

Forum:[Hack Forums](#)

Thread: [help|steal the ftp u&p from a keylogger's exe](#)

zzx - October 10, 2009, 3:19 pm

hello

I have a file from some werz site then i know he infected (some one bulid)
now how can i know to where the file upload the logs
and steal it ?

hope every one understand me and my poor english

ZedNull - October 10, 2009, 3:32 pm

1) disassemble the file, find how it has encrypted the username and password and reverse that encryption

or

2) run it in a virtual machine while running wireshark, since FTP logins are plaintext.

zzx - October 11, 2009, 10:34 am

(Oct 10, 2009 03:32 PM)ZedNull Wrote: [\[CITE\]](#) 2) run it in a virtual machine while running wireshark, since FTP logins are plaintext.

can you give me a name ? of the soft

The Mystery* - October 11, 2009, 10:58 am

ZZX,

Just use "Hex Editor" soft...

I used it and you can allways find information about ftp on binded file... or mail...

ZedNull - October 11, 2009, 1:23 pm

VMware has virtual machine software, Microsoft has Virtual PC, there's VirtualBox; there are plenty of them.

Also, TheMystery, a simple store encrypted/small decryption routine on the strings would obscure them to a hex editor. You would be able to hex edit out the logins on some stealers, but definitely not "always."

zzx - October 11, 2009, 2:02 pm

hello there..

I download the "Hex Editor",setup it and open the file but i didnt find the username/email/FTP and nothig like this..

so i try in another file thet i bulid with Isteler 3.0 but still didnt find.

ZedNull:

I need a software thet when i run the infected EXE file, she follow the action he does.. and will show me where the file send the logs from my PC

wow my english is soooo disgusting

ZedNull - October 11, 2009, 2:35 pm

zzx, if you want, I could take a look at the file and maybe write up a quick lesson on finding this info. A disassembler would help for this process; I've heard good things about OllyDBG, but personally I use IDA Pro.

zzx - October 11, 2009, 3:09 pm

ZedNull:

take some stealer I found him on youtube (facebook hack)..

http://#.com/files/291757307/X-Force_Generator.exe.html

try to find to where the EXE send the log
and tell me how you find it..

tnx a lot agin!.

Excalibur - October 11, 2009, 10:50 pm

(Oct 11, 2009 03:09 PM)zzx Wrote: [\[CITE\]](#) ZedNull:

take some stealer I found him on youtube (facebook hack)..

http://#.com/files/291757307/X-Force_Generator.exe.html

try to find to where the EXE send the log
and tell me how you find it..

tnx a lot agin!.

i went thru that file yesterday but didnt find anything, but im new at this, maybe someone with more experience will catch what i couldnt

that file was posted with a ton of different hack videos, most nonrelated

ZedNull - October 12, 2009, 7:00 am

The logs are sent to a PHP page, similar to how iStealer 5 does it. There are a few DNS lookups it does:

kinoarts.com (64.27.5.204)

disciplinearts.com (66.45.246.155)

soloartsworld.com (69.10.35.253)

solofilmworks.com (66.197.207.41)

maximclock.com (64.120.164.40)

thezasite.com (64.191.90.183)

It also seems to get and run 2 parts: b.exe and c.exe; I haven't had a chance to analyze them yet. They seem to run in memory, so I'll need to take a snapshot and go from there. Stolen info is sent by POST data, and I haven't quite found the encryption yet. This is one of the stealers where it would be easy to spam fake logs after finding this part.

Also, b.exe seems to be able to restart itself; it downloads more malware too. I'm doing a memory dump of the running process now, and I'll read through it later (after I restore this VM snapshot to get rid of whatever else it downloaded)

zzx - October 12, 2009, 8:20 am

wow nice work..

this file is Spreading all around youtube and Facebook...

ZedNull - October 12, 2009, 9:39 am

Yeah, this is pretty heavily obfuscated; someone put a good bit of effort into this. Library calls are done in roundabout ways, functions are called in the middle of other instructions... It's an interesting bit of code.

A quick sample:

(This is some of the code that's half-roundabout called with my own comments)

```
Code xor edi, edi      #zero out edi
add edi, 15C8h         #prep edi with low word of location
sub eax, eax          #zero out eax
xor eax, 400000h       #prep eax with high word of location
add edi, eax          #set edi to full location: 0x004015C8
mov esi, [edi]         #set esi to the value at this location (little endian 04 a2 00 00)
add esi, eax          #add 0x00400000 to esi to get the full location (0x0040a204)
xor edi, edi          #zero out edi
sub edi, 794B65C2h     #set edi to -0x794b65c2; a two's compliment positive.
xor [esi], edi         #xor of that value with value held at 0x0040a204, stored there
add eax, 0B41127DDh    #uh... right
push 0E2FB4B84h        #exactly.
push edx              #what was edx again?
call sub_401A55         #this subroutine pushes esi, bitshifts edx, and returns 0x1C...
db 2Eh                #CS segment override prefix?
...
```

zzx - October 12, 2009, 1:52 pm

In the end you will find the location of the PHP,SQL?
or this is too much complicated?

ZedNull - October 12, 2009, 4:13 pm

Oh, I just got that from Wireshark when I ran the initial file in a virtual machine. Also the easiest way to defeat some crypters - the ones that recreate the original exe somewhere and run it.

Now I'm looking into the exes the initial program created, trying to find out the format of its data string that is sent. That way, I can spam a few thousand fake logs.

zzx - October 13, 2009, 6:27 am

hope you will find it!!

tylersmiles - October 18, 2009, 7:37 am

Seems pretty interesting, I'm going to try this out for sure

LoveToHax - October 18, 2009, 11:05 am

Dam, nice job!

That shit is obfuscated like crazy