ID: 755996
Sample Name: 2022-571-GLS.exe
Cookbook: default.jbs
Time: 13:15:07
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

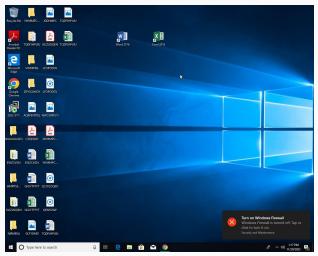
Windows Analysis Report

2022-571-GLS.exe

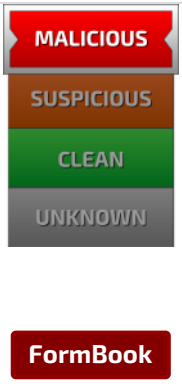
Overview

General Information

Sample Name:	2022-571-GLS.exe
Analysis ID:	755996
MD5:	6cc14805bbf5e6…
SHA1:	34836f2aa6a4e9..
SHA256:	029d4fe47cb21a..
Tags:	exe
Infos:	



Detection



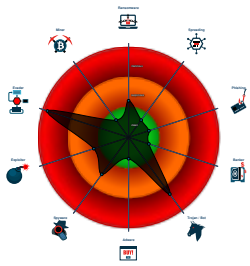
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Maps a DLL or memory area into an…
- Uses netsh to modify the Windows …
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- 2022-571-GLS.exe (PID: 5464 cmdline: C:\Users\user\Desktop\2022-571-GLS.exe MD5: 6CC14805BBF5E6BFB4DAAE5C8A61AF7E)
  - jsqqecy.exe (PID: 1236 cmdline: "C:\Users\user\AppData\Local\Temp\jsqqecy.exe" C:\Users\user\AppData\Local\Temp\xduyswx.up MD5: 07875284CE0A6276F406B25F9E429270)
    - jsqqecy.exe (PID: 1224 cmdline: "C:\Users\user\AppData\Local\Temp\jsqqecy.exe" C:\Users\user\AppData\Local\Temp\xduyswx.up MD5: 07875284CE0A6276F406B25F9E429270)
      - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - netsh.exe (PID: 6140 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - cmd.exe (PID: 4136 cmdline: /c del "C:\Users\user\AppData\Local\Temp\jsqqecy.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 4828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cdlcapitolsolutions.com/b31b/"
  ],
  "decoy": [
    "deltafxtrading.com",
    "alisonangl.com",
    "cdfqs.com",
    "easyentry.vip",
    "dentalinfodomain.com",
    "hiphoppianyc.com",
    "pools-62911.com",
    "supportteam26589.site",
    "delldaypa.one",
    "szanody.com",
    "diaper-basket.art",
    "ffscollab.com",
    "freediverconnect.com",
    "namesbrun.com",
    "theprimone.top",
    "lenzolab.com",
    "cikmas.com",
    "genyuei-no.space",
    "hellofstyle.com",
    "lamagall.com",
    "hallmarktb.com",
    "hifebou7.info",
    "sex5a.finance",
    "printrynner.com",
    "powerrestorationllc.com",
    "hirefiz.com",
    "uninvitedempire.com",
    "alpinemaintenance.online",
    "ppcadshub.com",
    "looking4.tours",
    "dirtyhandsmedia.com",
    "capishe.website",
    "cachorrospitbull.com",
    "mythic-authentication.online",
    "nordingcave.online",
    "gremep.online",
    "tryufabetcasino.com",
    "premiumciso.com",
    "powerful70s.com",
    "myminecraftrealm.com",
    "bssurgery.com",
    "steel-pcint.com",
    "iokailyjewelry.com",
    "barmanon5.pro",
    "kcrsw.com",
    "9393xx38.app",
    "kochen-mit-induktion.com",
    "indtradors.store",
    "giaxevn.info",
    "trungtambaohanhariston.com",
    "fulili.com",
    "crgabions.com",
    "matomekoubou.com",
    "duaidapduapjdp.site",
    "invissiblefriends.com",
    "cy3.space",
    "idqoft.com",
    "jamal53153.com",
    "lemagnetix.com",
    "anthroaction.com",
    "uspcff.top",
    "supplierdir.com",
    "counterpoint.online",
    "zarl.tech"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000000.300703858.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 34 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.jsqqecy.exe.1090000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.jsqqecy.exe.1090000.1.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
1.2.jsqqecy.exe.1090000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
1.2.jsqqecy.exe.1090000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
2.2.jsqqecy.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 19 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information

Yara detected FormBook

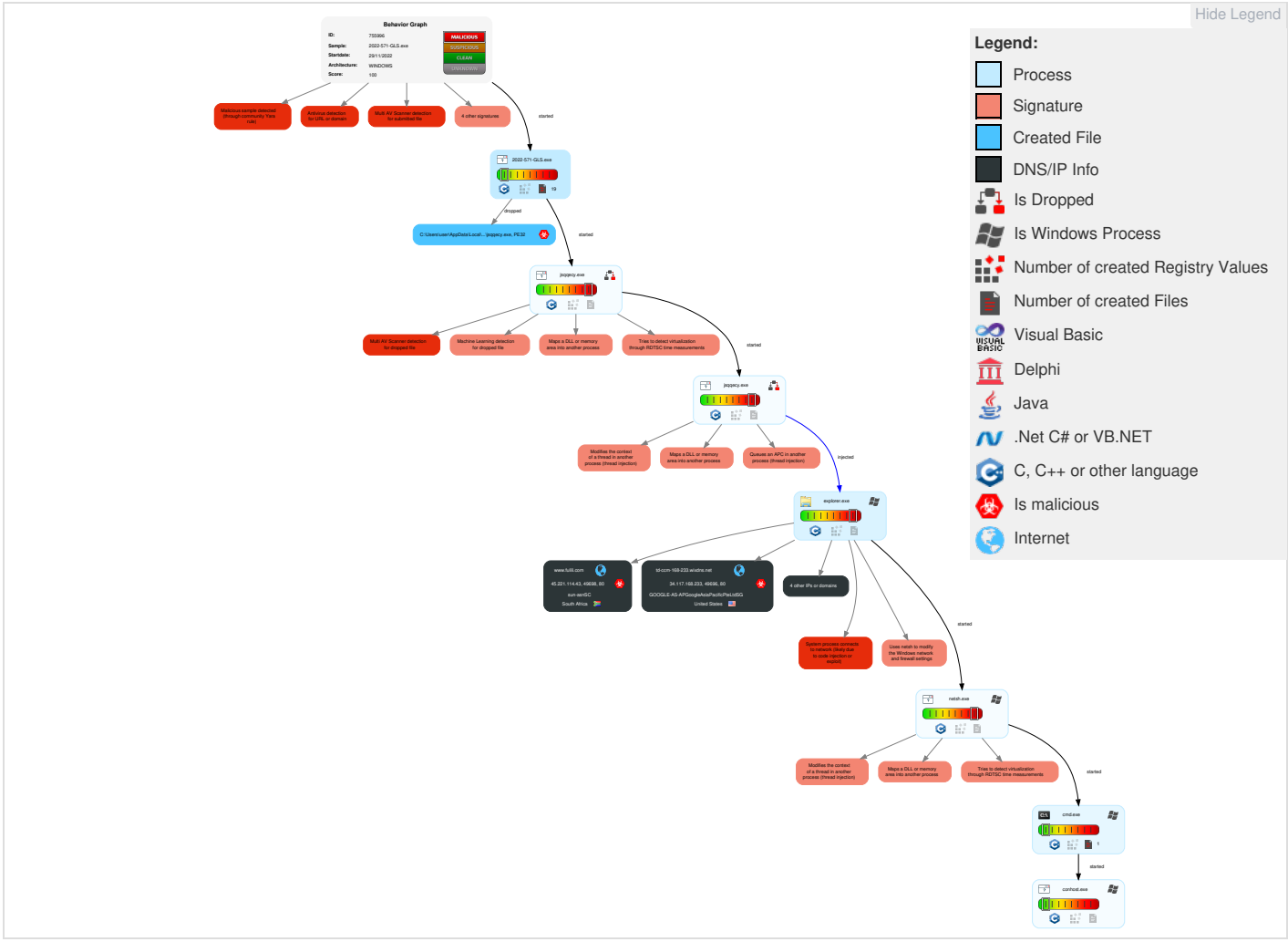
Remote Access Functionality

Yara detected FormBook

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 Command and Scripting Interpreter	Path Interception	4 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	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 Disable or Modify Tools	1 1 Input Capture	2 4 1 Security Software Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Virtualization/Sandbox Evasion	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 2 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	2 Clipboard Data	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System 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	3 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory 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	1 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

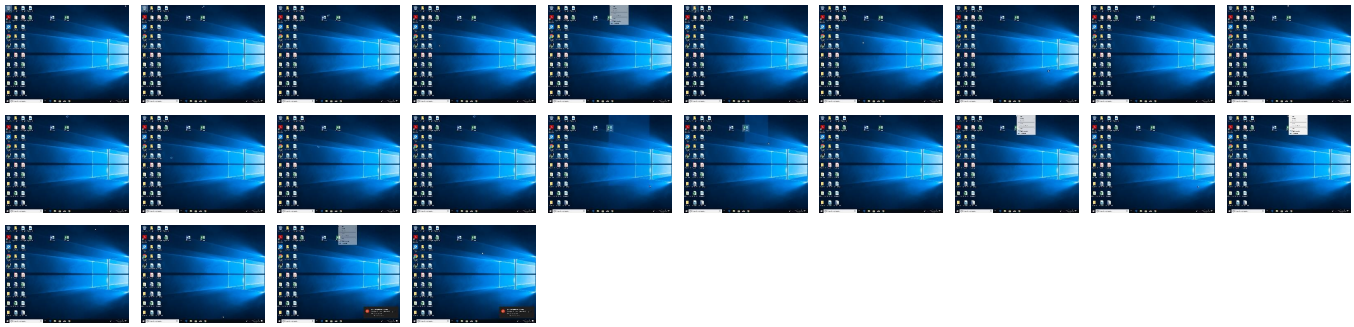
Behavior Graph



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
2022-571-GLS.exe	30%	ReversingLabs	Win32.Packed.Generic	
2022-571-GLS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\jsqqecy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\jsqqecy.exe	20%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.jsqqecy.exe.1090000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.2022-571-GLS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
2.0.jsqqecy.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.2022-571-GLS.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.jsqqecy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
td-ccm-168-233.wixdns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fulili.com/b31b/?8pq=tdO7S/Z/VqUa/I2xC15i+El5qu+HGrTkpc7PSFUM9PDChnmlJTvvTeLkqdaOGaksChda&q0DDzX=YreDi	0%	Avira URL Cloud	safe	
http://www.cdlcapitolsolutions.com/b31b/?8pq=gR42Xd1117OgJS+Outh2bFri+uyQrgf7E7TvWkJgQJ6aRmKfoh8EdM/DtT372TknNdyW&q0DDzX=YreDi	100%	Avira URL Cloud	malware	
http://www.easyentry.vip/b31b/?8pq=kQFV/3Ti5731GiKzPcF+l7m9iVSkkn86bXlgwK5ZhVk2Z3fCEdzJJK3qVV3FyS9CSUee&q0DDzX=YreDi	0%	Avira URL Cloud	safe	
www.cdlcapitolsolutions.com/b31b/	100%	Avira URL Cloud	malware	
www.cdlcapitolsolutions.com/b31b/	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-ccm-168-233.wixdns.net	34.117.168.233	true	true	• 0%, Virustotal, Browse	unknown
www.fulili.com	45.221.114.43	true	true		unknown
825610.parkingcrew.net	75.2.81.221	true	false		high
www.cdlcapitolsolutions.com	unknown	unknown	true		unknown
www.easyentry.vip	unknown	unknown	true		unknown

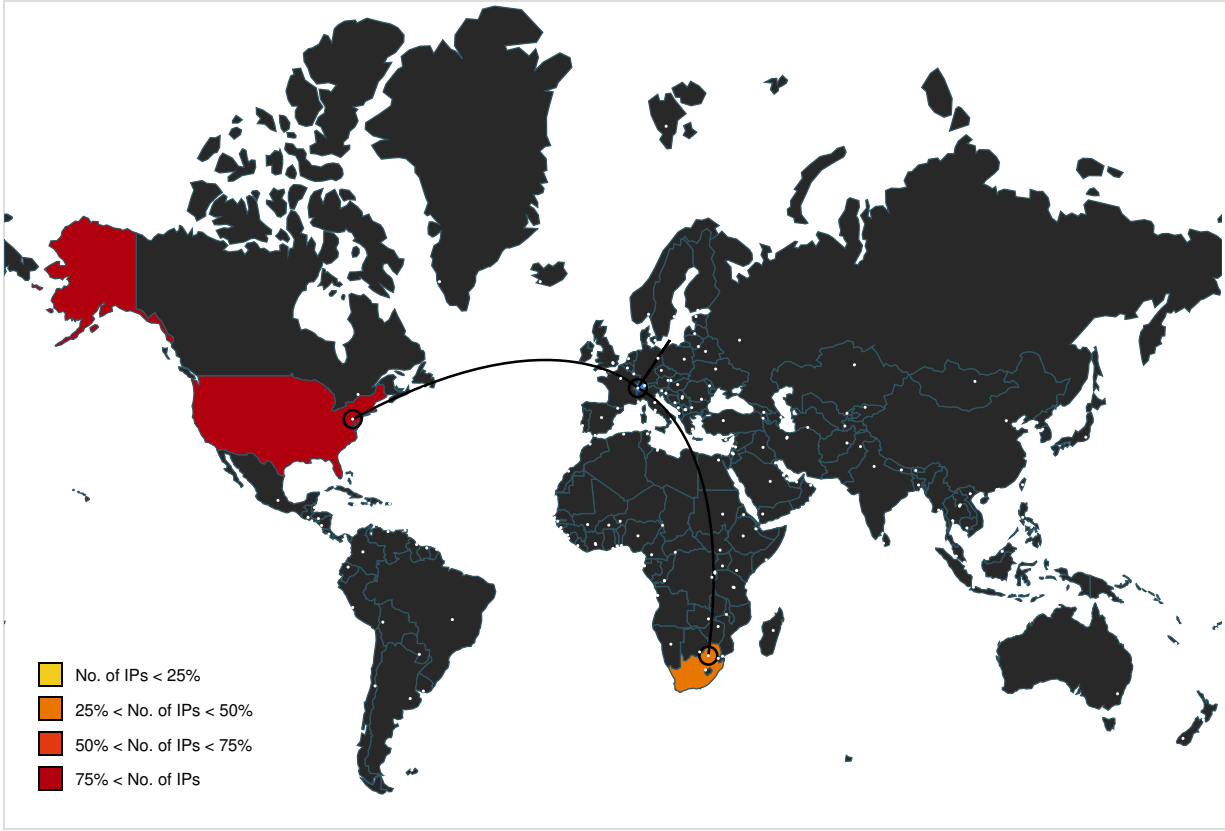
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cdlcapitolsolutions.com/b31b/?8pq=gR42Xd1117OgJS+Outh2bFri+uyQrgf7E7TvWkJgQJ6aRmKfoh8EdM/DtT372TknNdyW&q0DDzX=YreDi	true	• Avira URL Cloud: malware	unknown
http://www.fulili.com/b31b/?8pq=tdO7S/Z/VqUa/I2xC15i+El5qu+HGrTkpc7PSFUM9PDChnmlJTvvTeLkqdaOGaksChda&q0DDzX=YreDi	true	• Avira URL Cloud: safe	unknown
http://www.easyentry.vip/b31b/?8pq=kQFV/3Ti5731GiKzPcF+l7m9iVSkkn86bXlgwK5ZhVk2Z3fCEdzJJK3qVV3FyS9CSUee&q0DDzX=YreDi	true	• Avira URL Cloud: safe	unknown
www.cdlcapitolsolutions.com/b31b/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.36478190 9.0000000008260000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.317290516.0000000008260000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.347986981.000000 0008260000.00000004.00000001.00020000.00 000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	2022-571-GLS.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	2022-571-GLS.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.221.114.43	www.fulili.com	South Africa		328543	sun-asnSC	true
34.117.168.233	td-ccm-168-233.wixdns.net	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true
75.2.81.221	825610.parkingcrew.net	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755996
Start date and time:	2022-11-29 13:15:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2022-571-GLS.exe
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:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/4@3/3
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 68.9% (good quality ratio 59.8%) • Quality average: 70.7% • Quality standard deviation: 35.5%
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, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- 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\jsqqecy.exe

Process:	C:\Users\user\Desktop\2022-571-GLS.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	147968
Entropy (8bit):	6.1823629557808895
Encrypted:	false
SSDEEP:	3072:5qOPPLBLPd3kaQ+nBwYb+SxRC//LhYcglg7JdWGAwDY4Y4OCJiy:5qiLBLPdm/DhwgF4GduSv
MD5:	07875284CE0A6276F406B25F9E429270
SHA1:	38A67882404FE8CD7473C8B1949A0B5384B36F94
SHA-256:	AED6B2A3FB3845ECBC1AB0DFE26AED0CFFD1D220CA86F77BEBB44ECA02B3229E
SHA-512:	5DB9EF373A1535012BFEA4E4052616C4AF565B57535B2F5F381261AD2D13213592BB4AA80FFDE21139E00D8EB1B5A2612F205F72CA816613510F0D292C0A44C1

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...&.c.....@.....@.....@..... .....`.....\|.....text...0..... ..`.rdata..$t.....v.....@..@.data....%...@..... .....@....00cfg.....p.....&.....@..@.voltbl."....(.....rsrc.....*.....@..@.reloc.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nst2736.tmp

Process:	C:\Users\user\Desktop\2022-571-GLS.exe
File Type:	data
Category:	dropped
Size (bytes):	351352
Entropy (8bit):	7.441400818204764
Encrypted:	false
SSDEEP:	6144:FzKMbPJYY6ICfgM26evm226r8wqiLBLPdm/DhwgF4GduSv:08a+6xcqiLBLPcNnjdr
MD5:	F1E31AC6BD355DFA2F813075E84BCD0D
SHA1:	2C7C4B34C64E295DC9A1A7C803EB4E715AA00559
SHA-256:	39D893328B257A69AAB166D4843B16970AA8DF9B615A7356B8D3DB8351CFF089
SHA-512:	41B4422AB47A9FE2415678EA499D58F6AFF971044C581B95D8F6EC723248AD91CC622F6172D9B639DFEF4FAAFFD56F6180B63B03E3C1739C48FB54D34F510EF
Malicious:	false
Reputation:	low
Preview:	.....,.....[..... .....J.....!...j.....%..... ....

C:\Users\user\AppData\Local\Temp\xduyswx.up

Process:	C:\Users\user\Desktop\2022-571-GLS.exe
File Type:	data
Category:	dropped
Size (bytes):	5765
Entropy (8bit):	6.2092599243644075
Encrypted:	false
SSDEEP:	96:xqZQ5qvebu9XscBHOPNr9p1H9sBL3I9I4kcAlsRW1aR1vOj4GV8rqxyRG2OJkac/:xiQqGq9Xs+O1smVr+8WxyfikaF0MOJOY
MD5:	813EA3E20968DCA381FD705CCE6352AF
SHA1:	F5641EE0577E29603C5146827B0F3E920B307011
SHA-256:	BA88F948DE0F61DD0E1E09D5ABB977794A350380612C4F8E5AB7A7D5D3C5E108
SHA-512:	681484352435EF93B1E3EC909F30627C4373CB5F862A60C523DA9A02AE5DA9292004BD5C1787686E9025C81A19C47AB25F7B6F7072A86E3211728B02A95A63F3
Malicious:	false
Reputation:	low
Preview:	.f.. .\...+l.+l.+.+.+l...+. .\...zw+l.+$.+.-...\.V...=.0.+Z[.-.s..+jT.....+.z+-..Jc..w..+....j.....b+.=.-.....+.y .\...+l.+l.+.+.+l..'...\|.t...=.0.E..y.....c}...s....+.+}.z+.=.0U+..=.0.w+5 .=.0.K...v4.jC..-.....+.yy.zw+5.s.+gX+.d$..+|L+....+t`..+l...1..1..1}.=.0.+....|.N...{}.0V+..j[-.6.s...{....+}.....+.C...+.yy.zw .\...+l.+l.+.+.+l..0...|.-...+5.+.w1.....-.+...[.-.C...w.. =.0{+}.K.1}...Pd..+...+.Et.C.L..+.~.[.Er....g.EjL.....[.+..g..[.-.+5.+..C..15.w1.....[.+}.6.s..s.l..{.....+.z+-..Jc..w..+....E.....b+.=.-.....+.).....}....E}.1}..}.[.}.e.}...}.6.}.3C...C..... 1}.....1}.....1}.....1}.....1}.....1}..R..1}.....1}.....1}.s..1}.&...1}.....-..Y...1}<.cZ...-..l...1}...6...-.....1}.....-.....1}8.l....-.....1}D.zN...-.....1}...U...-.....1}..$.9..-....1}.s.l.....s.l....s.l.... es.l.....js.l....iE}.1}.C.....+}.l1}.C5..3`+}.s.....+}....+....h.s.+}.4h....s.l.....s.i...h.[.-.s.l.....s.i...h.[.-hs.l.....s.i....h.[.-ps.l

C:\Users\user\AppData\Local\Temp\zpnolg.oo

Process:	C:\Users\user\Desktop\2022-571-GLS.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.990584575642086**
Encrypted:	**true**
SSDEEP:	3072:lMbPJNjiLu5FhvUoerrdDaVCz37gMbapLPlA/evm2260F+8vV:lMbPJYY6ICfgM26evm226r89
MD5:	1CBA56AA7342010C42DE3448072BFFD6
SHA1:	41750AFCF5D21B6C3D1EF4D8B17CD5C283353206
SHA-256:	1F2933BB236406B4E5E0C84B64441F7103E8860C3DB1014E1D07BEABD47AC584
SHA-512:	E0DFB340E005729E784C828BEBFD428C147DB6EBC06A4261C960CE5CC2F5379A65DD723E7959A75A6D4F297AB5F7FC22ABE255D17E29E6D971E2E78845ADE 61

Malicious:	false
Reputation:	low
Preview:	......b......+...Z]..[.S=.+4..O|.....N..pF..X..+.L%..d..",.*.x....8-v@.).B!..g....:.@\f....r.jk...B..K.].C.../.xh....'e.i....._..?A..L.....%....-.l....5..[.P;.(.j.|..s..?c..;..Kr{2/...,.UPU.`.c..A\i....t\?=..Ox.(..1 ..,z-tf\V.@.._..AZ9..BB.....^..x.b;...ML.w...]B....:..g-..|.n....N...F..X..+.L ..d..",.*.xo.!..=p.;b...9.#..k...)e..};.....<3..Z..'"..>r.4$..)1\...'e.i.R.}../..Aj.!g.[%.{..w. .G...=....>.....p!dX..?c..;..WX./..<C....q.....]\i..r.K*%.U.....1 ..,z..3\V.@.....AZ....B.H..f^9.x.b....ML.w.2.]B....:...-.O|.....N..pF..X..+.L%..d..",.*.xo.!..=p.;b...9.#..k...)e..};.....<3..Z..'"..>r.4$..)1\...'e.i.R.}../..Aj.!g.[%.{..w. .G...=....>.....p!dX..?c..;..Kr{2/...>..qq..;_..A\i..r.K*%.U.O..(..1 ..,z..3\V.@.....AZ....B.H..f^9.x.b....ML.w.2.]B....:...-.O|.....N..pF..X..+.L%..d..",.*.xo.!..=p.;b...9.#..k...)e..};.....<3..Z..'"..>r.4$..)1\...'e.i.R.}../..Aj.!g.[%.{..w. .G...=....>.....p!dX..?c..;..Kr{2/...>..qq..;_..A\i..r.K*%.U.O..(..1 ..,z

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.93130981619841
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:	2022-571-GLS.exe
File size:	274453
MD5:	6cc14805bbf5e6bfb4daae5c8a61af7e
SHA1:	34836f2aa6a4e97705352a50d2a7147c857fea94
SHA256:	029d4fe47cb21a8f4e1dbe1863cf43cba6ac777e008b9675d381fda82986196b
SHA512:	5f1bb5a77d471e49e15ff414b24ac89858e5458884f8f672a92376434dd9363e6d80146d6448b4ee0233c70531f58c4c7d431d9f873e6d1a2fdacf680479b2c6
SSDEEP:	6144:QBn14u11x6y/QH2tw81qVegiZU/S4RaXFKia7ZiOfu:g4uRX4WvqMgiZgSXFKhZiO2
TLSH:	224412ABB2E70AB3C46345729F35B331E67EE910113456BF33E22E779E702979406291
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...ly.V.....^.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40324f
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:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796C [Sun Dec 27 05:38:52 2015 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:	ab6770b0a8635b9d92a5838920cfe770

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp

Instruction
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+1Ch], ebx
mov dword ptr [esp+14h], 00409130h
xor esi, esi
mov byte ptr [esp+18h], 00000020h
call dword ptr [004070B8h]
call dword ptr [004070B4h]
cmp ax, 00000006h
je 00007F91F4D06083h
push ebx
call 00007F91F4D08E71h
cmp eax, ebx
je 00007F91F4D06079h
push 00000C00h
call eax
push 004091E0h
call 00007F91F4D08DF2h
push 004091D8h
call 00007F91F4D08DE8h
push 004091CCh
call 00007F91F4D08DDEh
push 0000000Dh
call 00007F91F4D08E41h
push 0000000Bh
call 00007F91F4D08E3Ah
mov dword ptr [00423F84h], eax
call dword ptr [00407034h]
push ebx
call dword ptr [00407270h]
mov dword ptr [00424038h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007F91F4D08A71h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007F91F4D08A5Fh
push ebx
call dword ptr [00407144h]

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	0x73cc	0xa0	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x9e0	.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	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.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	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x9e0	0xa00	False	0.45625	data	4.509328731926377	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d190	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x2d478	0x100	data	English	United States
RT_DIALOG	0x2d578	0x11c	data	English	United States
RT_DIALOG	0x2d698	0x60	data	English	United States
RT_GROUP_ICON	0x2d6f8	0x14	data	English	United States
RT_MANIFEST	0x2d710	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, GetTempPathA, GetCommandLineA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, LoadLibraryA, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, WaitForSingleObject, ExitProcess, GetWindowsDirectoryA, GetProcAddress, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, WriteFile, MulDiv, LoadLibraryExA, GetModuleHandleA, MultiByteToWideChar, FreeLibrary
USER32.dll	GetWindowRect, EnableMenuItem, GetSystemMenu, ScreenToClient, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetForegroundWindow, PostQuitMessage, RegisterClassA, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, OpenClipboard, TrackPopupMenu, SendMessageTimeoutA, GetDC, LoadImageA, GetDlgItem, FindWindowExA, IsWindow, SetClipboardData, SetWindowLongA, EmptyClipboard, SetTimer, CreateDialogParamA, wsprintfA, ShowWindow, SetWindowTextA

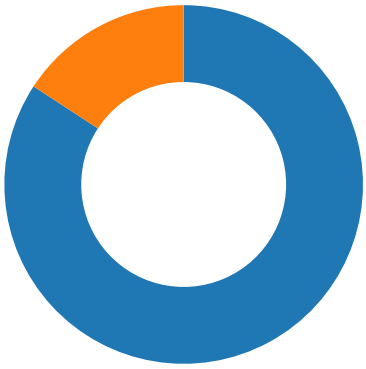
DLL	Import
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteValueA, SetFileSecurityA, RegOpenKeyExA, RegDeleteKeyA, RegEnumValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:17:16.933298111 CET	49696	80	192.168.2.4	34.117.168.233
Nov 29, 2022 13:17:16.956123114 CET	80	49696	34.117.168.233	192.168.2.4
Nov 29, 2022 13:17:16.956255913 CET	49696	80	192.168.2.4	34.117.168.233
Nov 29, 2022 13:17:16.956408024 CET	49696	80	192.168.2.4	34.117.168.233
Nov 29, 2022 13:17:16.978993893 CET	80	49696	34.117.168.233	192.168.2.4
Nov 29, 2022 13:17:17.045778036 CET	80	49696	34.117.168.233	192.168.2.4
Nov 29, 2022 13:17:17.045831919 CET	80	49696	34.117.168.233	192.168.2.4
Nov 29, 2022 13:17:17.045938969 CET	49696	80	192.168.2.4	34.117.168.233
Nov 29, 2022 13:17:17.046009064 CET	49696	80	192.168.2.4	34.117.168.233
Nov 29, 2022 13:17:17.068516970 CET	80	49696	34.117.168.233	192.168.2.4
Nov 29, 2022 13:17:37.271229029 CET	49697	80	192.168.2.4	75.2.81.221
Nov 29, 2022 13:17:37.290606976 CET	80	49697	75.2.81.221	192.168.2.4
Nov 29, 2022 13:17:37.290796041 CET	49697	80	192.168.2.4	75.2.81.221
Nov 29, 2022 13:17:37.291032076 CET	49697	80	192.168.2.4	75.2.81.221
Nov 29, 2022 13:17:37.310297966 CET	80	49697	75.2.81.221	192.168.2.4
Nov 29, 2022 13:17:37.432542086 CET	80	49697	75.2.81.221	192.168.2.4
Nov 29, 2022 13:17:37.432614088 CET	80	49697	75.2.81.221	192.168.2.4
Nov 29, 2022 13:17:37.432749987 CET	49697	80	192.168.2.4	75.2.81.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:17:37.432842016 CET	49697	80	192.168.2.4	75.2.81.221
Nov 29, 2022 13:17:37.447979927 CET	80	49697	75.2.81.221	192.168.2.4
Nov 29, 2022 13:17:37.448339939 CET	49697	80	192.168.2.4	75.2.81.221
Nov 29, 2022 13:17:37.452009916 CET	80	49697	75.2.81.221	192.168.2.4
Nov 29, 2022 13:17:57.920108080 CET	49698	80	192.168.2.4	45.221.114.43
Nov 29, 2022 13:17:58.118402004 CET	80	49698	45.221.114.43	192.168.2.4
Nov 29, 2022 13:17:58.127572060 CET	49698	80	192.168.2.4	45.221.114.43
Nov 29, 2022 13:17:58.127811909 CET	49698	80	192.168.2.4	45.221.114.43
Nov 29, 2022 13:17:58.326272964 CET	80	49698	45.221.114.43	192.168.2.4
Nov 29, 2022 13:17:58.326320887 CET	80	49698	45.221.114.43	192.168.2.4
Nov 29, 2022 13:17:58.332259893 CET	49698	80	192.168.2.4	45.221.114.43
Nov 29, 2022 13:17:58.332482100 CET	49698	80	192.168.2.4	45.221.114.43
Nov 29, 2022 13:17:58.530942917 CET	80	49698	45.221.114.43	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:17:16.879111052 CET	50911	53	192.168.2.4	8.8.8.8
Nov 29, 2022 13:17:16.917241096 CET	53	50911	8.8.8.8	192.168.2.4
Nov 29, 2022 13:17:37.245763063 CET	59683	53	192.168.2.4	8.8.8.8
Nov 29, 2022 13:17:37.270123005 CET	53	59683	8.8.8.8	192.168.2.4
Nov 29, 2022 13:17:57.618912935 CET	64167	53	192.168.2.4	8.8.8.8
Nov 29, 2022 13:17:57.917346954 CET	53	64167	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 13:17:16.879111052 CET	192.168.2.4	8.8.8.8	0xf9d3	Standard query (0)	www.cdlcapitolsolutions.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:17:37.245763063 CET	192.168.2.4	8.8.8.8	0x5ae3	Standard query (0)	www.easyentry.vip	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:17:57.618912935 CET	192.168.2.4	8.8.8.8	0x9a51	Standard query (0)	www.fulili.com	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
Nov 29, 2022 13:17:16.917241096 CET	8.8.8.8	192.168.2.4	0xf9d3	No error (0)	www.cdlcapitolsolutions.com	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 13:17:16.917241096 CET	8.8.8.8	192.168.2.4	0xf9d3	No error (0)	gcdn0.wixdns.net	td-ccm-168-233.wixdns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 13:17:16.917241096 CET	8.8.8.8	192.168.2.4	0xf9d3	No error (0)	td-ccm-168-233.wixdns.net		34.117.168.233	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:17:37.270123005 CET	8.8.8.8	192.168.2.4	0x5ae3	No error (0)	www.easyentry.vip	825610.parkingcrew.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 13:17:37.270123005 CET	8.8.8.8	192.168.2.4	0x5ae3	No error (0)	825610.parkingcrew.net		75.2.81.221	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:17:57.917346954 CET	8.8.8.8	192.168.2.4	0x9a51	No error (0)	www.fulili.com		45.221.114.43	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.cdlcapitolsolutions.com
- www.easyentry.vip
- www.fulili.com

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

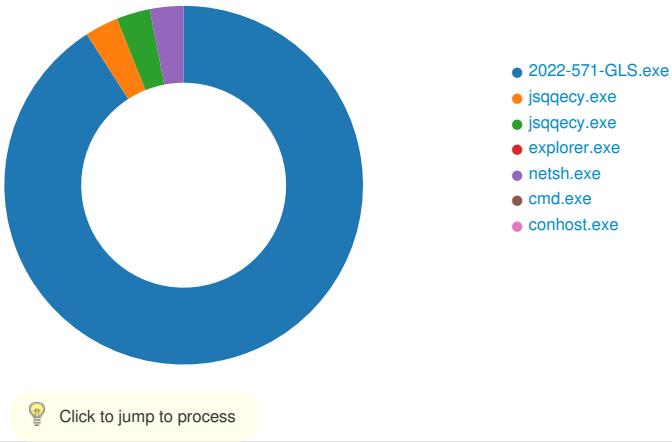
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xE5
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xE5
GetMessageW	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xE5
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xE5

Statistics

Behavior



System Behavior

Analysis Process: 2022-571-GLS.exe PID: 5464, Parent PID: 3528

General

Target ID:	0

Start time:	13:15:56
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\2022-571-GLS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\2022-571-GLS.exe
Imagebase:	0x400000
File size:	274453 bytes
MD5 hash:	6CC14805BBF5E6BFB4DAAE5C8A61AF7E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: jsqqecy.exe PID: 1236, Parent PID: 5464

General

Target ID:	1
Start time:	13:15:57
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\jsqqecy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\jsqqecy.exe" C:\Users\user\AppData\Local\Temp\xduyswx.up
Imagebase:	0xbc0000
File size:	147968 bytes
MD5 hash:	07875284CE0A6276F406B25F9E429270
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.304792498.0000000001090000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.304792498.0000000001090000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.304792498.0000000001090000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.304792498.0000000001090000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xduyswx.up	unknown	5765	success or wait	1	BC1A1D	ReadFile

Analysis Process: jsqqecy.exe PID: 1224, Parent PID: 1236

General

Target ID:	2
Start time:	13:15:57
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\jsqqecy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\jsqqecy.exe" C:\Users\user\AppData\Local\Temp\xduyswx.up
Imagebase:	0xbc0000
File size:	147968 bytes
MD5 hash:	07875284CE0A6276F406B25F9E429270

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.381040455.0000000001060000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.300703858.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.300703858.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.300703858.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.300703858.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.380708027.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.380708027.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.380708027.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.380708027.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.381071998.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.381071998.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.381071998.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.381071998.0000000001090000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3528**, Parent PID: **1224**

General

Target ID:	3
Start time:	13:16:01
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.352626169.000000000DF14000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.352626169.000000000DF14000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.352626169.000000000DF14000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.352626169.000000000DF14000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: netsh.exe PID: 6140, Parent PID: 3528

General

Target ID:	4
Start time:	13:16:33
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x7ff7c72c0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.562405405.0000000002930000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.562405405.0000000002930000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.562405405.0000000002930000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.562405405.0000000002930000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.562589613.0000000002E20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.562589613.0000000002E20000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.562589613.0000000002E20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.562589613.0000000002E20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.562707442.0000000002E50000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.562707442.0000000002E50000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.562707442.0000000002E50000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.562707442.0000000002E50000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	294A457	NtReadFile

Analysis Process: cmd.exe PID: 4136, Parent PID: 6140

General

Target ID:	5
Start time:	13:16:38
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\jsqqecy.exe"
Imagebase:	0xd90000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4828**, Parent PID: **4136**

General

Target ID:	6
Start time:	13:16:38
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly