ID: 756323
Sample Name: Lc8xQv8iZY.exe
Cookbook: default.jbs
Time: 01:23:15
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

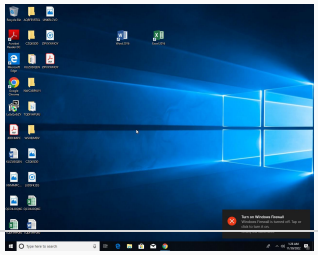
Windows Analysis Report

Lc8xQv8iZY.exe

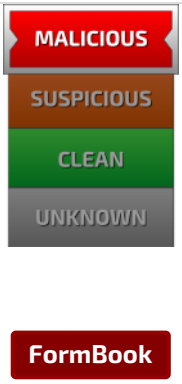
Overview

General Information

Sample Name:	Lc8xQv8iZY.exe
Analysis ID:	756323
MD5:	30571d64c9a9ed..
SHA1:	bfb81d8a7c9478..
SHA256:	85d6c9eac93fb8...
Tags:	32 exe Formbook trojan
Infos:	



Detection



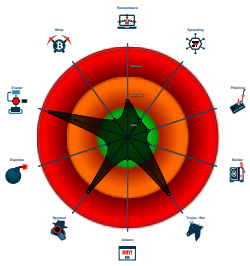
FormBook

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

Signatures

- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through...
- System process connects to networ...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Multi AV Scanner detection for drop...
- Snort IDS alert for network traffic
- Sample uses process hollowing tech...
- Tries to steal Mail credentials (via fi...
- Maps a DLL or memory area into an...
- Machine Learning detection for sam...

Classification



Process Tree

- **System is w10x64**
- Lc8xQv8iZY.exe (PID: 3376 cmdline: C:\Users\user\Desktop\Lc8xQv8iZY.exe MD5: 30571D64C9A9ED267159FA941A20840C)
  - hvbvmxm.exe (PID: 3052 cmdline: "C:\Users\user\AppData\Local\Temp\hvbvmxm.exe" C:\Users\user\AppData\Local\Temp\ijamguwvje.h MD5: 1EEBBBD92B2C0C60F896FF8DCBCEDCAA)
    - conhost.exe (PID: 3748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - hvbvmxm.exe (PID: 5420 cmdline: "C:\Users\user\AppData\Local\Temp\hvbvmxm.exe" C:\Users\user\AppData\Local\Temp\ijamguwvje.h MD5: 1EEBBBD92B2C0C60F896FF8DCBCEDCAA)
      - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - help.exe (PID: 1900 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.brennancorps.info/henz/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6611:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f070:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa8bf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17df7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17bf5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x176a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17cf7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17e6f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa48a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x168ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1dde7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edda:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a0e9:$sqlite3step: 68 34 1C 7B E1 • 0x1ac61:$sqlite3step: 68 34 1C 7B E1 • 0x1a12b:$sqlite3text: 68 38 2A 90 C5 • 0x1aca6:$sqlite3text: 68 38 2A 90 C5 • 0x1a142:$sqlite3blob: 68 53 D8 7F 8C • 0x1acbc:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000000.353715977.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.hvbvmxm.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.hvbvmxm.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6f48:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f9a7:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xb1f6:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1872e:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.hvbvmxm.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1852c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17fd8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1862e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x187a6:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xadc1:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17223:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1e71e:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1f711:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.hvbvmxm.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1aa20:$sqlite3step: 68 34 1C 7B E1 • 0x1b598:$sqlite3step: 68 34 1C 7B E1 • 0x1aa62:$sqlite3text: 68 38 2A 90 C5 • 0x1b5dd:$sqlite3text: 68 38 2A 90 C5 • 0x1aa79:$sqlite3blob: 68 53 D8 7F 8C • 0x1b5f3:$sqlite3blob: 68 53 D8 7F 8C
3.2.hvbvmxm.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 162.214.129.149

Timestamp:	192.168.2.4162.214.129.14949699802031453 11/30/22-01:25:33.429382
SID:	2031453

Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 162.214.129.149	−
Timestamp:	192.168.2.4162.214.129.14949699802031412 11/30/22-01:25:33.429382
SID:	2031412
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 206.233.197.135	−
Timestamp:	192.168.2.4206.233.197.13549697802031453 11/30/22-01:25:25.388400
SID:	2031453
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 206.233.197.135	−
Timestamp:	192.168.2.4206.233.197.13549697802031412 11/30/22-01:25:25.388400
SID:	2031412
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 162.214.129.149	−
Timestamp:	192.168.2.4162.214.129.14949699802031449 11/30/22-01:25:33.429382
SID:	2031449
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 206.233.197.135	−
Timestamp:	192.168.2.4206.233.197.13549697802031449 11/30/22-01:25:25.388400
SID:	2031449
Source Port:	49697
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 detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

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)

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

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

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

Remote Access Functionality

Yara detected FormBook

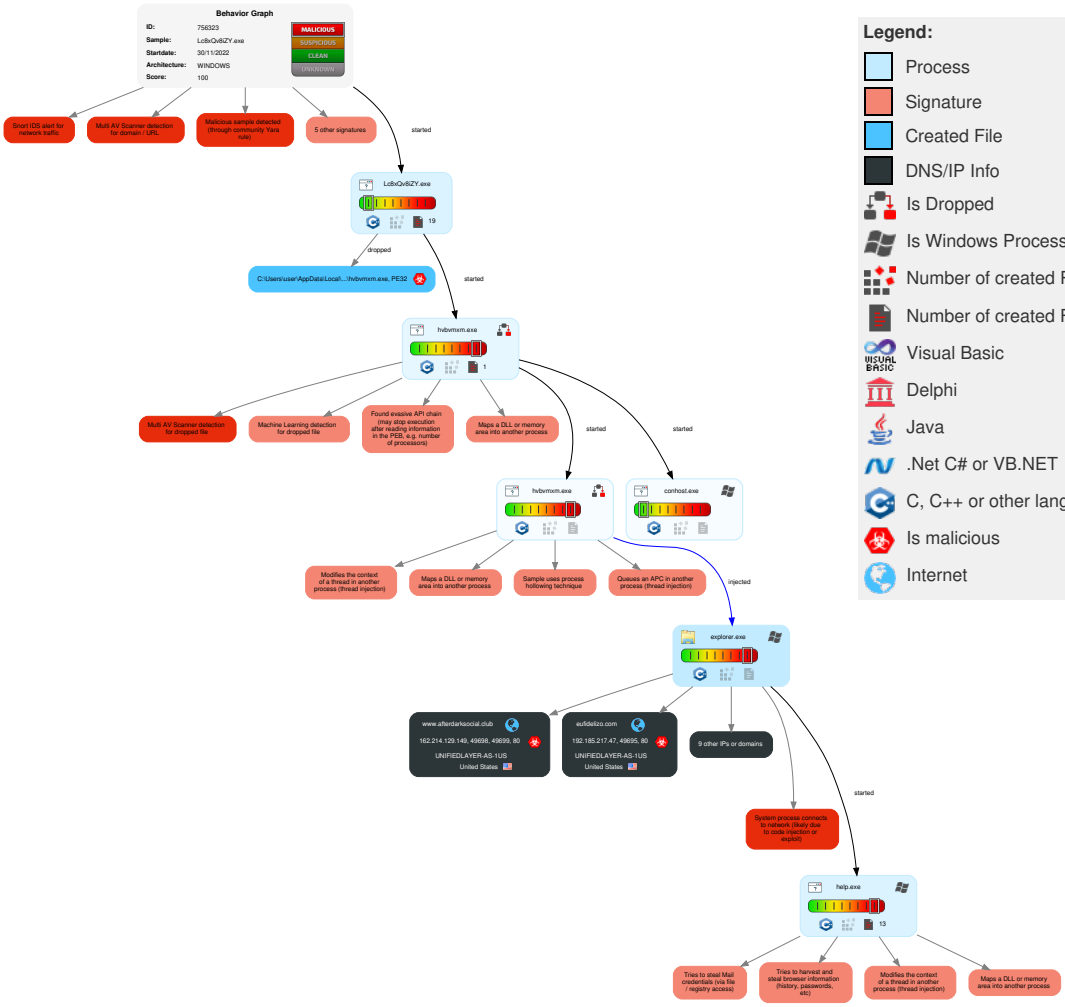
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	5 1 2 Process Injection	2 Virtualization/Sandbox Evasion	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	5 1 2 Process Injection	2 1 Input Capture	1 4 1 Security Software Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	4 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)	2 Obfuscated Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	2 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	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	Compile After Delivery	DCSync	1 5 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

Hide Legend



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Lc8xQv8iZY.exe	49%	ReversingLabs	Win32.Trojan.Injuke	
Lc8xQv8iZY.exe	47%	Virustotal		Browse
Lc8xQv8iZY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\hvbvmxm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\hvbvmxm.exe	54%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.hvbvmxm.exe.21b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.hvbvmxm.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.hvbvmxm.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Lc8xQv8iZY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
0.0.Lc8xQv8iZY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
www.patrickguarte.com	1%	Virustotal		Browse
brennancorps.info	1%	Virustotal		Browse
lopezmodeling.com	3%	Virustotal		Browse
www.foxwhistle.com	4%	Virustotal		Browse
eufidelizo.com	9%	Virustotal		Browse
www.lyonfinancialusa.com	0%	Virustotal		Browse
www.eufidelizo.com	7%	Virustotal		Browse
www.brennancorps.info	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.lopezmodeling.com/henz/?4hq=dpH6BKfQQ0cm5Imeo72RAP4DEbjLNfLp0vSyI4bn1RZjePkdeS9augOMgWVykt+ztx1R3MJW/gsn5nuFARzMtUktTfqb4tJ3+A==&o8=wR-h28Gxg	100%	Avira URL Cloud	malware	
http://www.eufidelizo.com/henz/?4hq=wcp3urA+/rGtUuNVdXHur6CaD7Rg4XGXlvUWG7FdGjeYGPzd5j/g1Govvww0i9Uvwfj8E4D4P4OVv2O692M0flOUm4qON1Jqzg==&o8=wR-h28Gxg	100%	Avira URL Cloud	malware	
http://www.brennancorps.info/henz/?4hq=P4ST2lJPckjMYpRf2FLdq0axEROKy7OOggEf6mHPhnME1yGBMW0egmkxYDI06dmXm7z7OVgXWzJ+YqSrULYkiycbwQA+qKMVmQ==&o8=wR-h28Gxg	100%	Avira URL Cloud	malware	
http://www.lopezmodeling.com/henz/	100%	Avira URL Cloud	malware	
http://www.brennancorps.info/henz/	100%	Avira URL Cloud	malware	
www.brennancorps.info/henz/	100%	Avira URL Cloud	malware	
http://www.lyonfinancialusa.com/henz/	100%	Avira URL Cloud	malware	
http://www.afterdarksocial.club/henz/	100%	Avira URL Cloud	malware	
http://www.foxwhistle.com/henz/	100%	Avira URL Cloud	malware	
http://www.patrickguarte.com/henz/	100%	Avira URL Cloud	malware	
http://206.119.101.137/ak_Address/Address.js	0%	Avira URL Cloud	safe	
http://www.patrickguarte.com/henz/?4hq=5p9Ov6C7qce51hIp6D8A72je8vUJddN77lLEFw6Ufibk2yN56suG3zROnD+rS7baXFO6PfoGYvZY6sqA3kYcUTUl/8Ylp7EDwQ==&o8=wR-h28Gxg	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.patrickguarte.com	155.159.61.221	true	true	• 1%, Virustotal, Browse	unknown
brennancorps.info	2.57.90.16	true	true	• 1%, Virustotal, Browse	unknown
lopezmodeling.com	192.185.35.86	true	true	• 3%, Virustotal, Browse	unknown
www.foxwhistle.com	154.22.100.62	true	true	• 4%, Virustotal, Browse	unknown
eufidelizo.com	192.185.217.47	true	true	• 9%, Virustotal, Browse	unknown
www.lyonfinancialusa.com	206.233.197.135	true	true	• 0%, Virustotal, Browse	unknown
www.afterdarksocial.club	162.214.129.149	true	true		unknown
www.eufidelizo.com	unknown	unknown	true	• 7%, Virustotal, Browse	unknown
www.brennancorps.info	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
www.19t221013d.tokyo	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.lopezmodeling.com	unknown	unknown	true		unknown

Contacted URLs

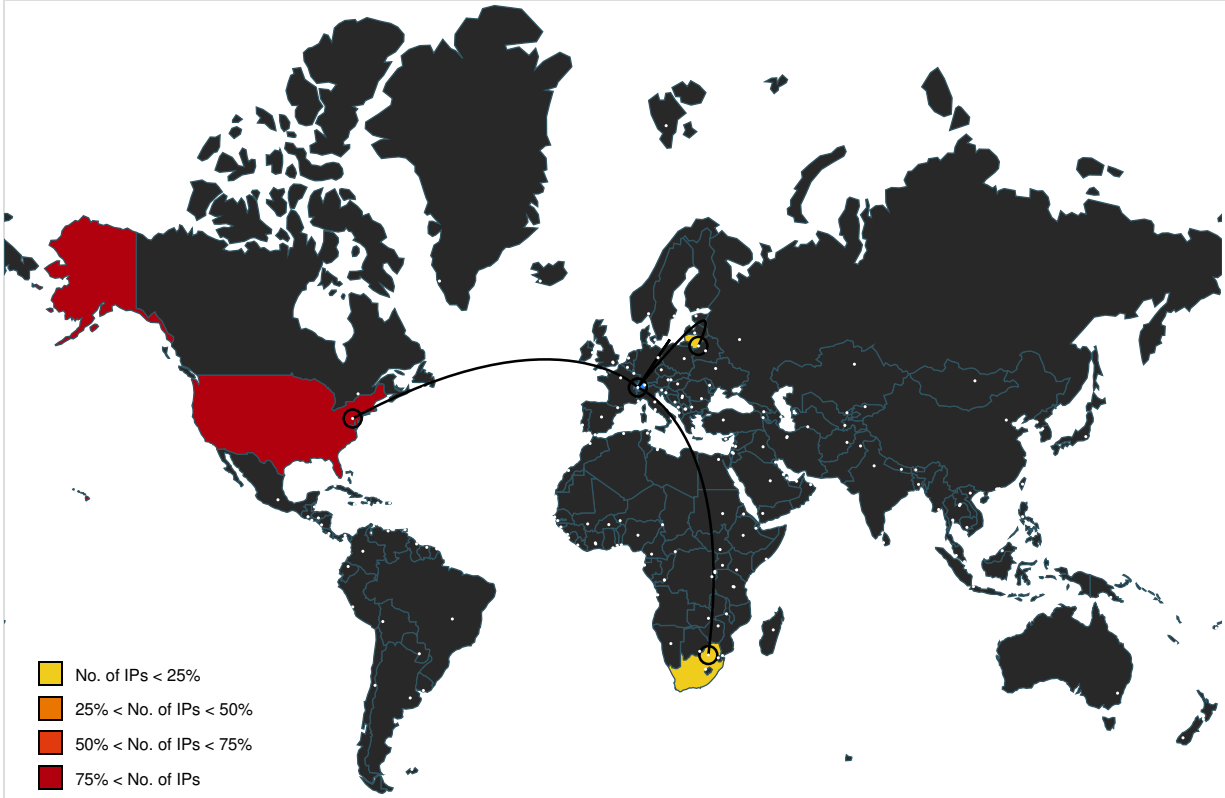
Name	Malicious	Antivirus Detection	Reputation
http://www.lyonfinancialusa.com/henz/	true	• Avira URL Cloud: malware	unknown
http://www.lopezmodeling.com/henz/	true	• Avira URL Cloud: malware	unknown
http://www.brennancorps.info/henz/	true	• Avira URL Cloud: malware	unknown
http://www.afterdarksocial.club/henz/	true	• Avira URL Cloud: malware	unknown
www.brennancorps.info/henz/	true	• Avira URL Cloud: malware	low
http://www.brennancorps.info/henz/?4hq=P4ST2lJPckjMYpRf2FLdq0axEROKy7OOggEf6mHPhnME1yGBMW0egmkxYDI06dmXm7z7OVgXWzJ+YqSrULYkiycbwQA+qKMVmQ==&o8=wR-h28Gxg	true	• Avira URL Cloud: malware	unknown
http://www.foxwhistle.com/henz/	true	• Avira URL Cloud: malware	unknown
http://www.eufidelizo.com/henz/?4hq=wcp3urA+/rGtUuNVdXHur6CaD7Rg4XGXlvUWG7FdGjeYGPzd5j/g1Govvww0i9Uvwfj8E4D4P4OVv2O692M0fIOUm4qON1Jqzg==&o8=wR-h28Gxg	true	• Avira URL Cloud: malware	unknown
http://www.lopezmodeling.com/henz/?4hq=dpH6BKfQQ0cm5Imeo72RAP4DEbjLNfLp0vSyI4bn1RZjePkdeS9augOMgWVykt+ztx1R3MJW/gsn5nuFARzMtUktTfqb4tJ3+A==&o8=wR-h28Gxg	true	• Avira URL Cloud: malware	unknown
http://www.patrickguarte.com/henz/	true	• Avira URL Cloud: malware	unknown
http://www.patrickguarte.com/henz/?4hq=5p9Ov6C7qce51hIp6D8A72je8vUJddN77lLEFw6Ufibk2yN56suG3zROnD+rS7baXFO6PfoGYvZY6sqA3kYcUTUl/8Ylp7EDwQ==&o8=wR-h28Gxg	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.34888065 9.0000000008260000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.323170503.0000000008260000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.368664553.000000 0008260000.00000004.00000001.00020000.00 000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	help.exe, 00000005.00000003.456470513.00 000000003D3000.00000004.00000020.0002000 0.00000000.sdmp, -ODfqI49.5.dr	false		high
http://https://duckduckgo.com/ac/?q=	-ODfqI49.5.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	help.exe, 00000005.00000003.456470513.00 000000003D3000.00000004.00000020.0002000 0.00000000.sdmp, -ODfqI49.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	help.exe, 00000005.00000003.456470513.00 000000003D3000.00000004.00000020.0002000 0.00000000.sdmp, -ODfqI49.5.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	-ODfqI49.5.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	help.exe, 00000005.00000003.456470513.00 000000003D3000.00000004.00000020.0002000 0.00000000.sdmp, -ODfqI49.5.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	Lc8xQv8iZY.exe	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	help.exe, 00000005.00000003.456470513.00 000000003D3000.00000004.00000020.0002000 0.00000000.sdmp, -ODfqI49.5.dr	false		high
http://gmpg.org/xfn/11	help.exe, 00000005.00000002.569583171.00 0000003996000.00000004.10000000.0004000 0.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	-ODfqI49.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	help.exe, 00000005.00000003.456470513.00 000000003D3000.00000004.00000020.0002000 0.00000000.sdmp, -ODfqI49.5.dr	false		high
http://nsis.sf.net/NSIS_Error	Lc8xQv8iZY.exe	false		high
http://https://hm.baidu.com/hm.js?d0766413c666e394f861185086d7f52f	help.exe, 00000005.00000002.569839214.00 0000004494000.00000004.10000000.0004000 0.00000000.sdmp, help.exe, 00000005.0000 0002.568262746.00000000007E0000.00000004 .00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://206.119.101.137/ak_Address/Address.js	help.exe, 00000005.00000002.569839214.00000000004494000.00000004.10000000.00040000.00000000.sdmp, help.exe, 00000005.00000002.568262746.00000000007E0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	-ODfql49.5.dr	false		high
http://code.jquery.com/jquery-3.3.1.min.js	help.exe, 00000005.00000002.569583171.00000000003996000.00000004.10000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.217.47	eufidelizo.com	United States		46606	UNIFIEDLAYER-AS-1US	true
206.233.197.135	www.lyonfinancialusa.com	United States		174	COGENT-174US	true
155.159.61.221	www.patrickguarte.com	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	true
154.22.100.62	www.foxwhistle.com	United States		174	COGENT-174US	true
162.214.129.149	www.afterdarksocial.club	United States		46606	UNIFIEDLAYER-AS-1US	true
2.57.90.16	brennancorps.info	Lithuania		47583	AS-HOSTINGERLT	true
192.185.35.86	lopezmodeling.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756323
Start date and time:	2022-11-30 01:23:15 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Lc8xQv8iZY.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:	10
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.spyw.evad.winEXE@7/5@9/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 78.6% (good quality ratio 73.1%) • Quality average: 73.2% • Quality standard deviation: 31.1%
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, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\-ODfqI49

Process:	C:\Windows\SysWOW64\help.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

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

Process:	C:\Users\user\Desktop\Lc8xQv8iZY.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	125952
Entropy (8bit):	6.271337362250939
Encrypted:	false
SSDEEP:	3072:hzNyHSqEF90sCFO/M7f9hUnBZFXBuioTLzJhiF:mHSqo9jE5hSFXEc
MD5:	1EEBBBD92B2C0C60F896FF8DCBCEDCAA
SHA1:	1291CC58A5664B1ACD50D9FD8E0580C519190477
SHA-256:	01B2D4443C383F07CCF3EA521AE9502527EEEDF352B92B90A382121B03992EC3
SHA-512:	67EFA564F026094BEC0A44AAF01FC8072412E6CDEFF019631689254A996C8B06CD0CCCCEE64B3D70B847E9ACA7C3DBCDE327D0A822988CC5295847990A8D915
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 54%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\.....2.....2.....2.....v..*.....*.t...*.....Rich .....PE..L.....c.....h.....@.....@.....0..... .....@...@..... .....text....f.....h..... ..`.rdata...k.....l...l.....@..@.data...(+.....@....gfids..... .....@..@.rsrc.....0.....@..@..... .....

C:\Users\user\AppData\Local\Temp\ijamguwvje.h

Process:	C:\Users\user\Desktop\Lc8xQv8iZY.exe
File Type:	data
Category:	dropped
Size (bytes):	5929
Entropy (8bit):	6.194305098271039
Encrypted:	false
SSDEEP:	96:l3ZCWD/FmJYgnXC7p7i7Q7+7J7Q737snGaMyyhcLofV1M+zzinQTDLEyoscdwQU4:7/FmJYIydOs6dcDqVycLoN1M+eAjoscb
MD5:	00815375B1B0AEF8D5F1C54050813CF2
SHA1:	E007F2C7D30FBD16A35A97E91B1B4719F46D28BB
SHA-256:	2C6C3495127AE142AAA4577D73B6C1EE3502B2C76BEE20EBF54CEA2C86404E63
SHA-512:	64EDF14579C02EBE2B27EA06A19C5753F08AEEA370E4C8BF93552086AA4FFB62EBF841E818D40CA091343BB789AD7F42A7FE2BFBB76FE870F19065A31AAE2FE2
Malicious:	false
Reputation:	low

Preview:	.....}.....i..i....i..L..}.....WV.i..!..6..Q.....K..Z6.....g...T.].L..W.Q....V.O.....gJ.....N._.....T.].L..X}.....i..i....i.q&..Y.....$d5Xk...6A...5.....L....QW.9...L....V.....Og",..T.L. .XXRWV.Q.7.f...a!...Y.....>.i....L5.d...Q....]s..Y...Z.....L5gZ.Q.....Q....Nv]..]"....L..XXRWV}.....i..i....i.q....Y....Q.AV.T.....9..Z9.k"\|5.V.....Nv.aNv...k..2$..".Nv...GZ. $..k.Nf.$g..Nv.GZ...Nf.GZ...Q.T5".b.QV.T5.L.ZA.....i.....Q.L..W.Q....V.....$..J.....Nv_.....T.].L..(.....1....$.1.....Z....."|A."|..kn.G...kB.G../kn.G..ykp.G..skD.G..mk..G. .wkD.G...k..G...kk.G..uk..G...k|.G...k..G.....G....d4.....qG.....q.....q..t.....54.....q..m.....4.....qi.....4.....qW.....4.....q/.....u4....=q!.....4....%..ij...\9N..i....\9...i....\ 9...ij...\9g..i....\9h$.A..."|....i..."..\.....k..68...N.]..d.Nwe.9.....e\9...ij.Nw.\..hj..Nwe.9Z.G..i..Nw.\..h..Nwe.9Z.e..i..N

C:\Users\user\AppData\Local\Temp\nsaAF5F.tmp

Process:	C:\Users\user\Desktop\Lc8xQv8iZY.exe
File Type:	data
Category:	dropped
Size (bytes):	329129
Entropy (8bit):	7.534660167276675
Encrypted:	false
SSDEEP:	6144:qOlZjKGnyqAVoJZmaEPokM0R/fyysHSqo9jE5hSFXEc:lZjLA2ZJYJGf+E5h
MD5:	0092575B985AE1E77D23EC215EE09C05
SHA1:	122945BC6AC3866DDF76ECF99127D9648F5024A6
SHA-256:	27BE4D2BA04D732C15B4916F2758D13928D2D31377228E575B61D8DA7A509CBD
SHA-512:	C0F19441D03AC8F95C38F5878B4B61C01BCB852CFABCBF26A9D793B74D6D731AC9FD78D1317E2EC90A439E0368FE869E6A660C5DD34D0950A7CC6843F6FBF 10
Malicious:	false
Reputation:	low
Preview:	p.....,.....W...x.....p..... .....J....."...j.....h..... ....

C:\Users\user\AppData\Local\Temp\ocoimqmpj.ep

Process:	C:\Users\user\Desktop\Lc8xQv8iZY.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.99864599001922**
Encrypted:	**true**
SSDEEP:	3072:plkkjPCMjKvjM3CqAVPQsKZCVbJ55QSX5HBmGwrVhQles+ALw0J/ECp:plZjKGnyqAVoJZmaEPokM0R/p
MD5:	ADD9CD4EACD9591A07875B761C8D1640
SHA1:	2047C17A31A7E83850DEF3CA6310572957E5D0B2
SHA-256:	0AF1AFDA6F616BEB76513577272E0E36EFB99CF8A3718B7725D60C9D88DFBC0B
SHA-512:	132281DC01506D09D5C7106105338179A9DB0D50309C94FFBC5E63A7FBF0E6D6DC5B31D26DB93E51FB4C994DA3F8D9B398D2C31F3CF8CF807F111BD9CCF761 C
Malicious:	false
Preview:	.y..V?.....a.v.Nrd....y..8..z....&.t.H...d.F..._..,(...&.....<.1.S..Z.....W..5fn]8.....F.....B..+.6.....iw%.G$.....2Y.....6..7....v...K.n.7AA.;PY..&clMd..0..>.$~_p.....)..t.:.x1..r. w.7s....y)..B..6.vf.H..d..;..%....T.o.2....Cl....t.V?..J.i.....=d.)d..e?^..$R...&.t.H"..G.F.....,(..v&.....T.'.XZ)W..1D.7B..c.u...Y.#..j.....D.4...\..[...#%.G$.....*.....(.....(.>R..<tz..DH. .7..a...E 0..>.$~_.q.+...)j..t(.c..`*rXw.7s..N...!..B..WS.vf.H..d!..;..%..<.T.C.2.....I....t.V?..J.i.....Fd..d..e?^..z....&.t.H...d.F..._..,(..v&.....T.'.XZ)W..1D.7B..c.u...Y.#..j.....D.4...\..[... #%.G$.....*.....(.....(.>R..<tz..DH..7..a...E 0..>.$~_p.....)...t(}c...*r.w.7s..N...!..B.W.vf.H..d!..;..%..<.T.C.2.....I....t.V?..J.i.....Fd..d..e?^..z....&.t.H...d.F..._..,(..v&.....T.'.XZ)W. .1D.7B..c.u...Y.#..j.....D.4...\..[...#%.G$.....*.....(.....(.>R..<tz..DH..7..a...E 0..>.$~_p.....)...t(}c...*r.w.7s..N...!..B.W.vf.H..d

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.934197714132832
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Lc8xQv8iZY.exe
File size:	278807
MD5:	30571d64c9a9ed267159fa941a20840c
SHA1:	bfb81d8a7c94781b3bd939bd17d500ae61b2ff70
SHA256:	85d6c9eac93fb8818d37dc15110ebd060b3e9df48043ee6bcf349df6aed047c5
SHA512:	5c8b708f3540b9347c36722934c8fc56098a94f8362688a8fa712da99e1b8c2564698eb0bed52e226cdfc40cf8b762e1860f6ea9928260e3f0f35bba9cfda82f
SSDEEP:	6144:QBn10/UR088uiPuDtJWn42Isu/20+kfAZLrYdwMPTnDMiQH7oPo9:gWLuiPh4rZOH5ZL/MLn4REo9

TLSH:	4854236595E0DCF3E6EF5E70AAAB87E6E3B3B0444525D9CAC3608D2F68211C58E1D142
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...ly.V.....^.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40324f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796C [Sun Dec 27 05:38:52 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ab6770b0a8635b9d92a5838920cfe770

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+1Ch], ebx
mov dword ptr [esp+14h], 00409130h
xor esi, esi
mov byte ptr [esp+18h], 00000020h
call dword ptr [004070B8h]
call dword ptr [004070B4h]
cmp ax, 00000006h
je 00007F51E0A2E4F3h
push ebx
call 00007F51E0A312E1h
cmp eax, ebx
je 00007F51E0A2E4E9h
push 00000C00h
call eax
push 004091E0h
call 00007F51E0A31262h
push 004091D8h
call 00007F51E0A31258h
push 004091CCh
call 00007F51E0A3124Eh

Instruction
push 0000000Dh
call 00007F51E0A312B1h
push 0000000Bh
call 00007F51E0A312AAh
mov dword ptr [00423F84h], eax
call dword ptr [00407034h]
push ebx
call dword ptr [00407270h]
mov dword ptr [00424038h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007F51E0A30EE1h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007F51E0A30ECFh
push ebx
call dword ptr [00407144h]

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73cc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x9e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x9e0	0xa00	False	0.45625	data	4.509328731926377	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, GetTempPathA, GetCommandLineA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, LoadLibraryA, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, WaitForSingleObject, ExitProcess, GetWindowsDirectoryA, GetProcAddress, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, WriteFile, MulDiv, LoadLibraryExA, GetModuleHandleA, MultiByteToWideChar, FreeLibrary
USER32.dll	GetWindowRect, EnableMenuItem, GetSystemMenu, ScreenToClient, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetForegroundWindow, PostQuitMessage, RegisterClassA, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, OpenClipboard, TrackPopupMenu, SendMessageTimeoutA, GetDC, LoadImageA, GetDlgItem, FindWindowExA, IsWindow, SetClipboardData, SetWindowLongA, EmptyClipboard, SetTimer, CreateDialogParamA, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteValueA, SetFileSecurityA, RegOpenKeyExA, RegDeleteKeyA, RegEnumValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4162.214.129.14949699802031453 11/30/22-01:25:33.429382	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.4	162.214.129.149
192.168.2.4162.214.129.14949699802031412 11/30/22-01:25:33.429382	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.4	162.214.129.149
192.168.2.4206.233.197.13549697802031453 11/30/22-01:25:25.388400	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49697	80	192.168.2.4	206.233.197.135
192.168.2.4206.233.197.13549697802031412 11/30/22-01:25:25.388400	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49697	80	192.168.2.4	206.233.197.135
192.168.2.4162.214.129.14949699802031449 11/30/22-01:25:33.429382	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49699	80	192.168.2.4	162.214.129.149
192.168.2.4206.233.197.13549697802031449 11/30/22-01:25:25.388400	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49697	80	192.168.2.4	206.233.197.135

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:25:17.361155033 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.493072987 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.493242025 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.530616999 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.662348032 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671255112 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671319962 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671411037 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671453953 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671489000 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.671535969 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671556950 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.671602964 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671647072 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671689987 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.671710014 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671755075 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671791077 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671813011 CET	49695	80	192.168.2.4	192.185.217.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:25:17.671848059 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:17.671983004 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.672039986 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.672449112 CET	49695	80	192.168.2.4	192.185.217.47
Nov 30, 2022 01:25:17.804025888 CET	80	49695	192.185.217.47	192.168.2.4
Nov 30, 2022 01:25:22.856251001 CET	49696	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:23.108297110 CET	80	49696	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:23.108417034 CET	49696	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:23.108675003 CET	49696	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:23.360415936 CET	80	49696	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:23.608623028 CET	80	49696	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:23.608676910 CET	80	49696	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:23.608916998 CET	49696	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:24.117248058 CET	49696	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:25.133325100 CET	49697	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:25.388127089 CET	80	49697	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:25.388283968 CET	49697	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:25.388400078 CET	49697	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:25.642827034 CET	80	49697	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:25.881593943 CET	80	49697	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:25.881633997 CET	80	49697	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:25.881783009 CET	49697	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:25.881913900 CET	49697	80	192.168.2.4	206.233.197.135
Nov 30, 2022 01:25:26.136291027 CET	80	49697	206.233.197.135	192.168.2.4
Nov 30, 2022 01:25:31.058685064 CET	49698	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:31.228578091 CET	80	49698	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:31.228790045 CET	49698	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:31.228866100 CET	49698	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:31.398617983 CET	80	49698	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:31.398947954 CET	80	49698	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:31.398994923 CET	80	49698	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:31.399027109 CET	80	49698	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:31.399061918 CET	80	49698	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:31.399125099 CET	49698	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:31.399125099 CET	49698	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:32.245378971 CET	49698	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.259099007 CET	49699	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.429162025 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:33.429264069 CET	49699	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.429382086 CET	49699	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.599260092 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:33.599673986 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:33.599761009 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:33.599796057 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:33.599829912 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:33.599961996 CET	49699	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.599961996 CET	49699	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.600157022 CET	49699	80	192.168.2.4	162.214.129.149
Nov 30, 2022 01:25:33.769869089 CET	80	49699	162.214.129.149	192.168.2.4
Nov 30, 2022 01:25:38.800184965 CET	49700	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:39.009787083 CET	80	49700	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:39.010145903 CET	49700	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:39.010220051 CET	49700	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:39.219959974 CET	80	49700	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:39.220068932 CET	80	49700	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:39.220103025 CET	80	49700	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:39.220248938 CET	49700	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:40.026948929 CET	49700	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:41.041326046 CET	49701	80	192.168.2.4	155.159.61.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:25:41.266415119 CET	80	49701	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:41.267105103 CET	49701	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:41.267249107 CET	49701	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:41.493232965 CET	80	49701	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:41.493326902 CET	80	49701	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:41.493360043 CET	80	49701	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:41.493607998 CET	49701	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:41.512168884 CET	49701	80	192.168.2.4	155.159.61.221
Nov 30, 2022 01:25:41.737354040 CET	80	49701	155.159.61.221	192.168.2.4
Nov 30, 2022 01:25:54.098124027 CET	49702	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:54.130537033 CET	80	49702	2.57.90.16	192.168.2.4
Nov 30, 2022 01:25:54.130795002 CET	49702	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:54.144684076 CET	49702	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:54.177130938 CET	80	49702	2.57.90.16	192.168.2.4
Nov 30, 2022 01:25:54.177197933 CET	80	49702	2.57.90.16	192.168.2.4
Nov 30, 2022 01:25:54.177283049 CET	80	49702	2.57.90.16	192.168.2.4
Nov 30, 2022 01:25:54.177361965 CET	49702	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:55.156131029 CET	49702	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:56.167906046 CET	49703	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:56.204200029 CET	80	49703	2.57.90.16	192.168.2.4
Nov 30, 2022 01:25:56.204314947 CET	49703	80	192.168.2.4	2.57.90.16
Nov 30, 2022 01:25:56.204452991 CET	49703	80	192.168.2.4	2.57.90.16

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:25:17.332652092 CET	56572	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:17.350507975 CET	53	56572	8.8.8.8	192.168.2.4
Nov 30, 2022 01:25:22.682940006 CET	50911	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:22.855253935 CET	53	50911	8.8.8.8	192.168.2.4
Nov 30, 2022 01:25:30.889216900 CET	59683	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:31.057456017 CET	53	59683	8.8.8.8	192.168.2.4
Nov 30, 2022 01:25:38.630486965 CET	64167	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:38.799020052 CET	53	64167	8.8.8.8	192.168.2.4
Nov 30, 2022 01:25:46.529058933 CET	58565	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:47.344357967 CET	53	58565	8.8.8.8	192.168.2.4
Nov 30, 2022 01:25:48.363827944 CET	52239	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:48.895919085 CET	53	52239	8.8.8.8	192.168.2.4
Nov 30, 2022 01:25:54.045008898 CET	56807	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:25:54.096646070 CET	53	56807	8.8.8.8	192.168.2.4
Nov 30, 2022 01:26:01.252393007 CET	61007	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:26:01.374481916 CET	53	61007	8.8.8.8	192.168.2.4
Nov 30, 2022 01:26:08.846963882 CET	60686	53	192.168.2.4	8.8.8.8
Nov 30, 2022 01:26:09.028095007 CET	53	60686	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 01:25:17.332652092 CET	192.168.2.4	8.8.8.8	0xb919	Standard query (0)	www.eufidelizo.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:22.682940006 CET	192.168.2.4	8.8.8.8	0xf6a5	Standard query (0)	www.lyonfinancialusa.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:30.889216900 CET	192.168.2.4	8.8.8.8	0xcf4c	Standard query (0)	www.afterdarksocial.club	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:38.630486965 CET	192.168.2.4	8.8.8.8	0xffbe	Standard query (0)	www.patrickguarte.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:46.529058933 CET	192.168.2.4	8.8.8.8	0xb251	Standard query (0)	www.19t221013d.tokyo	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:48.363827944 CET	192.168.2.4	8.8.8.8	0x878e	Standard query (0)	www.19t221013d.tokyo	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 01:25:54.045008898 CET	192.168.2.4	8.8.8.8	0x55e9	Standard query (0)	www.brennancorps.info	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:26:01.252393007 CET	192.168.2.4	8.8.8.8	0xcecd	Standard query (0)	www.lopezmodeling.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:26:08.846963882 CET	192.168.2.4	8.8.8.8	0xca60	Standard query (0)	www.foxwhistle.com	A (IP address)	IN (0x0001)	false

DNS Answers

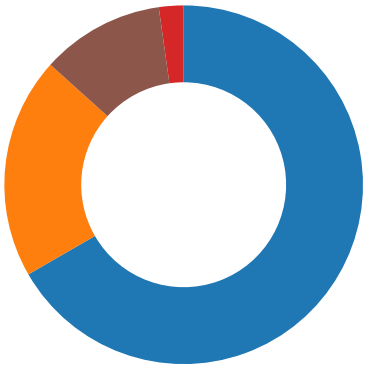
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 01:25:17.350507975 CET	8.8.8.8	192.168.2.4	0xb919	No error (0)	www.eufidelizo.com	eufidelizo.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:25:17.350507975 CET	8.8.8.8	192.168.2.4	0xb919	No error (0)	eufidelizo.com		192.185.217.47	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:22.855253935 CET	8.8.8.8	192.168.2.4	0xf6a5	No error (0)	www.lyonfinancialusa.com		206.233.197.135	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:31.057456017 CET	8.8.8.8	192.168.2.4	0xcf4c	No error (0)	www.afterdarksocial.club		162.214.129.149	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:38.799020052 CET	8.8.8.8	192.168.2.4	0xffbe	No error (0)	www.patrickguarte.com		155.159.61.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:47.344357967 CET	8.8.8.8	192.168.2.4	0xb251	Server failure (2)	www.19t221013d.tokyo	none	none	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:48.895919085 CET	8.8.8.8	192.168.2.4	0x878e	Server failure (2)	www.19t221013d.tokyo	none	none	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:25:54.096646070 CET	8.8.8.8	192.168.2.4	0x55e9	No error (0)	www.brennancorps.info	brennancorps.info		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:25:54.096646070 CET	8.8.8.8	192.168.2.4	0x55e9	No error (0)	brennancorps.info		2.57.90.16	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:26:01.374481916 CET	8.8.8.8	192.168.2.4	0xcecd	No error (0)	www.lopezmodeling.com	lopezmodeling.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:26:01.374481916 CET	8.8.8.8	192.168.2.4	0xcecd	No error (0)	lopezmodeling.com		192.185.35.86	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:26:09.028095007 CET	8.8.8.8	192.168.2.4	0xca60	No error (0)	www.foxwhistle.com		154.22.100.62	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.eufidelizo.com
- www.lyonfinancialusa.com
- www.afterdarksocial.club
- www.patrickguarte.com
- www.brennancorps.info
- www.lopezmodeling.com
- www.foxwhistle.com

Statistics

Behavior



- Lc8xQv8iZY.exe
- hvbvmxm.exe
- conhost.exe
- hvbvmxm.exe
- explorer.exe
- help.exe

Click to jump to process

System Behavior

Analysis Process: Lc8xQv8iZY.exe PID: **3376**, Parent PID: **3528**

General

Target ID:	0
Start time:	01:24:07
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\Lc8xQv8iZY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Lc8xQv8iZY.exe
Imagebase:	0x400000
File size:	278807 bytes
MD5 hash:	30571D64C9A9ED267159FA941A20840C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: hvbvmxm.exe PID: **3052**, Parent PID: **3376**

General

Target ID:	1
Start time:	01:24:08
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\hvbvmxm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\hvbvmxm.exe" C:\Users\user\AppData\Local\Temp\ijamguwvje.h
Imagebase:	0x400000
File size:	125952 bytes
MD5 hash:	1EEBBBD92B2C0C60F896FF8DCBCEDCAA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 54%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ijamguwvje.h	unknown	5929	success or wait	1	409809	ReadFile
C:\Users\user\AppData\Local\Temp\ocoimqmpj.ep	unknown	189440	success or wait	1	B804C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B815CB	ReadFile

Analysis Process: conhost.exe PID: **3748**, Parent PID: **3052**

General

Target ID:	2
Start time:	01:24:08
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: hvbvmxm.exe PID: **5420**, Parent PID: **3052**

General

Target ID:	3
Start time:	01:24:09
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\hvbvmxm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\hvbvmxm.exe" C:\Users\user\AppData\Local\Temp\ijamguwvje.h
Imagebase:	0x400000
File size:	125952 bytes
MD5 hash:	1EEBBBD92B2C0C60F896FF8DCBCEDCAA
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: 00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.385960005.00000000005A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.386021250.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.386021250.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.386021250.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.386021250.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.385717427.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.385717427.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.385717427.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.385717427.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41DF9E	NtReadFile

Analysis Process: explorer.exe PID: **3528**, Parent PID: **5420**

General

Target ID:	4
Start time:	01:24:13
Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.353715977.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.353715977.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.353715977.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.353715977.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.376694506.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.376694506.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.376694506.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.376694506.000000000D6C1000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: help.exe PID: 1900, Parent PID: 3528

General

Target ID:	5
Start time:	01:24:44
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x110000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000005.00000002.568390844.0000000003040000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.568390844.0000000003040000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.568390844.0000000003040000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.568390844.0000000003040000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.568316286.0000000002D40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.568316286.0000000002D40000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.568316286.0000000002D40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.568316286.0000000002D40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.567455523.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.567455523.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.567455523.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.567455523.0000000000270000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hvbvmxm.exe	success or wait	1	305C897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\-ODfqI49	object name not found	1	305C897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\-ODfqI49	sharing violation	1	305C897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\-ODfqI49	sharing violation	1	305C897	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	305C867	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly