ID: 830459
Sample Name:
Tender_QUOTATION__LH22000309AA2023.exe
Cookbook: default.jbs
Time: 11:54:01
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

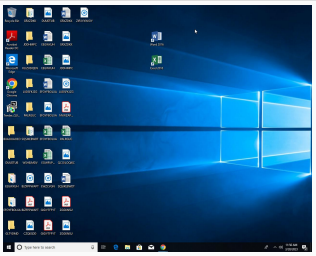
Windows Analysis Report

Tender_QUOTATION__LH22000309AA2023.exe

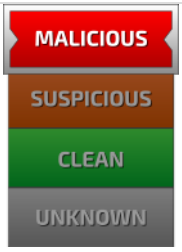
Overview

General Information

Sample Name:	Tender_QUOTATION__LH22000309AA2023.exe
Analysis ID:	830459
MD5:	e615251b8031…
SHA1:	56f3a2dcf6d73…
SHA256:	b4a5e199a297…
Tags:	AgentTesla exe
Infos:	



Detection



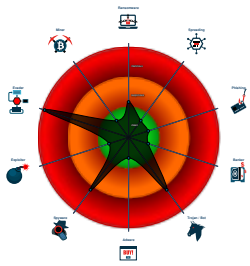
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected AgentTesla
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for drop…
- Detected unpacking (creates a PE f…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- Tender_QUOTATION__LH22000309AA2023.exe (PID: 5428 cmdline: C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe MD5: E615251B80317473A68488A21A1D0457)
  - rtvzitvzef.exe (PID: 5404 cmdline: "C:\Users\user~1\AppData\Local\Temp\rtvzitvzef.exe" C:\Users\user~1\AppData\Local\Temp\ggbdhaflcbm.cer MD5: 18995C06B5CE38C0D46A65451B5AAFB0)
    - conhost.exe (PID: 5348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rtvzitvzef.exe (PID: 5760 cmdline: C:\Users\user~1\AppData\Local\Temp\rtvzitvzef.exe MD5: 18995C06B5CE38C0D46A65451B5AAFB0)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Host": "gtasportsltd.com",
  "Username": "vestorfile@gtasportsltd.com",
  "Password": "00$rqv^A,;te     "
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.507831904.00000000025E1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: rtvzitvzef.exe PID: 5760	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Detected unpacking (creates a PE file in dynamic memory)

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

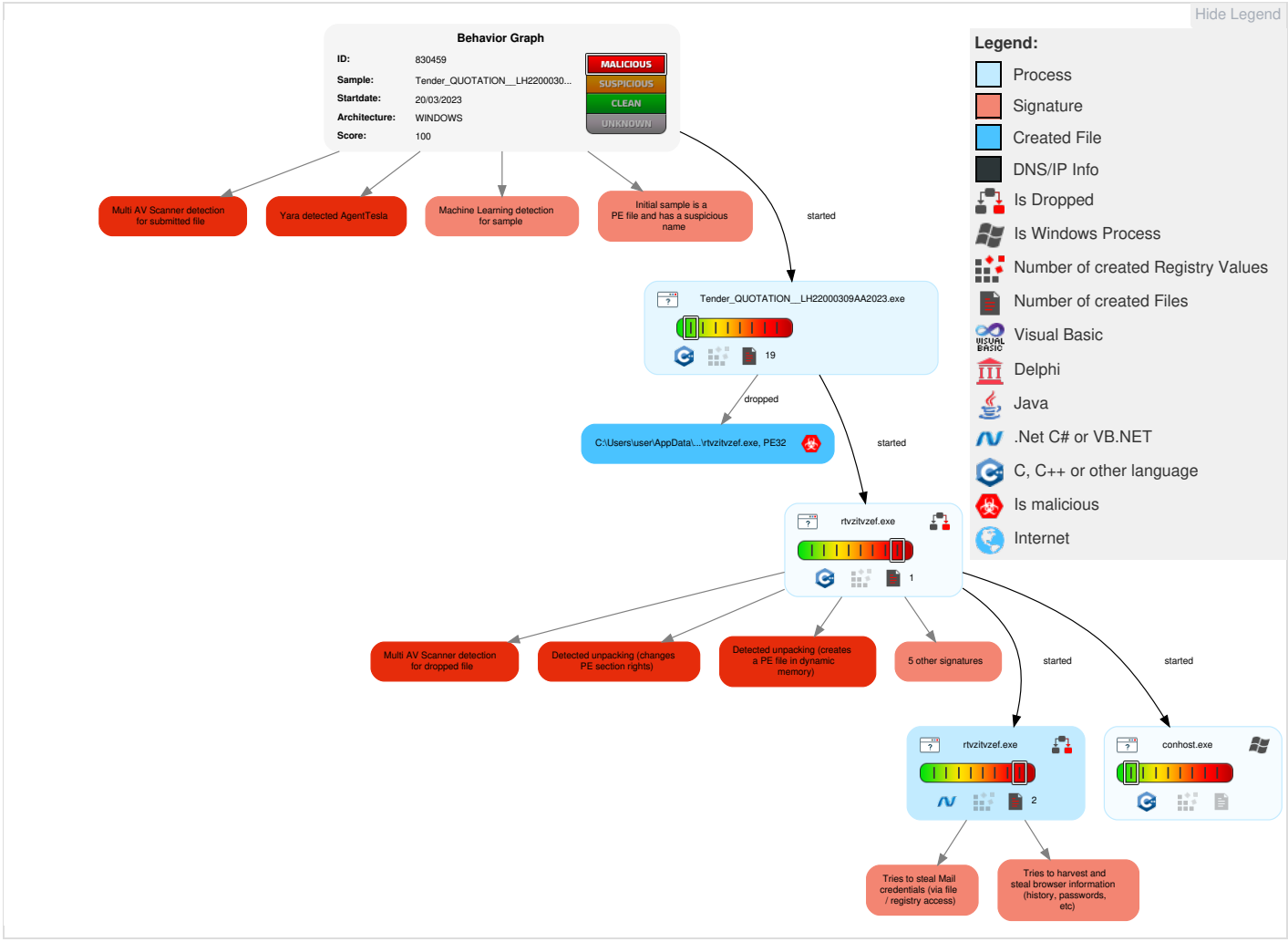
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 2 Virtualization/Sandbox Evasion	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	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)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 Software Packing	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 2 8 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
Tender_QUOTATION__LH22000309AA2023.exe	44%	ReversingLabs	Win32.Trojan.Leoncem	
Tender_QUOTATION__LH22000309AA2023.exe	46%	Virustotal		Browse
Tender_QUOTATION__LH22000309AA2023.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\rtvzitvzef.exe	22%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Local\Temp\rtvzitvzef.exe	38%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rtvzitvzef.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.rtvzitvzef.exe.4950000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	Tender_QUOTATION__LH22000309AA2023.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830459
Start date and time:	2023-03-20 11:54:01 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Number of analysed new started processes analysed:	15
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
Sample file name:	Tender_QUOTATION__LH22000309AA2023.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 21% (good quality ratio 19.5%) • Quality average: 79.3% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code 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\buvzkr.sej

Process:	C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe
File Type:	data
Category:	dropped
Size (bytes):	268825
Entropy (8bit):	7.970949330830082
Encrypted:	false
SSDEEP:	6144:7/ENh2fSlLKY2EFQTQ19y8Iryj6JOhIX4CPVuaj5j2xP2jVP9l6HSZz:7sN0KsYRp9nITcCpVTj5SxA9AHSV
MD5:	07BDC7754FD2D24ABECF19BEA0D8EDBA
SHA1:	571FE777A979FFCEC0DA4B23218728B747353054
SHA-256:	72A97E584B67FE97623C6B121149AE588BA1DAAF74650EF0AE24803B4CFBADF6
SHA-512:	34DF6BC7C58EBADE6D16510548FB1916BEB3A27348AEB659AF4423DF23971D7EF1FF3E6BF0E27A9F915E2C471FC595379E4BD349CE0A69007B3922F72B089454
Malicious:	false
Reputation:	low
Preview:	'.a7|._..\.4BF3.u...0.9.1C&B....3n(..E....W..mw..]......ZD..o....w...j. ..H....t.5w1..Hwa....m....-...-_.7..O....)..h..c...A.t.f,.v.n..y.7>.F..k.....p.M...~.!9..I.).8.}A.Va&0B..7..||.P.[.. ..c...c^. m.>v.H?7.....=..K..| .D....].$&K.~.yx..k...Mt.x7._..0.4M&z..\|..0.9..C&BH...Y.....E...mW..mwS.]......HD.z...7.rw..#..a..$U.Y.e.M.1.<...DH..f.}...y...t..-.W.[.B.B...h.c...5 t{..7..?w.....d.A.!|.bF.^Zyj..<.K.@.S.W2>....D.....k.z.Y.7t.r.....aAOAK..6Q..+o...6X...~....v23...tPPDA7A..]c%..k...M.y.Q..._..t.4.43...0+9..C&B....3n(.d.E.;..X..mw`.]....dD.z. .7.rw<....aE.$W9@X..M.1.E....kH..f....y...tP.-.W.[.].F..3B..c.0..t{..7...w....%...9\|.bF.^^ZRj..<.K.@.S.W2>...l=.I.....k.z.Y.7t.r.....aAOAK.,.Q..+o...6X...~....v23...tPPDA7A..]c%. .k...Mt.x7._.H\.4.=3...0.9..C&B....3n(..E....W..mw..]......ZD.z...7.rw<....a..$U.Y.e.M.1.....DH..f.....y...tP.-.W.[.].B...h..c...5t{..7..uw....%...9|.bF.^Zyj..<.K.@.S.W2>...l=.I.. ...k.z.Y.7t.r.....aAOAK.,.Q..+o...6X...~....v2

C:\Users\user\AppData\Local\Temp\ggbdhaflcbm.cer

Process:	C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe
File Type:	data

Category:	dropped
Size (bytes):	5718
Entropy (8bit):	7.169750536212027
Encrypted:	false
SSDEEP:	96:Farc6oYCg/DrYugk2XO5oSwYM1VmnjMoCMdSNyJ5c8/miYyGCZS7zmzuZPVed:FarcRiohX1S9SEATcSwJ5c8/m1sVzSy
MD5:	0B8A956CD495CC12BE4D2BB8BCB56A64
SHA1:	B80FE7CBDB389FB044C63BDEB124F866945E24AC
SHA-256:	6B2AB38F6B3F0F3254B9C9E288814C6D61CA2848A827D8F4FA815A422CEAFE9D
SHA-512:	E09C8200EEDE41AA352C531EB7300A2682611FEB53922EF97E30C275CACBD41658F21FBE919B5B1460BD828E81A383B6D9F07E8A8C6F15B12346056E7B6D23E2
Malicious:	false
Reputation:	low
Preview:	.005m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0....^..M....3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}..u.{.w....}.p013.....u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M.....v.ZXK.J.E.....}.]..O.F.....u.X_.M.M.....H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.:.q%..5M%.}.;.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e.....dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\nshC7D4.tmp

Process:	C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe
File Type:	data
Category:	dropped
Size (bytes):	383871
Entropy (8bit):	7.654896703470905
Encrypted:	false
SSDEEP:	6144:Y/ENh2fSlLKY2EFQTQ19y8Iryj6JOhIX4CPVuaj5j2xP2jVP9l6HSZe4GKGsGZEC:YsN0KsYRp9nITcCpVTj5SxA9AHSY4GKI
MD5:	FBC486075C71561D6180F4B65D3B5D37
SHA1:	4AC420FF2FDF3460A4DB48AF0C603E96E4DABA9C
SHA-256:	DEA9F7094037B7097AB67F6C9508F14E7532792CA4D0AF4D68F72BDB497A4C9D
SHA-512:	EB01FF7D5AA373C457A5F9B5B18E43C2141CC11691CE0B2EE95A80DFF39823676ACC585613A4DE2A025E0F742C18A3A6C7D24BF6DC4156BFD0132BAF97887EEC
Malicious:	false
Reputation:	low
Preview:	.5.....,.....I.....64.....5.....F..... .....G.....j.....^..... ....

C:\Users\user\AppData\Local\Temp\rtvzitvzef.exe

Process:	C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	95744
Entropy (8bit):	6.22624690688885
Encrypted:	false
SSDEEP:	1536:w0ZlV4KXc4OxQEsGZDmS+jtBaK/eRuZocSZUpxwkyBp+NnFsSW81kxgsWJjcdvCk:pd4KALsGZDN+x/yuZocSTkyBw9y8eASL
MD5:	18995C06B5CE38C0D46A65451B5AAFB0
SHA1:	BCD38033C62BD2D7200201C785C2E5A7AEDDA81A
SHA-256:	BCAEE4AED66E705BD14ED4994B7376FE06830BF2CE864FBCC307BBBF9613A7FA
SHA-512:	FB8C76B256EF7E98BA6C96C2E6D0C167E5B292A004FFDFD70B361E8D4EF9E4FE223F3F81A54E0473F248418C13F0E7F5696E53D446C6C74D8690BBDF1AFD5B6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 22% • Antivirus: Virustotal, Detection: 38%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7...s...s...8...y...8.....8...g.....U.....b.....`...8...j...s.....r.....r.. .Richs.....PE..L.....d.....!.....|....."..... @.....|k.....^.....]..@..... .....text..... ..`.rdata...f.....h.....@..@.data...l.....l.....@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.932897306880799
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:	Tender_QUOTATION__LH22000309AA2023.exe
File size:	316771
MD5:	e615251b80317473a68488a21a1d0457
SHA1:	56f3a2dcf6d730126426ce2d65ae5819ca4c753e
SHA256:	b4a5e199a29723b27c6aced8f28c7b39f29738bfb2ea3ada079e38c4aad366f4
SHA512:	5cc554d11ed4f89b8993ad04276929978ec1c4840cf5a5e1e013b77eb3a87138e17e550815bae461085caa7ab81b916c7f24c12f3bdfa796b1e06fd8cf21aab9
SSDEEP:	6144:/Ya6WT4gMl7QMZVzkNrIXjsh+IHqneS8p1ARssPdP5lkNxbZ:/YQsgorXsHqneJVdpZ
TLSH:	1D64235577F6CC8BDDE1093339B20B124E5A6F030AA98B4B5358CB4DBA271C7E52B352
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h

Instruction
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
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 00007F785CBEDDEAh
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, FFFFFFD0h
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 00007F785CBEDDBAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], 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	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xcf0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0xcf0	0xe00	False	0.4252232142857143	data	4.244072202507094	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b1d8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x3b4c0	0x100	data	English	United States
RT_DIALOG	0x3b5c0	0x11c	data	English	United States
RT_DIALOG	0x3b6e0	0x60	data	English	United States
RT_GROUP_ICON	0x3b740	0x14	data	English	United States
RT_VERSION	0x3b758	0x254	data	English	United States
RT_MANIFEST	0x3b9b0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), 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
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, 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

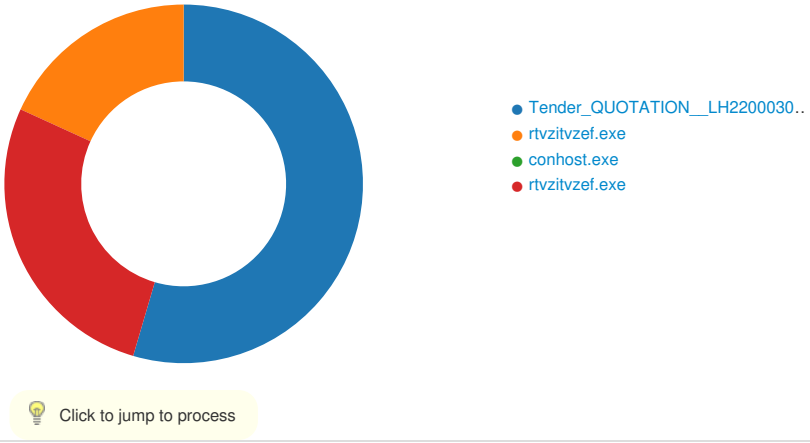
Possible Origin		
Language of compilation system	**Country where language is spoken**	**Map**
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: Tender_QUOTATION__LH22000309AA2023.exe PID: 5428, Parent PID: 3320

General	
Target ID:	0
Start time:	11:54:55
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe
Imagebase:	0x400000
File size:	316771 bytes
MD5 hash:	E615251B80317473A68488A21A1D0457
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	405C22	CreateDirectoryW
C:\Users\user~1\AppData\Local\Temp\nsmC7A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\nshC7D4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\nscC804.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	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	405C22	CreateDirectoryW
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user~1\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	405C22	CreateDirectoryW
C:\Users\user~1\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	405C22	CreateDirectoryW
C:\Users\user~1\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	405C22	CreateDirectoryW
C:\Users\user~1\AppData\Local\Temp\nscC804.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	405BE2	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user~1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user~1\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	405C22	CreateDirectoryW
C:\Users\user~1\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	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\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	405C22	CreateDirectoryW
C:\Users\user~1\AppData\Local\Temp\buvzkr.sej	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user~1\AppData\Local\Temp\ggbdhaflcbm.cer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user~1\AppData\Local\Temp\rtvzitvzef.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmC7A4.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nscC804.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nshC7D4.tmp	0	28122	00 35 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 11 00 00 fd 00 00 00 fd 21 00 00 00 00 00 00 36 34 00 00 01 00 00 00 00 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 46 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	5,!645F	success or wait	19	406224	WriteFile
C:\Users\user\AppData\Local\Temp\buvzkr.sej	0	16384	27 fd 61 37 7c fd 5f 1c fd 5c fd 34 42 46 33 fd 75 fd fd fd 30 fd 39 fd 31 43 26 42 fd fd fd fd 33 6e 28 fd 9a 45 1e fd fd fd 57 12 fd 6d 77 fd 1b 5d fd fd fd fd fd fd 5a 44 fd fd 6f fd 1e c2 05 77 fd 17 fd 6a 1d 20 fd fd 48 fd fd fd fd 74 32 35 77 31 0f 1d 48 77 61 fd fd fd 06 6d fd fd fd fd 2d fd fd 07 2d 5f fd 37 fd fd 4f 0b fd fd fd 29 15 fd 68 fd fd 63 fd fd fd 41 fd 74 fd 66 2c 0b 76 fd 6e fd 09 79 fd 37 3e fd 46 fd fd 6b fd fd 17 fd fd 02 14 70 12 4d fd fd 0d 7e fd 21 39 13 0c 49 fd 29 fd 38 fd 7d 41 fd 56 61 26 30 42 1d 01 37 1b 2c 7c 7c 02 50 fd 5b 2e bc fd fd 63 fd fd 07 63 5e fd 20 6d fd 3e 76 fd 48 3f 37 fd fb 90 fd fd 3d 04 fd 4b fd fd 7c 20 fd 44 14 fd fd fd 5d fd 24 26 4b 07 7e fd 79 78 10 0c 6b fd fd 23	'a7|_\4BF3u091C&B3n(EWmw]ZDowj Ht5w1Hwam--_7O)hcAtf,vny7>Fkp M~!9I)8}AVa&0B7,||P[.cc ^ m>vH?7=K| D]$&K~yxk	success or wait	17	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ggbdhaflcbm.cer	0	5718	c6 30 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	005mfF<05o:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L $mrD;Fokcm;4q? <@40mu<f@%`4D'dO $A5=<r	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\rtvzitvzef.exe	0	16384	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 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 37 fd fd fd 73 fd fd fd 73 fd fd fd 73 fd fd fd 38 fd fd fd 79 fd fd fd 38 fd fd fd fd fd fd fd 38 fd fd fd 67 fd fd fd fd fd fd 55 fd fd fd fd fd 62 fd fd fd fd fd fd 60 fd fd fd 38 fd fd fd 6a fd fd fd 73 fd fd fd fd fd fd fd fd fd fd 72 fd fd fd fd fd fd 72 fd fd fd 52 69 63 68 73 fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0d fd 17 64 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7sss8y88gUb`8j srrRichsPELd	success or wait	6	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe	unknown	512	success or wait	74	4061F5	ReadFile
C:\Users\user\Desktop\Tender_QUOTATION__LH22000309AA2023.exe	unknown	16384	success or wait	18	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nshC7D4.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nshC7D4.tmp	unknown	13568	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nshC7D4.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nshC7D4.tmp	unknown	16384	success or wait	24	4061F5	ReadFile

Analysis Process: rtvzitvzef.exe PID: **5404**, Parent PID: **5428**

General

Target ID:	1
Start time:	11:54:56
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\rtvzitvzef.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\rtvzitvzef.exe" C:\Users\user~1\AppData\Local\Temp\ggbdhaflcbm.cer

Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	18995C06B5CE38C0D46A65451B5AAFB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	- Detection: 22%, ReversingLabs - Detection: 38%, Virustotal, Browse
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ggbdhaflcbm.cer	unknown	4096	success or wait	1	407824	ReadFile
C:\Users\user\AppData\Local\Temp\ggbdhaflcbm.cer	unknown	4096	success or wait	1	407824	ReadFile
C:\Users\user\AppData\Local\Temp\buvzkr.sej	unknown	247808	success or wait	1	9F0A25	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	9F0E77	ReadFile

Analysis Process: conhost.exe

PID: **5348**, Parent PID: **5404**

General

Target ID:	2
Start time:	11:54:56
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: rtvzitvzef.exe

PID: **5760**, Parent PID: **5404**

General

Target ID:	3
Start time:	11:54:57
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\rtvzitvzef.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\rtvzitvzef.exe
Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	18995C06B5CE38C0D46A65451B5AAFB0
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.507831904.00000000025E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C81B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71C81B4F	ReadFile

Disassembly

No disassembly