ID: 764036
Sample Name: 6k00SOeMjU.dll
Cookbook: default.jbs
Time: 10:59:19
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

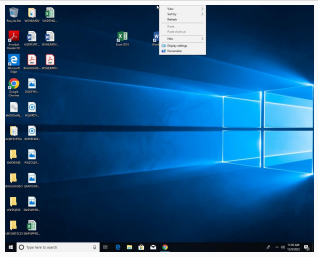
Windows Analysis Report

6k00SOeMjU.dll

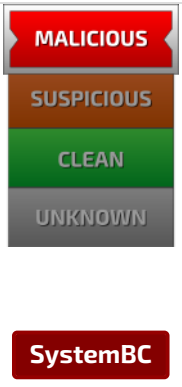
Overview

General Information

Sample Name:	6k00SOeMjU.dll
Analysis ID:	764036
MD5:	0d079a931e42f5..
SHA1:	d5f1ab52221019..
SHA256:	ead2c5aaf92fe07..
Tags:	32 dll exe
Infos:	



Detection



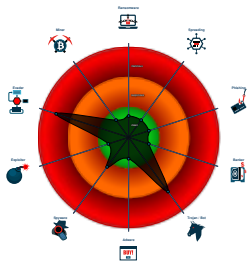
SystemBC

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Yara detected SystemBC
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Hides threads from debuggers
- Overwrites code with unconditional j…
- Overwrites code with function prolog…
- Tries to evade analysis by executio…
- Tries to detect virtualization through…
- PE file contains section with specia…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5308 cmdline: loaddll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 5264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4080 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2064 cmdline: rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5160 cmdline: rundll32.exe C:\Users\user\Desktop\6k00SOeMjU.dll,rundll MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5336 cmdline: rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",rundll MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.646021570.0000000010005000.00000004.00000001.01000000.00000003.sdmp	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x173:$sx1: -WindowStyle Hidden -ep bypass -file • 0x0:$sx2: BEGINDATA • 0x1af:$sx3: GET %s HTTP/1.0 • 0x1ca:$s5: User-Agent: • 0x11b:$s8: ALLUSERSPROFILE
00000003.00000002.645972498.0000000010005000.00000004.00000001.01000000.00000003.sdmp	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x173:$sx1: -WindowStyle Hidden -ep bypass -file • 0x0:$sx2: BEGINDATA • 0x1af:$sx3: GET %s HTTP/1.0 • 0x1ca:$s5: User-Agent: • 0x11b:$s8: ALLUSERSPROFILE

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000005.00000002.646001533.0000000010005000.00000004.00000001.01000000.00000003.sdmp	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x173:$sx1: -WindowStyle Hidden -ep bypass -file • 0x0:$sx2: BEGINDATA • 0x1af:$sx3: GET %s HTTP/1.0 • 0x1ca:$s5: User-Agent: • 0x11b:$s8: ALLUSERSPROFILE
Process Memory Space: rundll32.exe PID: 5160	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x33c2:$sx1: -WindowStyle Hidden -ep bypass -file • 0x34dd:$sx1: -WindowStyle Hidden -ep bypass -file • 0x32e8:$sx2: BEGINDATA • 0x3325:$sx2: BEGINDATA • 0x33fe:$sx3: GET %s HTTP/1.0 • 0x3516:$sx3: GET %s HTTP/1.0 • 0x3419:$s5: User-Agent: • 0x2b21:$s8: ALLUSERSPROFILE • 0x336a:$s8: ALLUSERSPROFILE • 0x348c:$s8: ALLUSERSPROFILE • 0x62de:$s8: ALLUSERSPROFILE • 0x6300:$s8: ALLUSERSPROFILE
Process Memory Space: rundll32.exe PID: 5160	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.10000000.0.unpack	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x2f54:$sx1: -WindowStyle Hidden -ep bypass -file • 0x2de1:$sx2: BEGINDATA • 0x2f90:$sx3: GET %s HTTP/1.0 • 0x2fab:$s5: User-Agent: • 0x2efc:$s8: ALLUSERSPROFILE
4.2.rundll32.exe.10000000.0.unpack	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	
4.2.rundll32.exe.10000000.0.unpack	MALWARE_Win_EXEPWSH_DLAgent	Detects SystemBC	ditekSHen	• 0x2f49:$pwsh: powershell • 0x2f90:$s1: GET %s HTTP/1 • 0x2fab:$s2: User-Agent: • 0x2f54:$s3: -WindowStyle Hidden -ep bypass -file " • 0x2f85:$s4: LdrLoadDll • 0x2de1:$v1: BEGINDATA • 0x2deb:$v2: HOST1: • 0x2e1e:$v2: HOST2: • 0x2e51:$v3: PORT1: • 0x2e5d:$v4: TOR: • 0x2ef6:$v6: start
3.2.rundll32.exe.10000000.0.unpack	EXT_MAL_SystemBC_Mar22_1	Detects unpacked SystemBC module as used by Emotet in March 2022	Thomas Barabosch, Deutsche Telekom Security	• 0x2f54:$sx1: -WindowStyle Hidden -ep bypass -file • 0x2de1:$sx2: BEGINDATA • 0x2f90:$sx3: GET %s HTTP/1.0 • 0x2fab:$s5: User-Agent: • 0x2efc:$s8: ALLUSERSPROFILE
3.2.rundll32.exe.10000000.0.unpack	JoeSecurity_SystemBC	Yara detected SystemBC	Joe Security	
Click to see the 4 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

System process connects to network (likely due to code injection or exploit)

System Summary

Malicious sample detected (through community Yara rule)

PE file contains section with special chars

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Overwrites code with function prologues

Malware Analysis System Evasion

Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected SystemBC

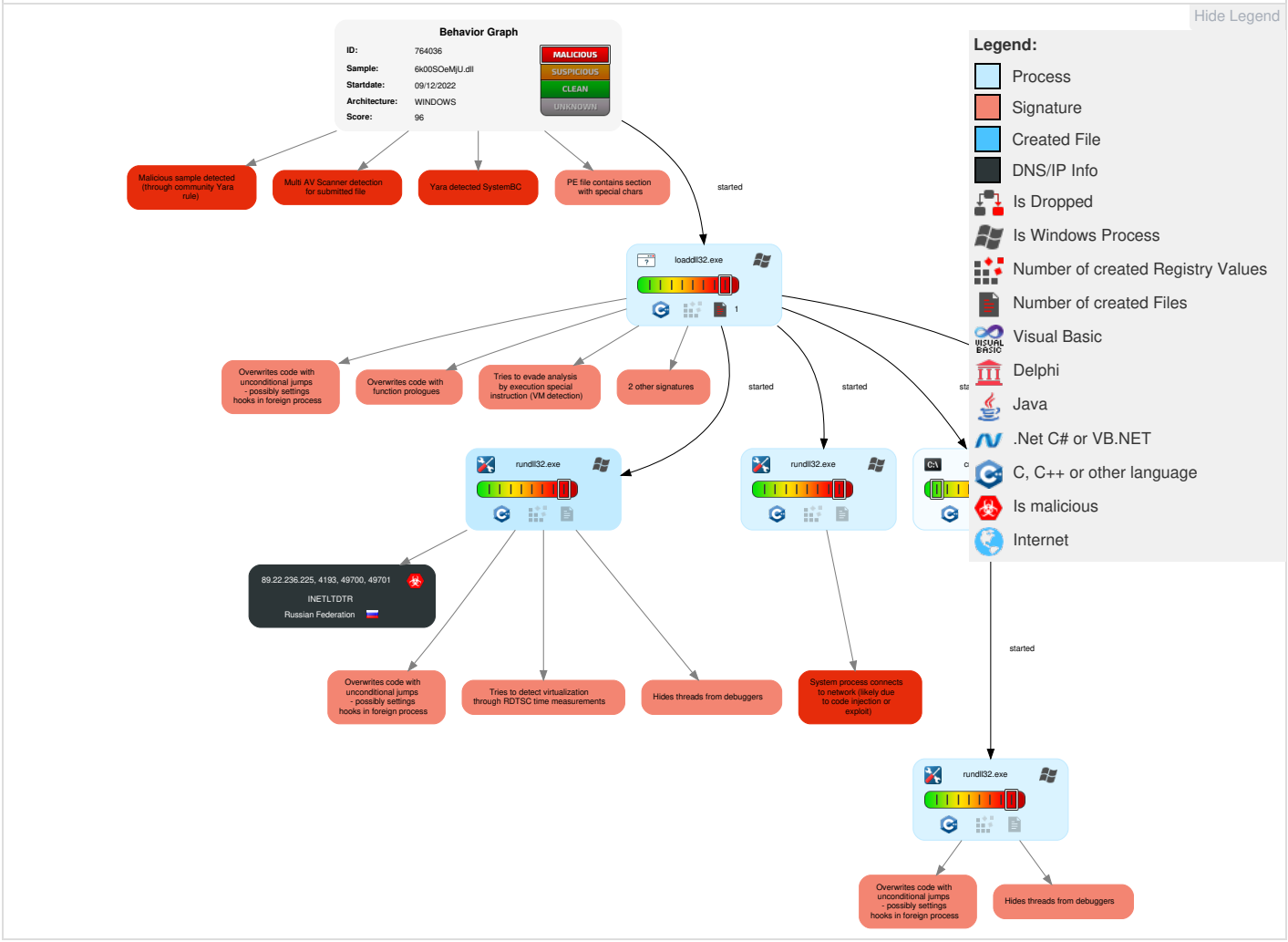
Remote Access Functionality

Yara detected SystemBC

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Rundll32	1 Credential API Hooking	3 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	1 2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	2 1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

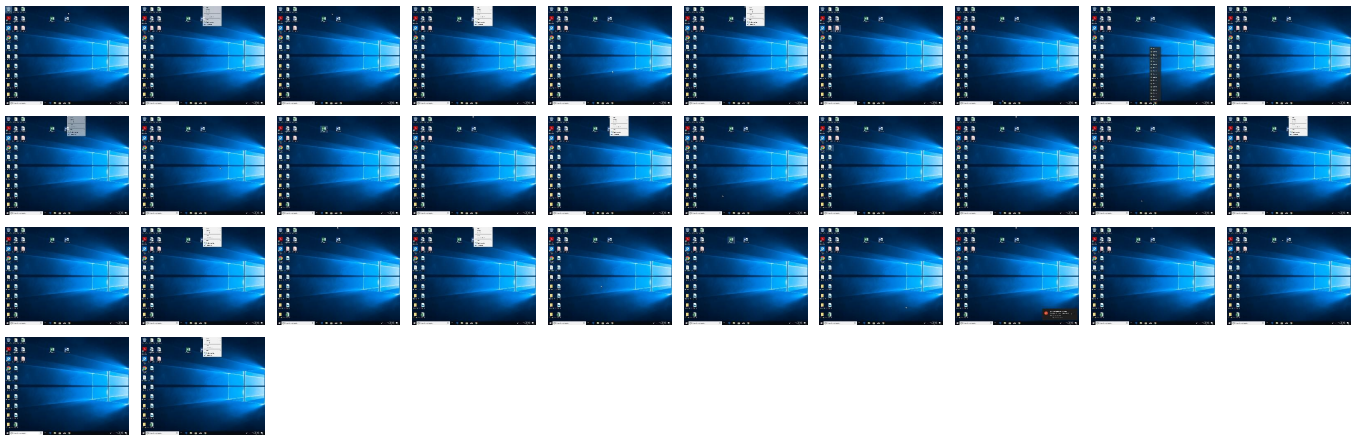
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
6k00SOeMjU.dll	17%	Virustotal		Browse
6k00SOeMjU.dll	23%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.innosetup.com	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	

Domains and IPs

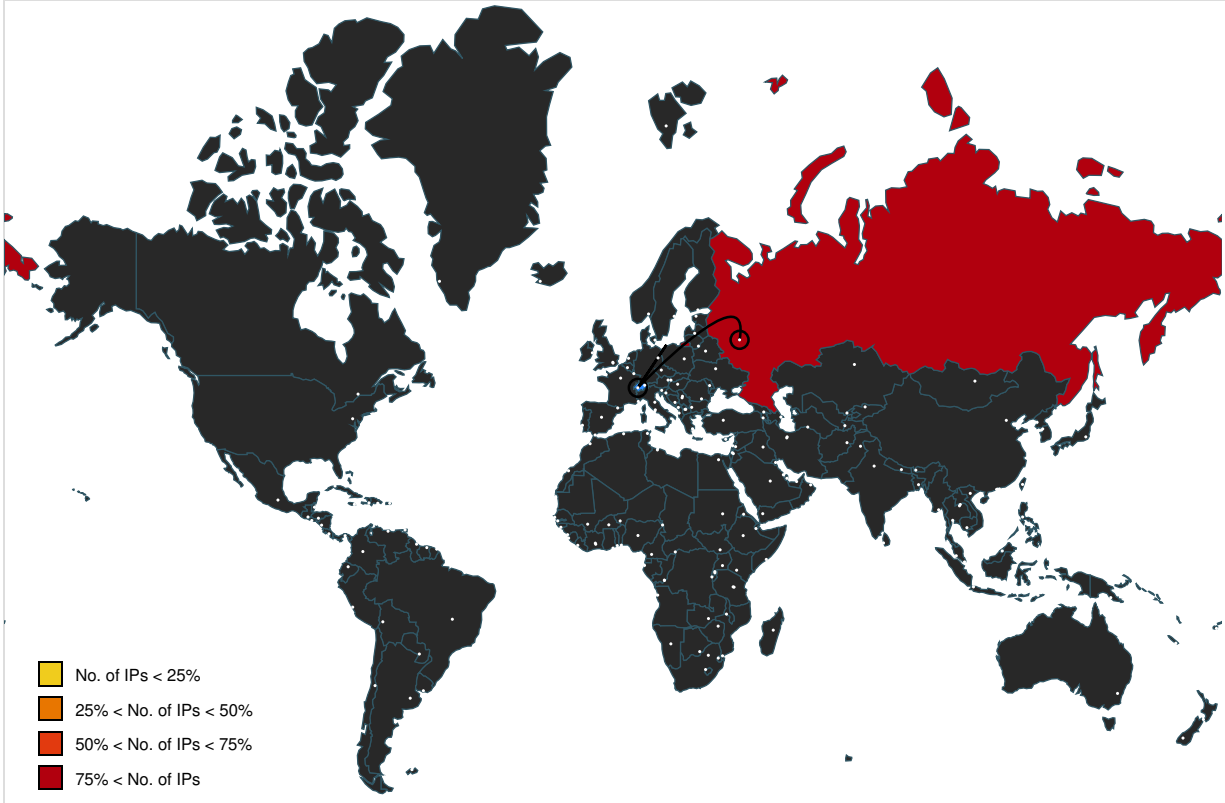
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	6k00SOeMjU.dll	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	6k00SOeMjU.dll	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	6k00SOeMjU.dll	false	• URL Reputation: safe	unknown
http://www.innosetup.com	rundll32.exe, 00000003.00000002.65181907 6.0000000010B69000.00000002.00000001.010 00000.00000003.sdmp, rundll32.exe, 00000 004.00000002.651817589.0000000010B69000. 00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000005.00000002.651818549.000000 0010B69000.00000002.00000001.01000000.00 000003.sdmp, 6k00SOeMjU.dll	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	6k00SOeMjU.dll	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.22.236.225	unknown	Russian Federation		197328	INETLTDTR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764036
Start date and time:	2022-12-09 10:59:19 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6k00SOeMjU.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winDLL@10/0@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.976819466268135
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	6k00SOeMjU.dll
File size:	7566544
MD5:	0d079a931e42f554016db36476e55ba7
SHA1:	d5f1ab52221019c746f1cc59a45ce18d0b817496
SHA256:	ead2c5aaf92fe07db45b99587f586c7a45f92c67220cd8113a5d2e7bcb320798
SHA512:	1496f1296df89e1da8780f175631e2551300a99e6c7ea43d2750653fdf6e7ed096fdedd9f0d23b94190ecf418da09cf9c9b6caee5821ba1c457f0294063bbc9e
SSDEEP:	196608:l3ksPqmzcl+LG314Hujb7KgkYCbGNBmHTER:lUON+2HBb8
TLSH:	5776332F16980415E4EECC3A85EBBE9132F5073A9E8278BCA5DA5DC13A354F5B702163
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8.ob.....!....."...@.....=XT.....@.....Ft...../..E..

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x1054583d
Entrypoint Section:	nUPwRZiK
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x626FE238 [Mon May 2 13:52:56 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5

OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	d3a98daa37dbe78969711cc1194ce51b

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=fumbling corp.
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/8/2022 9:12:34 AM 12/8/2023 9:32:34 AM
Subject Chain	• CN=fumbling corp.
Version:	3
Thumbprint MD5:	BFCF38BCEDDC6D492EE1D807C07B0E02
Thumbprint SHA-1:	92A18235585F157E75D33B92CC8E394210AEAD16
Thumbprint SHA-256:	E3FCBA8CB056D8C4B5F3C974DD82C3CD9C96AF2621722C26119E478F35637E99
Serial:	78919934276F458544703D1C7FC21303

Entrypoint Preview
Instruction
push edx
mov edx, 3F442022h
pushfd
xor edx, 7B9D646Dh
xor dl, dl
mov edx, dword ptr [esp+edx-44D943FCh]
mov dword ptr [esp+04h], 8EECC51Ah
push dword ptr [esp+00h]
popfd
lea esp, dword ptr [esp+04h]
call 00007F741533A873h
xchg al, al
pushfd
lahf
shr al, FFFFFF8Fh
shl ah, FFFFFF86h
pop dword ptr [edi]
bt eax, ecx
and ax, 00007B5Bh
xchg al, ah
mov eax, dword ptr [esi]
cmp si, bp
lea esi, dword ptr [esi+00000004h]
xor eax, ebx
jmp 00007F74153F1EF7h
stosb
retf A814h
jmp far 0F97h : 3CD32403h
stosd
enter B68Dh, 01h
add byte ptr [eax], al
add cl, al
loopne 00007F741535E373h
xor cl, bl
btr ax, dx
or ax, bp
not cl
add al, ah

Instruction
bts eax, ebp
sar al, cl
add cl, 0000007Eh
shld ax, si, 00000065h
bts ax, sp
not ah
xor cl, 0000006Bh
cmovno ax, dx
movsx eax, si
rol ax, 0000h
rol cl, 1
cmovno ax, bx
xor bl, cl
movzx eax, dx
lahf
lea edi, dword ptr [edi-00000002h]
btr ax, 0046h
sal al, FFFFFF9Dh
mov word ptr [edi], cx
mov eax, dword ptr [esi]
add esi, 00000004h
jmp 00007F7415286521h
push ebp
ret
rol eax, 1
sub eax, 000066B4h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xaf2fa4	0x45	nUPwRZiK
IMAGE_DIRECTORY_ENTRY_IMPORT	0x660b3c	0x104	nUPwRZiK
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6a000	0x800	K)'tLNvc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x735e00	0x16d0	nUPwRZiK
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb69000	0x5d4	$u!6XeN&
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x433000	0x78	0Ys'"rSd
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
*;>%1sXO	0x1000	0x219c	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
7rP!Ni:j	0x4000	0x845	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
bkE<E2?8	0x5000	0x250	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
8*7`Joyq	0x6000	0x42c264	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
0Ys'"rSd	0x433000	0x4a4	0x600	False	0.06575520833333333	OpenPGP Public Key	0.4141326418166997	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
nUPwRZiK	0x434000	0x734590	0x734600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
$u!6XeN&	0xb69000	0x5d4	0x600	False	0.53515625	data	4.2912698570834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
K)'tLNvc	0xb6a000	0x800	0x800	False	0.44287109375	data	3.8514204088109953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb6a0fc	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	Dutch	Netherlands
RT_GROUP_ICON	0xb6a3e4	0x14	data	Dutch	Netherlands
RT_VERSION	0xb6a3f8	0x408	data	English	United States

Imports

DLL	Import
user32.dll	SendMessageA
kernel32.dll	LocalFree
advapi32.dll	GetSidSubAuthority
wsock32.dll	WSAStartup
shell32.dll	CommandLineToArgvW
ws2_32.dll	freeaddrinfo
ole32.dll	CoUninitialize
secur32.dll	GetUserNameExA
psapi.dll	GetModuleFileNameExA
kernel32.dll	GetSystemTimeAsFileTime
user32.dll	CharUpperBuffW
kernel32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, ExitProcess, LoadLibraryA, GetModuleHandleA, GetProcAddress

Exports

Name	Ordinal	Address
rundll	1	0x1000100c

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
English	United States	

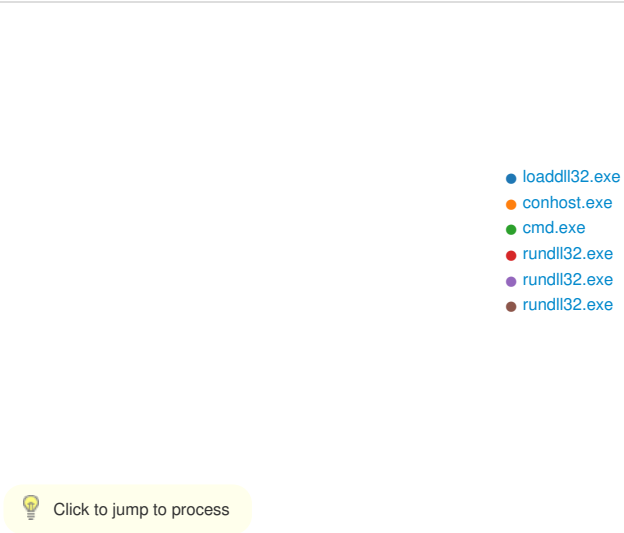
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:00:32.281683922 CET	49700	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:32.307775021 CET	4193	49700	89.22.236.225	192.168.2.3
Dec 9, 2022 11:00:32.307951927 CET	49700	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:32.396655083 CET	49700	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:32.437968969 CET	4193	49700	89.22.236.225	192.168.2.3
Dec 9, 2022 11:00:33.257164001 CET	49701	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:33.283178091 CET	4193	49701	89.22.236.225	192.168.2.3
Dec 9, 2022 11:00:33.283364058 CET	49701	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:33.337862015 CET	49701	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:33.364196062 CET	4193	49701	89.22.236.225	192.168.2.3
Dec 9, 2022 11:00:33.970604897 CET	49702	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:33.996262074 CET	4193	49702	89.22.236.225	192.168.2.3
Dec 9, 2022 11:00:33.996412992 CET	49702	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:34.061677933 CET	49702	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:00:34.087173939 CET	4193	49702	89.22.236.225	192.168.2.3
Dec 9, 2022 11:01:32.937953949 CET	4193	49700	89.22.236.225	192.168.2.3
Dec 9, 2022 11:01:32.938110113 CET	49700	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:01:34.985507011 CET	4193	49702	89.22.236.225	192.168.2.3
Dec 9, 2022 11:01:34.985593081 CET	49702	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:01:34.985784054 CET	4193	49701	89.22.236.225	192.168.2.3
Dec 9, 2022 11:01:34.985846043 CET	49701	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:02:34.379544020 CET	4193	49700	89.22.236.225	192.168.2.3
Dec 9, 2022 11:02:34.379733086 CET	49700	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:02:36.426181078 CET	4193	49701	89.22.236.225	192.168.2.3
Dec 9, 2022 11:02:36.426312923 CET	49701	4193	192.168.2.3	89.22.236.225
Dec 9, 2022 11:02:36.427087069 CET	4193	49702	89.22.236.225	192.168.2.3
Dec 9, 2022 11:02:36.427201033 CET	49702	4193	192.168.2.3	89.22.236.225

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5308, Parent PID: 3452

General

Target ID:	0

Start time:	11:00:15
Start date:	09/12/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll"
Imagebase:	0xa0000
File size:	116736 bytes
MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5264, Parent PID: 5308

General

Target ID:	1
Start time:	11:00:16
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 4080, Parent PID: 5308

General

Target ID:	2
Start time:	11:00:16
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5160**, Parent PID: **5308**

General	
Target ID:	3
Start time:	11:00:16
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6k00SOeMjU.dll,rundll
Imagebase:	0xad0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000003.00000002.645972498.0000000010005000.00000004.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2064**, Parent PID: **4080**

General	
Target ID:	4
Start time:	11:00:16
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1
Imagebase:	0xad0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000004.00000002.646021570.0000000010005000.00000004.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security
Reputation:	high

Analysis Process: rundll32.exe PID: **5336**, Parent PID: **5308**

General	
Target ID:	5
Start time:	11:00:21
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",rundll
Imagebase:	0xad0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000005.00000002.646001533.0000000010005000.00000004.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security

Reputation:	high

Disassembly

No disassembly