

JOeSandbox Cloud BASIC



ID: 561346

Sample Name: 9u4xTDR5bG

Cookbook: default.jbs

Time: 11:27:47

Date: 27/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 9u4xTDR5bG	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	4
AV Detection	4
Networking	4
Data Obfuscation	4
Malware Analysis System Evasion	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	7
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
URLs from Memory and Binaries	7
World Map of Contacted IPs	7
General Information	7
Warnings	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	8
C:\Users\user\AppData\Local\Temp\gamer.txt	9
C:\Users\user\AppData\Local\Temp\nsm4CBF.tmp\System.dll	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Authenticode Signature	10
Entrypoint Preview	10
Rich Headers	11
Data Directories	11
Sections	12
Resources	12
Imports	12
Version Infos	13
Possible Origin	13
Network Behavior	13
Statistics	13
System Behavior	13
Analysis Process: 9u4xTDR5bG.exePID: 3224, Parent PID: 396	13
General	13
File Activities	14
File Created	14
File Deleted	15
File Written	15
File Read	16
Disassembly	16

Windows Analysis Report

9u4xTDR5bG

Overview

General Information

Sample Name:	9u4xTDR5bG (renamed file extension from none to exe)
Analysis ID:	561346
MD5:	82c5cdde9df0a7...
SHA1:	7b391b4429dfb1..
SHA256:	243ae30d42e900..
Tags:	32 exe signed trojan
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected GuLoader

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Uses 32bit PE files

Drops PE files

Contains functionality to read the PE...

Contains functionality to shutdown /...

Uses code obfuscation techniques (...)

Detected potential crypto function

PE / OLE file has an invalid certifica...

Classification

Process Tree

- System is w10x64
- 9u4xTDR5bG.exe (PID: 3224 cmdline: "C:\Users\user\Desktop\9u4xTDR5bG.exe" MD5: 82C5CDDE9DF0A76E2933C1CD8BFC7887)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  
  "Payload URL": "https://bangladeshshoecity.com/images/2w"  
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.764364094.0000000002A50000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Networking



C2 URLs / IPs found in malware configuration

Data Obfuscation



Yara detected GuLoader

Malware Analysis System Evasion

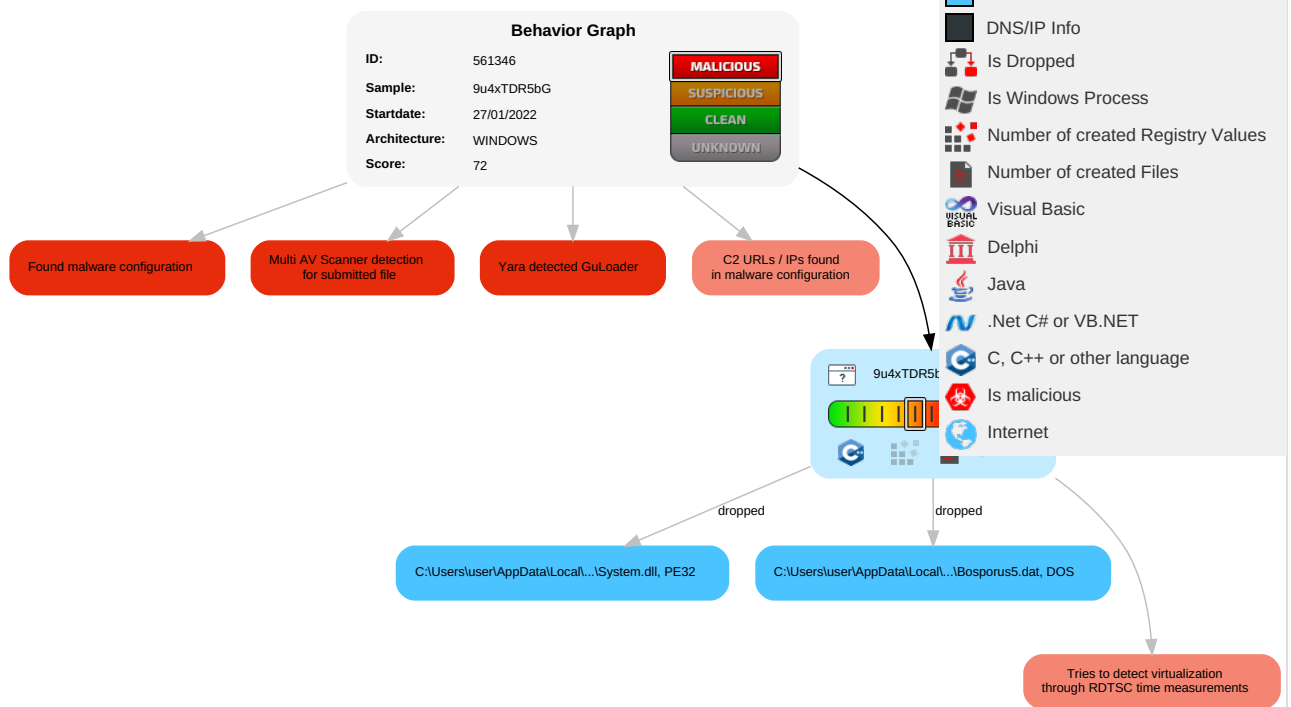


Tries to detect virtualization through RDTSC time measurements

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	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	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

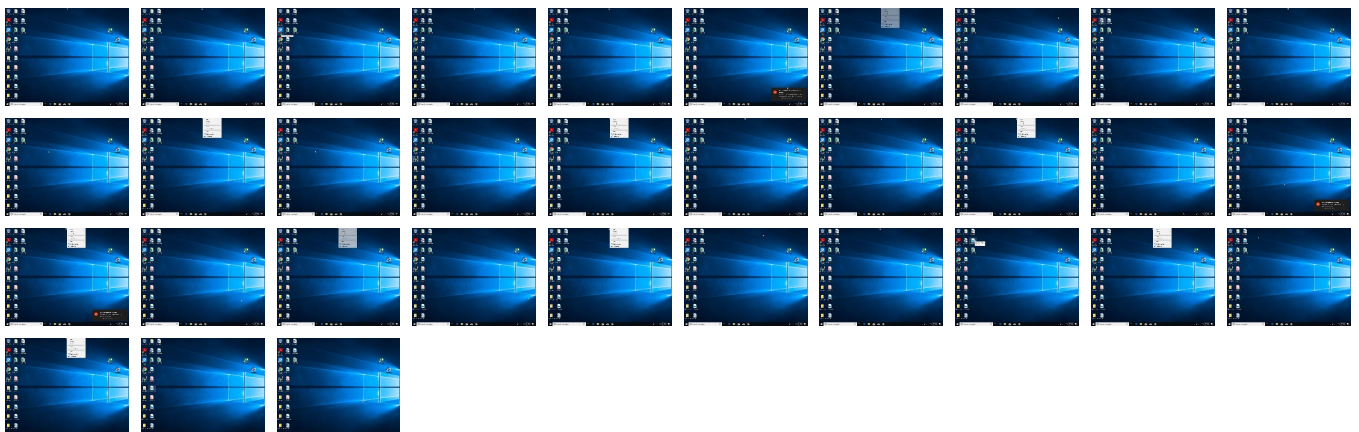
Behavior Graph



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
9u4xTDR5bG.exe	31%	Virustotal		Browse
9u4xTDR5bG.exe	11%	Metadefender		Browse
9u4xTDR5bG.exe	44%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Insm4CBF.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Insm4CBF.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

⊘ No Antivirus matches

Domains

⊘ No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://https://bangladeshshoecity.com/images/2w	0%	Avira URL Cloud	safe	

Domains and IPs
Contacted Domains
 No contacted domains info

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://bangladeshshoecity.com/images/2w	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	9u4xTDR5bG.exe	false		high

World Map of Contacted IPs
 No contacted IP infos

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	561346
Start date:	27.01.2022
Start time:	11:27:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9u4xTDR5bG (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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:	mal72.troj.evad.winEXE@1/3@0/0
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 40.2% (good quality ratio 39.6%) - Quality average: 86.9% - Quality standard deviation: 21.2%
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0

Cookbook Comments:

- Adjust boot time
- Enable AMSI
- Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, displaycatalog.mp.mi crosoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.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

C:\Users\user\AppData\Local\Temp\Bosporus5.dat



Process:	C:\Users\user\Desktop\9u4xTDR5bG.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	33702
Entropy (8bit):	7.640543622166051
Encrypted:	false
SSDEEP:	768:1FwMrbBIFp7y+OzxSaYStTVsui/XXjqC4iYBnDyvfWjbx0K:nwMrbnFp7y1wJSJVsPGChMevOF
MD5:	2C2658C12C970777B7D352045683823D
SHA1:	6EEDC661A65C91EBF2F0CB013ED683CFD704757E
SHA-256:	2514D174967C285492114476DC13AAABBB4248A756770BDD2B60117EE347752
SHA-512:	C6778168D222A85C58B7FE38AD81E96413D05DA70603130B74454ACB9A2CA759E8707F71CAEFD1DC16ECF8F4F419A9C4171814D346297280DF78DB0786F8667
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%

Reputation:	low
Preview:	._?_u...u...u.....o...lt...s..svu...3...B].*...W...o...Z1..4..u.N...9.u.W.....N..U...t.....2D.B.h....R..D..b..K7\$"jX[...1...a.....^W....oz.'.Ut'..7.Hg..G....pY...3n...u.).\4.....ugUB...'.vw._@_iPr..v.5...8.l.....F..W...8..k)...M.c.P.....O...!b...!G.A.....m.....]S5.....Jl.s8<K.w.<G...g.<.....7)...<.M...5.&.....!A...N..\{X...P....bt.N.u.N...>..u.NH....V.j...w.N.....0.Lu...N....[X.j....A.g.w.H.iFwX..vo...T/u...!N.O...L.cic.Ev/({.N..P...R..#.@..-).u.w..\u..._u..9.N.....L.u.O...N.u1.Pu.jQ_...ZQ.5>o}).cX::}.2S X").....I6..l.?B.r'.N.-.AX.....X..\...L...t.e...~...'.N..^G....!r^w...Xz.w.r...j..i..A.....t....2.5.l.1~.F..d..4..XJ..jZ0..k)p.....Xz.Qv.J..j.\$D..N..u&....kO.ub..YW..qlj...Z.(.l})...ZZ..2.k0...p...&R.t.N.<.....v.P..j&d..Fz..@.....SOF&..6...%..`7yDP.....O.u`G.....(.).5...\$R..t.NF#U...l0,u...J.5...z.....l.z.[Fc"TZe...*%R.Pw

C:\Users\user\AppData\Local\Temp\gamer.txt	
Process:	C:\Users\user\Desktop\9u4xTDR5bG.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16555
Entropy (8bit):	5.9518641421213605
Encrypted:	false
SSDEEP:	384:HpBOK6soHG6Nun3UPBApXPE8eMag91API7ee872UmLZ7:HmkfOG6NNyp/dn19N7U71mLZ
MD5:	695A2030432B3D981B012A42EDCA055A
SHA1:	31283CF8F970E22E7C9B6FCB811B9C1608997211
SHA-256:	F0568B8400FE6F4621B3E62C56B3C3AB9712DD6D30966A348EB3497ACF6B226A
SHA-512:	0095FE21135FCCB9C5723D583C2087FB9D9CD61CB90BB5C96E11EA76469A3744B7F068B7301F7342AF95642D18921763B250FBB9E8F16F5CC9124300E6A97C5C
Malicious:	false
Reputation:	low
Preview:	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4lRaWjctEH1l3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5n xMeoxlojgOUJAvAZef0Nak7gm0ix8xSE70QeFJMfJjvEAWRFFftZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NACxJ4DHeCdzb6hW8i8 otpHEpw0OGDSzOwMI9VcfHuXxhaw0zVcWRcWKg1sABn5d7OrJ2xhlYvPjqrY5w7z8FN0FgE8XtOgiSbRGn0toQLHc2vjr52VFWESFWMUHsKSZfQ4Pbqkill zeyL0vDdo44fuucajegzqku9brw7f8p9R2zFXqoBphSkPzHY6XmnyhU3WyDWzX4CroF6xRQXhjjk7OqKFaLu4ORq54CnRXdgGfPhd7dzPgYFqxUkZaqo2ckBxUeh3QLr4p 1ievUJewtab3AdAT2kjQDq4NVPoAQ5jJvQkApXm49qXhPrrU2YzKVhY5ajHSj55DsleOSI066y24ayag5YtldlInpkasB3iqzZiXwJJSOwZVHVJGChfSumllKT835iwi6 k9utWFP5wlpTCqM6CflHh1JSg5HTMqV8fq5VseXa9XzYpdeJu9OBtsanwwES7WtQoLDnmScaolfCjrlqw61PPDM8QEGM14KrtcVF5ERKQSh6jPyKwNObsN9T s4FbeSzqr0KnDMekc8p8tRrSRckLbRBA58jfVkjWjcQeuGU8J8gr9f2EG5bdrGEds4pfOwG1TGJcUCr6T8jH9Q82m4wdSeL3wJD5rHYJN0ESkrvn77s4vH90F55tPEmd6Z jNlnCzW2BOZfhfO10qnfhHa7ZhuyiWVf05P6uzThDVcRpFtjJVtGcBTjxS6LEiUlof2CsVigpyEGuXekStdPsfIqGf5sMzMxKIDJc6mtYp7glqQODeycT

C:\Users\user\AppData\Local\Temp\nsm4CBF.tmp\System.dll 	
Process:	C:\Users\user\Desktop\9u4xTDR5bG.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWtIt70m5Aj/IQ0sEWD/wtYbBHFNaDybc7y+XBz0QPi:FHQIt70mij/IQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501F866F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......qr*.5.D.5.D...J.2.D.5.E.!D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L...Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text... ..".....`..rdata..c....@.....&.....@..@.data...x...P.....*.....@...reloc.....`.....@..B.....

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.524133406272662
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	9u4xTDR5bG.exe
File size:	95632

MD5:	82c5cdde9df0a76e2933c1cd8bfc7887
SHA1:	7b391b4429dfbf19030fb49ce750aa3c8b844a6b
SHA256:	243ae30d42e9000b882779fae40e0056eab332b95e2c938446138a80868909e
SHA512:	ee64b01a269422e45a458d9e77151435ecfbdeb96b2c7d80e961f3e4cfbacb9626f2df1cb32790dfa174aa2d517868abd4fd8a9fbed3c5b8feac3dae0a790c7e
SSDEEP:	1536:2/T2X/jN2vxZz0DTHUpouZZbUc6JgjJPQPovf/5AmNHLBH8k29xE+1GI1c:2bG7N2kDTHUpouZZbUc6JgjJ4PKfRAI6
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......1...Pf..Pf..Pf.*_9..Pg.LPf.*_..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon	
	
Icon Hash:	b2a88c96b2ca6a72

Static PE Info	
General	
Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature	
Signature Valid:	false
Signature Issuer:	E=Overorganizes@Unprincipledness.Dy, CN=VRDIOMRAADERNE, OU=Specialprogrammeringer1, O=protoloph, L=Budcykler2, S=Semipiousness8, C=WS
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	1/23/2022 7:50:12 AM 1/23/2023 7:50:12 AM
Subject Chain	E=Overorganizes@Unprincipledness.Dy, CN=VRDIOMRAADERNE, OU=Specialprogrammeringer1, O=protoloph, L=Budcykler2, S=Semipiousness8, C=WS
Version:	3
Thumbprint MD5:	A0E586DC6F36D2B05AA723846EDECA3F
Thumbprint SHA-1:	5930C7EB1C7523DFDABC8145BE3CB723E4CA4F29
Thumbprint SHA-256:	B0DA08480B8FCBD3467A408ABC7F8FC17E3386E77474C654BDF4633441981F3A
Serial:	00

Entrypoint Preview	
Instruction	
push ebp	
mov ebp, esp	
sub esp, 000003F4h	
push ebx	
push esi	
push edi	
push 00000020h	
pop edi	
xor ebx, ebx	

Instruction
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F151CB8E85Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F151CB8E82Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers
Programming Language: [EXP] VC++ 6.0 SP5 build 8804

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4c000	0xe28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x160d8	0x14b8	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x8000	0x2b0	.rdata
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
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0xe28	0x1000	False	0.378662109375	data	4.00654037497	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources						
Name	RVA	Size	Type	Language	Country	
RT_ICON	0x4c208	0x2e8	data	English	United States	
RT_DIALOG	0x4c4f0	0x100	data	English	United States	
RT_DIALOG	0x4c5f0	0x11c	data	English	United States	
RT_DIALOG	0x4c710	0xc4	data	English	United States	
RT_DIALOG	0x4c7d8	0x60	data	English	United States	
RT_GROUP_ICON	0x4c838	0x14	data	English	United States	
RT_VERSION	0x4c850	0x294	data	English	United States	
RT_MANIFEST	0x4cae8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States	

Imports	
DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos	
Description	Data
LegalCopyright	Lesney Products
FileVersion	1.2.1
CompanyName	Lesney Products
LegalTrademarks	Lesney Products
Comments	Lesney Products
ProductName	Lesney Products
FileDescription	Lesney Products
Translation	0x0409 0x04b0

Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior
 No network behavior found

Statistics
 No statistics

System Behavior	
Analysis Process: 9u4xTDR5bG.exe PID: 3224, Parent PID: 396	
General	
Target ID:	0
Start time:	11:28:45
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\9u4xTDR5bG.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9u4xTDR5bG.exe"
Imagebase:	0x400000
File size:	95632 bytes
MD5 hash:	82C5CDDE9DF0A76E2933C1CD8BFC7887
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.764364094.0000000002A50000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp\	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user\AppData\Local\Temp\insl4A9B.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	40609B	GetTempFileNameW	
C:\Users	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user\AppData	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user\AppData\Local\Temp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	406059	CreateFileW	
C:\Users\user\AppData\Local\Temp\gamer.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	406059	CreateFileW	
C:\Users\user\AppData\Local\Temp\insm4CBF.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	40609B	GetTempFileNameW	
C:\Users	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	
C:\Users\user\AppData	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\insm4CBF.tmp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\insm4CBF.tmp\System.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\insm4CBF.tmp\System.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	object name collision	5	406059	CreateFileW

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\insl4A9B.tmp				success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\insm4CBF.tmp				success or wait	1	405C78	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	0	17955	fd 5f 5f fd 3f fd 75 0e fd 7f 03 00 75 08 fd 7f 04 00 75 02 fd c1 fd 00 03 00 00 fd fd 6f 01 00 00 fd 49 74 c1 fd 10 9c 73 fd fd 73 76 75 1e fd fd 04 33 0c fd fd fd 7f 42 5d fd fd 2a fd fd fd 57 fd fd 6f 01 00 00 5a 31 fd fd 34 07 2e 75 fd 4e fd fd fd 04 39 fd 75 fd 57 fd fd fd fd fd cf fd 4e 2e fd 55 fd 2d fd 74 20 04 fd fd 12 fd 32 44 16 42 fd 68 14 0b 0c fd 52 fd 7f 44 0f 1b 62 1d 17 4b 37 24 22 6a 58 5b 2c fd fd c5 31 fd fd fd 61 03 fd fd 01 fd ba fd fd 5e 57 10 fd 14 fd 04 6f 7a fd 27 fd 55 74 fd 27 fd fd 37 fd 48 67 fd fd 47 fd fd fd 0d fd 70 59 fd fd 33 6e 1a 3a fd 75 11 fd 29 fd ef 5c 10 34 fd 1f fd fd fd fd 75 67 55 42 fd fd 06 60 fd fd 76 77 fd 40 5f 69 50 72 9e fd 76 19 35 fd fd fd 38 fd 6c	__?uuuoltssvu3B]*WoZ14.uN9uWN.U-t2DBhRDbK7\$"jX[,1a^Woz'Ut'7HgGpY3n:u)\4ugUB`vw@_iPrv58l	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gamer.txt	0	16555	45 4d 72 38 74 30 48 68 71 37 31 35 52 51 6a 70 56 38 6c 39 4c 6f 6f 55 64 57 4a 67 4d 74 4d 66 32 70 45 38 33 55 32 77 73 73 73 38 31 47 35 4b 4a 46 4c 65 49 58 4d 61 31 54 39 33 48 47 6a 4e 45 62 46 66 79 34 49 52 61 57 6a 63 74 45 48 31 49 33 68 57 47 37 34 77 73 4a 59 64 5a 58 4e 6d 4c 54 71 54 65 6e 76 67 65 63 38 71 70 75 39 38 5a 70 34 58 6c 72 72 41 68 62 75 56 65 50 42 67 35 6e 78 4d 65 6f 78 49 6f 6a 67 6c 4f 75 4a 41 76 41 5a 65 66 30 4e 61 6b 37 67 6d 30 69 78 38 78 53 45 37 30 51 65 46 4a 4d 46 6a 4a 76 45 41 57 52 46 46 46 74 5a 4f 59 6b 63 48 68 43 67 65 77 70 37 59 42 45 38 4f 65 6b 4f 73 4f 72 63 65 78 61 66 52 47 34 41 64 5a 61 57 42 7a 33 79 43 45 34 71 4d 50 30 4e 41 63 78 4a 34 44 48 65 43 64 7a 62 63 36 68 57 38 69 38 6f 74 70 48 45	EMr8t0Hhq715RQjpV8l9L ooUdWJgMt Mf2pE83U2wsss81G5KJ FLeIXMa1T93 HGjNEbFfy4lRaWjctEH1l 3hWG74wsJ YdZXNmLTqTenvgec8qp u98Zp4XlrrA hbuVePBg5nxMeoxlojgl OuJAvAZef0 Nak7gm0ix8xSE70QeFJ MFjJvEAWRFF FtZOYkcHhCgewp7YBE 8OekOsOrcexa fRG4AdZaWBz3yCE4qM P0NAcxJ4DHeC dzbc6hW8i8otpHE	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsm4CBF.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.\$qr*5D5D5DJ2D5E !D2Da0t1DV1n4D3@4DR ich5DPELOa.!**	success or wait	1	4060F9	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\Desktop\9u4xTDR5bG.exe	unknown	512	success or wait	81	4060CA	ReadFile	
C:\Users\user\Desktop\9u4xTDR5bG.exe	unknown	4	success or wait	2	4060CA	ReadFile	
C:\Users\user\Desktop\9u4xTDR5bG.exe	unknown	4	success or wait	7	4060CA	ReadFile	
C:\Users\user\AppData\Local\Temp\Bosporus5.dat	unknown	33702	success or wait	1	73202C59	ReadFile	

Disassembly

 No disassembly

