ID: 756313
Sample Name: qHpeBvr9cR.exe
Cookbook: default.jbs
Time: 01:08:08
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

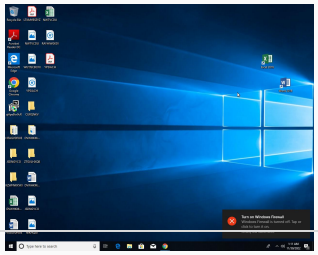
Windows Analysis Report

qHpeBvr9cR.exe

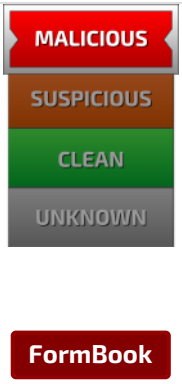
Overview

General Information

Sample Name:	qHpeBvr9cR.exe
Analysis ID:	756313
MD5:	f5bea76ffac05af…
SHA1:	93ef457bfcbc5f0…
SHA256:	40dcfb70411226..
Tags:	32 exe Formbook trojan
Infos:	



Detection

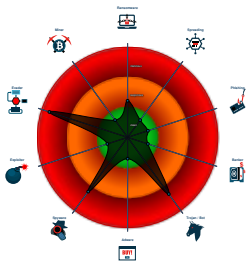


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Uses netsh to modify the Windows …

Classification



Process Tree

- **System is w10x64**
- qHpeBvr9cR.exe (PID: 5588 cmdline: C:\Users\user\Desktop\qHpeBvr9cR.exe MD5: F5BEA76FFAC05AFBE19274595801184E)
  - febcldoukq.exe (PID: 5816 cmdline: "C:\Users\user\AppData\Local\Temp\febcldoukq.exe" C:\Users\user\AppData\Local\Temp\uebzn.cef MD5: 96E050F99502FE7C52FD9B0F10202578)
    - febcldoukq.exe (PID: 5828 cmdline: "C:\Users\user\AppData\Local\Temp\febcldoukq.exe" C:\Users\user\AppData\Local\Temp\uebzn.cef MD5: 96E050F99502FE7C52FD9B0F10202578)
      - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - autochk.exe (PID: 3624 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
        - netsh.exe (PID: 5920 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
- **cleanup**

Malware Configuration

Threatname: FormBook

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.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
00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.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
00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.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
00000005.00000002.561579336.0000000001100000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.febcldoukq.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.febcldoukq.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x7d48:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x207a7:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbff6:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1952e:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.2.febcldoukq.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1932c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18dd8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1942e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x195a6:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xbbc1:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18023:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1f51e:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20511:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.febcldoukq.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1b820:$sqlite3step: 68 34 1C 7B E1 • 0x1c398:$sqlite3step: 68 34 1C 7B E1 • 0x1b862:$sqlite3text: 68 38 2A 90 C5 • 0x1c3dd:$sqlite3text: 68 38 2A 90 C5 • 0x1b879:$sqlite3blob: 68 53 D8 7F 8C • 0x1c3f3:$sqlite3blob: 68 53 D8 7F 8C
2.2.febcldoukq.exe.400000.0.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: 192.168.2.5 - Destination IP: 206.233.197.135

Timestamp:	192.168.2.5206.233.197.13549710802031453 11/30/22-01:10:42.253815
SID:	2031453

Source Port:	49710
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: 162.214.129.149	−
Timestamp:	192.168.2.5162.214.129.14949712802031453 11/30/22-01:10:50.366888
SID:	2031453
Source Port:	49712
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: 206.233.197.135	−
Timestamp:	192.168.2.5206.233.197.13549710802031449 11/30/22-01:10:42.253815
SID:	2031449
Source Port:	49710
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: 162.214.129.149	−
Timestamp:	192.168.2.5162.214.129.14949712802031412 11/30/22-01:10:50.366888
SID:	2031412
Source Port:	49712
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: 206.233.197.135	−
Timestamp:	192.168.2.5206.233.197.13549710802031412 11/30/22-01:10:42.253815
SID:	2031412
Source Port:	49710
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: 162.214.129.149	−
Timestamp:	192.168.2.5162.214.129.14949712802031449 11/30/22-01:10:50.366888
SID:	2031449
Source Port:	49712
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)

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)

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information

Yara detected FormBook

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

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

Remote Access Functionality

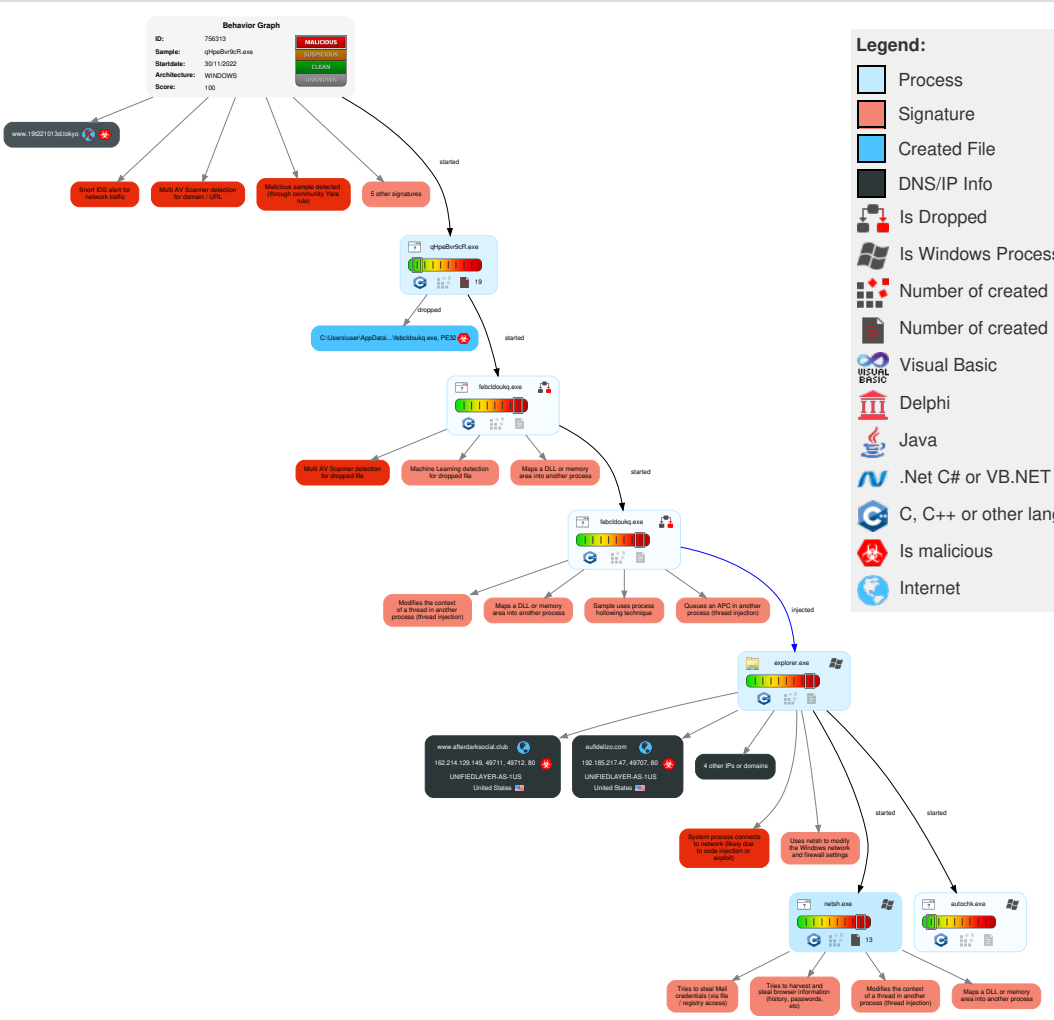
Yara detected FormBook

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	1 Disable or Modify Tools	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 Shared Modules	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	1 1 Input Capture	1 3 1 Security Software Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	1 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

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	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
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	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

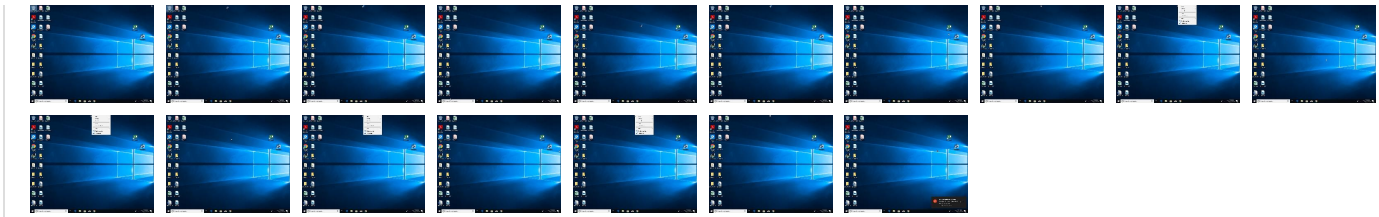
Behavior Graph



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
qHpeBvr9cR.exe	41%	ReversingLabs	Win32.Trojan.Garf	
qHpeBvr9cR.exe	37%	Virustotal		Browse
qHpeBvr9cR.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.febcldoukq.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.febcldoukq.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.qHpeBvr9cR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
0.2.qHpeBvr9cR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.2.febcldoukq.exe.17b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.patrickguarte.com	1%	Virustotal		Browse
eufidelizo.com	9%	Virustotal		Browse
www.lyonfinancialusa.com	0%	Virustotal		Browse
www.eufidelizo.com	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.eufidelizo.com/henz/?ChMxG4C=wcp3urA+/rGtUuNVdXHur6CaD7Rg4XGXlvUWG7FdGjeYGPzd5j/g1Govvww0i9Uvwfj8E4D4P4OVv2O692MpWFmEiKCsF21Xzw==&8p08qr=2d0X	100%	Avira URL Cloud	malware	
http://www.patrickguarte.com/henz/?ChMxG4C=5p9Ov6C7qce51hIp6D8A72je8vUJddN77lLEFw6Ufibk2yN56suG3zROnD+rS7baXFO6PfoGYvZY6sqA3kYBdz817Owqh44+wA==&8p08qr=2d0X	100%	Avira URL Cloud	malware	
www.brennancorps.info/henz/	100%	Avira URL Cloud	malware	
http://www.patrickguarte.com/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	

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
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.19t221013d.tokyo	unknown	unknown	true		unknown

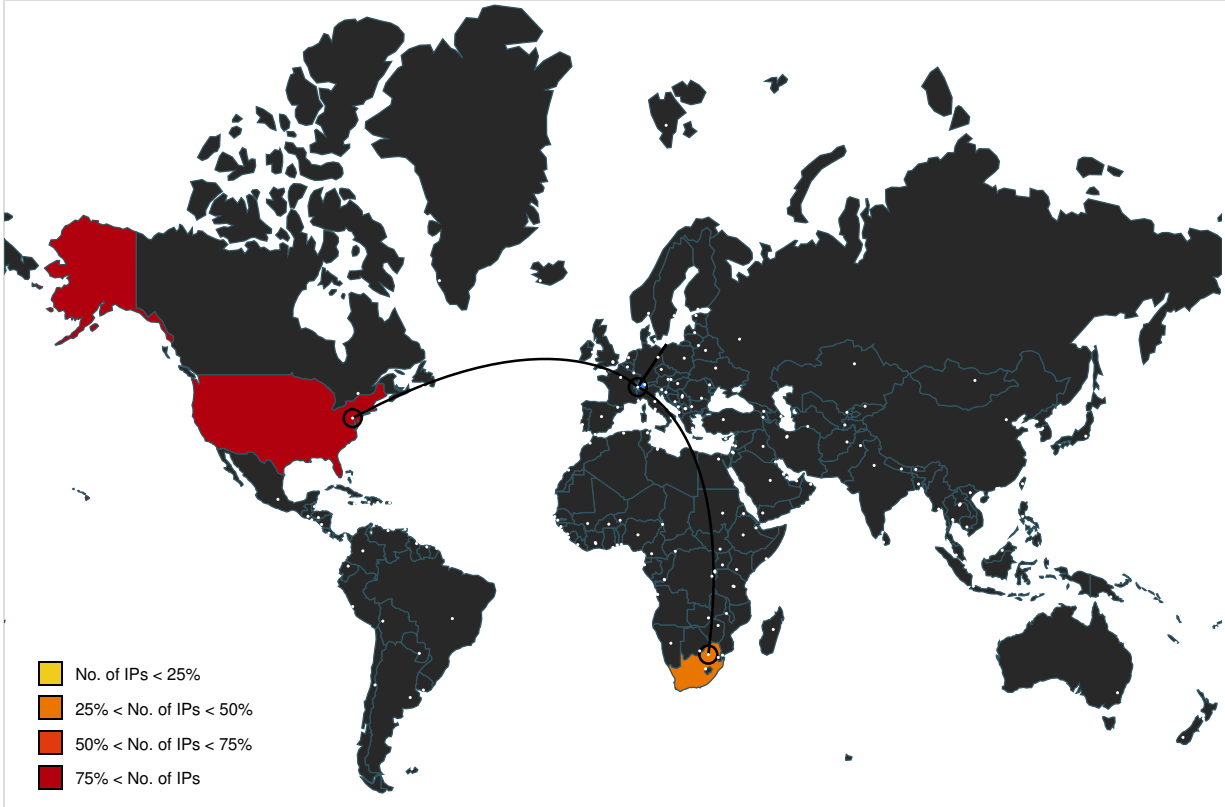
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.lyonfinancialusa.com/henz/	true	• Avira URL Cloud: malware	unknown
http://www.eufidelizo.com/henz/?ChMxG4C=wcp3urA+/rGtUuNVdXHur6CaD7Rg4XGXlvUWG7FdGjeYGPzd5j/g1Govvww0i9Uvwfj8E4D4P4OVv2O692MpWFmEiKCsF21Xzw==&8p08qr=2d0X	true	• Avira URL Cloud: malware	unknown
http://www.patrickguarte.com/henz/?ChMxG4C=5p9Ov6C7qce51hIp6D8A72je8vUJddN77lLEFw6Ufibk2yN56suG3zROnD+rS7baXFO6PfoGYvZY6sqA3kYBdz817Owqh44+wA==&8p08qr=2d0X	true	• Avira URL Cloud: malware	unknown
http://www.patrickguarte.com/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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	-ODfql49.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	-ODfql49.5.dr	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.35615643 9.000000000091F000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.336262975.000000000091F000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.303735560.000000 000091F000.00000004.00000020.00020000.00 000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	-ODfql49.5.dr	false		high
http://https://duckduckgo.com/ac/?q=	-ODfql49.5.dr	false		high
http://nsis.sf.net/NSIS_Error	qHpeBvr9cR.exe	false		high
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	-ODfql49.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	-ODfql49.5.dr	false		high
http:// https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	-ODfql49.5.dr	false		high
http:// https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	-ODfql49.5.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	qHpeBvr9cR.exe	false		high
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	-ODfql49.5.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	-ODfql49.5.dr	false		high
http://code.jquery.com/jquery-3.3.1.min.js	netsh.exe, 00000005.00000002.565764534.0 000000003B56000.00000004.10000000.000400 00.00000000.sdmp	false		high
http://gmpg.org/xfn/11	netsh.exe, 00000005.00000002.565764534.0 000000003B56000.00000004.10000000.000400 00.00000000.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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
162.214.129.149	www.afterdarksocial.club	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756313
Start date and time:	2022-11-30 01:08:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qHpeBvr9cR.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:	9
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@7/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 76.9% (good quality ratio 67.7%) • Quality average: 68.7% • Quality standard deviation: 34.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.90
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, e16604.g.akamaiedge.net, ctldl.windowsupdate.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly 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\netsh.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):	1.287139506398081
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3 1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

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

Process:	C:\Users\user\Desktop\qHpeBvr9cR.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	147968
Entropy (8bit):	6.182768531900874
Encrypted:	false
SSDEEP:	3072:ZOPPLcLPR2kaQ+nYwZbBPUxRC/akBYcgVg7JkWmjwaY4YFOnJSwy:ZiLcLPRi/xB8gFLm8oJSd
MD5:	96E050F99502FE7C52FD9B0F10202578
SHA1:	9ACE01D602E21FF8BF364A3BB2F46BC7FD285A7B
SHA-256:	C7207F58E7A5BAD6EFC38C7DDFDDBC3B32C28F6BBA01D4251A44F6BBDABE4BC3
SHA-512:	E09EDF0C05667FD2B684AD48F6938A0FB41C9B346197D5065FE828093789140B1A1F79279D8504428C9BA0B8049FAD9D7242015C43B746C854688AA883898E1E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low

Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....c.....@.....@.....@..... .....`.....\|.....text..... ..`.rdata..$t.....v.....@..@.data....%...@..... .....@....00cfg.....p.....&.....@..@.voltbl."..... (.....rsrc.....*.....@..@.reloc.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsx95CC.tmp

Process:	C:\Users\user\Desktop\qHpeBvr9cR.exe
File Type:	data
Category:	dropped
Size (bytes):	347987
Entropy (8bit):	7.481309990466636
Encrypted:	false
SSDEEP:	6144:RucNUhVyZTV2GQFRx0+EzyfkKisTiLcLPRi/xB8gFLm8oJSd:32jyZTgGL3cimiLcLPsPDC8n
MD5:	3D3DFD7BB3B31CA9F6A9085FF03A933F
SHA1:	C445CD44742166B12BC976C54EB0422E7B377C73
SHA-256:	74B5FDE9425C99AEB58669440FEE9206A57CAA8790635253E7F5C215973F4FB5
SHA-512:	202322D77C9697C31197F059DEF5879089D15CFCAA5BAA34C9603487ACC73F9E6D3EE5CD693B9523A57A24176604D588F0DFFA1A2C8E6229BCCE345485194BA
Malicious:	false
Reputation:	low
Preview:	v.....,.....>.....^..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\rcibkfyfwn.yxq

Process:	C:\Users\user\Desktop\qHpeBvr9cR.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.9986039311688**
Encrypted:	**true**
SSDEEP:	3072:8fFUilhKe4N7QY77ozZs4cwNwnj9XGKjbMVcRx0+DBhaQmmmXzbwaf6f03uftUZj:8NUhVyZTV2GQFRx0+EzyfkKisy
MD5:	9929DD1C8831360C68C176ADB59CA947
SHA1:	6CB9F8D296878B31DB696038EA01470613AEED9F
SHA-256:	5F3B667FA88AAD6BA21374E37014E72C2AAD0317ED1DE2C1D6DE839A61F9F541
SHA-512:	390D7426188347A9F64D9EEA2A9B89807443BBDAC1409DB20532CD504A56637005B75B8FE23D29E5F8187D9D1DEB238B10FE8734ED504C13AE9E5478667F0E9
Malicious:	false
Reputation:	low
Preview:	..u..2..q..... .W.....0ng!Pz..a.8.4..Y.....o..%.a..u.j.:V...p....<!.....P[.$..GiQO.P:.@..}~...:,..aN.i>.....-pF.j0..D...EM....4...../.$....i*..t.f.z.W. %hO.....?.O[8....n...a.1....CK.7 %=.....;G...ku.....=.080..J.(.....`.,..U.N..xm..:..#.p\;..2..$o...t.....[.'.5b{'..a(8....Y....qo..%.a(..u.j.:.....,a.U-...Je/Z....A.E..TF.4.F.{4.p.../7.@.=..m.....s0..D....*.1.~T..0Y.'(>....Hx. ...\h5.....(@.3`.....,?.O[8...k...ua.1-J,..|I..9.f.....;G.G...EVz....(80..J.(..R...S.,..!.N.dxm...:.O#.d\;..2..o...t..6$..O[.'.5b.'z..a.8.4..Y.....o..%.a..u.j.:.....,a.U-...Je/Z....A.E..TF.4.F.{4 .p.../7.@.=..m.....s0..D....*.1.~T..0Y.'(>....Hx....\h5.....(@.3`.....,?.O[8....n...a.1.....SI...6f....;G.G...EVz....080..J.(..R...S.,..!.N.dxm..:.O#.d\;..2..o...t..6$..O[.'.5b.'z..a.8.4.. Y.....o..%.a..u.j.:.....,a.U-...Je/Z....A.E..TF.4.F.{4.p.../7.@.=..m.....s0..D....*.1.~T..0Y.'(>....Hx....\h5.....(@.3`.....,?.O[8....n...a.1.....SI...6f....;G.G...EVz....080..J.(.

C:\Users\user\AppData\Local\Temp\uebzn.cef

Process:	C:\Users\user\Desktop\qHpeBvr9cR.exe
File Type:	data
Category:	dropped
Size (bytes):	5837
Entropy (8bit):	6.204282040759092
Encrypted:	false
SSDEEP:	96:FMlgVSPVGToJyq52wK33eDdEA2GVnb3+EFxIhP/mny+lDMv4h3UboO:7StrNtK3eBEAHb37PnN3/O
MD5:	28373E2B7E834278BBFC8597EA79A659
SHA1:	674506B6D8C29D724529B2154D2EDCABEC4DB4EB
SHA-256:	C8BD6B365CE4C504FD875CC967B7B498E8D79A27E877DBF1B3128EAD638C1B57
SHA-512:	4B1CB1CFE3DB15617511826351738010044DB5742E2BE522D3661D36AA532EF52CD59776A211C51BC58F118CF64B126ADC0296D537ACEECE7E66E7D6D7034BE
Malicious:	false
Reputation:	low

Preview:	;.....s.....U..>.s....."...B.....Z.....=.Z=.....T....>..."L.....=.\#BS3!..b.).#.X.T...;...T....>..s..... ..B.....Z..g.....*.2.Z...[U.Z[U..>.."....Z.....$.....*.....T. ...>....."....a.....1....9....)....."..Z...D.a.B....."..A.Z...[T".....Q.....a==..>.....s.....s0..B....."..2.....%.....%.....%.Z.....a....Q...Q..T...g.Y.Z..Q..T...\g.Y.....g....Q*.. (.U..*..1...."....a..."....2....G.Z=..Z...[T"...>..."L.....=.\#BS3!g...b.).#.Q.T...A...T....>.>....a.v....g.v..^`.6.`.?.`.@.`.A.`.B...2.....\|.....~.....H.....J.....D.....F.....P.....R..... L.....N.....X.....Z.....T.Z...VB.....>..u0...>B.....@...>B.....r..W...>B.....f.7.F...>B8.....j...A...>B(.....0...>BX.....n.H.Z...>BH.....z.zc...>Bx.....Z.Z.`.....Z.S:.`.....Z.#:.`.....Z.Z. `.....Z.S:.`....g.2..^.:.=!..:.:.:.:.....:$.....^.X..:.P....b..:....=).Z.Z..P..6.[.[..P....S...Z.S:..P..6.[.S3..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9356650255872205
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:	qHpeBvr9cR.exe
File size:	285325
MD5:	f5bea76ffac05afbe19274595801184e
SHA1:	93ef457bfcbc5f0860b1b7f6353ed6e9b0afd60e
SHA256:	40dcfb704112265b383679baa3064cd7355bd02119b117f396e1b0283342362c
SHA512:	3e1537258907bc3707c5cd0a54b4b5d35516e1ccb2443dfcfb493ecd931a734acf85bf2fb9aede36893b7dd12ee71baac7df48506117aee972bdab68e6a08ab3
SSDEEP:	6144:QBn1RomeugRHbNAtHRgt/GVl9tSvOBFRQecwcwHa:gavFRy5Ot/OceFRbfHa
TLSH:	2554233734CA95BBD8674633C8B3A1E6D37FE2034422115B1BD50F66B6987C3C26299B
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

Instruction
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 00007F445C64C0C3h
push ebx
call 00007F445C64EEB1h
cmp eax, ebx
je 00007F445C64C0B9h
push 00000C00h
call eax
push 004091E0h
call 00007F445C64EE32h
push 004091D8h
call 00007F445C64EE28h
push 004091CCh
call 00007F445C64EE1Eh
push 0000000Dh
call 00007F445C64EE81h
push 0000000Bh
call 00007F445C64EE7Ah
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 00007F445C64EAB1h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007F445C64EA9Fh
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x9e0	0xa00	False	0.45625	data	4.509328731926377	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

DLL	Import
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

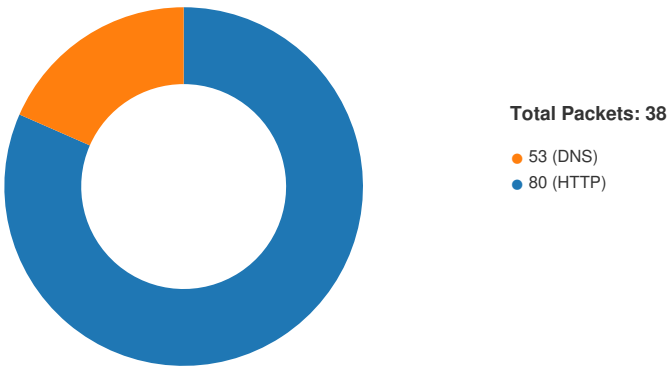
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5206.233.197.1354971080203145311/30/22-01:10:42.253815	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49710	80	192.168.2.5	206.233.197.135
192.168.2.5162.214.129.1494971280203145311/30/22-01:10:50.366888	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49712	80	192.168.2.5	162.214.129.149
192.168.2.5206.233.197.1354971080203144911/30/22-01:10:42.253815	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49710	80	192.168.2.5	206.233.197.135
192.168.2.5162.214.129.1494971280203141211/30/22-01:10:50.366888	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49712	80	192.168.2.5	162.214.129.149
192.168.2.5206.233.197.1354971080203141211/30/22-01:10:42.253815	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49710	80	192.168.2.5	206.233.197.135
192.168.2.5162.214.129.1494971280203144911/30/22-01:10:50.366888	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49712	80	192.168.2.5	162.214.129.149

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:10:29.024822950 CET	49707	80	192.168.2.5	192.185.217.47
Nov 30, 2022 01:10:29.147394896 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.149022102 CET	49707	80	192.168.2.5	192.185.217.47
Nov 30, 2022 01:10:29.149192095 CET	49707	80	192.168.2.5	192.185.217.47
Nov 30, 2022 01:10:29.271584988 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279675961 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279721975 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279748917 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279777050 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279805899 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279834986 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279865026 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279892921 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279922009 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279942989 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.279959917 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:29.280064106 CET	49707	80	192.168.2.5	192.185.217.47
Nov 30, 2022 01:10:29.280209064 CET	49707	80	192.168.2.5	192.185.217.47
Nov 30, 2022 01:10:29.280512094 CET	49707	80	192.168.2.5	192.185.217.47
Nov 30, 2022 01:10:29.402862072 CET	80	49707	192.185.217.47	192.168.2.5
Nov 30, 2022 01:10:39.706011057 CET	49709	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:39.960129976 CET	80	49709	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:39.960378885 CET	49709	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:39.960500956 CET	49709	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:40.214560032 CET	80	49709	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:40.547215939 CET	80	49709	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:40.547250032 CET	80	49709	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:40.547370911 CET	49709	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:40.964452982 CET	49709	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:41.980474949 CET	49710	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:42.253413916 CET	80	49710	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:42.253650904 CET	49710	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:42.253814936 CET	49710	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:42.526724100 CET	80	49710	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:42.818850040 CET	80	49710	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:42.818918943 CET	80	49710	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:42.819215059 CET	49710	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:42.822645903 CET	49710	80	192.168.2.5	206.233.197.135
Nov 30, 2022 01:10:43.106801987 CET	80	49710	206.233.197.135	192.168.2.5
Nov 30, 2022 01:10:48.010961056 CET	49711	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:48.177367926 CET	80	49711	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:48.177628040 CET	49711	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:48.177809000 CET	49711	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:48.344197035 CET	80	49711	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:48.344644070 CET	80	49711	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:48.344672918 CET	80	49711	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:48.344693899 CET	80	49711	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:48.344713926 CET	80	49711	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:48.344789028 CET	49711	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:48.344860077 CET	49711	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:49.184077024 CET	49711	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:50.200092077 CET	49712	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:50.366451979 CET	80	49712	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:50.366700888 CET	49712	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:50.366888046 CET	49712	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:50.533267021 CET	80	49712	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:50.533715010 CET	80	49712	162.214.129.149	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:10:50.533760071 CET	80	49712	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:50.533793926 CET	80	49712	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:50.533827066 CET	80	49712	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:50.533952951 CET	49712	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:50.534199953 CET	49712	80	192.168.2.5	162.214.129.149
Nov 30, 2022 01:10:50.700480938 CET	80	49712	162.214.129.149	192.168.2.5
Nov 30, 2022 01:10:55.727615118 CET	49713	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:55.949546099 CET	80	49713	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:55.949732065 CET	49713	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:55.949861050 CET	49713	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:56.171719074 CET	80	49713	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:56.171799898 CET	80	49713	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:56.171852112 CET	80	49713	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:56.171915054 CET	49713	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:56.965632915 CET	49713	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:58.089121103 CET	49714	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:58.301402092 CET	80	49714	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:58.301616907 CET	49714	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:58.301866055 CET	49714	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:58.514004946 CET	80	49714	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:58.514065027 CET	80	49714	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:58.514106989 CET	80	49714	155.159.61.221	192.168.2.5
Nov 30, 2022 01:10:58.514235973 CET	49714	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:58.514421940 CET	49714	80	192.168.2.5	155.159.61.221
Nov 30, 2022 01:10:58.726452112 CET	80	49714	155.159.61.221	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:10:28.856163025 CET	65323	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:10:29.011351109 CET	53	65323	8.8.8.8	192.168.2.5
Nov 30, 2022 01:10:39.525219917 CET	63446	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:10:39.704725981 CET	53	63446	8.8.8.8	192.168.2.5
Nov 30, 2022 01:10:47.853636980 CET	56751	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:10:48.007566929 CET	53	56751	8.8.8.8	192.168.2.5
Nov 30, 2022 01:10:55.547888041 CET	55039	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:10:55.726146936 CET	53	55039	8.8.8.8	192.168.2.5
Nov 30, 2022 01:11:03.553632021 CET	59220	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:11:04.318644047 CET	53	59220	8.8.8.8	192.168.2.5
Nov 30, 2022 01:11:05.325809002 CET	56682	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:11:06.344841003 CET	56682	53	192.168.2.5	8.8.8.8
Nov 30, 2022 01:11:06.350476027 CET	53	56682	8.8.8.8	192.168.2.5
Nov 30, 2022 01:11:07.118748903 CET	53	56682	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 30, 2022 01:11:07.119535923 CET	192.168.2.5	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 01:10:28.856163025 CET	192.168.2.5	8.8.8.8	0xdc74	Standard query (0)	www.eufidelizo.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:10:39.525219917 CET	192.168.2.5	8.8.8.8	0xccc6	Standard query (0)	www.lyonfinancialusa.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:10:47.853636980 CET	192.168.2.5	8.8.8.8	0x22da	Standard query (0)	www.afterdarksocial.club	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:10:55.547888041 CET	192.168.2.5	8.8.8.8	0x18f9	Standard query (0)	www.patrickguarte.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 01:11:03.553632021 CET	192.168.2.5	8.8.8.8	0x4db1	Standard query (0)	www.19t221013d.tokyo	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:11:05.325809002 CET	192.168.2.5	8.8.8.8	0xf47d	Standard query (0)	www.19t221013d.tokyo	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:11:06.344841003 CET	192.168.2.5	8.8.8.8	0xf47d	Standard query (0)	www.19t221013d.tokyo	A (IP address)	IN (0x0001)	false

DNS Answers

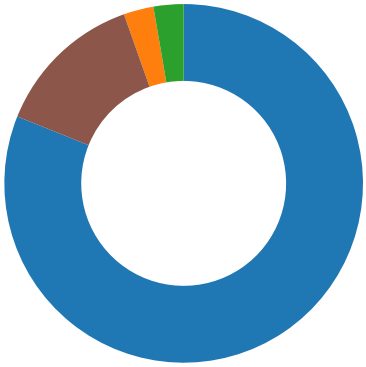
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 01:10:29.011351109 CET	8.8.8.8	192.168.2.5	0xdc74	No error (0)	www.eufidelizo.com	eufidelizo.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:10:29.011351109 CET	8.8.8.8	192.168.2.5	0xdc74	No error (0)	eufidelizo.com		192.185.217.47	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:10:39.704725981 CET	8.8.8.8	192.168.2.5	0xccc6	No error (0)	www.lyonfinancialusa.com		206.233.197.135	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:10:48.007566929 CET	8.8.8.8	192.168.2.5	0x22da	No error (0)	www.afterdarksocial.club		162.214.129.149	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:10:55.726146936 CET	8.8.8.8	192.168.2.5	0x18f9	No error (0)	www.patrickguarte.com		155.159.61.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:11:04.318644047 CET	8.8.8.8	192.168.2.5	0x4db1	Server failure (2)	www.19t221013d.tokyo	none	none	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:11:06.350476027 CET	8.8.8.8	192.168.2.5	0xf47d	Server failure (2)	www.19t221013d.tokyo	none	none	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:11:07.118748903 CET	8.8.8.8	192.168.2.5	0xf47d	Server failure (2)	www.19t221013d.tokyo	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.eufidelizo.com
- www.lyonfinancialusa.com
- www.afterdarksocial.club
- www.patrickguarte.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: qHpeBvr9cR.exe PID: 5588, Parent PID: 3324

General

Target ID:	0
Start time:	01:09:00
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\qHpeBvr9cR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\qHpeBvr9cR.exe
Imagebase:	0x400000
File size:	285325 bytes
MD5 hash:	F5BEA76FFAC05AFBE19274595801184E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: febcldoukq.exe PID: 5816, Parent PID: 5588

General

Target ID:	1
Start time:	01:09:00
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\febcldoukq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\febcldoukq.exe" C:\Users\user\AppData\Local\Temp\uebzn.cef
Imagebase:	0xb10000
File size:	147968 bytes
MD5 hash:	96E050F99502FE7C52FD9B0F10202578
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\uebzn.cef	unknown	5837	success or wait	1	B11A1D	ReadFile

Analysis Process: febcldoukq.exe PID: **5828**, Parent PID: **5816**

General

Target ID:	2
Start time:	01:09:00
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\febcldoukq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\febcldoukq.exe" C:\Users\user\AppData\Local\Temp\uebzn.cef
Imagebase:	0xb10000
File size:	147968 bytes
MD5 hash:	96E050F99502FE7C52FD9B0F10202578
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.395778723.0000000000F00000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.395778723.0000000000F00000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.395778723.0000000000F00000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.395778723.0000000000F00000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.393576373.0000000000B80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.393576373.0000000000B80000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.393576373.0000000000B80000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.393576373.0000000000B80000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.393032745.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.393032745.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.393032745.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.393032745.0000000000400000.00000040.80000000.00040000.00000000.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: **3324**, Parent PID: **5828**

General

Target ID:	3
Start time:	01:09:06
Start date:	30/11/2022
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: 00000003.00000000.369567476.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.369567476.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.369567476.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.369567476.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.347863799.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.347863799.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.347863799.000000000E3B5000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.347863799.000000000E3B5000.00000040.00000001.00040000.00000000.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: autochk.exe PID: **3624**, Parent PID: **3324**

General

Target ID:	4
Start time:	01:09:38
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0xbd0000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: netsh.exe PID: **5920**, Parent PID: **3324**

General

Target ID:	5
Start time:	01:09:44
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x1280000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.555011698.00000000007D0000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.561579336.0000000001100000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.561579336.0000000001100000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.561579336.0000000001100000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.561579336.0000000001100000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.559931003.00000000010D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.559931003.00000000010D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.559931003.00000000010D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.559931003.00000000010D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

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\febcldoukq.exe	cannot delete	1	7EC897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\-ODfqI49	object name not found	1	7EC897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\-ODfqI49	sharing violation	1	7EC897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\-ODfqI49	sharing violation	1	7EC897	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	7EC867	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