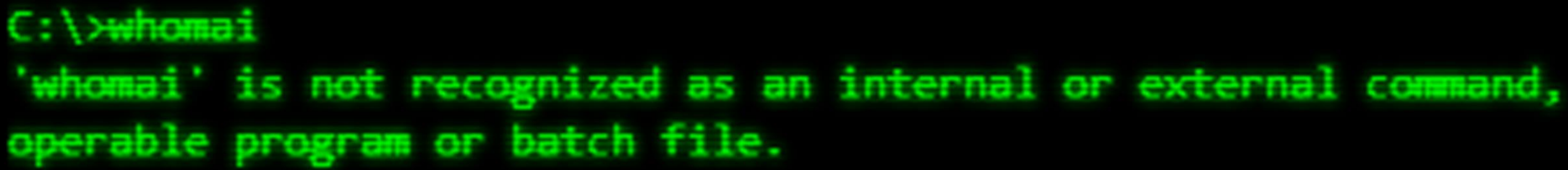
Malicious Macros

And Where to Find Them



```
C:\>whomai
'whomai' is not recognized as an internal or external command,
operable program or batch file.
```

- Zach
- InfoSec enthusiast
- Security Engineer

Malware analysis – Reading the Matrix

- False
- Frustrating
- Mind numbing
- Malware Analysis is what all the cool kids are doing

You don’t have to be Neo

- Assembly not a requirement
- Simple tools to generate IoCs/Intelligence
- Sunglasses are still OK
- Leather trench coat is NOT OK

Where to start

- Isolated environment
    - VM guests
        - Linux
        - Windows
    - Non-production host
        - No difference – I prefer Linux
    - Segregated networking
        - Direct to internet connection
        - No possible route to other network
    - Some free tools
        - Kali – linux based comes with many tools
        - Flarevm – windows based contains many great tools
- Curiosity
- Time

Some Free tools

- Olevba from oletools by decalage2 (Philippe Lagadec)
- Didier Stevens has many great tools
- LibreOffice – or whatever office
- Hexeditor – HXD is my favvy for windows

You promised IoCs – ENHANCE!

Go deeper

The first hop is not enough for generating intelligence

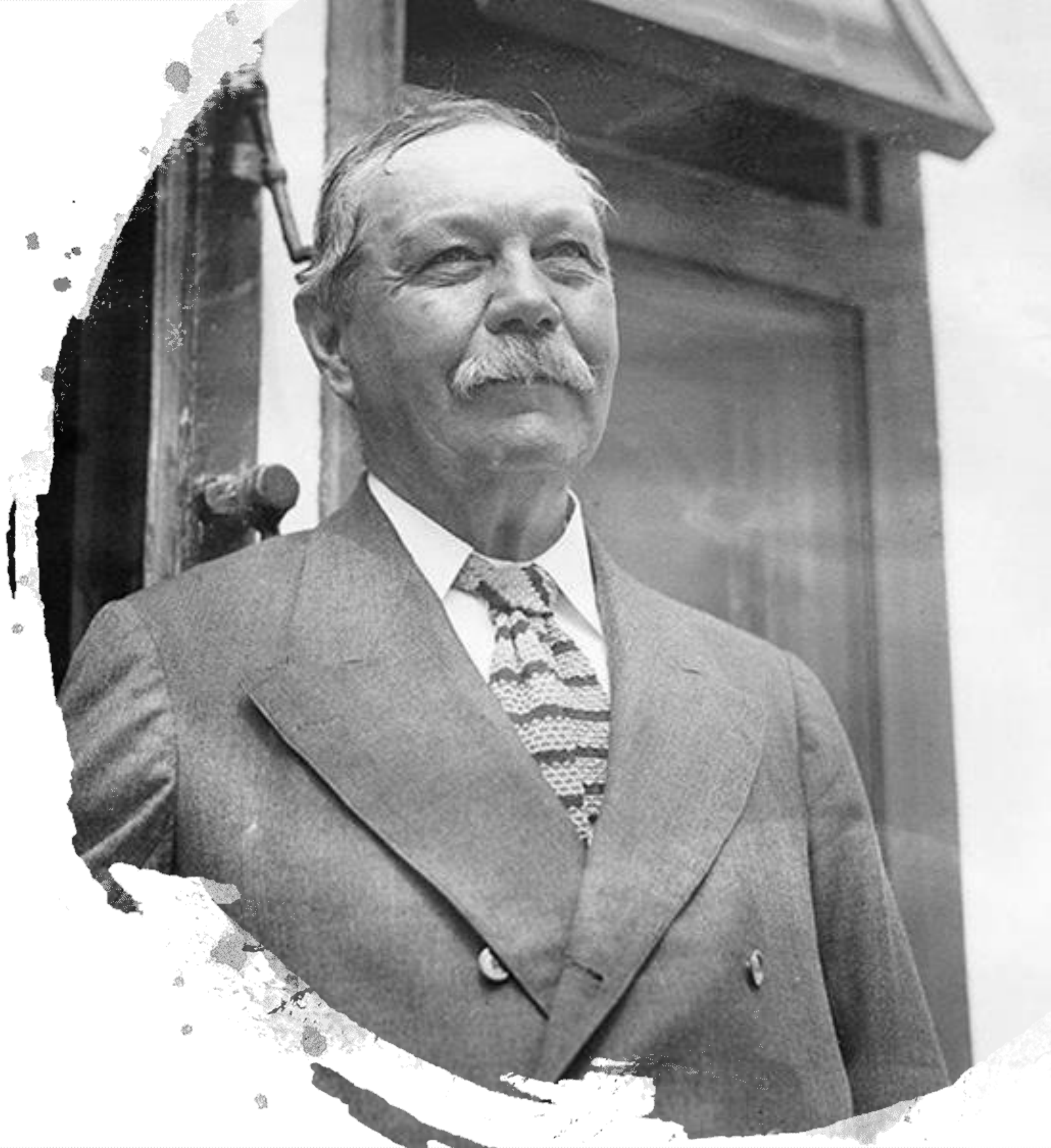
Be aware of corporate/legal boundaries

Do what you feel is best for your career

I’m not a lawyer

“It is a capital mistake to theorize before one has data. Insensibly one begins to **twist facts to suit theories**, instead of **theories** to **suit facts**.”

— Sir Arthur Conan Doyle, Sherlock Holmes

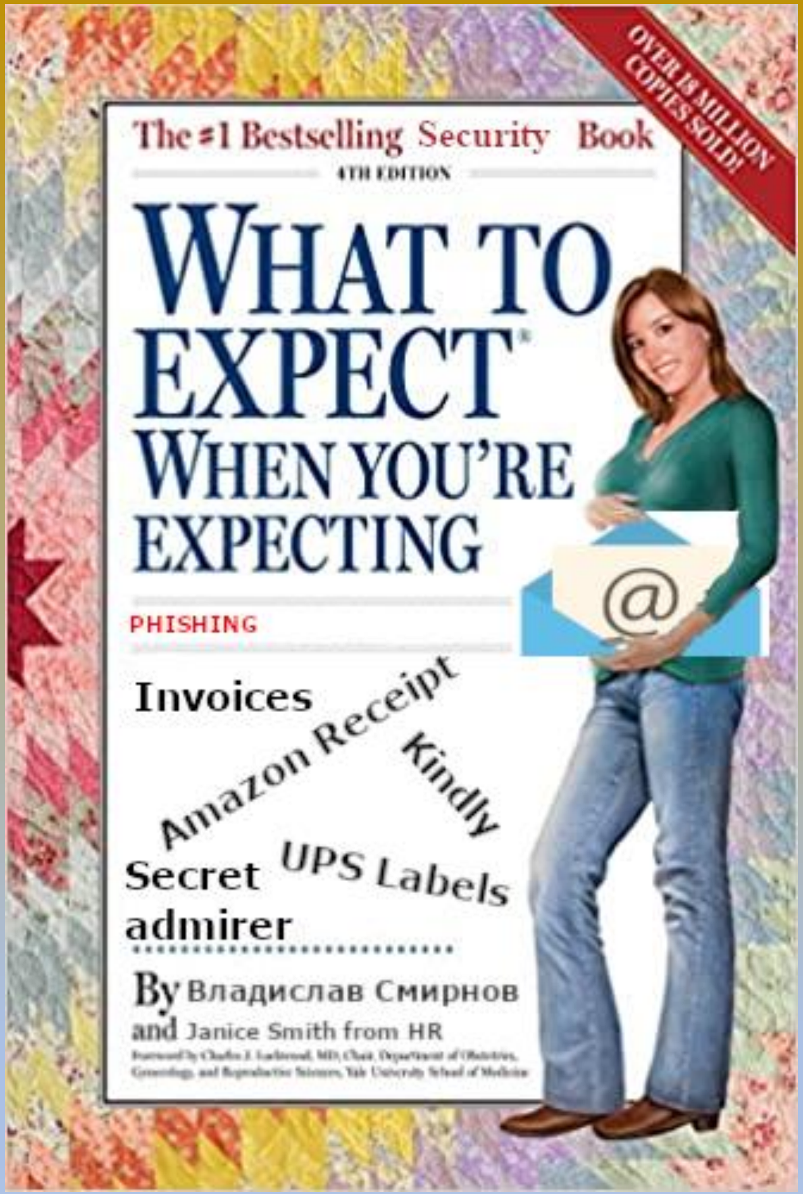


How much is enough?

- As much as you can reliably go without guesswork
- Email IOC’s
  - Sender and/or ReplyTo address
  - Source mail server
  - Attachment name/hash
  - Subject
- Document IoCs
  - Hash/Name
  - Macro content
    - What is it decoded to
    - behavior
      - Contacted domains
      - Dropped files
- Link IoCs
  - Domain
  - Destination file
  - Password Harvester

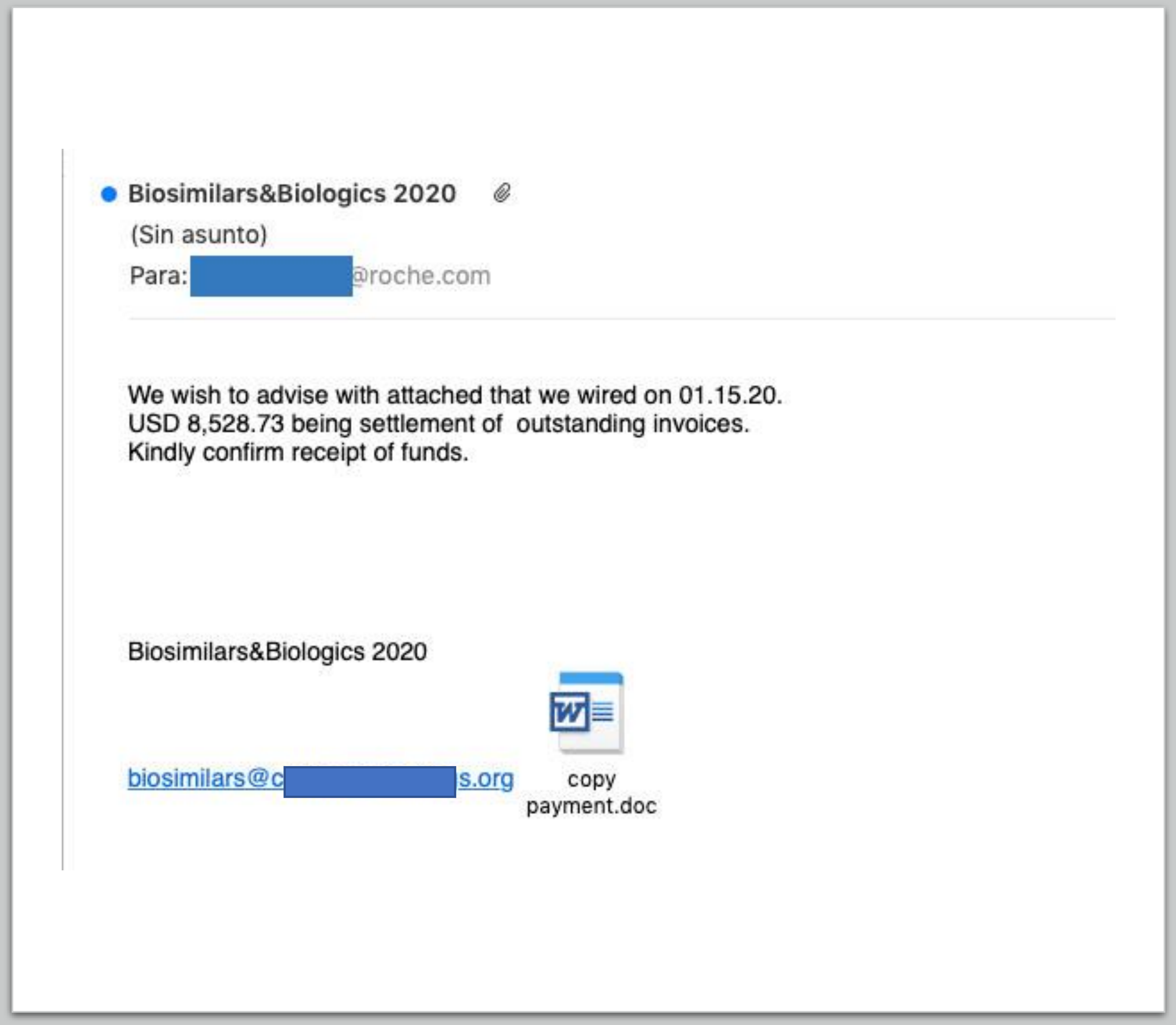
How much is enough? (cont.)

- Dropper IoCs
  - Contacted Ips/Domains
  - obfuscation
- 2nd state payload
  - Behavior
  - Persistence methods
- C2
  - Domain or IP address
  - Agent configs
  - Panel type


OVER 18 MILLION COPIES SOLD!
The #1 Bestselling Security Book
4TH EDITION
WHAT TO EXPECT® WHEN YOU'RE EXPECTING
PHISHING
@
Invoices
Amazon Receipt
Kindly
Secret admirer
UPS Labels
By Владислав Смирнов
and Janice Smith from HR
Foreword by Charles J. Lockwood, MD, Chair, Department of Obstetrics, Gynecology, and Reproductive Sciences, Yale University School of Medicine

The E-mail

- Usually simple
- Some sort of time sensitive issue
- Most likely impacting cash flow



Biosimilars&Biologics 2020

(Sin asunto)

Para: [redacted]@roche.com

We wish to advise with attached that we wired on 01.15.20.
USD 8,528.73 being settlement of outstanding invoices.
Kindly confirm receipt of funds.

Biosimilars&Biologics 2020

biosimilars@c[redacted]s.org

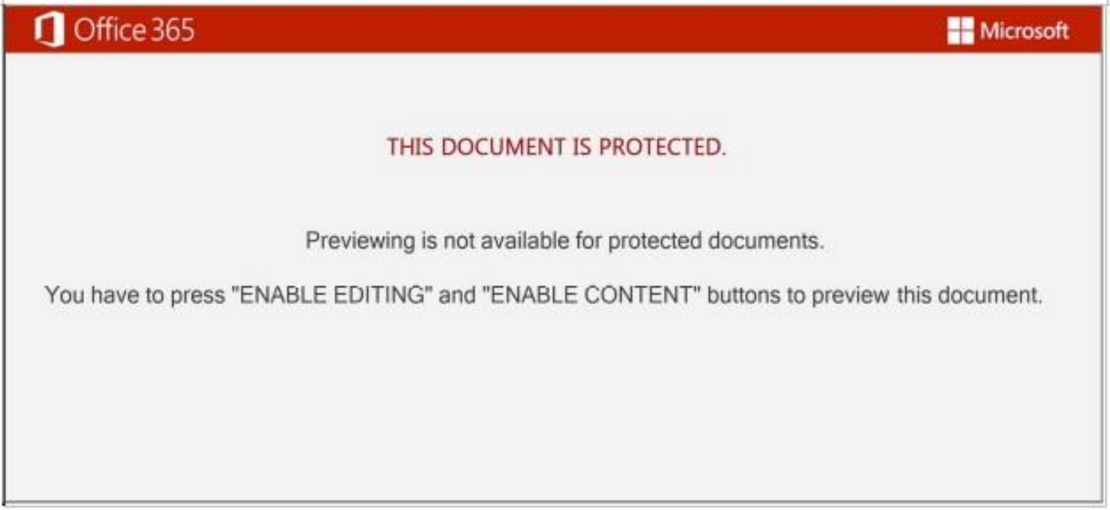
copy payment.doc

Email Artifacts

- Name is not very telling
- .DOC or .XLS instead of .DOCX or .XLSX
- Documents contain a macro
- It states to “enable and allow”
- Macro is not readable

The Document

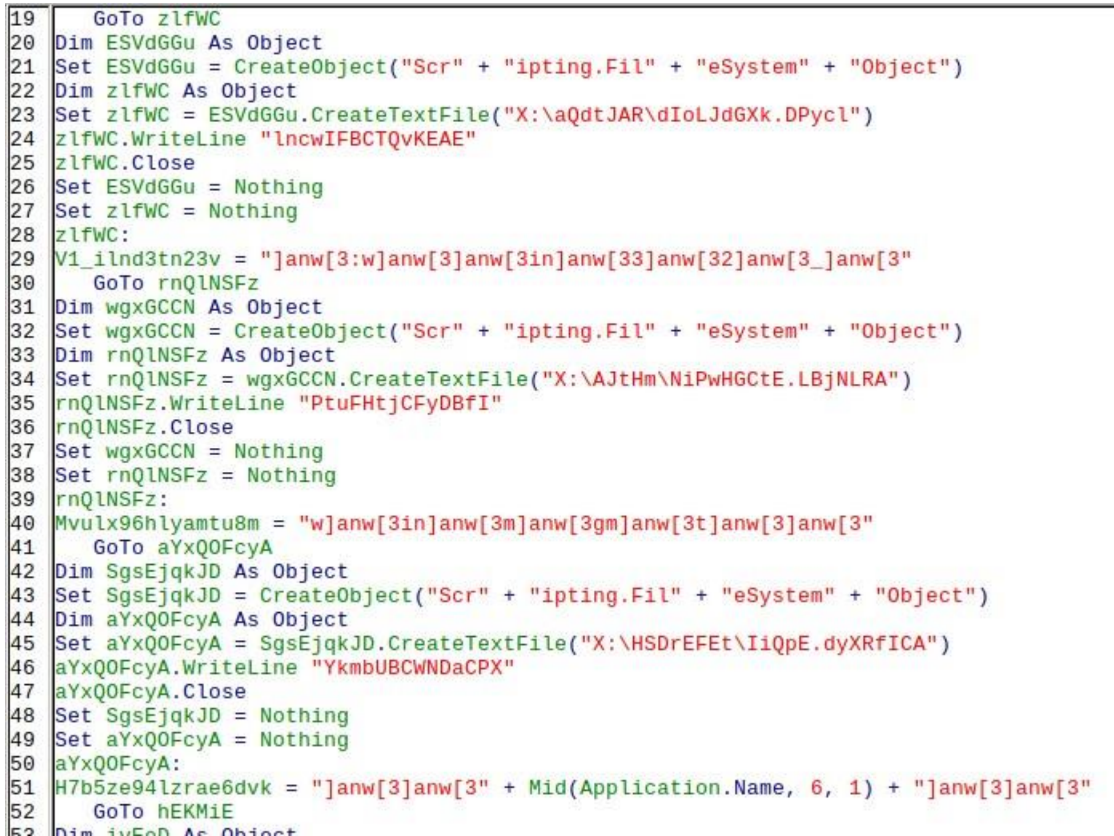
- Very generic
- Asks to turn off the settings that are saving your life
- Difficult to read VBA code



THIS DOCUMENT IS PROTECTED.

Previewing is not available for protected documents.

You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.



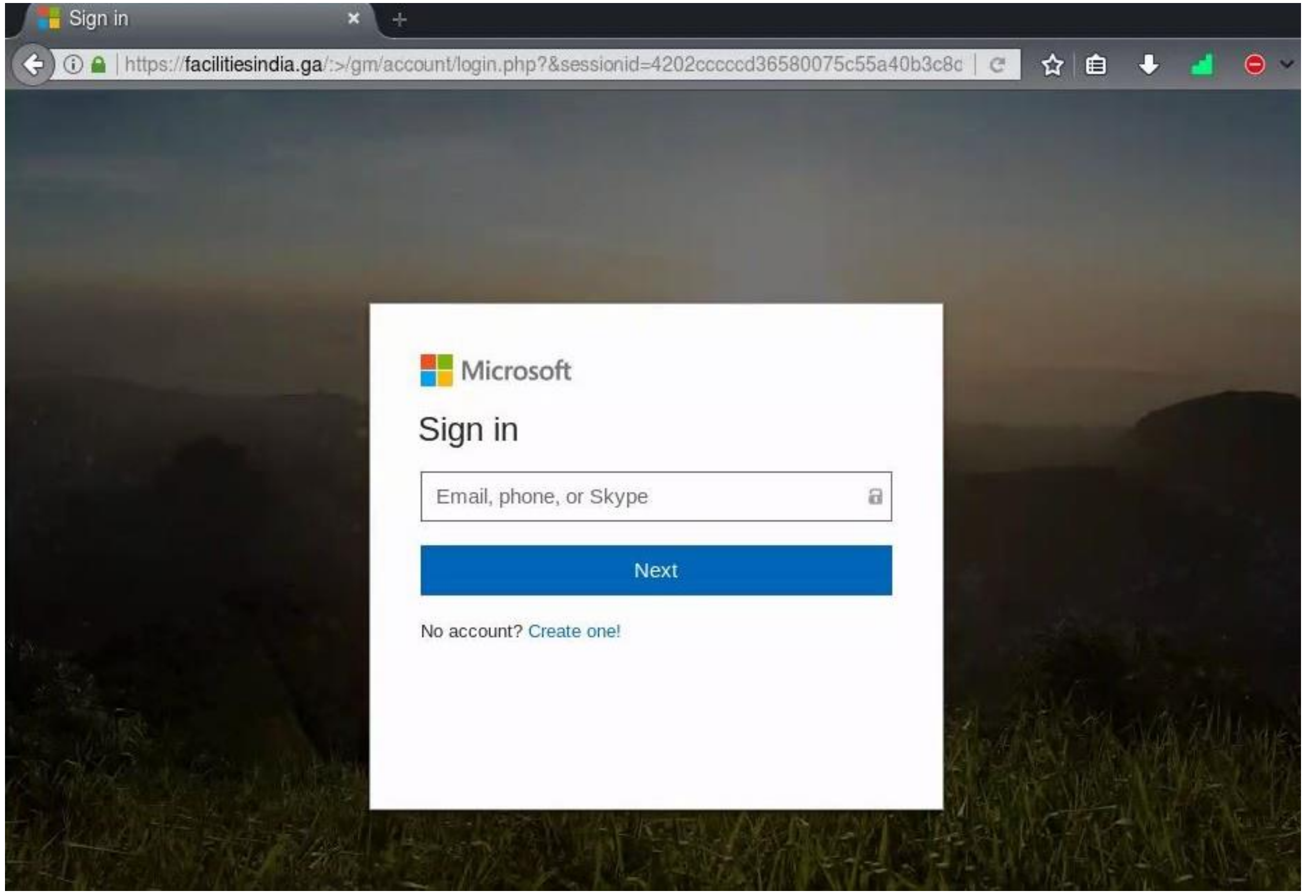
```
   GoTo zlfWC
Dim ESVdGGu As Object
Set ESVdGGu = CreateObject("Scr" + "ipting.Fil" + "eSystem" + "Object")
Dim zlfWC As Object
Set zlfWC = ESVdGGu.CreateTextFile("X:\aQdtJAR\dIoLJdGXk.DPycl")
zlfWC.WriteLine "lncwIFBCTQvKEAE"
zlfWC.Close
Set ESVdGGu = Nothing
Set zlfWC = Nothing
zlfWC:
V1_ilnd3tn23v = "]anw[3:w]anw[3]anw[3in]anw[33]anw[32]anw[3_]anw[3"
   GoTo rnQlNSFz
Dim wgxGCCN As Object
Set wgxGCCN = CreateObject("Scr" + "ipting.Fil" + "eSystem" + "Object")
Dim rnQlNSFz As Object
Set rnQlNSFz = wgxGCCN.CreateTextFile("X:\AJtHm\NiPwHGCtE.LBjNLRA")
rnQlNSFz.WriteLine "PtuFHtjCFyDBfI"
rnQlNSFz.Close
Set wgxGCCN = Nothing
Set rnQlNSFz = Nothing
rnQlNSFz:
Mvulx96hlyamtu8m = "w]anw[3in]anw[3m]anw[3gm]anw[3t]anw[3]anw[3"
   GoTo aYxQOFcyA
Dim SgsEjqkJD As Object
Set SgsEjqkJD = CreateObject("Scr" + "ipting.Fil" + "eSystem" + "Object")
Dim aYxQOFcyA As Object
Set aYxQOFcyA = SgsEjqkJD.CreateTextFile("X:\HSDrEFEt\IiQpE.dyXRfICA")
aYxQOFcyA.WriteLine "YkmbUBCWNDaCPX"
aYxQOFcyA.Close
Set SgsEjqkJD = Nothing
Set aYxQOFcyA = Nothing
aYxQOFcyA:
H7b5ze94lzrae6dvk = "]anw[3]anw[3" + Mid(Application.Name, 6, 1) + "]anw[3]anw[3"
   GoTo hEKMiE
Dim ivFoD As Object
```

Document Artifacts

- ‘Re:’ in the Subject without previous conversation
- Differing ‘Sender:’ and ‘ReplyTo:’
- Sending Server is unexpected
- The word “kindly” is used
- You have some attachment not related to work or outside your business function

Credential Harvesting

- Fairly common
- Visually indistinguishable (sometimes)



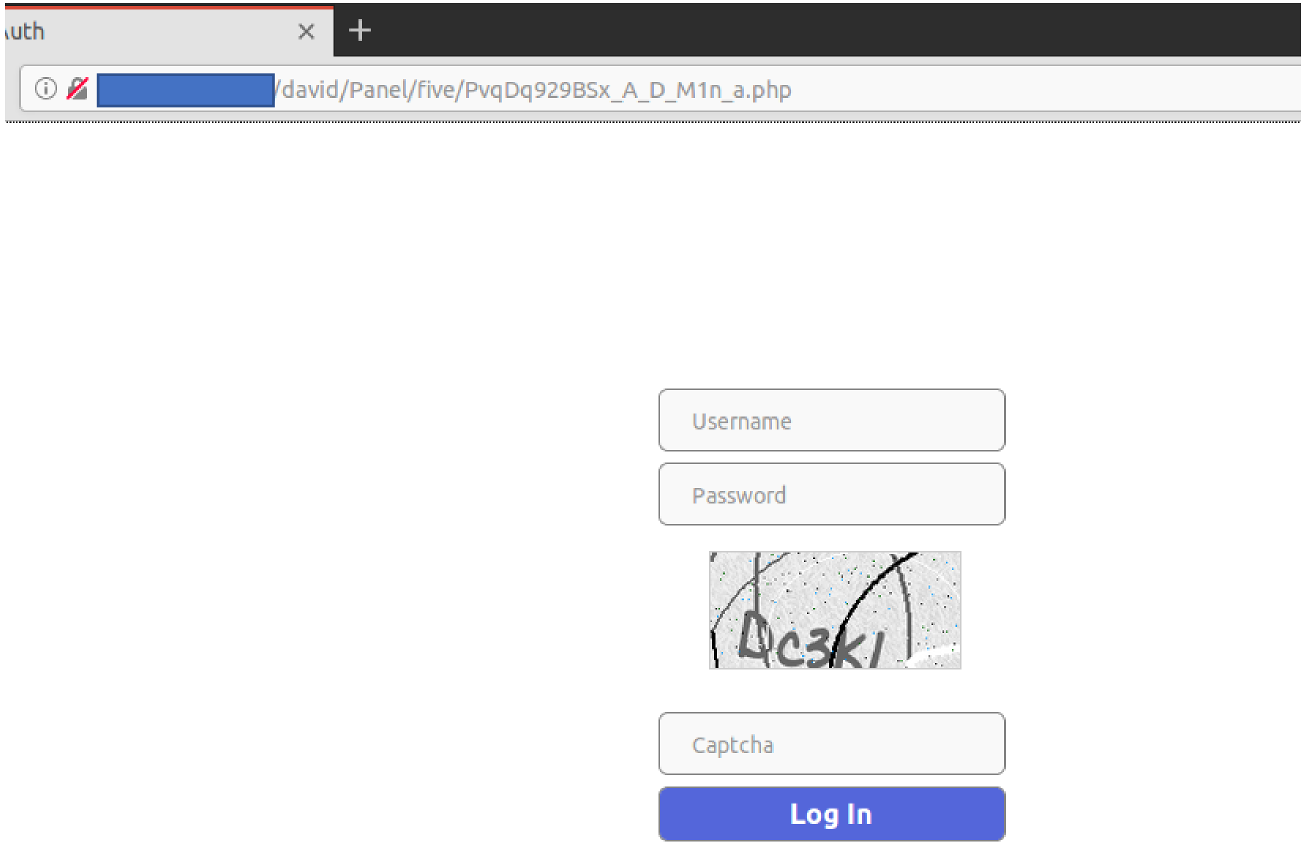
https://facilitiesindia.ga/:>/gm/account/login.php?&sessionid=4202cccccd36580075c55a40b3c8c

Link Artifacts

- Domain name and full URL
- Content on page
- Files/content referenced by page
- If possible, email address harvested creds get sent to

The C2

- Sometimes you see something like this (LokiBot)
- There might be webshells
- Maybe just an open control panel



[redacted]/david/Panel/five/PvqDq929BSx_A_D_M1n_a.php

Be careful, active reconnaissance against an unowned system ~~may be~~ is definitely illegal

C2 Artifacts

- Domain or IP address
- Common directories may yield information of the type if C2/Panel and version.
- Maybe it’s not password protected 🤷‍♀️
- Maybe you have access to the database 🤷‍♀️
- Could be a stage one server, config or executable possibly available

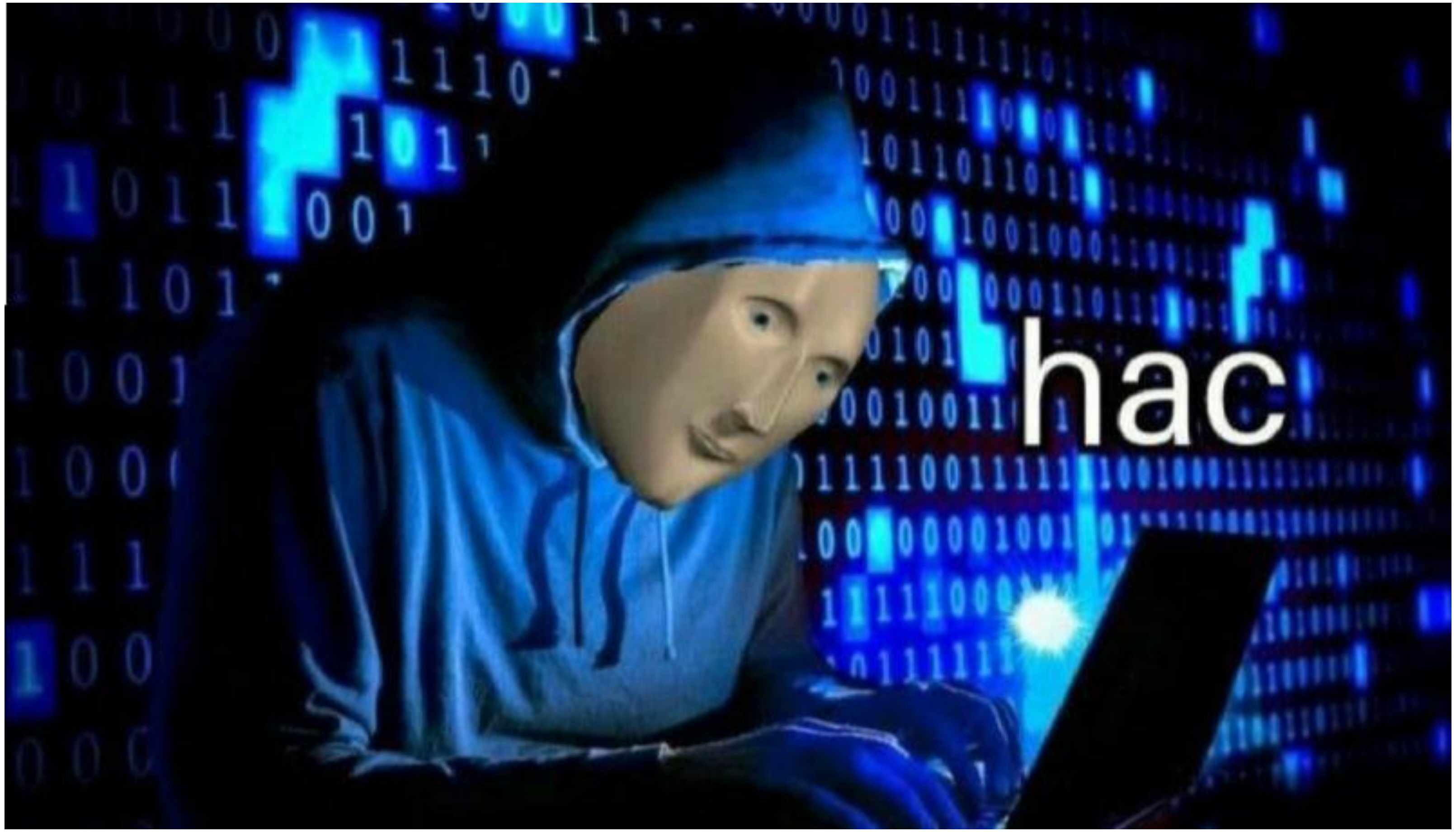
It won’t be that simple

There will be roadblocks the entire way

Obfuscation abound

Shouldn’t be too hard just take your time

But Zach h0w do I be<0m3 31337 H4X0R!?



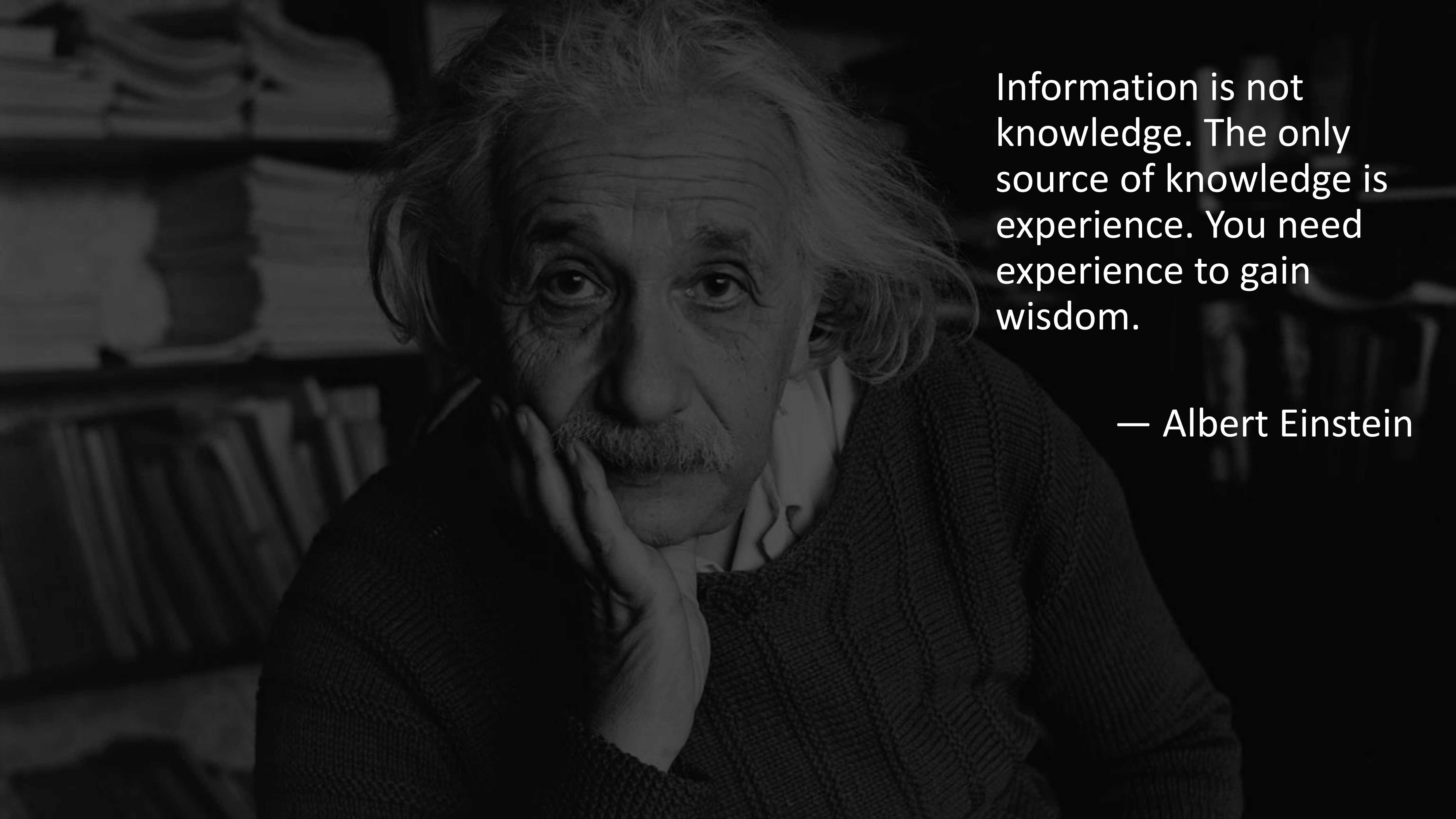
Get güd

Gain skill by doing

Experience is king

Be curious

WANT to know why a thing does a thing



Information is not knowledge. The only source of knowledge is experience. You need experience to gain wisdom.

— Albert Einstein

Emotet - GONE

- Major phishing tactic and initial downloader
- Multi-National effort to take them down
- No elite hacker lair or glowing blinky boxes cycling code on a screen
- Gold bars though

LIVE DEMO