ID: 877001
Sample Name: 06625899.exe
Cookbook: default.jbs
Time: 10:45:08
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

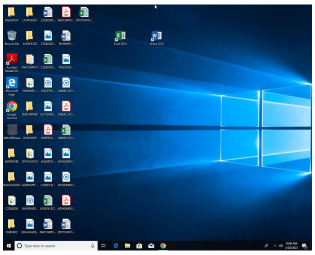
Windows Analysis Report

06625899.exe

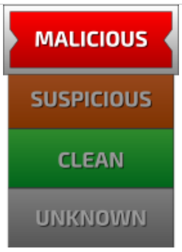
Overview

General Information

Sample Name:	06625899.exe
Analysis ID:	877001
MD5:	22cd094d925fb..
SHA1:	c316b3fa0e135..
SHA256:	9edb64bf31021..
Infos:	



Detection



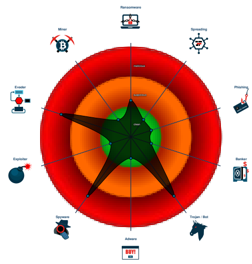
Vidar

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

Signatures

- Found malware configuration
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Vidar stealer
- Detected unpacking (changes PE se…
- Tries to steal Crypto Currency Walle…
- Tries to harvest and steal Putty / W…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- C2 URLs / IPs found in malware con…
- Found many strings related to Crypt…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- 06625899.exe (PID: 7120 cmdline: C:\Users\user\Desktop\06625899.exe MD5: 22CD094D925FB41F446ED4DB24CC8C35)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	http://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Vidar

```
{
  "C2 url": [
    "https://steamcommunity.com/profiles/76561199508624021",
    "https://t.me/looking_glassbot"
  ],
  "Botnet": "667e85c8112da056f901292caf82b3ed"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.412273904.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000003.355865725.0000000002380000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.412969264.00000000025C5000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.06625899.exe.2320e67.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.06625899.exe.2320e67.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.3.06625899.exe.2380000.0.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.2.06625899.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0.3.06625899.exe.2380000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Vidar stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Found many strings related to Crypto-Wallets (likely being stolen)

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

Remote Access Functionality

Yara detected Vidar stealer

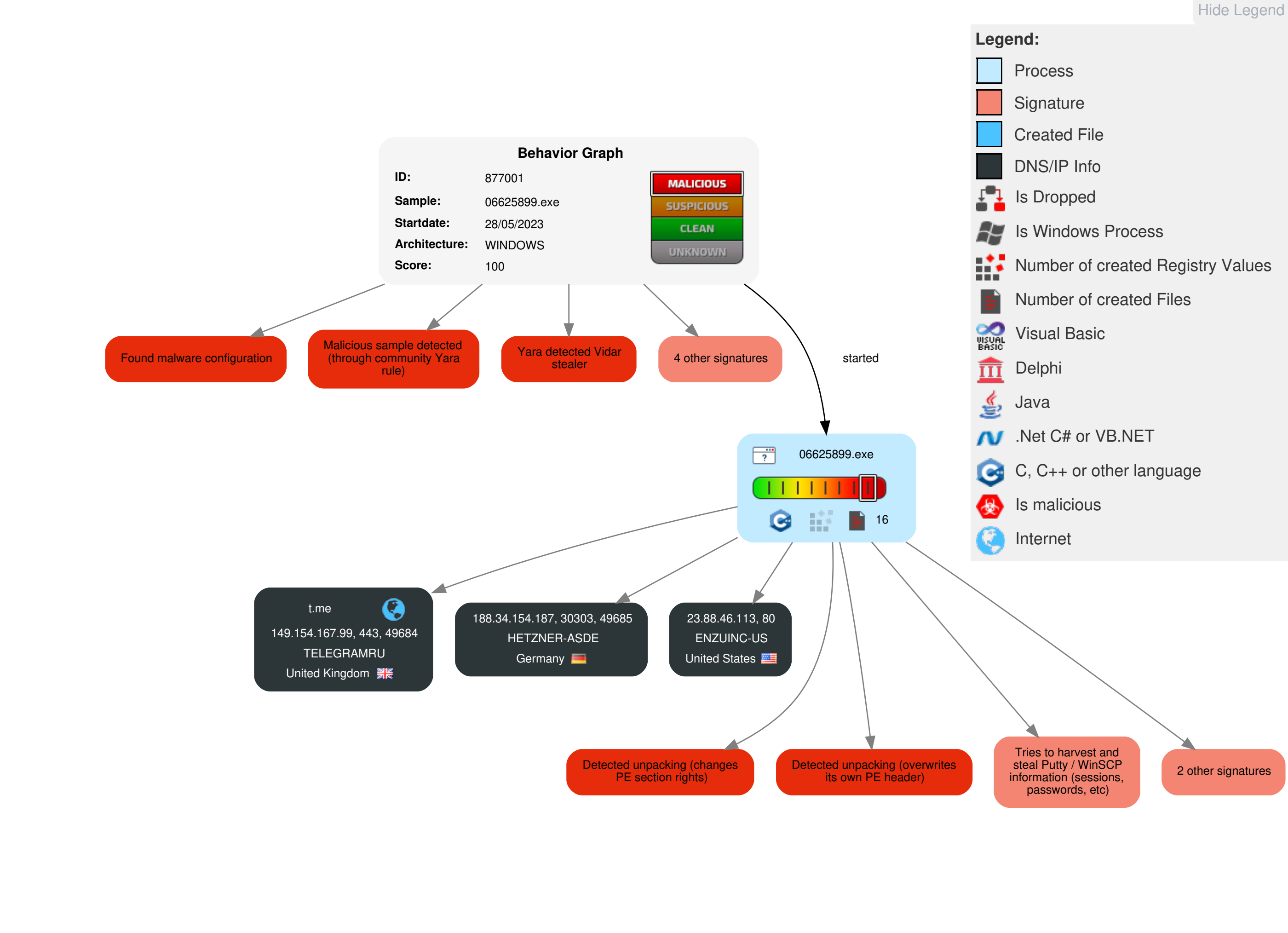
Mitre Att&ck Matrix

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 Windows Management Instrumentation	Path Interception	Path Interception	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	1 Credentials in Registry	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 2 Software Packing	NTDS	5 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 2 Process 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	Compile After Delivery	DCSync	1 System Owner/User 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 Remote System 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

Hide Legend



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
06625899.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://freebl3.dllmozglue.dllmsvcp140.dllnss3.dllsoftokn3.dllvcruntime140.dll	0%	URL Reputation	safe	
http://188.34.154.187:30303;	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/:	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303//	0%	Avira URL Cloud	safe	
http://ctldl.windowsup30303/667e85c8112da056f901292caf82b3ed	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/addon.zip=u&y	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/n	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303//	1%	Virustotal		Browse
http://188.34.154.187:30303/667e85c8112da056f901292caf82b3edZ5	0%	Avira URL Cloud	safe	
http://23.88.46.113/667e85c8112da056f901292caf82b3ed8	0%	Avira URL Cloud	safe	
http://23.88.46.113/667e85c8112da056f901292caf82b3edx	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/e5	0%	Avira URL Cloud	safe	
http://23.88.46.113:8A	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/T	0%	Avira URL Cloud	safe	
http://23.88.46.113/667e85c8112da056f901292caf82b3ed	0%	Avira URL Cloud	safe	
http://23.88.46.113:80	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/667e85c8112da056f901292caf82b3ed	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/CVOHV.xlsx	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/addon.zip	0%	Avira URL Cloud	safe	
http://23.88.46.113:80/	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/	0%	Avira URL Cloud	safe	
http://23.88.46.113:80peppppzxc.ziphttps://t.me/looking_glassbotlookataddon.zipMozilla/5.0	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/addon.zip&u;y	0%	Avira URL Cloud	safe	
http://188.34.154.187:30303/addon.zip0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t.me	149.154.167.99	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://t.me/looking_glassbot	false		high
http://188.34.154.187:30303/667e85c8112da056f901292caf82b3ed	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199508624021	false		high
http://188.34.154.187:30303/addon.zip	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/	false	• Avira URL Cloud: safe	unknown

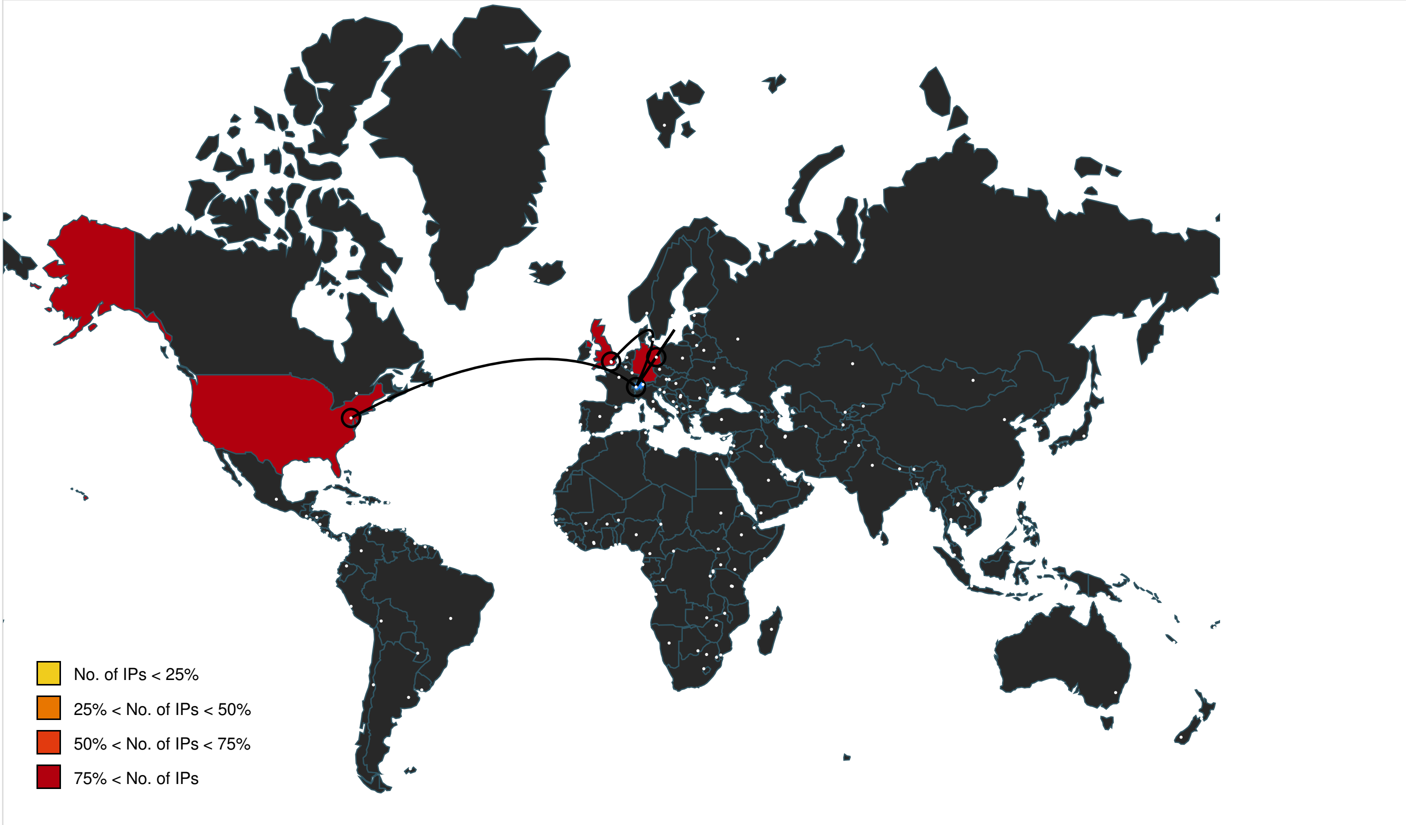
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	06625899.exe, 00000000.00000003.40485479 7.00000000031BF000.00000004.00000020.000 20000.00000000.sdmp, 2291996409618366596 1703616.0.dr, 50764714324176067669882221.0.dr	false		high
http://https://t.me/	06625899.exe, 00000000.00000002.41255511 3.000000000086A000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://188.34.154.187:30303;	06625899.exe, 00000000.00000002.41296926 4.00000000025C5000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://t.me/looking_glassbotJ	06625899.exe, 00000000.00000002.41255511 3.000000000086A000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	50764714324176067669882221.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	06625899.exe, 00000000.00000003.404854797.00000000031BF000.00000004.00000020.00020000.00000000.sdmp, 22919964096183665961703616.0.dr, 50764714324176067669882221.0.dr	false		high
http://188.34.154.187:30303	06625899.exe, 00000000.00000003.402473646.00000000008F2000.00000004.00000020.00020000.00000000.sdmp, 06625899.exe, 00000000.00000002.412969264.00000000025C5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/:	06625899.exe, 00000000.00000002.412555113.00000000008DC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ctldl.windowsup30303/667e85c8112da056f901292caf82b3ed	06625899.exe, 00000000.00000002.412555113.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303//	06625899.exe, 00000000.00000002.413121737.0000000003160000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/addon.zip=u&y	06625899.exe, 00000000.00000002.412555113.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/n	06625899.exe, 00000000.00000002.413121737.0000000003160000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/667e85c8112da056f901292caf82b3edZ5	06625899.exe, 00000000.00000002.412555113.00000000008DC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	06625899.exe, 00000000.00000003.404854797.00000000031BF000.00000004.00000020.00020000.00000000.sdmp, 22919964096183665961703616.0.dr, 50764714324176067669882221.0.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	50764714324176067669882221.0.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	06625899.exe, 00000000.00000003.404854797.00000000031BF000.00000004.00000020.00020000.00000000.sdmp, 22919964096183665961703616.0.dr, 50764714324176067669882221.0.dr	false		high
http://23.88.46.113/667e85c8112da056f901292caf82b3ed8	06625899.exe, 00000000.00000002.412555113.00000000008CB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.46.113/667e85c8112da056f901292caf82b3edx	06625899.exe, 00000000.00000002.412555113.00000000008CB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/e5	06625899.exe, 00000000.00000002.412555113.00000000008DC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.46.113:8A	06625899.exe, 00000000.00000002.412510711.0000000000838000.00000040.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://t.me/looking_glassbotC	06625899.exe, 00000000.00000002.412555113.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	06625899.exe, 00000000.00000003.404854797.00000000031BF000.00000004.00000020.00020000.00000000.sdmp, 22919964096183665961703616.0.dr, 50764714324176067669882221.0.dr	false		high
http://https://freebl3.dllmozglue.dllmsvcp140.dllnss3.dllsoftokn3.dllvcruntime140.dll	06625899.exe, 00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp, 06625899.exe, 00000000.00000002.412273904.0000000000400000.00000040.00000001.01000000.00000003.sdmp, 06625899.exe, 00000000.00000003.355865725.0000000002380000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	50764714324176067669882221.0.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	06625899.exe, 00000000.00000003.404854797.00000000031BF000.00000004.00000020.00020000.00000000.sdmp, 22919964096183665961703616.0.dr, 50764714324176067669882221.0.dr	false		high
http://188.34.154.187:30303/T	06625899.exe, 00000000.00000002.413121737.0000000003160000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/V	06625899.exe, 00000000.00000002.412555113.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://23.88.46.113/667e85c8112da056f901292caf82b3ed	06625899.exe, 00000000.00000002.412555113.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.46.113:80	06625899.exe, 06625899.exe, 00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp, 06625899.exe, 00000000.00000002.412273904.0000000000400000.00000040.00000001.01000000.00000003.sdmp, 06625899.exe, 00000000.00000003.355865725.0000000002380000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://188.34.154.187:30303/CVOHV.xlsx	06625899.exe, 00000000.00000002.413121737.00000000031BF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.46.113:80/	06625899.exe, 00000000.00000002.412969264.00000000025C5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.88.46.113:80peppppzxc.ziphttps://t.me/looking_glassbotlookataddon.zipMozilla/5.0	06625899.exe, 00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp, 06625899.exe, 00000000.00000002.412273904.0000000000400000.00000040.00000001.01000000.00000003.sdmp, 06625899.exe, 00000000.00000003.355865725.0000000002380000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://188.34.154.187:30303/addon.zip&u;y	06625899.exe, 00000000.00000002.412555113.000000000086A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	50764714324176067669882221.0.dr	false		high
http://188.34.154.187:30303/addon.zip0	06625899.exe, 00000000.00000003.404755514.00000000008F8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	06625899.exe, 00000000.00000002.423731237.0000000061ED3000.00000004.00001000.00020000.00000000.sdmp, 06625899.exe, 00000000.00000002.415215690.000000000DF12000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://steamcommunity.com/profiles/76561199508624021openopen_NULL%s	06625899.exe, 00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp, 06625899.exe, 00000000.00000002.412273904.0000000000400000.00000040.00000001.01000000.00000003.sdmp, 06625899.exe, 00000000.00000003.355865725.0000000002380000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.34.154.187	unknown	Germany		24940	HETZNER-ASDE	false
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false
23.88.46.113	unknown	United States		18978	ENZUINC-US	false

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877001
Start date and time:	2023-05-28 10:45:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 56s
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:	3
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:	06625899.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/4@1/3
EGA Information:	Failed

HDC Information:	• Successful, ratio: 30.2% (good quality ratio 27.9%) • Quality average: 72.1% • Quality standard deviation: 31.8%
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 • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:46:24	API Interceptor	1x Sleep call for process: 06625899.exe modified

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:\ProgramData\22919964096183665961703616

Process:	C:\Users\user\Desktop\06625899.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false

SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3......@ ....-...........=..[5...........*..

C:\ProgramData\36067264576515806059430256

Process:	C:\Users\user\Desktop\06625899.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CE F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3......@ ....[5..

C:\ProgramData\50764714324176067669882221

Process:	C:\Users\user\Desktop\06625899.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3......@ ....-...........=..[5...........*..

C:\ProgramData\57469657185917597184786931

Process:	C:\Users\user\Desktop\06625899.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7

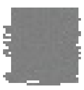
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3......@ ....[5.........g...$..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.134474155007553
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:	06625899.exe
File size:	404992
MD5:	22cd094d925fb41f446ed4db24cc8c35
SHA1:	c316b3fa0e1357ed5815002b0354e8503d5ee038
SHA256:	9edb64bf310212bffcc2fa176b22b570d071fb38873292a1a1ada19f8536231c
SHA512:	606163e06f58b8fa1003ca0aa9a8a30344fc49fe20259beda6ae6fb006f7a1440ac61a8ed7a79a64ac802618613943119fb7b2289718a341edf19f3a7fceb895
SSDEEP:	6144:QY/jZT7vRNMKOO3PFmc7rPZWM5khCVYPnZe+QSdixrmwVUTtiKG:Qq5hOOMc7fLVYPnZ3QSd8yFTtib
TLSH:	40847D1392A1BD40E9664F769E1FC6E8761EF5708F593B69322CBA1F48700F2D263B11
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......&...b...b...b...|.......|.......|...H...EX..k...b.......|...c...|...c...|...c...Richb...................PE..L......a...........

File Icon



Icon Hash:	514145494155691d

Static PE Info

General

Entrypoint:	0x404e59
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x61FA08E2 [Wed Feb 2 04:30:26 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:	2d9ed3462f8a74bfd1231e2e9de56b43

Entrypoint Preview

Instruction
call 00007F5B55084253h
jmp 00007F5B5507F8EDh

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F5B5507FA96h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F5B5507FAC0h
test ecx, 00000003h
jne 00007F5B5507FA61h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F5B5507FA5Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F5B5507FAA4h
test ah, ah
je 00007F5B5507FA96h
test eax, 00FF0000h
je 00007F5B5507FA85h
test eax, FF000000h
je 00007F5B5507FA74h
jmp 00007F5B5507FA3Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret

Instruction
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x445a8	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x28c000	0x19398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2a6000	0xde4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
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	0x4406a	0x44200	False	0.8737528669724771	data	7.818078308305934	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x46000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x28c000	0x19398	0x19400	False	0.37881922957920794	data	4.263849351344956	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2a6000	0x3450	0x3600	False	0.2173755787037037	data	2.4461769922107117	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x28c730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x28d5d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x28de80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x290428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2914d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x291988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x292830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2930d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x293640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x295be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x296c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x297618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x297ae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x298990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x299238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x299900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x299e68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x29c410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x29d4b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x29d988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x29e830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x29f0d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x29f640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x2a1be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2a2c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x2a3618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x2a3d20	0x664	data		
RT_STRING	0x2a4388	0x59e	data		
RT_STRING	0x2a4928	0x29a	data		
RT_STRING	0x2a4bc8	0x248	data		
RT_STRING	0x2a4e10	0x582	data		
RT_GROUP_ICON	0x2a3a80	0x68	data		
RT_GROUP_ICON	0x291938	0x4c	data		
RT_GROUP_ICON	0x29d920	0x68	data		
RT_GROUP_ICON	0x297a80	0x68	data		
RT_VERSION	0x2a3ae8	0x238	data		

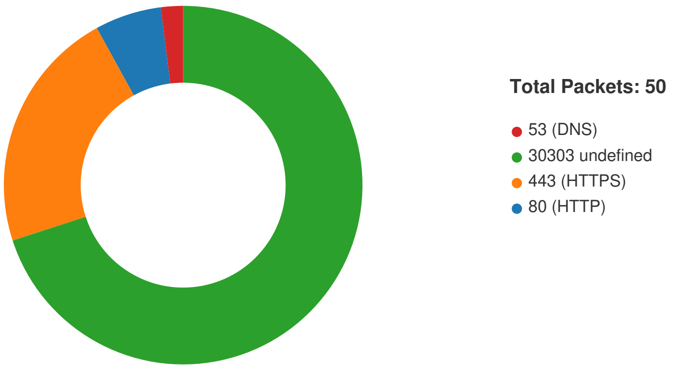
Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleHandleW, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, AttachConsole, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetLongPathNameA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:46:01.248292923 CEST	49679	80	192.168.2.3	23.88.46.113
May 28, 2023 10:46:04.249680996 CEST	49679	80	192.168.2.3	23.88.46.113
May 28, 2023 10:46:10.250323057 CEST	49679	80	192.168.2.3	23.88.46.113
May 28, 2023 10:46:22.357672930 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.357745886 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.357866049 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.375677109 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.375749111 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.448298931 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.448596954 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.651189089 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.651254892 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.651915073 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.651990891 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.655484915 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.691979885 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.692039967 CEST	443	49684	149.154.167.99	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:46:22.692131042 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.692161083 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.692228079 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.692233086 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.692368984 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.696513891 CEST	49684	443	192.168.2.3	149.154.167.99
May 28, 2023 10:46:22.696552992 CEST	443	49684	149.154.167.99	192.168.2.3
May 28, 2023 10:46:22.732084990 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:22.754019022 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:22.754215002 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:22.754666090 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:22.779701948 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.136292934 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.136447906 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.140424967 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.162672997 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163690090 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163734913 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163753986 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163773060 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163791895 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163810968 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163835049 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163839102 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.163855076 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.163887024 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.163959026 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.164143085 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.164161921 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.164221048 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.164277077 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.185832024 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.185858011 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.185884953 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.185910940 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.185925961 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.185925961 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.185940027 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.185967922 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.185973883 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.185973883 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.185991049 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.185996056 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186033964 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186042070 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186069965 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186080933 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186083078 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186106920 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186131954 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186132908 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186157942 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186181068 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186181068 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186183929 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186204910 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186211109 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186229944 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186233044 CEST	30303	49685	188.34.154.187	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:46:23.186249971 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186254978 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186275959 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186283112 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186296940 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186302900 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186316967 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186321020 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186345100 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.186346054 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186362028 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.186393976 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.208338976 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208372116 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208400011 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208427906 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208458900 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208487988 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208498955 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.208499908 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.208499908 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.208517075 CEST	30303	49685	188.34.154.187	192.168.2.3
May 28, 2023 10:46:23.208542109 CEST	49685	30303	192.168.2.3	188.34.154.187
May 28, 2023 10:46:23.208542109 CEST	49685	30303	192.168.2.3	188.34.154.187

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:46:22.339339018 CEST	59869	53	192.168.2.3	8.8.8.8
May 28, 2023 10:46:22.353594065 CEST	53	59869	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 10:46:22.339339018 CEST	192.168.2.3	8.8.8.8	0x7ede	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 10:46:22.353594065 CEST	8.8.8.8	192.168.2.3	0x7ede	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- t.me
- 188.34.154.187:30303

Statistics

No statistics

System Behavior

Analysis Process: 06625899.exe PID: 7120, Parent PID: 3452

General

Target ID:	0
Start time:	10:46:00
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\06625899.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\06625899.exe
Imagebase:	0x400000
File size:	404992 bytes
MD5 hash:	22CD094D925FB41F446ED4DB24CC8C35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.412273904.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.412801899.0000000002320000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000003.355865725.0000000002380000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.412969264.00000000025C5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.412510711.0000000000838000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\57469657185917597184786931	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	41A84E	CopyFileA
C:\ProgramData\36067264576515806059430256	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	41A4F4	CopyFileA
C:\ProgramData\22919964096183665961703616	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	41AD27	CopyFileA
C:\ProgramData\50764714324176067669882221	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	41527D	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\57469657185917597184786931	success or wait	1	41AC59	DeleteFileA
C:\ProgramData\36067264576515806059430256	success or wait	1	41A73F	DeleteFileA
C:\ProgramData\22919964096183665961703616	success or wait	1	41AFCD	DeleteFileA
C:\ProgramData\50764714324176067669882221	success or wait	1	4153FE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\574696571859175 97184786931	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 11 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 11 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 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 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	SQLite format 3@ .[5g$	success or wait	1	41A84E	CopyFileA
C:\ProgramData\360672645765158 06059430256	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 02 00 2e 5b 35 05 00 00 00 01 07 fd 00 00 00 00 10 07 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 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	SQLite format 3@ .[5	success or wait	1	41A4F4	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\22919964096183665961703616	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 04 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	41AD27	CopyFileA
C:\ProgramData\50764714324176067669882221	0	94208	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 04 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 3d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 04 00 2e 5b 35 05 00 00 00 05 07 fd 00 00 00 00 2a 07 fd 07 fd 07 fd 07 fd 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ -=.[5*	success or wait	1	41527D	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61356	success or wait	1	414F6A	ReadFile
C:\ProgramData\57469657185917597184786931	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\57469657185917597184786931	0	4096	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\57469657185917597184786931	24	16	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\36067264576515806059430256	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\36067264576515806059430256	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\22919964096183665961703616	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\22919964096183665961703616	0	2048	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\50764714324176067669882221	0	100	success or wait	1	61E33FB7	ReadFile
C:\ProgramData\50764714324176067669882221	0	2048	success or wait	1	61E33FB7	ReadFile

Disassembly

No disassembly