

Forum:[Hack Forums](#)

Thread: [\[help\] HOI4 Cheat reversing](#)

Pluralistic ignorance - September 23, 2022, 3:48 pm

Hello all,

Due to an influx of hackers/script kiddies in the Hearts of Iron IV (hoi4) community I started investigating...

Website called jewishtricks.me sells the cheats \$10 a pop. Pretty cheap, so I got my hands on the executable provided when you purchase the cheat.

After doing a little digging I found that the file was packed with themida - so I submitted the .exe to an unpacking website called unpac.me. The file linked below is the .bin output of the original .exe.

[https://drive\[WARNING POSSIBLY INFECTED\]google.com/file/d/1gTzaizSHeCY0x_laMhRU7Gn07usPft46/view?usp=sharing](https://drive.google.com/file/d/1gTzaizSHeCY0x_laMhRU7Gn07usPft46/view?usp=sharing)

<https://www.virustotal.com/gui/file/ac18d73c7ed967cec773fae76f7a2eb9e85a5e6d7c8182d93daff69fd248b879/detection>

Is there anyone on this forum that can assist with decrypting/reversing this .bin? ?

Here's a snippet of the strings provided on unpac.me

Spoiler ([Click to View](#))

Code Fd9~H~?

}A@oh%{

6(6,6D6T6X6\6`6d6h6|6

Pn "Z7q

hudgB?!

DaX8x%3

`typeof

Failed to set SO_KEEPALIVE on fd %d

u79o8u)9o<u\$

\$/""6

FD %s:%d accept() = %d

D \$H(Z

M\kg<YU

A38B~D/Z

>">,>?>D>I>N>g>I>q>v>

Excessive password length for proxy auth

Hostname in DNS cache was stale, zapped

schannel: unexpected content type '%d' when extracting certificate from CA file '%s'

'_LuNQ:

e&.0zZh

1>2pB.Y

: ;2;U;

us-ascii

7\$7,747<7D7L7T7\7d7l7t7

8"9D.;

invalid string: control character U+000A (LF) must be escaped to \u000A or \n

invalid string: control character U+0002 (STX) must be escaped to \u0002

x\$"]\$R`

,q*AXNp

zoA/xRo0

.?AV?\$basic_ofstream@DU?\$char_traits@D@std@@@std@@@

-----END CERTIFICATE-----

A@b"PxZR

D)Sut@J=

config.ini

C:\vcpkg\buildtrees\curl\src\7a634d33bf-24fa6e04fd.clean\lib\escape.c

"qS\$&z\$

/,4xZlj

g-KE?[Y1

CLIENT libcurl 7.78.0-DEV

2ky0'ZJ

a S}y0k

X<\<`<x<|<

Received HTTP/0.9 when not allowed

jrNkc'

;;;B;H;Z;`;g;q;v;|;

2ijEgiVF

.rtc\$TAA

7"26ypoXnht

Af95n(S

pluMe%|

EXTEND ASCII

h}@f)o[

socks4a

Ue B;/"

.F18+"m

.?AV?\$wconv_to_utf@D\$00@impl@conv@locale@boost@@

NZ3;9:uj

999[9~9

Got an error writing an RTP packet

SEC_I_CONTINUE_NEEDED

;7;@;g;l;r;|;

RtlInitUnicodeString

CALG_RSA_KEYX

e\$i@h<]ao

+4/rqW<

NtTerminateThread

@\$?|Y=3

5,5f5p5|5

(!.Jod@

|~`p%E'

HR"}o0W^i!

\$h=r,Z

invalid string: control character U+0013 (DC3) must be escaped to \u0013

?R_2>WVp

Got a %03d ftp-server response when 220 was expected

0"0V0}0
C.!f10.
serially
r<+r8tf
>(,>0>8>P>`>d>|>
y_YOxKs
'YIToXr 6
>Q>\>a>l>q><>
e)p>|Xe
=H>e>v>
;c;u;};
\$vrdrOi
ADVAPI32.dll
d63r5JQ
<Yq)8^:
=(0=8=@=H=P=\|=|=
&8d<MH+
s=][[-a/
\$J7fUS0
Content-Range: bytes %s%l64d/%l64d
9"989>9H9R9_9h9r9|9
:D\$,u#j
KENNaL32.%
blksize is smaller than min supported
CompareStringEx
Kerberos
 </security>
machine
4\$XUT]R
4\$XUT]W
IFC`mbv
g\ym0b`
/Jwoe\$Oy};
e*bWR\$A`
schannel: added %d certificate(s) from CA file '%s'
X-J.?W)
;sha256//
FD %s:%d sclose(%d)
2 i\$'Q(
MOeAR x
1\$1,1<1L1T1`1
yS{,\$'C
2\$2)2=2
l2wAT3o
NtResumeProcess
d8<(<M0
CURL_SSL_BACKEND

.?AV?\$_Binder@U_Unforced@std@@A6A_N_KAAV?\$vector@_KV?\$allocator@_K@std@@@2
@I@ZABU?\$_Ph@\$00@2@V?\$reference_wrapper@V?\$vector@_KV?\$allocator@_K@std@@@
std@@@2@AAI@std@@@
?0?@?D?H?L?P?X?p?
i_w;c_U

\8(k_v
=\$=3=g=
@qlCIW}
RESOLVE %s:%d is wildcard, enabling wildcard checks
~ry8|1v
'vszW`ePGHr`
Jb@SWc:
Vki]EpKrX
'eh?][~
6%7;7}7
Cix_T%(
NTLM send, close instead of sending %l64d bytes
B-Dr>X1O
9x(r 8XE
0;0b0i0p0u0~0
iE:"\U @
Z0Up0Vr
'nAcyDN
3,\$1,\$3,\$\VT^
ZlIb[XR
yNH@D=N
-a!~*xr,
L\$ QUPV
%s IAC %d
> ?@?H?P?X?`?h?p?x?
?!?-?C?L?U?
.Pc@:'`F
(v@sH.B
9,:l:f:
cN+B*J/z
%s IAC %s
.?AVIAsmHelper@blackbone@@
SEC_I_COMPLETE_AND_CONTINUE
3z(z|o+x
5<5O5g5
?Ci<
%s6n|\$l.&A
SEC_E_UNSUPPORTED_PREAUTH
Username
%04d%02d%02d %02d:%02d:%02d GMT
8o\;[2%
8%9,959>9X9c9m9>:M:\:k:z:
schannel: CA file '%s' is not correctly formatted
2D)`v61
6N6[6z6
D\$DPh\$6O
H |w"rV
Connection #%ld is still name resolving, can't reuse
;";;-d;y;~;
operator<=>
'Qt@y[.
Av~!(n#N%
[WhOqvU

e))XAH2
T6G xpJ
1)10181P1^1f1~1
1.2.840.10046.2.1
>y@0~(d
address family not supported
3 @sL_=
h \-0_
Illegal byte sequence
no such file or directory
q"J k8
KNK#0Z`
<discarded>
"a:bG:/
h*h3an*
SEC_E_SMARTCARD_LOGON_REQUIRED
: uTR[tB
qF3c`8*
>D?S?a?~?
Bad argument
X^_m5?8Q4
+*4K9dk
1"2l2r2
5 7(8B8P8
>yh_k s
\$R[D@3G
hgskkuM
secur32.dll
1,\$3,\$1,\$_
k IP;E3
ablflNg
2V3u3~3
VBer-_qz;
2'323;3
pt\$91`/
RX0\$[T=
2 Pk8 v
.?AVbad_alloc@std@@
Malformed encoding found
U~/R]]i
A libcurl function was given a bad argument
Account:
IT90s%-
hs-'PVJAZ
,\$\RUhQJ
`"TM!Zm
\$3<0iuQ
S[IFg\7
executable format error
failed to resolve the address provided to PORT: %s
n@t@HVh
8nP.`Q<
ftp@example.com

Pt^ /BBn
'0IUD\$<
DH)1OD;
b9VWPX<
f\$L{@tOw
393F3m3
<vT"n ~
XtlttxYx
r`htY%LkF
Uh,?_w]
inflate 1.2.11 Copyright 1995-2017 Mark Adler
D!HFd+H
0d-:|po
~^+3hdOZ]
e78*@D5
4\$Z_ qL
O""dc`{
\$h4L?+[
{WhyX;~
OhaUqnH
--:--:--
multipart/mixed
. ?AV_Ref_count_base@std@@
T[w[
TIMING MARK
APOP %s %s
E)HtJ(h
]34\$14\$34\$
oYQSY[K
30474C4c4
4\$[RTZP
4\$[RTZQ
h0%/yKS
4\$[RTZU
5\$5,585@5t5
MM/dd/yy
FGu[ek_
fwxZA/<
Socket is unsupported
,-lc-+l
. ?AV?\$converter_to_utf@D@impl@conv@locale@boost@@
;B;R;c;
\$tcaJ l*
J\$1x&d;
jhXjbYjnf
`q" LDlt
invalid hash bucket count
5@5S5y5
&iF]V6\
~<@ 1"v
O9mZ7i&
?f/`W[po
4)53595C5l5y5

P0YR5,<
PROT %c
5&525>5J5V5b5n5z5
YSrh>w8-
v%V`^!C=
.?AVtype_error@detail@nlohmann@@
t+Lfo_
.?AV?\$codecv@DDU_Mbstatet@@@std@@
6 6T6v6
mO?u.A|
uCFf;t\$
3\$434L4:5D5Q5
*:%<f4DYh
L>]vsn
KtpoD 9
3,\$1,\$3,\$\R
~`yp3e2
r`fprl
it# Vfk
}QaZf?t
,WYZ'Ve
SoftwareNtm
1\sC/Nv
&J`h.eQ]>
.?AV?\$messages@_W@std@@
y"4qh=Z
B^srHE&
4\$\h*}B/
m#!UYq
3{hViBx
^Jl,Q&!Y
\[294A
CALG_ECDH_EPHEM
m_k" hwb
Connection refused
.rtc\$IAA
Authentication problem. Ignoring this.
x#V-4Hvd
5,6H6R6[6
llc" .s
<1<;<F<
5 5(50585@5H5P5X5`5h5p5x5
-----BEGIN CERTIFICATE-----
cd? =Xd[
'pCA.Dl
Tha_k_yXu
Can't add itself as a subpart!
0Oi'SvWq
i =\$GHL
bM"f1o
map/set too long
9%ZY \$:
~8-^P8|

2=QRAdCj
Qi|#/Rq
not enough memory
1)1E1U1n1~1
C:\vcpkg\buildtrees\curl\src\7a634d33bf-24fa6e04fd.clean\lib\socketpair.c
t5;L\$\$s/V
?<?D?\?p?
dM\$&iP
Z}imO^KA!h
m B;/"g
t`@4s'c
OLEAUT32.dll
f<1T El+o
Unable to send initial SOCKS5 request.
Y08IW|ST
V:H, (p
G ;F u)
XBH_FNT
#HttpOnly_
Failed to receive SSPI encryption response.
SSL server certificate status verification FAILED
}<`u9@:
kz3\$=,C
<"<:<B<q<
(*\$(O)T)
X)! ^S?
],` \ir
response reading failed
invalid seek
t@rw~D'
|T-\5(L
0/GPNOW0J
FY{T3h'P
4\$]QTYV
4\$]QTYU
|1|x|EL
file exists
2#212H2N2X2b2x2~2
,\$PhgDt
4\$[PTXQ
dFO U}p5
schannel: failed to create certificate chain engine: %s
7g_% _

From what I gathered the cheat works by contacting an RPC server located on the jewishtricks.me domain. Then it executes the instructions in game to activate the cheat.

That's about all I got so far.

dizzymizzy - February 25, 2024, 12:49 pm

did the cheat work tho

K947AGENT - June 18, 2024, 11:39 am

the link isnt working tho if u can send me the account to download it and i can investegiate it