 14, 2009, 9:49 pm

(Oct 14, 2009 09:33 PM)LittleFighter Wrote: [\[CITE\]](#) setup of adramax
I havent tested it with keyloggers yet, No one test it until I get it FUD

newbie223 - October 15, 2009, 9:04 am

killer panther your crypter is scantime or runtime? atm im doing scantime using rc4 i was thinking is there a method using md5?

xSilent - October 15, 2009, 9:44 am

(Oct 15, 2009 09:04 AM)newbie223 Wrote: [\[CITE\]](#) killer panther your crypter is scantime or runtime?
atm im doing scantime using rc4 i was thinking is there a method using md5?
Its runtime and if you try and crypt something thats clean, my stub will kill it

newbie223 - October 15, 2009, 10:23 am

lol mine sharing what should i learn to make runtime crypter?

bryan54 - October 15, 2009, 10:33 am

If you want to make your Stub more UD:

- Add new Icon
- Add Form, Module.
- Add Junk Code and Junk Function
- Change Version Info, Comment, Copyright, etc...
- Use Source Undetector for Crypt all the Strings of your Stub

Now you are more UD or maybe Totally FUD!

xSilent - October 15, 2009, 3:48 pm

(Oct 15, 2009 10:33 AM)bryan54 Wrote: [\[CITE\]](#) If you want to make your Stub more UD:

- Add new Icon
- Add Form, Module.
- Add Junk Code and Junk Function
- Change Version Info, Comment, Copyright, etc...
- Use Source Undetector for Crypt all the Strings of your Stub

Now you are more UD or maybe Totally FUD!
where would i find a Source Undetector? UPDATE!

Binder Stub is Now 3/23 and Crypter Stub is 8/23

It is almost ready for release

And thanks to bryan54 for suggestions ? I tip my hat to you

I need someone good with GUI, so PM me if you are

xSilent - October 18, 2009, 6:34 pm

Hex Editing in Progress

Binder 3/24

Crypter 7/24

Sikandar - October 18, 2009, 7:33 pm

add some more modules and try the callAPI method.....then to bypass avira..change its icon manually.....i think kaspersky has something to do with split method so drop by in hackhound and find cobain's split alternative.....nod32 is hard to bypass...try using avfuckers for it...

i RaT YoU - October 18, 2009, 8:46 pm

did this work for anyone???

Therion - October 19, 2009, 3:18 am

There are people who think, randomly adding or changing values in hex will help.

It will not and also wont work because what's in hex, the opcodes etc. they are all quite definite - many calls are related to memory addresses etc which are calculated so if you change them your program will break 100%.

There are of course sections you can overwrite...

xSilent - October 19, 2009, 3:02 pm

ok, thanks and no one test this crypter yet, I'll ask for beta testers when I'm ready (currently testing with RATS, botnets etc)

GGGuardian - October 19, 2009, 9:55 pm

Just split the Stub into halves and keep splitting till you find the detected thread in the stub that wil make it UD again.

xSilent - October 20, 2009, 1:31 am

UPDATE

I changed the GUI completely from the first design (I didn't really care about the binder design)

Still working on the stubs

crypter 7/24

binder 3/24

with school, I don't have that much time to work on it so bare with me

Changed GUI

[IMG]<http://i416.photobucket.com/albums/pp241/4thkyutest/cap1.jpg>[IMG]

[IMG]<http://i416.photobucket.com/albums/pp241/4thkyutest/cap2.jpg>[IMG]

? I hope I can have this done within the week

Bare with me guys and I suck a GUI so comment about the new look ?

RUS7Y - October 20, 2009, 3:22 am

Change the name of all the strings it will surely help u

\$weet - October 30, 2009, 11:12 pm

check on hackhound.net man, there are plenty of tut's there which will help you with hexing :P

Pentoxide - October 31, 2009, 2:25 am

Ahhh, nice program, will you PM Me when you've done? :) lol.

Need a crypter asap :(

killerguy - October 31, 2009, 2:36 am

this loser has been posting this in every forums hackhound.org hackhound.net and now hackforums just go to hell with your stupid crypter+binder coz you are retarded

Cry0quak3 - October 31, 2009, 3:00 am

Looks like a good crypter, I hope you get help for the hexing!

iDarky - October 31, 2009, 3:05 am

(Oct 10, 2009 04:07 PM)xKillerxPanther Wrote: [\[CITE\]](#) My AV sucks at just scanning files, but what AV do you suggest?

Use MultiAV scanner when hexediting.

[/quote]

Do you have a link for a one that works? the one I have cant open files

If you do, thanks

[/quote]

Cant u use novirusthanks?

xSilent - October 31, 2009, 2:21 pm

GUI Changed Again and it Will not let me update the title

[IMG]http://i416.photobucket.com/albums/pp241/4thkyutest/screen1.jpg[/IMG]

[IMG]http://i416.photobucket.com/albums/pp241/4thkyutest/snp3.jpg[/IMG]

Hexing in Progress [Most AV's tagged parts I need so I may have to find another way]

CaLLMeReaacT - November 24, 2009, 10:23 am

<p><div style="font-family:Arial,sans-serif;font-size:11px;">Sign by Danasoft - Get Your Free Sign</p></div>

assihodensack - January 15, 2010, 7:38 am

good work, man

does it still work?

csebharat - March 3, 2010, 12:30 pm

is there no 100% crypters?

Mega-Scorpion - March 3, 2010, 12:35 pm

great

thanks

?MrRoot - *December 18, 2013, 11:08 am*

If you are still active, I can help you making it fud, Skype: les.de

iMalware - *December 18, 2013, 1:54 pm*

Wow. you just gravedigged a thread from 2009...