

Forum:[Hack Forums](#)

Thread: [\[Challenge\] CRACK THIS IF YOU CAN \[CHALLENGE\]](#)

hf_l33t - April 20, 2011, 8:30 am

[size=medium][b]Hey guys i have a challenge for all of you just try to Crack it & you will have a secret message on it ..

Well after you crack it PM me the Message and the Method you used: in short

But i think no one can crack it including Kobac in HF

VIRUS SCAN :- <http://my-avscan.com/result.php?scan=MTU5Mzl=>
[color=#FFD700]
[deleted]

MultiMedio - April 20, 2011, 8:39 am

Nice i didnt manage to crack :' (, btw kobac can easily crack. u just remove the hole system.

Remmember: Nothing is UnCrackabel, but u can make it hard as fuck.

vaibhuvcool@gmail.com - April 20, 2011, 8:47 am

Cant crack it Bro its too hard...

I think nobody can crack it...

pr0t0typ3 - April 20, 2011, 9:03 am

Looks like a bad try to infect HF.

Nazworth - April 20, 2011, 9:31 am

(Apr 20, 2011 09:03 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Looks like a bad try to infect HF.

Haha, I'm glad you pointed that out. There shouldn't be a RunPE in a crack me :)

Elbobo - April 20, 2011, 9:39 am

i also noticed it(the pe dropped in memory) tried to access mozilla sqlite dll's, its trying to steal passwords :/

pr0t0typ3 - April 20, 2011, 9:45 am

Uhm a .net crack me does not need a RunPE and a installation routine.

Even if you would store hashes (wtf has this to do with a RunPE) you don't need to install your application to startup.

Helios. - April 20, 2011, 10:09 am

(Apr 20, 2011 09:03 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Looks like a bad try to infect HF.

And it seems that his "Forum" (hackforall.com) that is in his signature is not so innocent as his application:

<http://www.virustotal.com/file-scan/report.html?id=6a0d5caea143c16e653c09eea3dbda89cb76a36bd04a41ca5910c262e42e0386-1303317398>

http://anubis.iseclab.org/?action=result&task_id=185000a00724d2564ade4800605e4e3c7&format=pdf or
http://anubis.iseclab.org/?action=result&task_id=185000a00724d2564ade4800605e4e3c7&format=html

(Apr 20, 2011 09:03 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Looks like a bad try to infect HF.

op shud at least obfuscate his shit if he wants to infect members

(Apr 20, 2011 09:03 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Looks like a bad try to infect HF.

I opened that file in .net Reflector and looks legit:

He the part you can see is the loader which does get the actually application from resources and invokes it in memory and I unpacked it...

Would you mind telling me how you did that?

TVqQ\$M\$\$\$\$E\$\$\$//8\$G\$Q\$2\$4fug4\$t\$nNlbg!TM0hVGhpcy!wcm9ncmFtIGNhbm5vdC!iZS
ydW4gaW4gRE9TIG1vZGUuDO0KJ\$TDRS!v2x68Fdsev!XbHrwV2x68F9sevC/c3HwVmx68NRwd

P!\$bHrwNXNp8F5sev!XbHvwMWx68L9zcP\$3bHrw72p88FZsev!SaWNoV2x68\$\$UEU\$\$Ew!!\$\$/yeV
L\$\$Dg\$\$8!CwEG\$\$!w!\$\$\$0\$\$HUR!\$\$\$E\$\$\$I\$E\$\$\$Q\$\$\$E\$\$\$!\$\$\$Q\$\$!\$\$c\$U\$\$!\$\$C\$\$\$Q\$\$\$
Q\$\$!\$\$\$!\$\$Q\$\$\$!gzQQ\$e\$\$!g!Q!0C\$\$I\$E\$M\$!\$\$udGV4d\$\$\$\$EJj!\$\$\$E\$\$\$H\$E\$\$\$Q\$\$\$g\$\$!gLnJk
YXRh\$\$!qVw\$\$\$I\$E\$\$!g\$\$\$\$g\$Q\$\$\$Q\$\$\$QC5kYXRh\$\$\$\$1Hk\$\$\$Dg!\$\$\$Y\$\$\$\$O\$E\$\$\$E\$\$\$M\$ucn
NyYw\$\$\$HQI\$\$\$\$Y\$U\$\$!\$\$\$!\$!Q\$\$\$!\$\$\$!\$\$FWL
?

if so that makes some cence

pr0t0typ3 - April 20, 2011, 10:31 am

(Apr 20, 2011 10:29 AM)StaTiX Wrote: [\[CITE\]](#) do you mean this ?

Spoiler ([Click to View](#))

Code

TVqQ\$\$M\$\$\$\$E\$\$\$\$/8\$\$Lg\$\$Q\$\$2\$\$4fug4\$t\$nNlbg!TM0hVGhpcy!wcm9ncmFtIGNhbm5vdC!iZS!
ydW4gaW4gRE9TIG1vZGUuDQ0KJ\$\$TDRSjV2x68Fdsev!XbHrwV2x68F9sevC/c3HwVmx68NRwd
P!\$bHrwNXNp8F5sev!XbHvwMWx68L9zcP\$3bHrw72p88FZsev!SaWNoV2x68\$\$UEU\$\$Ew!!\$\$/yeV
L\$\$Dg\$\$8!CwEG\$\$!w!\$\$\$0\$\$HUR!\$\$\$E\$\$\$I\$E\$\$\$Q\$\$\$E\$\$\$!\$\$\$Q\$\$!\$\$c\$U\$\$!\$\$C\$\$\$Q\$\$\$
Q\$\$!\$\$\$!\$\$Q\$\$\$!gzQQ\$e\$\$!g!Q!0C\$\$I\$E\$M\$!\$\$udGV4d\$\$\$\$EJj!\$\$\$E\$\$\$H\$E\$\$\$Q\$\$\$g\$\$!gLnJk
YXRh\$\$!qVw\$\$\$I\$E\$\$!g\$\$\$\$g\$Q\$\$\$Q\$\$\$QC5kYXRh\$\$\$\$1Hk\$\$\$Dg!\$\$\$Y\$\$\$\$O\$E\$\$\$E\$\$\$M\$ucn
NyYw\$\$\$HQI\$\$\$\$Y\$U\$\$!\$\$\$!\$!Q\$\$\$!\$\$\$!\$\$FWL
?

if so that makes some cenceYeah exatly that is it.

If you replace some of the characters you get a valid base64 string which can be decoded and opened in reflector.

Inveno - April 20, 2011, 11:04 am

This link has found to be infected/harmful.

If you downloaded this link, you may want to visit the [HJT SECTION](#)