ID: 755939
Sample Name: SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
Cookbook: default.jbs
Time: 10:40:46
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

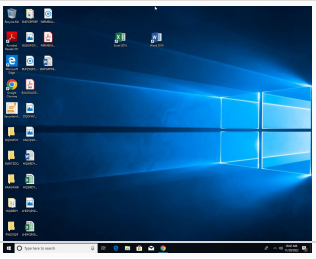
Windows Analysis Report

SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe

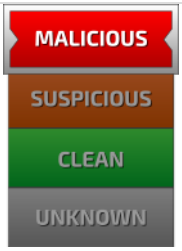
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
Analysis ID:	755939
MD5:	f536ea8fb5b6586.
SHA1:	313804060f2511..
SHA256:	e539f80082f961c..
Tags:	exe
Infos:	



Detection



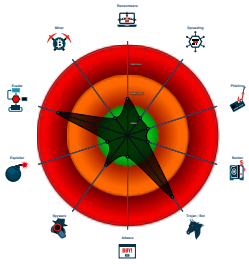
DBatLoader, FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected DBatLoader
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe (PID: 6024 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe MD5: F536EA8FB5B6586BB2FFC764CD52ABFF)
  - wscript.exe (PID: 5988 cmdline: C:\Windows\System32\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - luigzwjd.exe (PID: 3208 cmdline: "C:\Users\Public\Libraries\luigzwjd.exe" MD5: F536EA8FB5B6586BB2FFC764CD52ABFF)
        - wscript.exe (PID: 1264 cmdline: C:\Windows\System32\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - luigzwjd.exe (PID: 1848 cmdline: "C:\Users\Public\Libraries\luigzwjd.exe" MD5: F536EA8FB5B6586BB2FFC764CD52ABFF)
        - wscript.exe (PID: 5044 cmdline: C:\Windows\System32\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.brainbookgroup.com/nvp4/"
  ]
}
```

Threatname: DBatLoader

```
{
  "Download Url": "https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21850&authkey=AEcOcvbyHqeCMT0"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\djwzgiuI.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x58:$hotkey: \x0AHotKey=7 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\djwzgiuI.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x7d58:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x20787:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xc026:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1954e:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1934c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18df8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1944e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x195c6:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xbbf1:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18043:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1f4fe:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x204f1:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1b820:$sqlite3step: 68 34 1C 7B E1 • 0x1c398:$sqlite3step: 68 34 1C 7B E1 • 0x1b862:$sqlite3text: 68 38 2A 90 C5 • 0x1c3dd:$sqlite3text: 68 38 2A 90 C5 • 0x1b879:$sqlite3blob: 68 53 D8 7F 8C • 0x1c3f3:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.564946662.0000000004830000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.2720000.2.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
0.2.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.2a2eed8.3.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
1.2.wscript.exe.10410000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.wscript.exe.10410000.3.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x7d58:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x20787:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xc026:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1954e:$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.wscript.exe.10410000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1934c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18df8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1944e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x195c6:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xbbf1:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18043:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1f4fe:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x204f1:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 6 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 / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected DBatLoader

Malware Analysis System Evasion

WScript reads language and country specific registry keys (likely country aware script)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

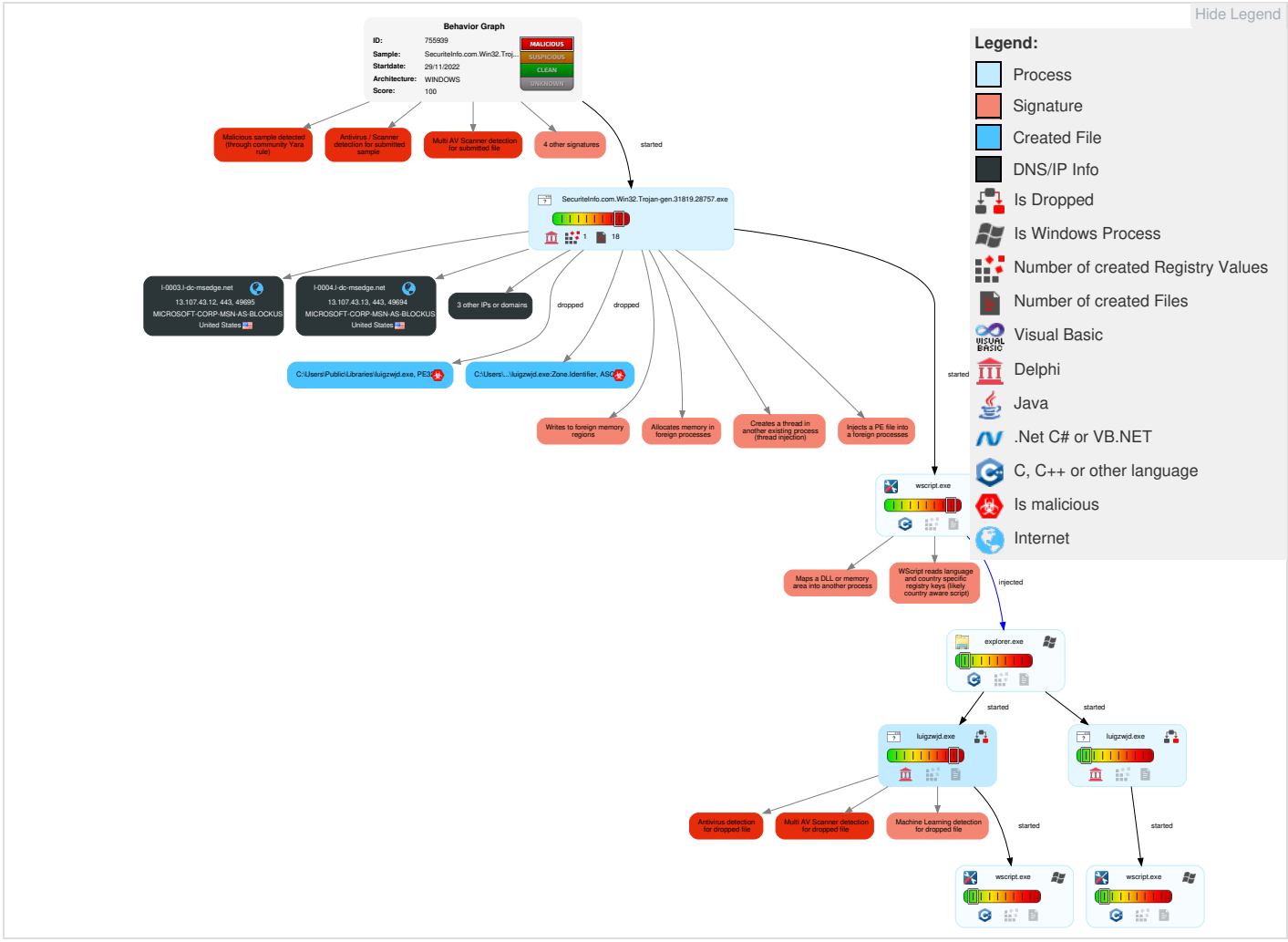
Yara detected FormBook

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	1 Native API	1 Registry Run Keys / Startup Folder	5 2 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	5 2 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 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)	1 Deobfuscate/Decode Files or Information	NTDS	3 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated 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	1 Software Packing	Cached Domain Credentials	1 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 DLL Side-Loading	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

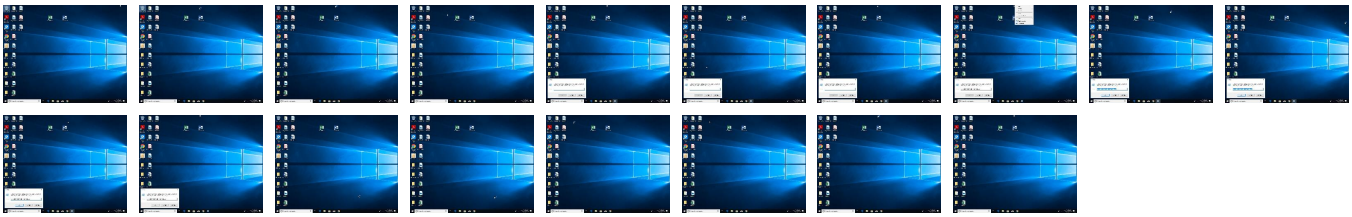
Behavior Graph



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
SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe	15%	ReversingLabs	Win32.Trojan.Generic	
SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe	31%	Virustotal		Browse
SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe	100%	Avira	HEUR/AGEN.1214697	
SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\luigzwjd.exe	100%	Avira	HEUR/AGEN.1214697	
C:\Users\Public\Libraries\luigzwjd.exe	100%	Joe Sandbox ML		
C:\Users\Public\Libraries\luigzwjd.exe	15%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.25c8248.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.wscript.exe.10410000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.2581218.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1214697		Download File
1.0.wscript.exe.10410000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.wscript.exe.5d50000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.wscript.exe.10410000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.wscript.exe.10410000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.wscript.exe.10410000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.2720000.2.unpack	100%	Avira	TR/Hijacker.Gen		Download File
0.2.SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe.2a2eed8.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.luigzwjd.exe.2438248.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.brainbookgroup.com/nvp4/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0003.l-dc-msedge.net	13.107.43.12	true	false		unknown
l-0004.l-dc-msedge.net	13.107.43.13	true	false		unknown
onedrive.live.com	unknown	unknown	false		high
oyuurg.ph.files.1drv.com	unknown	unknown	false		high

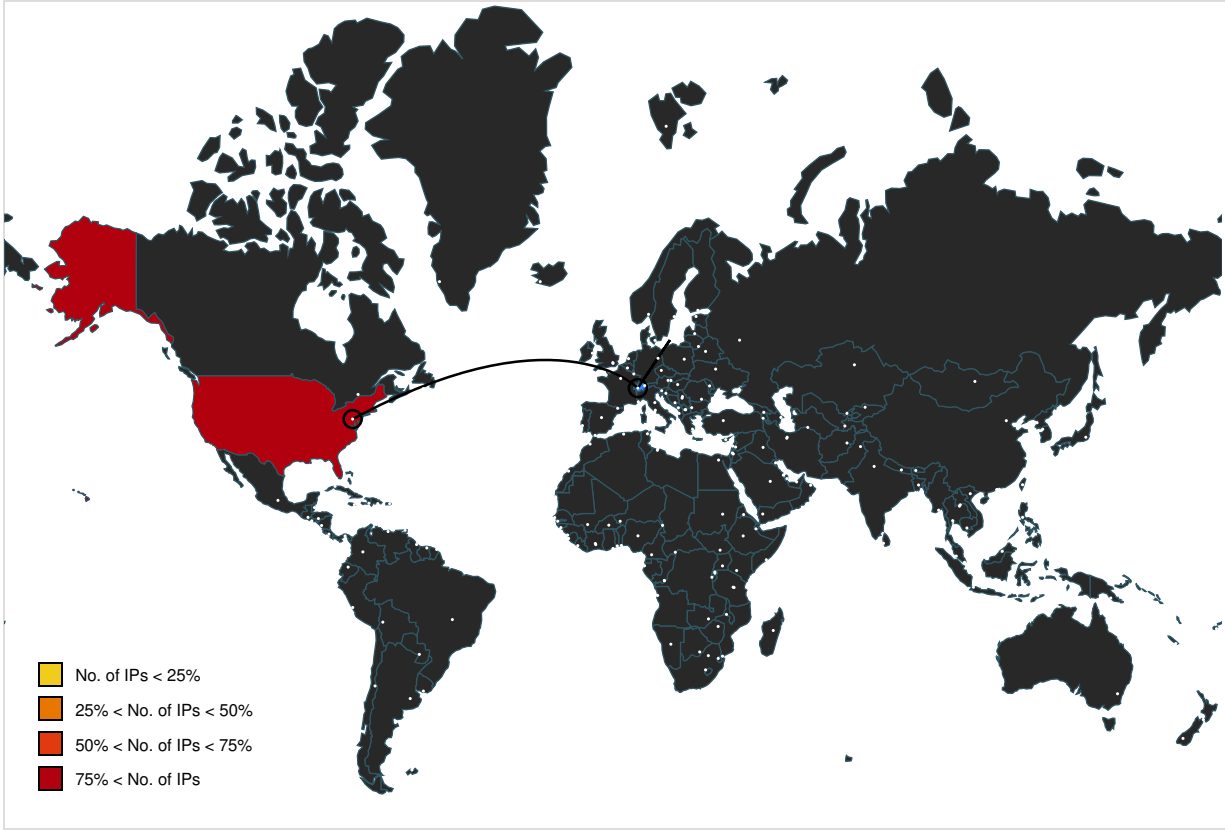
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21850&authkey=AEcOcvbyHqeCMT0	false		high
www.brainbookgroup.com/nvp4/	true	• Avira URL Cloud: safe	low
http://https://oyuurg.ph.files.1drv.com/y4mJr27PXKP1w7VmweyBhr9jXuXcCKUmjp-l0AjYgYvmFILscr-gs1ZCYQgPakl85NdXiyluyI2K__n-DTHXtIuKBfix9QJgWA8xZXLmTFKCzO-QrrlJfjFNlxYKvj4CV1InzMNLAsu2pDihkqbVzbigQu3lZ2fbCWy9RogAq5NxzuJ1VRoowitd9q4QmyU6H1eR5JdbJA1JsNbjwDPqFHy3g/luigzwjduoa?download&psid=1	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000000.32819089 0.000000000F270000.00000004.00000001.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.43.12	l-0003.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.43.13	l-0004.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755939
Start date and time:	2022-11-29 10:40:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.Trojan-gen.31819.28757.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:	18
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@10/5@2/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 99.8% (good quality ratio 86.8%) • Quality average: 74.2% • Quality standard deviation: 34.1%
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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, odc-web-brs.onedrive.akadns.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, fs.microsoft.com, ocsp.digicert.com, odc-web-geo.onedrive.akadns.net, ph-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, ctldl.windowsupdate.com, odc-ph-files-geo.onedrive.akadns.net, odc-ph-files-brs.onedrive.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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
10:41:50	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe modified
10:41:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run luigzwjd C:\Users\Public\Libraries\djwzgiuI.url
10:42:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run luigzwjd C:\Users\Public\Libraries\djwzgiuI.url
10:42:10	API Interceptor	2x Sleep call for process: luigzwjd.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:\Users\Public\Libraries\luigzwjd

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
File Type:	data
Category:	dropped
Size (bytes):	189869
Entropy (8bit):	**7.993154525475343**
Encrypted:	**true**
SSDEEP:	3072:JB2rul114IXlkeukze3mxOVeFRTe8a+opBUMkNtSx1WOUzM80SAjWsNhX5deg/+V:JB2rRxuZmxOVuTe8lozUMWtS2grfx+V
MD5:	7AC99DA57C0EE5DEC172741B47903FA4
SHA1:	90BD8551DD694D2AB0A857731735761F25D6FD29
SHA-256:	867D6D0F50C2C377B44B4988A55C484C29CAFE4306032F72809C749178E05F7A
SHA-512:	0AD7A7B6FF56F9F2AAF3DCAAD013D22D5A4D592DFD2B01D5419CDECA49BE8F4C7433ABB5948C22E92181A37CF74E372A1287E2092C09AD93EEB832B2CA8AA8BF
Malicious:	false
Reputation:	low
Preview:	....4.e.4..kk.4.....kk.4.....4..o..}..}..yq..uo..o..o.swos...m.q..us...q.s.....w.....4.e.4..kk.4.....kk.4.....4..us.....{m....4.e.4..kk.4.....kk.4.....47)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'.....-..7.9...77'...').1./.97)..9.....%...7...9.'....Y.^..._....j...0..-.2sW..(TD..M>."....6)y.s.Tl...#....K3-.h.....(.H.....(....'zI...hS(.#&n.....C".`..O..TG

C:\Users\Public\Libraries\luigzwjd.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	750592
Entropy (8bit):	6.871648147377771
Encrypted:	false
SSDEEP:	12288:i1qMhtVLzLypCggIh36+O9dvjpQVeri442qKk/RqIkr:WFhHzmQgn6+8T/r7PaqI
MD5:	F536EA8FB5B6586BB2FFC764CD52ABFF
SHA1:	313804060F2511B8382D369A3949D5524C1ADAEF
SHA-256:	E539F80082F961C600E6FF2A21E969D0641AA787831259D3FDD772B28D469721
SHA-512:	873E0A7174BE40DB35F8E8F06FD7FFAF340128E7EE6EC09F691CA8857AAC9B1F4C5D6CDB76841858EF4E52B2FA5A4A9A185882215676 26FE1474B8B101CEF8EA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....b.....&.....0....@.....@..... ...%.....$.....p...n.....`..... ..$'.....text...,..... ..`.itext..$.... ....`.data.....0.....@....bss....`6.....idata...%... ...&.....@....tls.. ..4....P.....rdata.....`.....@..@.reloc...n...p...p.....@..B.rsrc....$.....$...N.....@..@.....r.....@..@..... .....

C:\Users\Public\Libraries\luigzwjd.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\Public\Libraries\djwzgiul.url

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\luigzwjd.exe">), ASCII text, with CRLF line terminators

Category:	modified
Size (bytes):	100
Entropy (8bit):	5.05252935030364
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMVKSsGKd6dbP6v:HRYFVmTWDyz/SsbMPE
MD5:	94A7CAD400BB0ED39AE61258D1388317
SHA1:	E3F698F5EAA841B12F2077F1884F1719CF6BADF0
SHA-256:	89A9D4CDBC1953F6092CF9A15E8AEB63E599B5600345E2297E075C95CE2DC0AC
SHA-512:	ECF712A5F03DE0D19D8B83E11A579B5C5056548F08C15BD79F8DCBA6E671AF0C0B3C0AF60D97038D98D316774277DFD28223CF2EF188EC1F58BEC53EBB093 E3
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\djwzgiul.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\djwzgiul.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\luigzwjd.exe"..IconIndex=28..HotKey=79..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\luigzwjduoa[1]

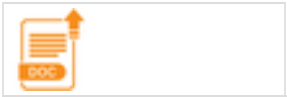
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
File Type:	data
Category:	dropped
Size (bytes):	189869
Entropy (8bit):	**7.993154525475343**
Encrypted:	**true**
SSDEEP:	3072:JB2rul114IXlkeukze3mxOVeFRTe8a+opBUMkNtSx1WOUzM80SAjWsNhX5deg/+V:JB2rRxuZmxOVuTe8lozUMWtS2grfx+V
MD5:	7AC99DA57C0EE5DEC172741B47903FA4
SHA1:	90BD8551DD694D2AB0A857731735761F25D6FD29
SHA-256:	867D6D0F50C2C377B44B4988A55C484C29CAFE4306032F72809C749178E05F7A
SHA-512:	0AD7A7B6FF56F9F2AAF3DCAAD013D22D5A4D592DFD2B01D5419CDECA49BE8F4C7433ABB5948C22E92181A37CF74E372A1287E2092C09AD93EEB832B2CA8A 8BF
Malicious:	false
Preview:	....4.e.4..kk.4........kk.4.......4..o..}..}..yq..uo..o..o.swos...m.q..us...q.s.....w.......4.e.4..kk.4........kk.4.......4..us.....{m....4.e.4..kk.4........kk.4.......47)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'........-..7.9...77'...'.)1./.97)..9.....%...7...9.'.....Y.^..._....j...0..-.2sW..(TD..M>."....6)y.s.Tl...#....K3-.h.....(.H.....(....'zI...hS(.#&n......C".`..O..TG

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.871648147377771
TrID:	• Win32 Executable (generic) a (10002005/4) 99.38% • InstallShield setup (43055/19) 0.43% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
File size:	750592
MD5:	f536ea8fb5b6586bb2ffc764cd52abff
SHA1:	313804060f2511b8382d369a3949d5524c1adaef
SHA256:	e539f80082f961c600e6ff2a21e969d0641aa787831259d3fdd772b28d469721
SHA512:	873e0a7174be40db35f8e8f06fd7ffaf340128e7ee6ec09f691ca8857aac9b1f4c5d6cdb76841858ef4e52b2fa5a4a9a18588221567626fe1474b8b101cef8ea
SSDEEP:	12288:i1qMhtVLzLypCgglh36+O9dvjpQVeri442qKk/Rqlkr:WFhHzmQgn6+8T/r7Paql
TLSH:	FFF47E6761D04537D02716398C1BA7A8596F7EE03F14BC6667E03DCC9F382CA74292AB
File Content Preview:	MZP.....................@...!..L.!..This program must be run under Win32..$7..

File Icon



Icon Hash:	2321270727090923

Static PE Info

General

Entrypoint:	0x4626e8
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	5a047051636dce23e36a7dceaf1507c0

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0046105Ch
call 00007F450101B915h
mov ecx, dword ptr [0046D410h]
mov eax, dword ptr [0046D324h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00460A90h]
call 00007F450106E2EDh
mov eax, dword ptr [0046D324h]
mov eax, dword ptr [eax]
call 00007F450106E361h
call 00007F4501019A18h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x72000	0x25ac	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x42400	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x77000	0x6eec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x76000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x72724	0x5e4	.idata
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	0x6022c	0x60400	False	0.5191025771103897	data	6.531038724700122	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0x62000	0x724	0x800	False	0.57373046875	data	5.847823102407548	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x63000	0xa49c	0xa600	False	0.08546686746987951	data	6.483179375342552	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x6e000	0x3660	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x72000	0x25ac	0x2600	False	0.32452713815789475	data	5.139331879404015	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x75000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x76000	0x18	0x200	False	0.05078125	data	0.2108262677871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x77000	0x6eec	0x7000	False	0.6196986607142857	data	6.6810323966616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x42400	0x42400	False	0.4435620577830189	data	6.403601787519998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7ef0c	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"	English	United States
RT_CURSOR	0x7f040	0x134	data	English	United States
RT_CURSOR	0x7f174	0x134	data	English	United States
RT_CURSOR	0x7f2a8	0x134	data	English	United States
RT_CURSOR	0x7f3dc	0x134	data	English	United States
RT_CURSOR	0x7f510	0x134	data	English	United States
RT_CURSOR	0x7f644	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	English	United States
RT_BITMAP	0x7f778	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7f8a0	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7f9c8	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7faf0	0xe8	Device independent bitmap graphic, 13 x 16 x 4, image size 128	English	United States
RT_BITMAP	0x7fbd8	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x7fd00	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7fe28	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States
RT_BITMAP	0x7fef8	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80020	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80148	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80270	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80398	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x804c0	0xe8	Device independent bitmap graphic, 12 x 16 x 4, image size 128	English	United States
RT_BITMAP	0x805a8	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x806d0	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x807f8	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States
RT_BITMAP	0x808c8	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x809f0	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80b18	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80c40	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80d68	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80e90	0xe8	Device independent bitmap graphic, 13 x 16 x 4, image size 128	English	United States
RT_BITMAP	0x80f78	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x810a0	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x811c8	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States
RT_BITMAP	0x81298	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x813c0	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_ICON	0x814e8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0x82590	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x84b38	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736		
RT_ICON	0x89fc0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864		
RT_STRING	0x93468	0x200	data		
RT_STRING	0x93668	0x188	data		
RT_STRING	0x937f0	0xc8	data		
RT_STRING	0x938b8	0x350	data		
RT_STRING	0x93c08	0x3d8	data		
RT_STRING	0x93fe0	0x388	data		
RT_STRING	0x94368	0x418	data		
RT_STRING	0x94780	0x140	data		
RT_STRING	0x948c0	0xcc	data		
RT_STRING	0x9498c	0x1ec	data		
RT_STRING	0x94b78	0x3b0	data		
RT_STRING	0x94f28	0x354	data		
RT_STRING	0x9527c	0x2a4	data		
RT_RCDATA	0x95520	0x10	data		
RT_RCDATA	0x95530	0x2a7c2	GIF image data, version 89a, 300 x 168	English	United States
RT_RCDATA	0xbfcf4	0x254	data		

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0xbff48	0x3e0	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xc0328	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc033c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc0350	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc0364	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc0378	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc038c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc03a0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xc03b4	0x3e	data		

Imports

DLL	Import
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
user32.dll	GetKeyboardType, DestroyWindow, LoadStringA, MessageBoxA, CharNextA
kernel32.dll	GetACP, Sleep, VirtualFree, VirtualAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, CompareStringA, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageW, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageW, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameA, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, Polyline, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetPixel, GetPaletteEntries, GetObjectA, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExcludeClipRect, DeleteObject, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, lstrcatA, _lread, _lopen, _llseek, _lclose, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalFindAtomA, GlobalDeleteAtom, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegFlushKey, RegCloseKey, IsValidSid
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit

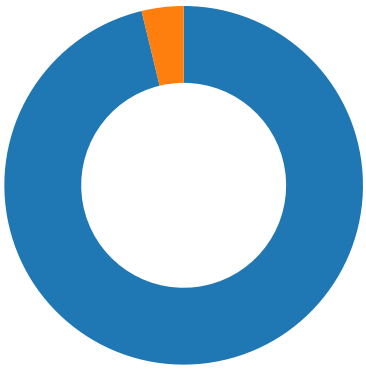
DLL	Import
comctl32.dll	_TrackMouseEvent, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
comdlg32.dll	GetOpenFileNameA
URL	AutodialHookCallback

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 10:41:51.260737896 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.260787964 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:51.260881901 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.301680088 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.301722050 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:51.396750927 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:51.396946907 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.686289072 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.686328888 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:51.687253952 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:51.687335968 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.690499067 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:51.690519094 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:52.246649027 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:52.246813059 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:52.246871948 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:52.246985912 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:52.258460045 CET	49694	443	192.168.2.3	13.107.43.13
Nov 29, 2022 10:41:52.258503914 CET	443	49694	13.107.43.13	192.168.2.3
Nov 29, 2022 10:41:52.373297930 CET	49695	443	192.168.2.3	13.107.43.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:41:52.373383999 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.373493910 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.375330925 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.375380039 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.472461939 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.472654104 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.473560095 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.473710060 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.496169090 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.496221066 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.496706009 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.496802092 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.497447014 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.497464895 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.742984056 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.743009090 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.743072033 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.743086100 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.743117094 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.743138075 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.743154049 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.743190050 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.743197918 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.743208885 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.743266106 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.743283987 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767354965 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767493010 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767518997 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767570972 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767627001 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767640114 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767678022 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767690897 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767709017 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767723083 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767776966 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767807961 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767818928 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767868996 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767869949 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767894030 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.767936945 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767970085 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.767982960 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.768018961 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.768029928 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.768042088 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.768094063 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.768187046 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.768193960 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.768244028 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.768263102 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.768348932 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.768362045 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.768424034 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793473005 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793580055 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793592930 CET	443	49695	13.107.43.12	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:41:52.793620110 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793670893 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793687105 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793699980 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793730021 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793749094 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793764114 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793796062 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793840885 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793847084 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793863058 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.793920040 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793945074 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.793955088 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.794003963 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.794007063 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.794028044 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.794070959 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.794096947 CET	49695	443	192.168.2.3	13.107.43.12
Nov 29, 2022 10:41:52.794107914 CET	443	49695	13.107.43.12	192.168.2.3
Nov 29, 2022 10:41:52.794154882 CET	49695	443	192.168.2.3	13.107.43.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 10:41:51.199362993 CET	54397	53	192.168.2.3	8.8.8.8
Nov 29, 2022 10:41:52.304203033 CET	59324	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 10:41:51.199362993 CET	192.168.2.3	8.8.8.8	0x4698	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:41:52.304203033 CET	192.168.2.3	8.8.8.8	0x7cef	Standard query (0)	oyuurg.ph.files.1drv.com	A (IP address)	IN (0x0001)	false

DNS Answers

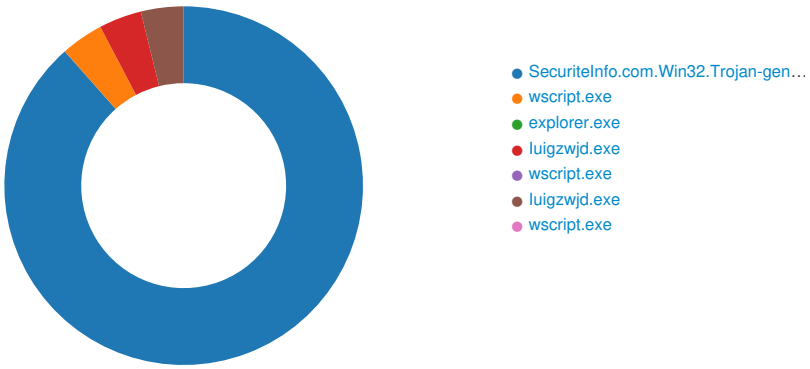
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 10:41:51.242723942 CET	8.8.8.8	192.168.2.3	0x4698	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:41:51.242723942 CET	8.8.8.8	192.168.2.3	0x4698	No error (0)	l-0004.l-dc-msedge.net		13.107.43.13	A (IP address)	IN (0x0001)	false
Nov 29, 2022 10:41:52.369076967 CET	8.8.8.8	192.168.2.3	0x7cef	No error (0)	oyuurg.ph.files.1drv.com	ph-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:41:52.369076967 CET	8.8.8.8	192.168.2.3	0x7cef	No error (0)	ph-files.fe.1drv.com	odc-ph-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 10:41:52.369076967 CET	8.8.8.8	192.168.2.3	0x7cef	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- onedrive.live.com
- oyuurg.ph.files.1drv.com

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe PID: **6024**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:41:46
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan-gen.31819.28757.exe
Imagebase:	0x400000
File size:	750592 bytes
MD5 hash:	F536EA8FB5B6586BB2FFC764CD52ABFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.278011909.0000000002520000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.278530431.0000000002A2E000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: wscript.exe PID: **5988**, Parent PID: **6024**

General

Target ID:	1
Start time:	10:41:52
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\wscript.exe
Imagebase:	0x850000

File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: 00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.576405249.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.564946662.0000000004830000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.564946662.0000000004830000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.564946662.0000000004830000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.564946662.0000000004830000.00000040.10000000.00040000.00000000.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	1042DF9E	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5988**

General

Target ID:	2
Start time:	10:41:56
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: luigzwjd.exe PID: **3208**, Parent PID: **3452**

General

Target ID:	12

Start time:	10:42:04
Start date:	29/11/2022
Path:	C:\Users\Public\Libraries\luigzwjd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\luigzwjd.exe"
Imagebase:	0x400000
File size:	750592 bytes
MD5 hash:	F536EA8FB5B6586BB2FFC764CD52ABFF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 15%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\luigzwjd	unknown	189869	success or wait	1	22F33F1	ReadFile

Analysis Process: wscript.exe PID: **1264**, Parent PID: **3208**

General

Target ID:	13
Start time:	10:42:10
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\wscript.exe
Imagebase:	0x7ff68f300000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: luigzwjd.exe PID: **1848**, Parent PID: **3452**

General

Target ID:	14
Start time:	10:42:13
Start date:	29/11/2022
Path:	C:\Users\Public\Libraries\luigzwjd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\luigzwjd.exe"
Imagebase:	0x400000
File size:	750592 bytes
MD5 hash:	F536EA8FB5B6586BB2FFC764CD52ABFF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\luigzwjd	unknown	189869	success or wait	1	22E33F1	ReadFile

Analysis Process: wscript.exe PID: **5044**, Parent PID: **1848**

General

Target ID:	15
Start time:	10:42:29
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\wscript.exe
Imagebase:	0x850000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly