



DETECTING THE HUMAN

An Introduction to User-Interaction Detection in Malware

Kyle Cucci, Malware Researcher

ABOUT ME

- ▶ A human.
- ▶ For Fun -> Malware Researcher
- ▶ For Profit -> Cyber security @ Bank

Twitter: @d4rksystem

LinkedIn: <https://www.linkedin.com/in/kylecucci>



DETECTING HUMANS – WAIT, BUT WHY?

Why would malware want to detect human interaction?

- ▶ *To sense if the target system is actively being used by a real person.*
- ▶ *To determine if the target system is a malware sandbox or analysis lab.*
- ▶ *To gather information and identify human behavior patterns.*

TIP: This type of technique is sometimes called a “Reverse-Turing Test”!



TECHNIQUE 1: DETECT MOUSE AND KEYBOARD INTERACTION

Objective:

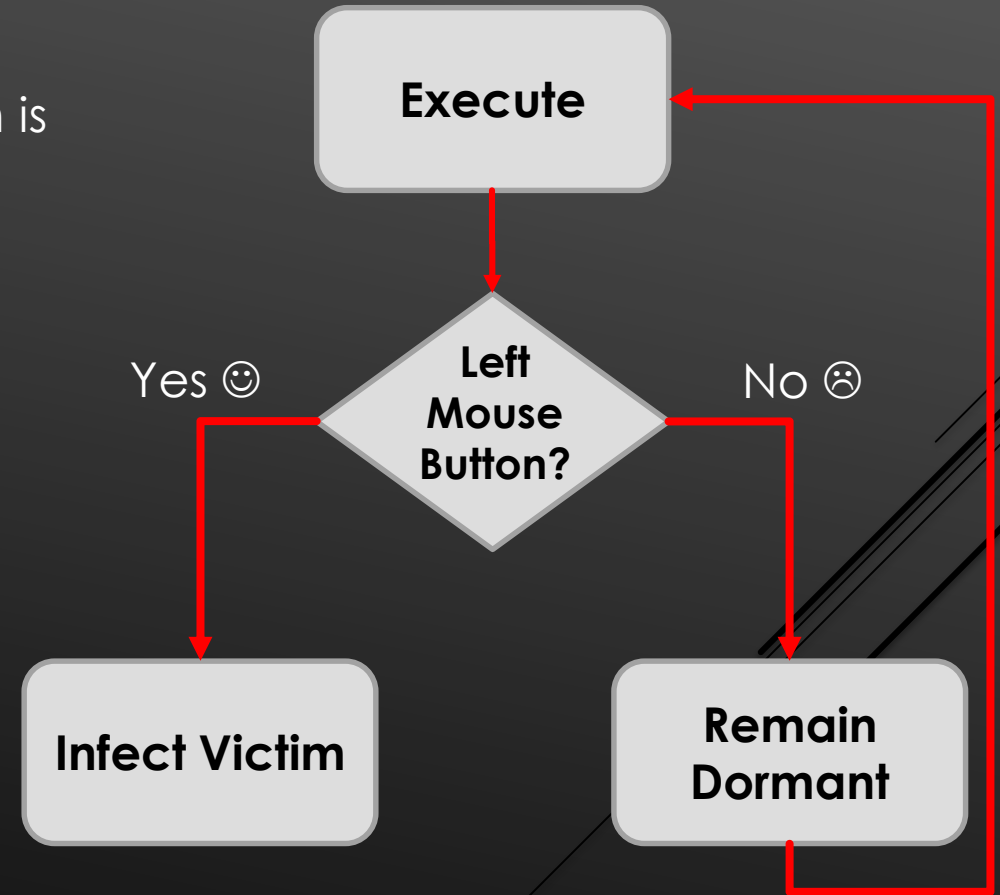
- ▶ Sense device interaction and test if the victim system is “real”.

Example Methods:

- ▶ `GetCursorPos` – Returns the current mouse cursor coordinates.
- ▶ **`GetAsyncKeyState`** – Checks on the state of mouse/keyboard buttons. →

Example Malware:

- ▶ “UpClicker”



TECHNIQUE 1: DETECT MOUSE AND KEYBOARD INTERACTION

Objective:

- ▶ Sense device interaction and test if the victim system is “real”.

Example Methods:

- ▶ **GetCursorPos** – Returns the current mouse cursor coordinates. →
- ▶ **GetAsyncKeyState** – Checks on the state of mouse/keyboard buttons.

Example Malware:

- ▶ “UpClicker”

```
GetCursorPos (&CursorPos1)
Sleep (5)
GetCursorPos (&CursorPos2)

if (CursorPos1 == CursorPos2)
    TerminateProcess ()
```

TECHNIQUE 2: CHECK OPEN WINDOWS

Objective:

- ▶ Detect or locate open Windows.

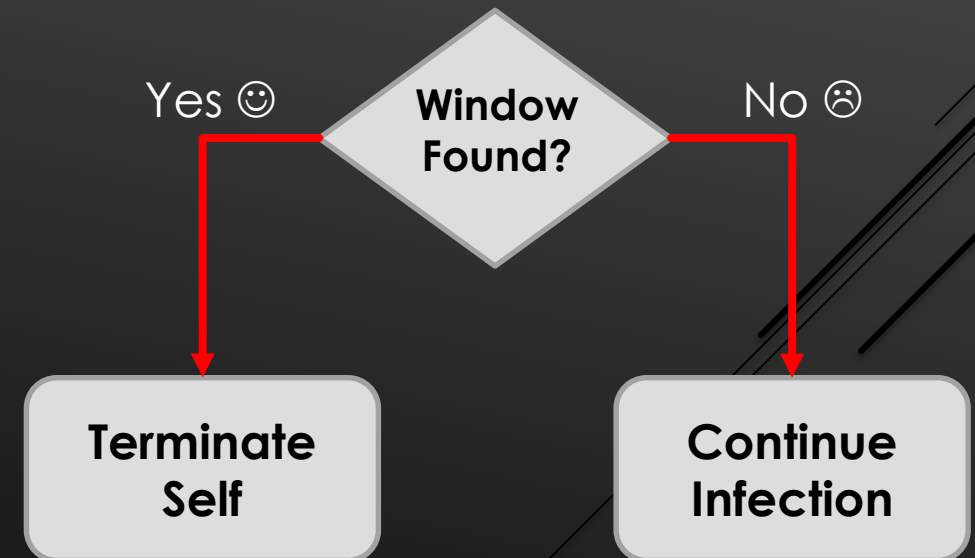
00402DA2	56	push esi	
00402DA3	50	push eax	eax: L"OLLYDBG"
00402DA4	FFD7	call edi	call FindWindowW
00402DA6	85C0	test eax, eax	eax: L"OLLYDBG"
00402DA8	0F85 B3020000	jne ev11.403061	

Example Methods:

- ▶ GetForegroundWindow – Returns a handle to the foreground window.
- ▶ **FindWindow** – Locates a specific window via its name. →
- ▶ EnumWindow – Enumerates open windows.

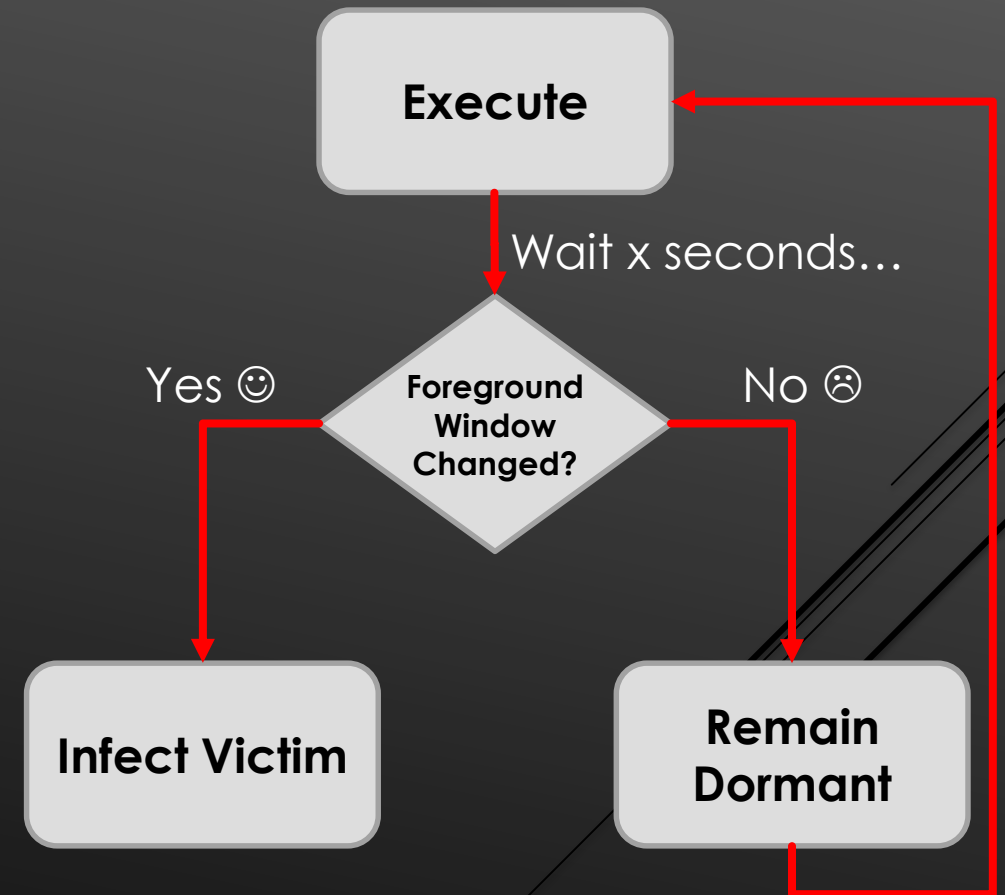
Example Malware:

- ▶ Satan (Ransomware)
- ▶ GuLoader (Loader)



EXAMPLE: GETFOREGROUNDWINDOW

0045B958	0E82 CB000000	jae evil.45BA28
0045B95E	E8 A5B3FAFF	call <JMP.&GetForegroundWindow>
0045B963	8BD8	mov ebx,eax
0045B965	6A 64	push 64
0045B967	E8 D8F6FAFF	call <JMP.&Sleep>
0045B96C	E8 97B3FAFF	call <JMP.&GetForegroundWindow>
0045B971	8BF8	mov esi,eax
0045B973	8BC3	mov eax,ebx
0045B975	33D2	xor edx,edx
0045B977	52	push edx
0045B978	50	push eax
0045B979	8D45 FC	lea eax,dword ptr ss:[ebp-4]
0045B97C	E8 3BCBFAFF	call evil.40848C
0045B981	8B45 FC	mov eax,dword ptr ss:[ebp-4]
0045B984	E8 5B8DFAFF	call evil.4046E4
0045B989	50	push eax
0045B98A	E8 29AFFAFF	call <JMP.&OutputDebugStringA>
0045B98F	3BF3	cmp esi,ebx
0045B991	74 D2	je evil.45B965



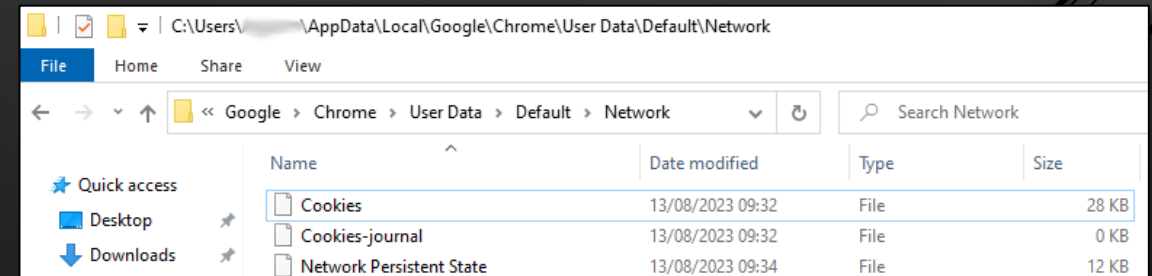
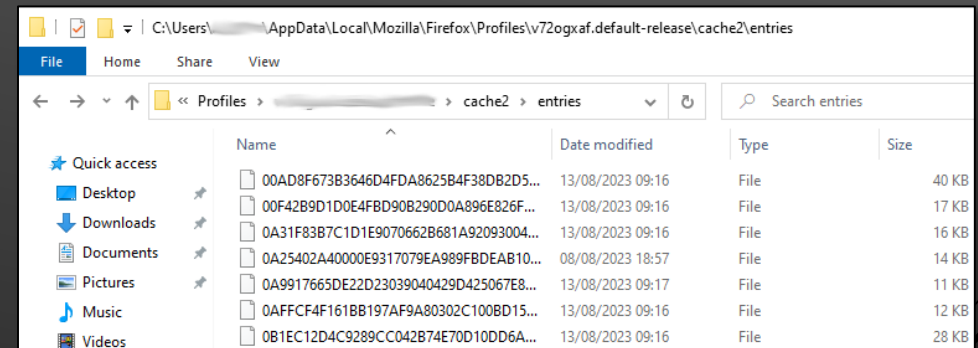
TECHNIQUE 3: COLLECT BROWSER DATA

Objective:

- ▶ Enumerate browser data (humans use browsers! Sandboxes don't..)

Example Methods:

- ▶ Enumerate and verify cookies.
- ▶ Enumerate and verify cache data.
- ▶ Enumerate and verify browsing history



TECHNIQUE 4: SENSING USAGE OF MS OFFICE

Objective:

- ▶ Sense active usage of MS Office applications (real humans interact with MS Office!)

Example Methods:

- ▶ Check if user is scrolling the document.
- ▶ Execute malicious code only on a certain action. →

Example Malware:

- ▶ Various stage 1 droppers/downloaders.

Macro name	When it runs
AutoExec	When you start Word or load a global template
AutoNew	Each time you create a new document
AutoOpen	Each time you open an existing document
AutoClose	Each time you close a document
AutoExit	When you exit Word or unload a global template

Source: MSDN

OTHER INTERESTING TECHNIQUES

- ▶ Check if default wallpaper has been changed.
- ▶ Query the system's uptime →
- ▶ Check Office recent files
 - ▶ "C:\Documents and Settings\<user>\Application Data\Microsoft\Office\Recent"

0x10D1A = ~1 minute

76562A3F	CC	int3	EAX	00010D1A
76562A40	51	push ecx	EBX	04FEF000
76562A41	FF15 84185C76	call dword ptr ds:[&GetTickCount]	ECX	00C0FB20 "ès\x07"
76562A47	59	pop ecx	EDX	000005A0 L"
76562A48	C3	ret	EBP	008FFE34 &" p t"
76562A49	CC	int3		

SIMPLE WAYS TO BE A HUMAN



Move the mouse and click all the buttons.



Open, change, and use applications.



Populate the browser cache and history.



Create fake files in Desktop, Documents, etc.

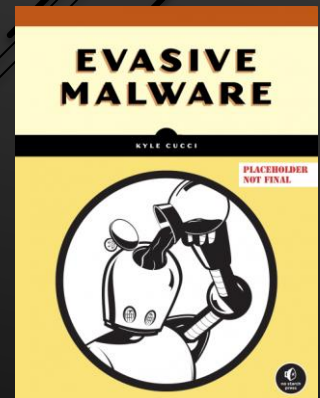


"Fake" system uptime.



REFERENCES AND FURTHER READING

- ▶ **UpClicker Malware** - <https://threatpost.com/upclicker-trojan-evades-sandbox-detection-hiding-mouse-click-121412/77320/>
- ▶ **GuLoader Malware** - <https://www.crowdstrike.com/blog/guloader-dissection-reveals-new-anti-analysis-techniques-and-code-injection-redundancy/>
- ▶ **The UnProtect Project** - <https://unprotect.it/>
- ▶ My Book - “**Evasive Malware: Understanding Deceptive and Self-Defending Threats**” from No Starch Press. Release early 2024 😊






BONUS: HOW WOULD CHAT-GPT DETECT A HUMAN?



What are some funny ways malware may try to detect if it is in a sandbox?



Certainly, let's approach this from a purely fictional and humorous perspective, while keeping in mind the ethical considerations. Here are some whimsical ways malware might attempt to detect if it's in a sandbox environment:   

- ▶ The malware spawns a chat interface and tells funny jokes. If the malware receives an "LOL" in the chat, the malware assumes the victim is a real person and not a sandbox.
- ▶ The malware generates a virtual crossword puzzle, with the answers being malware analysis terms. If the malware receives the right answers, it assumes the system is owned by a malware analyst.
- ▶ The malware spawns a virtual pet that requires constant attention and care. If it notices that the pet's happiness level remains consistently high, it is not in a sandbox.