ID: 756155
Sample Name:
0321423605241625.exe
Cookbook: default.jbs
Time: 18:23:06
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

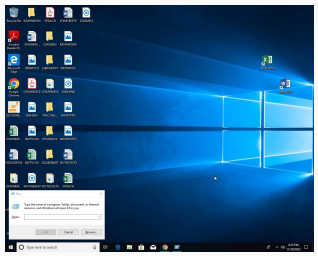
Windows Analysis Report

0321423605241625.exe

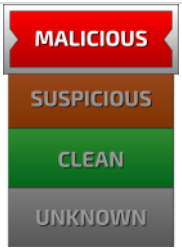
Overview

General Information

Sample Name:	0321423605241625.exe
Analysis ID:	756155
MD5:	edb1382c354ec6..
SHA1:	a1a5fbfce034731..
SHA256:	c2c6eec67a1561..
Tags:	exe modiloader xloader
Infos:	



Detection



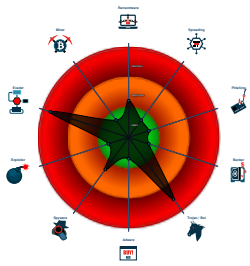
DBatLoader, FormBook

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 URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions

Classification



Process Tree

- **System is w10x64**
- 0321423605241625.exe (PID: 3140 cmdline: C:\Users\user\Desktop\0321423605241625.exe MD5: EDB1382C354EC6C09C53473E5335703A)
  - colorcpl.exe (PID: 3576 cmdline: C:\Windows\System32\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
    - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Mwqrxeuz.exe (PID: 5528 cmdline: "C:\Users\Public\Libraries\Mwqrxeuz.exe" MD5: EDB1382C354EC6C09C53473E5335703A)
        - colorcpl.exe (PID: 4028 cmdline: C:\Windows\System32\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
      - raserver.exe (PID: 5928 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 4028 cmdline: /c del "C:\Windows\SysWOW64\colorcpl.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rematedeldia.com/euv4/"
  ],
  "decoy": [
    "anniebapartments.com",
    "hagenbicycles.com",
    "herbalist101.com",
    "southerncorrosion.net",
    "kuechenpruefer.com",
    "tajniezdrzi.quest",
    "segurofunerarioar.com",
    "boardsandbeamsdecor.com",
    "alifdanismanlik.com",
    "pkem.top",
    "mddc.clinic",
    "handejqr.com",
    "crux-at.com",
    "awp.email",
    "hugsforbubbs.com",
    "cielotherepy.com",
    "turkcuyuz.com",
    "teamidc.com",
    "lankasirinspa.com",
    "68135.online",
    "oprimanumerodos.com",
    "launchclik.com",
    "customapronsnow.com",
    "thecuratedpour.com",
    "20dzwww.com",
    "encludemedia.com",
    "kreativevisibility.net",
    "mehfeels.com",
    "oecmgroup.com",
    "alert78.info",
    "1207rossmoyne.com",
    "spbutoto.com",
    "t1uba.com",
    "protection-onepa.com",
    "byausorsm26-plala.xyz",
    "bestpleasure4u.com",
    "allmnlenem.quest",
    "mobilpartes.com",
    "fabio.tools",
    "bubu3cin.com",
    "nathanmartinez.digital",
    "shristiprintingplaces.com",
    "silkyflawless.com",
    "berylgrote.top",
    "laidbackfurniture.store",
    "leatherman-neal.com",
    "uschargeport.com",
    "the-pumps.com",
    "deepootech.com",
    "drimev.com",
    "seo-art.agency",
    "jasabacklinkweb20.com",
    "tracynicolalamond.com",
    "dandtglaziers.com",
    "vulacils.com",
    "bendyourtongue.com",
    "gulfund.com",
    "ahmadfaizlajis.com",
    "595531.com",
    "metavillagehub.com",
    "librairie-adrienne.com",
    "77777.store",
    "gongwenbo.com",
    "game2plays.com"
  ]
}
```

Threatname: DBatLoader


```
{
  "Download Url": "https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21846&authkey=AOLP5PRESPN2npo"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\zuexrqwM.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x58:$hotkey: \x0AHotKey=2 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\zuexrqwM.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
00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6191:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1aee0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x97ef:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x148b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.553760643.0000000002D80000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 57 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.colorcpl.exe.10410000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.colorcpl.exe.10410000.3.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6191:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1aee0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x97ef:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x148b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Source	Rule	Description	Author	Strings
1.2.colorcpl.exe.10410000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
1.2.colorcpl.exe.10410000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
1.0.colorcpl.exe.10410000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 38 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 217.160.0.95

Timestamp:	192.168.2.5217.160.0.9549719802031453 11/29/22-18:26:33.912103
SID:	2031453
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 192.0.78.141

Timestamp:	192.168.2.5192.0.78.14149715802031453 11/29/22-18:26:08.582417
SID:	2031453
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 217.160.0.95

Timestamp:	192.168.2.5217.160.0.9549719802031412 11/29/22-18:26:33.912103
SID:	2031412
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 52.85.92.84

Timestamp:	192.168.2.552.85.92.8449717802031453 11/29/22-18:26:23.800962
SID:	2031453
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 217.160.0.95	
Timestamp:	192.168.2.5217.160.0.9549719802031449 11/29/22-18:26:33.912103
SID:	2031449
Source Port:	49719
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 192.0.78.141	
Timestamp:	192.168.2.5192.0.78.14149715802031449 11/29/22-18:26:08.582417
SID:	2031449
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 52.85.92.84	
Timestamp:	192.168.2.552.85.92.8449717802031412 11/29/22-18:26:23.800962
SID:	2031412
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 192.0.78.141	
Timestamp:	192.168.2.5192.0.78.14149715802031412 11/29/22-18:26:08.582417
SID:	2031412
Source Port:	49715
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 52.85.92.84	
Timestamp:	192.168.2.552.85.92.8449717802031449 11/29/22-18:26:23.800962
SID:	2031449
Source Port:	49717
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

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

Queues an APC in another process (thread injection)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

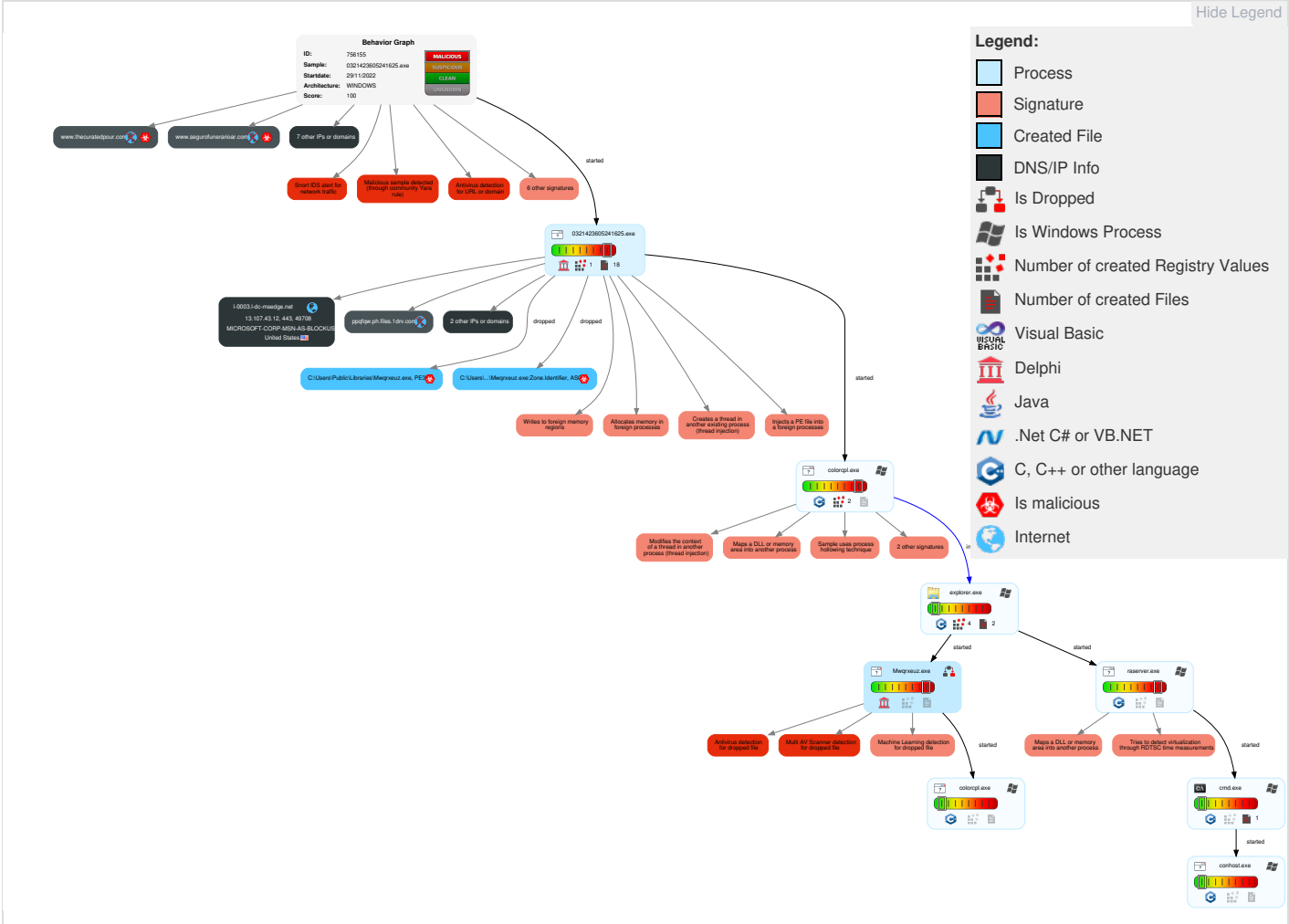
Yara detected FormBook

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	1 Native API	1 Registry Run Keys / Startup Folder	8 1 2 Process Injection	1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	2 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	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	8 1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	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 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

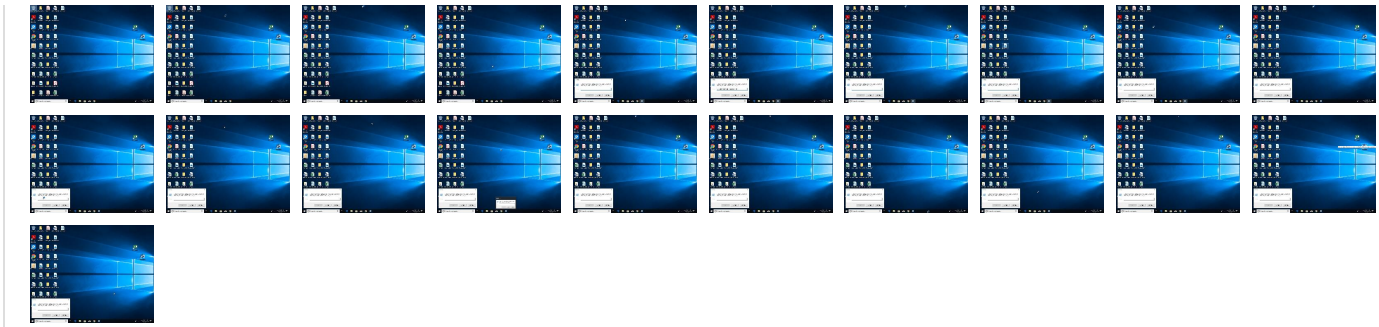
Behavior Graph



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
0321423605241625.exe	36%	ReversingLabs	Win32.Trojan.Generic	
0321423605241625.exe	41%	Virustotal		Browse
0321423605241625.exe	100%	Avira	HEUR/AGEN.1214697	
0321423605241625.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Mwqrxeuz.exe	100%	Avira	HEUR/AGEN.1214697	
C:\Users\Public\Libraries\Mwqrxeuz.exe	100%	Joe Sandbox ML		
C:\Users\Public\Libraries\Mwqrxeuz.exe	36%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.colorcpl.exe.10410000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.0321423605241625.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1214697		Download File
0.2.0321423605241625.exe.2170000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File
1.0.colorcpl.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.raserver.exe.525796c.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
1.0.colorcpl.exe.10410000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.colorcpl.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.raserver.exe.a3cda0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.0321423605241625.exe.3baeed8.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.Mwqrxeuz.exe.2598248.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.colorcpl.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.0321423605241625.exe.2231218.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.0321423605241625.exe.2278248.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.rematedeldia.com/euv4/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.kuechenpruefer.com	217.160.0.95	true	true		unknown
librairie-adrienne.com	192.0.78.141	true	true		unknown
l-0003.l-dc-msedge.net	13.107.43.12	true	false		unknown
www.customapronsnow.com	52.85.92.84	true	true		unknown
shops.myshopify.com	23.227.38.74	true	false		unknown
www.thecuratedpour.com	unknown	unknown	true		unknown
onedrive.live.com	unknown	unknown	false		high
www.segurofunerarioar.com	unknown	unknown	true		unknown
www.librairie-adrienne.com	unknown	unknown	true		unknown
ppqfqw.ph.files.1drv.com	unknown	unknown	false		high
www.rematedeldia.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.rematedeldia.com/euv4/	true	• Avira URL Cloud: malware	low
http://https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21846&authkey=AOLP5PRESPN2npo	false		high
http://https://ppqfqw.ph.files.1drv.com/y4mCDNCh3rnIYpJlqIqXCF9hAcHbqZ_4sWcNl3-omCYoNehN1gOwskkZvXxiCnSz1O3rlGujQmh2dpM-9vT8IEOnYjevggDBPg3L6krVTX5rpZ6Y9fWqq7mXN8HP0HSdlr6-fMy35G8DvzJqxvSasnXVIJpB-5dNG-tdgdNk_U_XYoTZ1ccJrC1sgInwIFqmsOi4T1bkt9-CIDRF_pvQqcEQA/Mwqrxeuzvim?download&psid=1	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ppqfqw.ph.files.1drv.com/y4mcSg4TVpIg-eA6Y1ciUp4Dzz62AcO4SwOj-306Rp8dovP_vJs6bBF8upLxcpz7eVd	0321423605241625.exe, 00000000.00000002.307309131.0000000000858000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000003.301144762.000000000850000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000002.307058995.00000000007FF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000000.35184529.000000000091F000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.310261242.000000000091F000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.434855289.0000000000921000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ppqfqw.ph.files.1drv.com/y4mCDNCh3rnIYpJlqIqXCF9hAcHbqZ_4sWcNl3-omCYoNehN1gOwskkZvXxiCnSz1O3	0321423605241625.exe, 00000000.00000003.301289184.000000000089F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ppqfqw.ph.files.1drv.com/U0	0321423605241625.exe, 00000000.00000003.301178169.0000000000864000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ppqfqw.ph.files.1drv.com/	0321423605241625.exe, 00000000.00000003.301194730.0000000000870000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000003.301178169.000000000864000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000002.307357943.0000000000862000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000003.299996979.000000000085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21846&authkey=AOLP5PR	0321423605241625.exe, 00000000.00000002.307058995.00000000007FF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ppqfqw.ph.files.1drv.com/_	0321423605241625.exe, 00000000.00000003.301194730.0000000000870000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000002.307576454.000000000874000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000003.299996979.000000000085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/	0321423605241625.exe, 00000000.00000002.307058995.00000000007FF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ppqfqw.ph.files.1drv.com/s	0321423605241625.exe, 00000000.00000003.301194730.0000000000870000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000002.307576454.000000000874000.00000004.00000020.00020000.00000000.sdmp, 0321423605241625.exe, 00000000.00000003.299996979.000000000085A000.00000004.00000020.00020000.00000000.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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756155
Start date and time:	2022-11-29 18:23:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0321423605241625.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:	12
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@11/5@8/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 98.9% (good quality ratio 86.8%) • Quality average: 75% • Quality standard deviation: 33.7%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.13
- Excluded domains from analysis (whitelisted): l-0004.l-msedge.net, odc-web-brs.onedrive.akadns.net, client.wns.windows.com, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, odc-web-geo.onedrive.akadns.net, ph-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, 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
18:23:59	API Interceptor	1x Sleep call for process: 0321423605241625.exe modified
18:24:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Mwqrxeuz C:\Users\Public\Libraries\zuexrqwM.url
18:24:14	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Mwqrxeuz C:\Users\Public\Libraries\zuexrqwM.url
18:24:18	API Interceptor	1x Sleep call for process: Mwqrxeuz.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\Mwqrxeuz

Process:	C:\Users\user\Desktop\0321423605241625.exe

File Type:	data
Category:	dropped
Size (bytes):	167894
Entropy (8bit):	7.836989185036909
Encrypted:	false
SSDEEP:	3072:oX7iyI1g1T9ZeIssvAq21B+OXSuWQ/e9WMEnOuljlyTe9iotErmwT46lcHNo9igQ:oX2yA8T9ZeIPoHBSDGDM9u4K9ioQESTQ
MD5:	A4230DEF1381688D96A42C48723B6FB4
SHA1:	DAC39DC194EB7525BE189B5BE47E7B3A70E8DF0B
SHA-256:	C3F4FA12B0F5A069BD9CEF7EE09AEEE8DADB2199A3A0F05009E068C0CC0CB3F8
SHA-512:	E6EA4CB1E3693DD84145D6475EA2EBB2D01C4D1BA980CE42924DC83D396669CC423C6E5589E050CA33FD1B1EF7B21AAF2DC7B4674294917684557D5C716CF 13
Malicious:	false
Reputation:	low
Preview:	....4.e.4..kk.4........kk.4.......4qwym.....qw.}.m.m..{.}...o.u......mw..m..mw...........w...u.......w{ws..wm{m..{uo.}m.q.q....s....4.e.4..kk.4........kk.4.......4..}..q...uy....4.e.4..kk.4 ....kk.4.......4....JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...F F...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF... J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^..... ..JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^......\.=....b.S.A...%.\.4O~.N.....!...e.P..zF.^..#...Uq...(..........:...8x.2...f.r.7Em X....b.F.g$.. ..ab..X...n:.IG|...W.{s.z.

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

Process:	C:\Users\user\Desktop\0321423605241625.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	750592
Entropy (8bit):	6.881084216281991
Encrypted:	false
SSDEEP:	12288:i1qMhtVLzLypCggIh36+O9dvjpQVeri4Z2qKk/RqIkr:WFhHzmQgn6+8T/r7saqI
MD5:	EDB1382C354EC6C09C53473E5335703A
SHA1:	A1A5FBFCE034731CBA1072BAB6B97B26C8A90C79
SHA-256:	C2C6EEC67A1561C3A49179DDF756480876D92588C2E83D64246A04C3D724CB3D
SHA-512:	7A39E02E0C6B5036763A7646A5960DE36230EAEF32DA6B36687AA71170BD2125775888EC71FF112FB76A38D17D77B650089257043288FAE82598DEE5E6987ED9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
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\Mwqrxeuz.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\0321423605241625.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\Desktop\0321423605241625.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Mwqrxeuz.exe">), ASCII text, with CRLF line terminators
Category:	modified

Size (bytes):	100
Entropy (8bit):	5.027627100346909
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMiCK0dAIvsGKd7DKCov:HRYFVmTWDyzM7vsb7uCy
MD5:	7DDCB7FA3CEA8198D5ADEBF8F7797F74
SHA1:	4552A0DFE75A7CF4875DDB3575800AE137F88E04
SHA-256:	7E678198AFD5C53ADDBD2133245E72EBF9D6885F20496F5ACAEF2CF56C54856D
SHA-512:	D985A2CEF6438CAA20E784A43CF752BCB1AF2608633C050DF55A194766D1C1BC3D106D7786D63E316DEF0E011E98D263C99510D7E843E8A6709F4DDFD1BA67 3
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\zuexrqwM.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\zuexrqwM.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Mwqrxeuz.exe"..IconIndex=31..HotKey=29..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Mwqrxeuzvim[1]

Process:	C:\Users\user\Desktop\0321423605241625.exe
File Type:	data
Category:	dropped
Size (bytes):	167894
Entropy (8bit):	7.836989185036909
Encrypted:	false
SSDEEP:	3072:oX7iyI1g1T9ZeIssvAq21B+OXSuWQ/e9WMEnOuljlyTe9iotErmwT46lcHNo9igQ:oX2yA8T9ZeIPoHBSDGDM9u4K9ioQESTQ
MD5:	A4230DEF1381688D96A42C48723B6FB4
SHA1:	DAC39DC194EB7525BE189B5BE47E7B3A70E8DF0B
SHA-256:	C3F4FA12B0F5A069BD9CEF7EE09AEEE8DADB2199A3A0F05009E068C0CC0CB3F8
SHA-512:	E6EA4CB1E3693DD84145D6475EA2EBB2D01C4D1BA980CE42924DC83D396669CC423C6E5589E050CA33FD1B1EF7B21AAF2DC7B4674294917684557D5C716CF 13
Malicious:	false
Preview:	....4.e.4..kk.4........kk.4.......4qwym.....qw.}.m.m..{.}...o.u......mw..m..mw............w...u.......w{ws..wm{m..{uo.}m.q.q....s....4.e.4..kk.4........kk.4.......4..}..q...uy....4.e.4..kk.4........kk.4.......4....JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.......JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^.....JddF^........J\....`T.b.NP^L....T..ZJ..FP\.\`FF\TJL.F.\..\dPL.b.....Z...FF...J..\.\..^......\.=....b.S.A...%.\.4O~.N.....!...e.P..zF.^..#...Uq...(..........:...8x.2...f.r.7Em X....b.F.g$....ab..X...n:.IG|...W.{s.z.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.881084216281991
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:	0321423605241625.exe
File size:	750592
MD5:	edb1382c354ec6c09c53473e5335703a
SHA1:	a1a5fbfce034731cba1072bab6b97b26c8a90c79
SHA256:	c2c6eec67a1561c3a49179ddf756480876d92588c2e83d64246a04c3d724cb3d
SHA512:	7a39e02e0c6b5036763a7646a5960de36230eaef32da6b36687aa71170bd2125775888ec71ff112fb76a38d17d77b650089257043288fae82598dee5e6987ed9
SSDEEP:	12288:i1qMhtVLzLypCgglh36+O9dvjpQVeri4Z2qKk/RqIkr:WFhHzmQgn6+8T/r7saqI
TLSH:	D4F47D6662D08637D02715389C07A7A8692FAEE02F14F8956BD53DCC5F383CE743926B
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 00007FDD10D0EC15h
mov ecx, dword ptr [0046D410h]
mov eax, dword ptr [0046D324h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00460A90h]
call 00007FDD10D615EDh
mov eax, dword ptr [0046D324h]
mov eax, dword ptr [eax]
call 00007FDD10D61661h
call 00007FDD10D0CD18h
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
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

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
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x77000	0x6eec	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	0.08553746234939759	data	6.533389727605739	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
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

Name	RVA	Size	Type	Language	Country
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		
RT_RCDATA	0xbff48	0x3e0	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xc0328	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States

Name	RVA	Size	Type	Language	Country
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
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

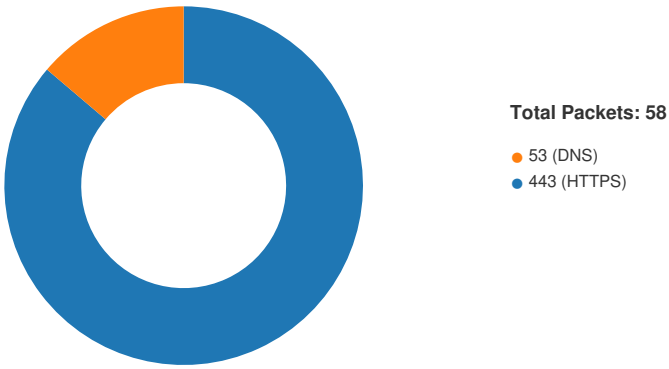
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5217.160.0.954 9719802031453 11/29/22-18:26:33.912103	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49719	80	192.168.2.5	217.160.0.95
192.168.2.5192.0.78.1414 9715802031453 11/29/22-18:26:08.582417	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49715	80	192.168.2.5	192.0.78.141
192.168.2.5217.160.0.954 9719802031412 11/29/22-18:26:33.912103	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49719	80	192.168.2.5	217.160.0.95
192.168.2.552.85.92.8449 717802031453 11/29/22-18:26:23.800962	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	52.85.92.84
192.168.2.5217.160.0.954 9719802031449 11/29/22-18:26:33.912103	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49719	80	192.168.2.5	217.160.0.95
192.168.2.5192.0.78.1414 9715802031449 11/29/22-18:26:08.582417	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49715	80	192.168.2.5	192.0.78.141
192.168.2.552.85.92.8449 717802031412 11/29/22-18:26:23.800962	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	52.85.92.84
192.168.2.5192.0.78.1414 9715802031412 11/29/22-18:26:08.582417	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49715	80	192.168.2.5	192.0.78.141
192.168.2.552.85.92.8449 717802031449 11/29/22-18:26:23.800962	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	52.85.92.84

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:24:02.150501013 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.150546074 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.150648117 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.152163029 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.152179956 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.254343033 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.254555941 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.255497932 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.255589962 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.267853975 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.267887115 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.268393040 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.268481970 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.269418001 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.269438982 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500678062 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500714064 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500811100 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500822067 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.500838041 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500870943 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.500896931 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.500904083 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500924110 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.500952005 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.500967026 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.500974894 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.501029968 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526240110 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526367903 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526443005 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526479006 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526498079 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526504993 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526525021 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526536942 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526561975 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526582003 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526590109 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526628017 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526633024 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526657104 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526691914 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526717901 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526727915 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526765108 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526782990 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526839972 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.526849031 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.526925087 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554421902 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554553032 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554594040 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554619074 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554632902 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554657936 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554661036 CET	49708	443	192.168.2.5	13.107.43.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:24:02.554682970 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554713964 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554738998 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554744959 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554785967 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554790974 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554811954 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554847002 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554872990 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554893017 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.554939032 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.554979086 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555042028 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555049896 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555092096 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555105925 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555126905 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555171967 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555187941 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555192947 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555222988 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555227995 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555243969 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555279016 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555296898 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555304050 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555342913 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555367947 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555430889 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.555437088 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.555522919 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.577827930 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.578022003 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.578116894 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.578166008 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.578205109 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.578243017 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.578641891 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.578684092 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.578753948 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.578780890 CET	443	49708	13.107.43.12	192.168.2.5
Nov 29, 2022 18:24:02.578811884 CET	49708	443	192.168.2.5	13.107.43.12
Nov 29, 2022 18:24:02.578839064 CET	49708	443	192.168.2.5	13.107.43.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:24:01.159205914 CET	49724	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:24:02.097614050 CET	61452	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:08.541414976 CET	59220	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:08.563268900 CET	53	59220	8.8.8.8	192.168.2.5
Nov 29, 2022 18:26:13.612112999 CET	55068	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:13.632412910 CET	53	55068	8.8.8.8	192.168.2.5
Nov 29, 2022 18:26:18.722286940 CET	56682	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:18.742017984 CET	53	56682	8.8.8.8	192.168.2.5
Nov 29, 2022 18:26:23.756469965 CET	58532	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:23.777184010 CET	53	58532	8.8.8.8	192.168.2.5
Nov 29, 2022 18:26:28.831734896 CET	62659	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:28.853539944 CET	53	62659	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:26:33.864237070 CET	56263	53	192.168.2.5	8.8.8.8
Nov 29, 2022 18:26:33.889528990 CET	53	56263	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 18:24:01.159205914 CET	192.168.2.5	8.8.8.8	0x3277	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:24:02.097614050 CET	192.168.2.5	8.8.8.8	0xb4c2	Standard query (0)	ppqfqw.ph.files.1drv.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:08.541414976 CET	192.168.2.5	8.8.8.8	0xcc02	Standard query (0)	www.librairie-adrienne.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:13.612112999 CET	192.168.2.5	8.8.8.8	0x953a	Standard query (0)	www.rematedeldia.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:18.722286940 CET	192.168.2.5	8.8.8.8	0xb26a	Standard query (0)	www.thecuratedpour.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:23.756469965 CET	192.168.2.5	8.8.8.8	0x5846	Standard query (0)	www.customapronsnow.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:28.831734896 CET	192.168.2.5	8.8.8.8	0xae1	Standard query (0)	www.segurofunerarioar.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:33.864237070 CET	192.168.2.5	8.8.8.8	0x5457	Standard query (0)	www.kuechenpruefer.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 18:24:01.202867985 CET	8.8.8.8	192.168.2.5	0x3277	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:24:02.146754980 CET	8.8.8.8	192.168.2.5	0xb4c2	No error (0)	ppqfqw.ph.files.1drv.com	ph-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:24:02.146754980 CET	8.8.8.8	192.168.2.5	0xb4c2	No error (0)	ph-files.fe.1drv.com	odc-ph-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:24:02.146754980 CET	8.8.8.8	192.168.2.5	0xb4c2	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:08.563268900 CET	8.8.8.8	192.168.2.5	0xcc02	No error (0)	www.librairie-adrienne.com	librairie-adrienne.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:26:08.563268900 CET	8.8.8.8	192.168.2.5	0xcc02	No error (0)	librairie-adrienne.com		192.0.78.141	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:08.563268900 CET	8.8.8.8	192.168.2.5	0xcc02	No error (0)	librairie-adrienne.com		192.0.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:13.632412910 CET	8.8.8.8	192.168.2.5	0x953a	No error (0)	www.rematedeldia.com	compralo1234.myshopify.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:26:13.632412910 CET	8.8.8.8	192.168.2.5	0x953a	No error (0)	compralo1234.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 18:26:13.632412910 CET	8.8.8.8	192.168.2.5	0x953a	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:18.742017984 CET	8.8.8.8	192.168.2.5	0xb26a	Name error (3)	www.thecuratedpour.com	none	none	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:23.777184010 CET	8.8.8.8	192.168.2.5	0x5846	No error (0)	www.customapronsnow.com		52.85.92.84	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:23.777184010 CET	8.8.8.8	192.168.2.5	0x5846	No error (0)	www.customapronsnow.com		52.85.92.99	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:23.777184010 CET	8.8.8.8	192.168.2.5	0x5846	No error (0)	www.customapronsnow.com		52.85.92.94	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:23.777184010 CET	8.8.8.8	192.168.2.5	0x5846	No error (0)	www.customapronsnow.com		52.85.92.122	A (IP address)	IN (0x0001)	false

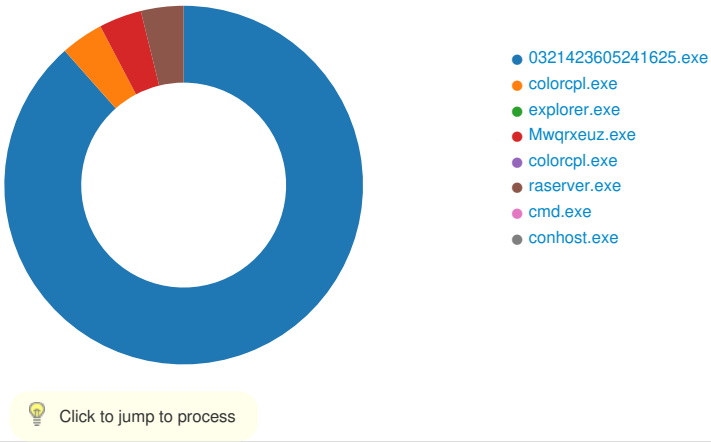
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 18:26:28.853539944 CET	8.8.8.8	192.168.2.5	0xae1	Name error (3)	www.seguro funerarioa r.com	none	none	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:33.889528990 CET	8.8.8.8	192.168.2.5	0x5457	No error (0)	www.kueche npruefer.com		217.160.0.95	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- ppqfqw.ph.files.1drv.com

Statistics

Behavior



System Behavior

Analysis Process: 0321423605241625.exe PID: 3140, Parent PID: 3324

General

Target ID:	0
Start time:	18:23:55
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\0321423605241625.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\0321423605241625.exe
Imagebase:	0x400000
File size:	750592 bytes
MD5 hash:	EDB1382C354EC6C09C53473E5335703A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.308860487.0000000003BAE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.309972284.0000000004A7F000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.309972284.0000000004A7F000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.309972284.0000000004A7F000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.309972284.0000000004A7F000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.308375056.00000000021D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Analysis Process: colorcpl.exe PID: **3576**, Parent PID: **3140**

General

Target ID:	1
Start time:	18:24:02
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\colorcpl.exe
Imagebase:	0x1140000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000001.00000000.305700476.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.305700476.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.305700476.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.305700476.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.305400692.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.305400692.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.305400692.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.305400692.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.306413915.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.306413915.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.306413915.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.306413915.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.306024723.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.306024723.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.306024723.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.306024723.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.498815518.0000000005140000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.498815518.0000000005140000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.498815518.0000000005140000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.498815518.0000000005140000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.525904098.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.525904098.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.525904098.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.525904098.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.495768965.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.495768965.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.495768965.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.495768965.0000000000F20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	104286D7	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **3324**, Parent PID: **3576**

General	
Target ID:	2
Start time:	18:24:05
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
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: 00000002.00000000.396763474.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.396763474.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.396763474.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.396763474.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.474871458.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.474871458.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.474871458.000000000E3BF000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.474871458.000000000E3BF000.00000040.00000001.00040000.00000000.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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: Mwqrxeuz.exe PID: **5528**, Parent PID: **3324**

General	
Target ID:	3
Start time:	18:24:14
Start date:	29/11/2022
Path:	C:\Users\Public\Libraries\Mwqrxeuz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Mwqrxeuz.exe"
Imagebase:	0x7ff7fcd70000
File size:	750592 bytes
MD5 hash:	EDB1382C354EC6C09C53473E5335703A
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.545995933.00000000046FE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.545995933.00000000046FE000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.545995933.00000000046FE000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.545995933.00000000046FE000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Mwqrxeuz	unknown	167894	success or wait	1	26333F1	ReadFile

Analysis Process: colorcpl.exe PID: **4028**, Parent PID: **5528**

General

Target ID:	4
Start time:	18:24:18
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\colorcpl.exe
Imagebase:	0x1140000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: raserver.exe PID: **5928**, Parent PID: **3324**

General

Target ID:	9
Start time:	18:25:26
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x870000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.553690913.0000000002C80000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.553760643.0000000002D80000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.553760643.0000000002D80000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.553760643.0000000002D80000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.553760643.0000000002D80000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.553544992.0000000000C20000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.553544992.0000000000C20000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.553544992.0000000000C20000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.553544992.0000000000C20000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2D986D7	NtReadFile

Analysis Process: cmd.exe PID: **4028**, Parent PID: **5928**

General

Target ID:	10
Start time:	18:25:37
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\SysWOW64\colorcpl.exe"
Imagebase:	0x11d0000
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: **1412**, Parent PID: **4028**

General

Target ID:	11
Start time:	18:25:38
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000

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