

Forum:[Hack Forums](#)

Thread: [\[Possible Warning\] Ownz Crypter](#)

The Janitor - September 21, 2010, 7:45 am

Hi hackforums,

Please take a good look at this

Ok so because of security reasons, i ran the borlo.exe in anubis, this is the report:

Spoiler ([Click to View](#))Quote:1. General Information

- Information about Anubis' invocation

Time needed: 21 s

Report created: 09/21/10, 14:34:17 UTC

Termination reason: All tracked processes have exited

Program version: 1.74.3110

- Popups

Process	Window Name	Window Text	Screenshot	Number of Displayed Times
csrss.exe	borlo.exe - Application Error	OK The application failed to initialize properly (0xc0000135). Click on OK to terminate the application.		1

2. borlo.exe

- General information about this executable

Analysis Reason: Primary Analysis Subject

Filename: borlo.exe

MD5: 3dad36ac2a27907de5b72e02c3d59648

SHA-1: 16e620bbbc9bf0a9a32298368f22fa66c3fd4e13

File Size: 25088 Bytes

Process-status at analysis end: dead

Exit Code: -1073741515

- Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900	0x000AF000

2.a) borlo.exe - Other Activities

- Windows SEH exceptions:

Description	Times
Exception 0xc0000135 at 0x7c96478e	

The DLL File it ran, i checked it . I found this on the internet about Ntdll.dll

Spoiler ([Click to View](#))Quote:Description: File ntdll.exe is located in the folder

C:\Windows\System32. Known file sizes on Windows XP are 138,760 bytes (75% of all occurrence), 216,064 bytes, 241,664 bytes.

The program has a visible window. There is no information about the maker of the file. The file is

not a Windows system file. The application is loaded during the Windows boot process (see Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run). Therefore the technical security rating is 42% dangerous, however also read the users reviews.

Recommended: Identify ntdll.exe related errors

External information from Paul Collins:

"ntdll" definitely not required. Added by the BIONET.404 TROJAN!

Important: Some malware camouflage themselves as ntdll.exe, particularly if they are located in c:\windows or c:\windows\system32 folder. Thus check the ntdll.exe process on your pc whether it is pest. We recommend Security Task Manager for verifying your computer's security. It is one of the Top Download Picks of 2005 of The Washington Post and PC World.

Than i scanned the crypter, same results.

Spoiler ([Click to View](#)) Quote:Analysis Report for Crypter.exe

Comment on this report

Summary:

No threats could be detected by Anubis. This does not imply that execution of this executable is safe.

Table of Contents

expand all collapse all

General information

Crypter.ex.exe

1. General Information

- Information about Anubis' invocation

Time needed: 45 s

Report created: 09/21/10, 14:41:43 UTC

Termination reason: All tracked processes have exited

Program version: 1.74.3110

- Popups

Process	Window Name	Window Text	Screenshot	Number of Displayed Times
---------	-------------	-------------	------------	---------------------------

csrss.exe	Crypter.ex.exe	- Application Error	OK	The application failed to initialize properly (0xc0000135). Click on OK to terminate the application.	1
-----------	----------------	---------------------	----	---	---

2. Crypter.ex.exe

- General information about this executable

Analysis Reason: Primary Analysis Subject

Filename: Crypter.ex.exe

MD5: fd8653759dff9f347ca26d04281dcf1a

SHA-1: 5b105780d02d2304bd0de03264451f285cc61c5a

File Size: 377856 Bytes

Process-status at analysis end: dead

Exit Code: -1073741515

- Load-time DLLs

Module Name Base Address Size
C:\WINDOWS\system32\ntdll.dll 0x7C900 0x000AF000

2.a) Crypter.exe - Other Activities

- Windows SEH exceptions:
Description Times
Exception 0xc0000135 at 0x7c96478e 1

I found the

Description Times
Exception 0xc0000135 at 0x7c96478e 1

Odd so i researched it.

It is possible it is an anti anubis.

Now tell me why does the crypter+the Borlo have an anti-anubis build in?

ALSO. My firewall said that the crypter is trying to act like a server and accept incoming connections, It was also trying to do something with .net error thing. So yeah thats what i found about it . Proof:

Spoiler ([Click to View](#)) [IMG]http://i56.[censored].com/nxqd01.jpg[/IMG]

Novirusthanks scans:

Borlo.exe
Spoiler ([Click to View](#))
File Info

Report date: 2010-09-20 22:43:58 (GMT 1)
File name: borlo-exe
File size: 25088 bytes
MD5 Hash: 3dad36ac2a27907de5b72e02c3d59648
SHA1 Hash: 16e620bbbc9bf0a9a32298368f22fa66c3fd4e13
Detection rate: 1 on 16 (6%)
Status: INFECTED

Detections

a-squared -
Avast -
AVG -
Avira AntiVir - TR/Dropper.Gen
BitDefender -
ClamAV -
Comodo -
Dr.Web -
F-PROT6 -
Ikarus T3 -

Kaspersky -
NOD32 -
Panda -
TrendMicro -
VBA32 -
VirusBuster -

Scan report generated by
NoVirusThanks.org

Now this doesnt mean ANYTHING , it just means that if you crypt its detected by avira, so no problems about this :]

Crypter:

Spoiler ([Click to View](#))
File Info

Report date: 2010-09-20 23:03:08 (GMT 1)
File name: crypter-exe
File size: 377856 bytes
MD5 Hash: fd8653759dff9f347ca26d04281dcf1a
SHA1 Hash: 5b105780d02d2304bd0de03264451f285cc61c5a
Detection rate: 0 on 16 (0%)
Status: CLEAN

Detections

a-squared -
Avast -
AVG -
Avira AntiVir -
BitDefender -
ClamAV -
Comodo -
Dr.Web -
F-PROT6 -
Ikarus T3 -
Kaspersky -
NOD32 -
Panda -
TrendMicro -
VBA32 -
VirusBuster -

Scan report generated by
NoVirusThanks.org

DLL File:

Spoiler ([Click to View](#))

File Info

Report date: 2010-09-17 21:31:13 (GMT 1)

File name: devcomponents-dotnetbar2-dll

File size: 3489792 bytes

MD5 Hash: 8b081fe5490845a366094324b45542ea

SHA1 Hash: 6de3a27289954c602d237b7fa6099b8e4bf3f9d1

Detection rate: 0 on 16 (0%)

Status: CLEAN

Detections

a-squared -

Avast -

AVG -

Avira AntiVir -

BitDefender -

ClamAV -

Comodo -

Dr.Web -

F-PROT6 -

Ikarus T3 -

Kaspersky -

NOD32 -

Panda -

TrendMicro -

VBA32 -

VirusBuster -

Scan report generated by

NoVirusThanks.org

Explain it to me :]

phillybiker1022 - September 21, 2010, 8:15 am

Quote:Description: File ntdll.exe is located in the folder C:\Windows\System32. Known file sizes on Windows XP are 138,760 bytes (75% of all occurrence), 216,064 bytes, 241,664 bytes.

The program has a visible window. There is no information about the maker of the file. The file is not a Windows system file. The application is loaded during the Windows boot process (see Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run). Therefore the technical security rating is 42% dangerous, however also read the users reviews.

Recommended: Identify ntdll.exe related errors

External information from Paul Collins:

"ntdll" definitely not required. Added by the BIONET.404 TROJAN!

Important: Some malware camouflage themselves as ntdll.exe, particularly if they are located in c:\windows or c:\windows\system32 folder. Thus check the ntdll.exe process on your pc whether it is pest. We recommend Security Task Manager for verifying your computer's security. It is one of the Top Download Picks of 2005 of The Washington Post and PC World.

i think thats definitely fishy, no offense to the person who made the crypter but that raises a lot of eyebrows. :-\ i'm going to run the crypter through a few programs and get back to this thread! :)

The Janitor - September 21, 2010, 8:18 am

(Sep 21, 2010 08:15 AM)phillybiker1022 Wrote: [\[CITE\]](#) i think thats definitely fishy, no offense to the person who made the crypter but that raises a lot of eyebrows. :-\ i'm going to run the crypter through a few programs and get back to this thread! :)

It's not just that theres more actually,

Description Times

Exception 0xc0000135 at 0x7c96478e 1

Sometimes is used for Anti-Anubis, it was found ON The crypter and the stub.

jonny5252 - September 21, 2010, 8:25 am

The netdll.dll is used by different Games and comes with Windows.

If you speak German you can read this

<http://forum.chip.de/windows-alte-versionen/ntdll-dll-ersetzen-520166.html>

The Janitor - September 21, 2010, 8:43 am

(Sep 21, 2010 08:25 AM)jonny5252 Wrote: [\[CITE\]](#) The netdll.dll is used by different Games and comes with Windows.

If you speak German you can read this

<http://forum.chip.de/windows-alte-versionen/ntdll-dll-ersetzen-520166.html>

Hi Johnny,

Even if its used for that (wich it isnt in this case) why would a crypter execute it? :] As you can see in my post, it can be used as malware to .

Kind regards

Gtacllick

jonny5252 - September 21, 2010, 9:01 am

I dont know.

I only wanted to say that the part Spoiler [\(Click to View\)](#) The program has a visible window. There is no information about the maker of the file. The file is not a Windows system file. wrong is.

The Janitor - September 21, 2010, 9:11 am

Hi Johnny,

As i said i looked it up on the internet, on a security site. They might say that the CUSTOME one isn't made by windows :]

Kind Regards, Gtacllick

Kotei - September 21, 2010, 9:51 am

(Sep 21, 2010 08:18 AM)gtacllick Wrote: [\[CITE\]](#) It's not just that theres more actually,

Description Times

Exception 0xc0000135 at 0x7c96478e 1

Sometimes is used for Anti-Anubis, it was found ON The crypter and the stub.

Anti-Anubis doesn't work as Anubis can't run .Net files.

So no anti-anubis was not found.

Fallenour - September 21, 2010, 9:57 am

its false positives. starts on boot up, kinda fishy, avira says its a trojan, but its a crypter, gonna say that. all in all, your into blackhat tools, and free ones at that, your gonna get good and bad ones, if you dont trust it or its source, trash it.

Galaxy Wave - September 21, 2010, 10:41 am

kind of fishy to be honest nice find

c6p0 - September 21, 2010, 10:43 am

lol its loopback for antidebugger !

my crypter its clean and my borlo avira detected the runpe .

the source crypter its protected ...

reflector dont view my source,whats problem with my n00b protect ?

you dont copy this ?

phillybiker1022 - September 21, 2010, 11:02 am

(Sep 21, 2010 10:43 AM)c6p0 Wrote: [\[CITE\]](#) lol its loopback for antidebugger !

my crypter its clean and my borlo avira detected the runpe .

the source crypter its protected ...

reflector dont view my source,whats problem with my n00b protect ?

you dont copy this ?

after looking at the crypter for a while, i'm going to have to agree with its maker. i was a bit skeptical at first (but that has nothing to do with c6po.. just in general of a lot of the users on here) so i looked into it and i dont think it is anything to thread over. :)

The Janitor - September 21, 2010, 12:42 pm

Hmm it might not, but it is possible,

At his update 1.3 he "accidently" uploaded a rat instead of his borlo, my firewall tripped and blocked it, i can find the post somewhere just a sec...

Ah here we go, the update of 1.3 with his "mistake" now i might be crazy but someone doesnt "accidently" upload a rat instead of a stub :]

(Sep 20, 2010 01:54 AM)gtaclick Wrote: [\[CITE\]](#) Lol you trying to infect us? With your rat ? Someone run stub in sandbox btw edit password! I cant effig crack

(Sep 20, 2010 01:32 AM)gtaclick Wrote: [\[CITE\]](#) Hmm, Hitman Pro Says the stub is a . Cybergate Backdoor.. No good.

Someone can run it in sandbox? XD (Sep 20, 2010 01:51 AM)c6p0 Wrote: [\[CITE\]](#) ok sorry wrong borlo !

redownload this and try !

forget to add write ressource in memory sorry !

thanks for feedback !

c6p0 - September 21, 2010, 1:06 pm

send borlo who do not walk I'm wrong!

I have 6 Borlo created so sometimes I'm wrong.

I do not answer to you in the post!.

and I did not answer a hitman either!

has nothing to do with a rat? .

but that tells you?

whats problem you have ? my loopback anti debugger or this old post with my wrong borlo ?

you sell crypt here ?

The Janitor - September 22, 2010, 6:06 am

LOOK:

As i said my firewall tripped because the crypter was trying to act like a server and accept incoming stuff, also the DLL it loads can be used as malware, so its possible its a virus. in version 1.3 YOU "accidentally" uploaded a RAT Instead of a borlo.exe and named it borlo.exe. NOW Why would you make 6 borlo wherefrom 1 is a rat! Please read the proof i posted

Jeff. - September 22, 2010, 6:15 am

I have to agree with the maker, sorry.

Anubis scan is because Anubis doesn't support .NET because I get the same error with all my applications so that's not evidence.

The maker has full right to encrypt his source, so I don't see the point is this warning anymore.

Even though he made one mistake we are on 1.5 now which is probably working great.

The Janitor - September 22, 2010, 6:22 am

Ok than, if one more person with over 500 posts says it's clean, i'll apologize to c6 and close the thread

axis10101 - September 22, 2010, 6:22 am

Yea me too, gtaclick download visual basic and make a program, that does nothing more than open a message box, then upload it to anubis... You will get the same result, DLL included.

There is no evidence he even uploaded a RAT, he has already explained that his reply of "sorry uploaded the wrong borlo" was not in response to the RAT comment.

I'm not saying who is right and who is wrong, but taking away your DLL point and more than likely the RAT point too, all you are left with is your firewall acting up, so until you can post some better proof than quoting random posts, I have to side with c6p0 on this.

The Janitor - September 22, 2010, 6:32 am

Ok than, i will look for more info , maybe reinstalling my firewall and than reacting what i did might come up with something :], if not ill close it

Jeff. - September 22, 2010, 6:33 am

COMODO Firewall is my advise and screen the outgoing connections for evidence.

The Janitor - September 22, 2010, 7:05 am

K then here we go:

[IMG][http://i56.\[censored\].com/nxqd01.jpg](http://i56.[censored].com/nxqd01.jpg)[/IMG]

I pressed block.

Translation:

Own'z Is trying to act like a server and accept incoming connections

If you want this program to accept incoming connections press 'Accept'. If not press 'Block' to not allow them

L4TINOK3D - September 22, 2010, 7:19 am

thank you very very very very much !!

The Janitor - September 22, 2010, 7:21 am

No problem :) , i have been infected several times, and just want to help you guys with keep being protected :]

ovelaye - September 22, 2010, 8:01 am

I have used this crypter sence the beginning and followed the updates...never had any prrobs or worries about it being a troj.. possible reasons of it acting like a server might be he might be working on an auto update feature for the stubs or future hwid for protection..

The Janitor - September 22, 2010, 8:06 am

I didn't find anything about an auto-update, anything i can think of is a RAT, keylogger, or a Stealer. There is no auto-updater included in the Crypter ;]

SIM-307931 - September 22, 2010, 8:20 am

Well I used version 1.0, 1.1 and 1.5 gonna test if I have anything suspicious in msconfig...

phillybiker1022 - September 22, 2010, 8:40 am

wait, if you didnt get a popup message like that through another program... how would you advise to stay protected? do you think i have a possibility of being infected?

The Janitor - September 22, 2010, 8:50 am

You might , scan your pc with malwarebytes anti malware , à up to date AV , Ans go to cmd and type netstat -b take à screen and upload it here

Jeff. - September 22, 2010, 9:49 am

I'm dutch myself but as for your firewall I don't even know your firewall and you can't be so sure that this is a RAT run it in a VM and check in your Firewall for incoming connections and port numbers you have to accept it to check it out but be more safe in a VM.

There is confirmation of high member that this is fully working without a problem so I still don't see the problem the source is encrypted against leecher and there are so many reasons that the crypter needs a connection.

The Janitor - September 22, 2010, 12:07 pm

(Sep 22, 2010 09:49 AM)Unflamed Wrote: [\[CITE\]](#) I'm dutch myself but as for your firewall I don't even know your firewall and you can't be so sure that this is a RAT run it in a VM and check in your Firewall for incoming connections and port numbers you have to accept it to check it out but be more safe in a VM.

There is confirmation of high member that this is fully working without a problem so I still don't see the problem the source is encrypted against leecher and there are so many reasons that the crypter needs a connection.

Because the source is protected against leechers doesnt mean it has to act like a server and accept incoming connections, even if it would like to send something out it would use OUTgoing connections, not incoming. Rat's send incoming, so do Keyloggers. Therefore its one of those :) Oh

btw here is link to my firewall:

<http://www.pctools.com/en/firewall/>

:']

The Janitor - *October 7, 2010, 9:09 am*

NOW JUST BECAUSE I DID THIS DOESNT MEAN YOU DONT HAVE TO USE IT, c6p0 IS A GREAT CODER AND RESPECTED BY ME, I JUST FOUND SOMETHING SUSPICIOUS

Novirusthanks:

Crypter:

Spoiler ([Click to View](#))

File Info

Report date: 2010-10-07 00:26:22 (GMT 1)

File name: crypter-exe

File size: 1976320 bytes

MD5 Hash: 6baada22ad7cd657643f8cf5420ce3f3

SHA1 Hash: 21d7a8f43260953ae884012a4f9f0ae9228f1be9

Detection rate: 0 on 16 (0%)

Status: CLEAN

Detections

a-squared -

Avast -

AVG -

Avira AntiVir -

BitDefender -

ClamAV -

Comodo -

Dr.Web -

F-PROT6 -

Ikarus T3 -

Kaspersky -

NOD32 -

Panda -

TrendMicro -

VBA32 -

VirusBuster -

Scan report generated by

NoVirusThanks.org

Borlo:

Spoiler ([Click to View](#))

File Info

Report date: 2010-10-07 17:47:00 (GMT 1)

File name: borlo-exe

File size: 34304 bytes
MD5 Hash: 79cc50cd7f2ed21649914d645f67419a
SHA1 Hash: 16b3bf37146dad817b947e312f25d0d2c14fbd81
Detection rate: 1 on 16 (6%)
Status: INFECTED

Detections

a-squared -
Avast -
AVG -
Avira AntiVir -
BitDefender -
ClamAV -
Comodo -
Dr.Web -
F-PROT6 - W32/MSIL_Troj.C.gen!Eldorado
Ikarus T3 -
Kaspersky -
NOD32 -
Panda -
TrendMicro -
VBA32 -
VirusBuster -

Scan report generated by
NoVirusThanks.org

ResHacker:

Spoiler ([Click to View](#))
File Info

Report date: 2010-10-07 17:48:48 (GMT 1)
File name: res-exe
File size: 334336 bytes
MD5 Hash: 4a1801a3a0e1f74cdf80193e3ef28156
SHA1 Hash: cebe9718b117610d69f0da941893be5fc0fa766e
Detection rate: 0 on 16 (0%)
Status: CLEAN

Detections

a-squared -
Avast -
AVG -
Avira AntiVir -
BitDefender -
ClamAV -
Comodo -
Dr.Web -
F-PROT6 -

Ikarus T3 -
Kaspersky -
NOD32 -
Panda -
TrendMicro -
VBA32 -
VirusBuster -

Scan report generated by
NoVirusThanks.org

Anubis Scans:

Crypter:
Spoiler ([Click to View](#))
Analysis Report for Crypter.exe

Comment on this report

Summary:

No threats could be detected by Anubis. This does not imply that execution of this executable is safe.

Table of Contents

expand all collapse all

General information
Crypter.ex.exe

1. General Information

- Information about Anubis' invocation

Time needed: 29 s

Report created: 10/07/10, 15:48:10 UTC

Termination reason: All tracked processes have exited

Program version: 1.74.3195

- Popups

Process	Window Name	Window Text	Screenshot	Number of Displayed Times
---------	-------------	-------------	------------	---------------------------

csrss.exe	Crypter.ex.exe	- Application Error	OK	The application failed to initialize properly (0xc0000135). Click on OK to terminate the application.
-----------	----------------	---------------------	----	---

1

2. Crypter.ex.exe

- General information about this executable

Analysis Reason: Primary Analysis Subject

Filename: Crypter.ex.exe

MD5: 6baada22ad7cd657643f8cf5420ce3f3

SHA-1: 21d7a8f43260953ae884012a4f9f0ae9228f1be9

File Size: 1976320 Bytes

Process-status at analysis end: dead

Exit Code: -1073741515

- Load-time DLLs

Module Name	Base Address	Size
-------------	--------------	------

C:\WINDOWS\system32\ntdll.dll	0x7C900	0x000AF000
-------------------------------	---------	------------

2.a) Crypter.ex.exe - Other Activities

- Windows SEH exceptions:

Description	Times
-------------	-------

Exception 0xc0000135 at 0x7c96478e	1
------------------------------------	---

Borlo.exe:

Spoiler ([Click to View](#))

Analysis Report for borlo.exe

Comment on this report

Summary:

No threats could be detected by Anubis. This does not imply that execution of this executable is safe.

Table of Contents

expand all collapse all

General information

borlo.exe

borlo.exe

Primary Analysis Subject

General Information

a) Other Activities

1. General Information

- Information about Anubis' invocation

Time needed: 25 s

Report created: 10/07/10, 15:50:56 UTC

Termination reason: All tracked processes have exited

Program version: 1.74.3195

- Popups

Process	Window Name	Window Text	Screenshot	Number of Displayed Times
---------	-------------	-------------	------------	---------------------------

csrss.exe	borlo.exe	- Application Error	OK	The application failed to initialize properly (0xc0000135). Click on OK to terminate the application.
-----------	-----------	---------------------	----	---

2. borlo.exe

- General information about this executable

Analysis Reason: Primary Analysis Subject

Filename: borlo.exe

MD5: 79cc50cd7f2ed21649914d645f67419a
SHA-1: 16b3bf37146dad817b947e312f25d0d2c14fbd81
File Size: 34304 Bytes
Process-status at analysis end: dead
Exit Code: -1073741515

- Load-time DLLs

Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900	0x000AF000

2.a) borlo.exe - Other Activities

- Windows SEH exceptions:

Description	Times
Exception 0xc0000135 at 0x7c96478e	1

Reshacker:

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

Anubis - Analysis Report

Analysis Report for Res.exe

Comment on this report

Summary:

Description Risk

Performs Registry Activities: The executable reads and modifies registry values. It may also create and monitor registry keys.

Table of Contents

expand all collapse all

General information

Res.exe

C:\Res.exe

Primary Analysis Subject

General Information

a) Registry Activities

b) File Activities

1. General Information

- Information about Anubis' invocation

Time needed: 241 s

Report created: 10/07/10, 15:59:03 UTC

Termination reason: Timeout

Program version: 1.74.3195

2. Res.exe

- General information about this executable

Analysis Reason: Primary Analysis Subject

Filename: Res.exe
MD5: 4a1801a3a0e1f74cdf80193e3ef28156
SHA-1: cebe9718b117610d69f0da941893be5fc0fa766e
File Size: 334336 Bytes
Command Line: "C:\Res.exe"
Process-status at analysis end: alive
Exit Code: 0

- Load-time DLLs

Module Name Base Address Size

C:\WINDOWS\system32\ntdll.dll	0x7C900	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800	0x000F6000
C:\WINDOWS\system32\advapi32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\comdlg32.dll	0x763B0000	0x00049000
C:\WINDOWS\system32\SHELL32.dll	0x7C9C0000	0x00817000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\oleaut32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\version.dll	0x77C00	0x00008000
C:\WINDOWS\system32\winmm.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\winpool.drv	0x7300	0x00026000

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll 0x773D0000 0x00103000

- Run-time DLLs

Module Name Base Address Size

C:\WINDOWS\system32\RICHED32.DLL	0x732E0000	0x00005000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\RICHED20.DLL	0x74E30000	0x0006D000
C:\WINDOWS\system32\IMAGEHLP.DLL	0x76C90000	0x00028000

- SigBuster Output

UPX All_Versions SN:1634

2.a) Res.exe - Registry Activities

- Registry Values Read:

Key Name Value Times

HKLM\SOFTWARE\Microsoft\CTF\SystemShared\	CUAS	0	1
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	CriticalSectionTimeout	2592000	1
HKLM\SYSTEM\Setup	SystemSetupInProgress	0	1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	Arial Baltic,186	Arial,186	4
HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	Arial CE,238		4
HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	Arial CYR,204	Arial,204	4

HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Arial Greek,161 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Arial TUR,162 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Courier New Baltic,186 4

 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Courier New CE,238
 Courier New,238 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Courier New CYR,204
 Courier New,204 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Courier New Greek,161
 Courier New,161 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Courier New TUR,162
 Courier New,162 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Helv MS Sans Serif 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Helvetica Arial 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes MS Shell Dlg Microsoft
 Sans Serif 2
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes MS Shell Dlg 2 Tahoma 4

 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Times Times New Roman
 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Times New Roman
 Baltic,186 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Times New Roman
 CE,238 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Times New Roman
 CYR,204 Times New Roman,204 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Times New Roman
 Greek,161 Times New Roman,161 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Times New Roman
 TUR,162 4
 HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes Tms Rmn 4
 HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers TransparentEnabled 1 1
 HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm
 wheel 1 1
 HKLM\System\CurrentControlSet\Control\Terminal Server TSUserEnabled 0 1
 HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle Language
 Hotkey 1 2
 HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle Layout Hotkey 2
 2

2.b) Res.exe - File Activities

- Files Created:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\rh_2.tmp

- Files Read:

C:\WINDOWS\win.ini

- Device Control Communication:

File Control Code Times

\Device\KsecDD 0x00390008 8

- Memory Mapped Files:

File Name

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\RICHED20.DLL
C:\WINDOWS\system32\RICHED32.DLL
C:\WINDOWS\system32\SHELL32.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\winmm.dll
C:\WINDOWS\system32\winspool.drv

International Secure Systems Lab
Vienna University of Technology, Eurecom France, UC Santa Barbara
Contact: anubis@iseclab.org

Now starting the program:

[IMG]<http://img227.imageshack.us/img227/654/proofedyproof.jpg>[IMG]

Uploaded with ImageShack.us

Translation:

Crypter.exe Could not be recognized and is trying to connect with the internet. If this is one of your daily used programs you can accept it.

Port 80 , could be the following things:

RAT
Keylogger

OR Because of his Log - In Thing

Could be safe, not sure tho

Use at own risk

U MAD CUZ I RUN XBL? - October 7, 2010, 9:10 am

weird i was wondering why avira detected that shit i only went on hf and minecraft and brazzers since i reformatted. And it picked up tons of shit.

c6p0 - October 7, 2010, 9:11 am

eh bro you forget to scann my multi downloader this use *beta
vbc.exe for compile .

and next update reactivate "make single viewable applications"
for you detect my loopback suspicious .
lol

The Janitor - October 7, 2010, 9:23 am

Im not gonna open or login to the file because of this,

People please be warned :]

XxTheGenocidexX - October 7, 2010, 10:11 am

tbh doesnt it want to make a connection for checking for "updates" becuase that is the new future of the crypt of c6p0

c6p0 - October 7, 2010, 10:16 am

he has reason to worry you never know!

the best go to "white hat" or member to "HJT team" send my crypter .

is already good but your better than a 2 times

Synurgy - October 7, 2010, 10:18 am

(Oct 7, 2010 10:16 AM)c6p0 Wrote: [\[CITE\]](#) he has reason to worry you never know!

the best go to "white hat" or member to "HJT team" send my crypter .

is already good but your better than a 2 times

Go learn english...

Damn your typing is annoying as fuck.

The Janitor - October 7, 2010, 10:28 am

(Oct 7, 2010 10:18 AM)Synurgy Wrote: [\[CITE\]](#) Go learn english...

Damn your typing is annoying as fuck.

Dont flame him for his english,

He is a great coder and contributes to the community.

Also he is still learning english

xene - October 28, 2010, 4:28 am

I downloaded and used the second newest version uptodate, also noticed connection tries, first i declined it on NetLimiter (which is best damn firewall since you do all the work) and it didnt open, so i allowed it and it worked. Not a biggy thou, but after i rebooted sometime ago, my HDD started acting up like hell. First it "freezed" on desktop and loading my quick launch icons took around 20-30seconds each, wierd. Then i got bored and hardbooted my pc and then i got this message in bios = "ntdll cannot be found" and system froze. After few reboots i gotto windows load screen, and froze there. I formated my HDD and did clean install, working like charm. Havent opened crypter in my USB stick after that and after this thread, i wont. I recommend crypting you servers in VM...

Xene out

The Janitor - October 28, 2010, 6:14 am

Thanks for contributing :]

I kind of became less active, will rescan the files when i got time ^^

Kind regards

Gtaclck

JackSkellington - January 4, 2011, 4:19 pm

Gta you have good reason to worry cause i used his new 1.4 and it infected me im going to send

you a screen and a pm because soo as i open the crypter my computer been trying to make outside connections and as for people defending him i dont trust them and as for another thing when i used black shades it detecd the crypter please email me ill put it in the pm

Dawncore - January 4, 2011, 6:11 pm

But isn't borlo the stub and if the stub isn't FUD it is going to get detected ?

Existonce - January 6, 2011, 12:16 am

(Jan 4, 2011 05:19 PM)kenkilla Wrote: [\[CITE\]](#) Gta you have good reason to worry cause i used his new 1.4 and it infected me im going to send you a screen and a pm because soo as i open the crypter my computer been trying to make outside connections and as for people defending him i dont trust them and as for another thing when i used black shades it detecd the crypter please email me ill put it in the pm

hahha, i tried the crypter. lots of problems.. well use another pc to run the crypter. that's what i did =PP and when i talked to him. seem like he wanted me to use my main pc to use it..

egabell1 - January 6, 2011, 6:29 am

This seems suspicious. What if I've used the crypter before?

I don't seem to got anything weird in msconfig, Eset Nod32 and Malwarebytes' hasn't found anything yet.

Anything I could do?

Thanks in advance!

-Egabell1

Dawncore - January 6, 2011, 7:31 am

OMFG, This is not infected he scanned 'BORLO' and that is the stub,

The stub was not FUD so it gets fucking detected

The Crypter itself:

The Stub (Borlo):

/thread

The MammoTh - January 6, 2011, 7:32 am

Nice thanks for sharing some things could be changed but it very handy.

Simonas00 - January 6, 2011, 7:33 am

Holy, I runned it before, now I am kind of suspicious tbh. Well I respect you gta for trying to help too, for me (I am happy) everything looks good, I didn't lost anything.

condom - January 6, 2011, 3:34 pm

makes me wonder too. malewarebytes picks up borlo.exe as worm with the live protection. just throwing that out there....

Spoiler ([Click to View](#))good program though.

?ami - January 6, 2011, 3:46 pm

(Sep 22, 2010 07:05 AM)gtaclick Wrote: [\[CITE\]](#) K then here we go:

[IMG]http://i56.[censored].com/nxqd01.jpg[/IMG]

I pressed block.

Translation:

Own'z Is trying to act like a server and accept incoming connections

If you want this program to accept incoming connections press 'Accept'. If not press 'Block' to not allow them

You are wrong here, it wants to access the internet and sends connections out BECAUSE he has a HWID system inbuilt to it, plus his crypter is hosted offshore on a web service, meaning it has to connect to the web server where it is hosted to unlock, that is why most of the errors you get when you try to login, they are from his hosting being down! Also the crypter has to check for updates.. so NO SHIT

The Janitor - January 7, 2011, 1:27 am

(Jan 6, 2011 04:46 PM)Pineapple Lump Wrote: [\[CITE\]](#) You are wrong here, it wants to access the internet and sends connections out BECAUSE he has a HWID system inbuilt to it, plus his crypter is hosted offshore on a web service, meaning it has to connect to the web server where it is hosted to unlock, that is why most of the errors you get when you try to login, they are from his hosting being down! Also the crypter has to check for updates.. so NO SHIT

The crypter 1.3, he "accidentally " uploaded a RAT as his stub, it should be somewhere in his old thread where i posted it, his answer was:

"I have 19 Stubs, people make mistake!"

I'm still really suspicious on this, he couldve binded something to his crypter. Why did he built the log-in? So we wouldn't get suspicious?

HJT Team should scan it, and stuff.

Thanks for contributing,

Another guy had the same problems with the crypter, connecting to internet and stuff.

Kind regards

Gtaclick

.Astro - January 7, 2011, 1:30 am

I'll come back with my report on this. Time to open up HexEditor and all that shit I used for File safety <3.~

The Janitor - January 7, 2011, 1:30 am

(Jan 7, 2011 02:30 AM)pyratepig Wrote: [\[CITE\]](#) I'll come back with my report on this. Time to open up HexEditor and all that shit I used for File safety <3.~

Thank you dont forget to post it :)

.Astro - January 7, 2011, 1:44 am

Alright, so from just a quick scan I managed to see a small code that imported items for mailing. Now, before jumping to any conclusions, this could be here to encrypt your email and password used in your keylogger, etc. So don't make any more assumptions just yet.

The stub log <http://pastebin.com/raw.php?i=gjpEuBBf>

CTRL + F and type in crss and you'll find words you can actually read, lol.

I tried to get the crypter log, but it won't load in notepad every time I try to copy and paste it.

JackSkellington - January 7, 2011, 2:19 pm

(Jan 6, 2011 04:46 PM)Pineapple Lump Wrote: [\[CITE\]](#) You are wrong here, it wants to access the internet and sends connections out BECAUSE he has a HWID system inbuilt to it, plus his crypter is hosted offshore on a web service, meaning it has to connect to the web server where it is hosted to unlock, that is why most of the errors you get when you try to login, they are from his hosting being down! Also the crypter has to check for updates.. so NO SHITOk listen you F****ing idiot When i bought it i wasnt asked for a loggin or HWID so obviously your trying to help him out and stuff i know what i did the only two things i downloaded was blackshades and that damn crypter and bam my pc is trying to connect to outside connections snd it slowed down my pc my pops was looking for it himself and couldnt find and hes a computer technician. anyway i want c6 banned thats all and julie for helping him

c6p0 - January 8, 2011, 3:43 pm

if you have download crypter another site .
i am not responsibility .

my crypter free its allway up check all you want its clean (if you download my link)
3 best coder in HF have my source code .

JackSkellington - January 8, 2011, 7:01 pm

(Jan 8, 2011 04:43 PM)c6p0 Wrote: [\[CITE\]](#) if you have download crypter another site .
i am not responsibility .

my crypter free its allway up check all you want its clean (if you download my link)
3 best coder in HF have my source code .from another site? only the one you gave me

D1G1T4LM4N_616 - January 8, 2011, 7:42 pm

the crypter isnt infected

ive opened it

it works

nothing has happened since

no offence to OP

.Astro - January 8, 2011, 8:44 pm

(Jan 8, 2011 04:43 PM)c6p0 Wrote: [\[CITE\]](#) if you have download crypter another site .
i am not responsibility .

my crypter free its allway up check all you want its clean (if you download my link)

3 best coder in HF have my source code .

I want your source code for the crypter o:

Been trying to make one, but need a template to go off of. I tried modding sources, but I broke the compiler and the codeom part roflmao.

Czarek580 - *January 13, 2011, 3:16 am*

he must have like 100k victims by now

DuctTape - *January 13, 2011, 4:48 pm*

yea...

not infected, definitely

Im a UN-official white hat hacker and its gud o.o

Odd Future - *January 13, 2011, 7:43 pm*

I don't understand..

Are they infecting the users who buy it or what?!

The Janitor - *May 28, 2011, 10:29 am*

(Jan 13, 2011 08:43 PM)Odd Future Wrote: [CITE](#) I don't understand..

Are they infecting the users who buy it or what?!

Both :) According to the information I found >.>

Reppin' - *May 28, 2011, 12:48 pm*

Hmm I think its a false positivee,