ID: 756109
Sample Name:
payment_copy2_receipt.exe
Cookbook: default.jbs
Time: 16:41:08
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

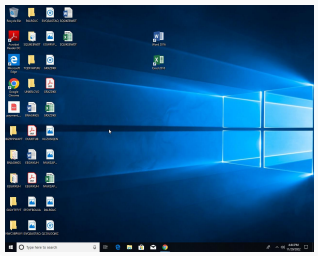
Windows Analysis Report

payment_copy2_receipt.exe

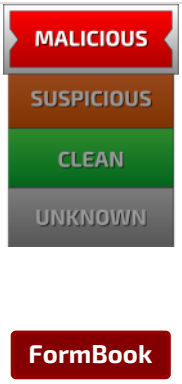
Overview

General Information

Sample Name:	payment_copy2_receipt.exe
Analysis ID:	756109
MD5:	9b8c61ded729ca..
SHA1:	37fc137e9aa09fc..
SHA256:	c1609447bd7a2e..
Tags:	exe Formbook
Infos:	



Detection



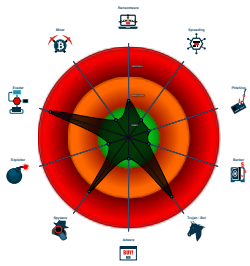
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Performs DNS queries to domains w…
- Found evasive API chain (may stop…

Classification



Process Tree

- **System is w10x64**
- payment_copy2_receipt.exe (PID: 6116 cmdline: C:\Users\user\Desktop\payment_copy2_receipt.exe MD5: 9B8C61DED729CA6C9D5F7FDED18EEF27)
  - fcvvthv.exe (PID: 6108 cmdline: "C:\Users\user~1\AppData\Local\Temp\fcvvthv.exe" C:\Users\user~1\AppData\Local\Temp\abggklv.q MD5: 353F7D8845E3DD77D50661A00EC7DF55)
    - conhost.exe (PID: 5180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - fcvvthv.exe (PID: 2828 cmdline: "C:\Users\user~1\AppData\Local\Temp\fcvvthv.exe" C:\Users\user~1\AppData\Local\Temp\abggklv.q MD5: 353F7D8845E3DD77D50661A00EC7DF55)
      - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - msdt.exe (PID: 5440 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.projectlis.online/veh0/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x100d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x8e07:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x86b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x8d07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x8e7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x78fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xee47:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xfe3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xb119:$sqlite3step: 68 34 1C 7B E1 • 0xbc91:$sqlite3step: 68 34 1C 7B E1 • 0xb15b:$sqlite3text: 68 38 2A 90 C5 • 0xbcd6:$sqlite3text: 68 38 2A 90 C5 • 0xb172:$sqlite3blob: 68 53 D8 7F 8C • 0xbcec:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.359853836.0000000000590000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.fcvvthv.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.fcvvthv.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6f48:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1fa07:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xb206:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1873e:$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.fcvvthv.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x1853c:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17fe8:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1863e:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x187b6:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xadd1:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17233:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1e77e:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1f771:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.fcvvthv.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1aa50:$sqlite3step: 68 34 1C 7B E1 • 0x1b5c8:$sqlite3step: 68 34 1C 7B E1 • 0x1aa92:$sqlite3text: 68 38 2A 90 C5 • 0x1b60d:$sqlite3text: 68 38 2A 90 C5 • 0x1aaa9:$sqlite3blob: 68 53 D8 7F 8C • 0x1b623:$sqlite3blob: 68 53 D8 7F 8C
3.2.fcvvthv.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

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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

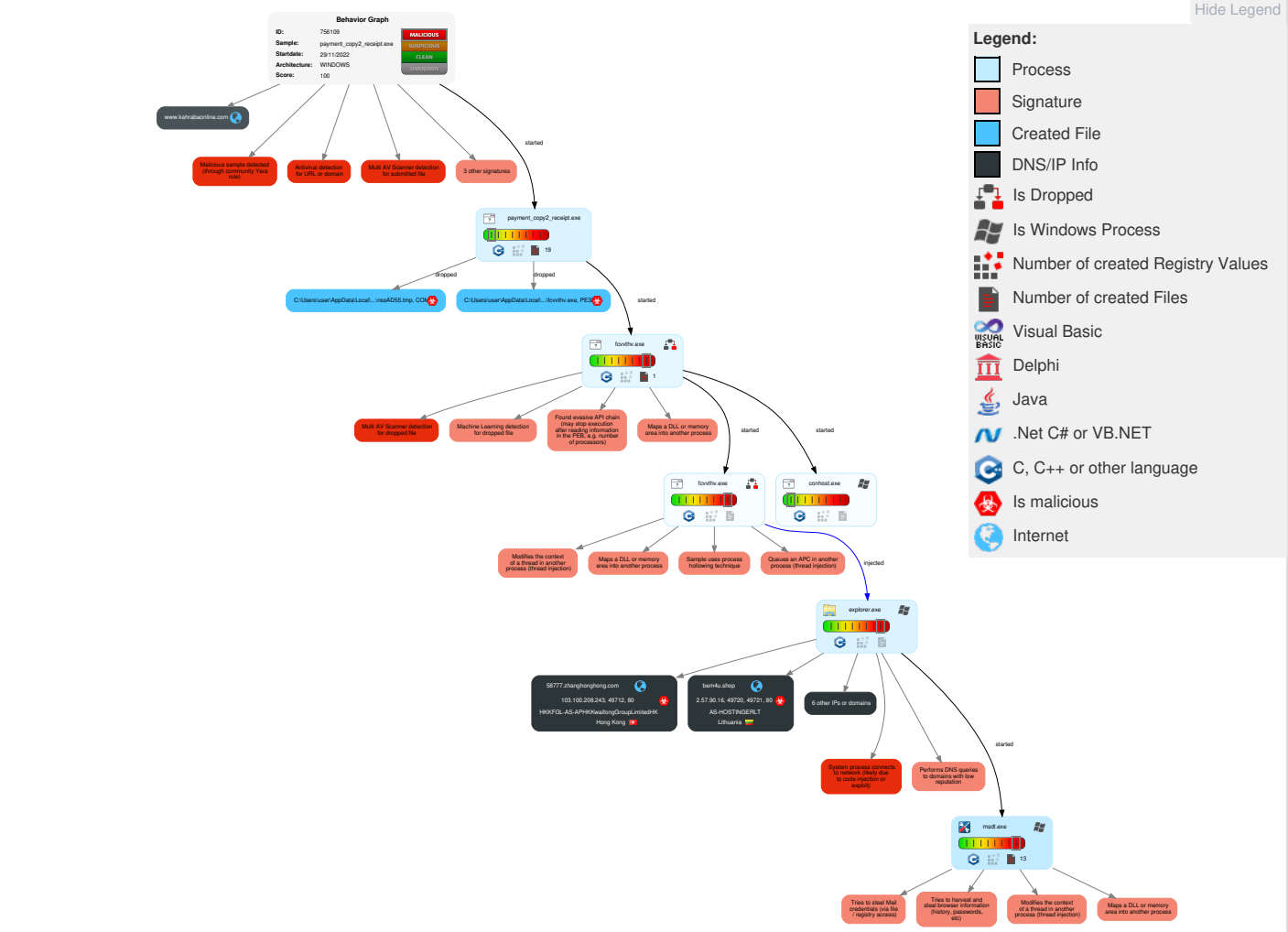
Yara detected FormBook

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	1 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

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

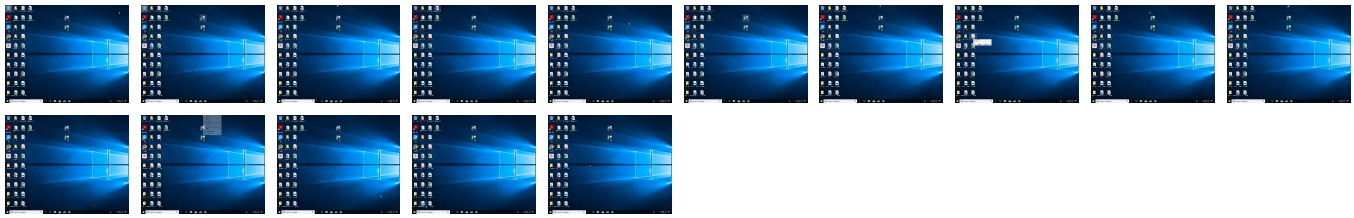
Behavior Graph



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
payment_copy2_receipt.exe	54%	ReversingLabs	Win32.Trojan.Injuke	
payment_copy2_receipt.exe	38%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\fcvvthv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\fcvvthv.exe	54%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\nssAD55.tmp	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.fcvvthv.exe.21d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.fcvvthv.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.payment_copy2_receipt.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
3.0.fcvvthv.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.payment_copy2_receipt.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
stephapproved.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.bem4u.shop/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=4D+PWXbgB4ogRjX6fs5PVj0HGmRsMlLoTFn3Q8gXNZCg8eDi41xcCT+RlNqelGXbdrjEsGoLW5hhUyw4icMG9EbpTlbOIKjETxFqhNsrxI+v	100%	Avira URL Cloud	malware	
http://www.030332.com/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=0RH+IT1kuvDJ9rkRmbuuDnrdLgu65XozQ/JOR96kX/EhF1f6QwJsxyvJPVJiAwnUlpNMH3LUUfaqGrsuBUI8TtociOaij3z8Rf/PV9bGuXJT	100%	Avira URL Cloud	malware	
http://www.vnsuda.lol/veh0/?V8Olq=H0phgvfvKBma6gvwGBFiiA3aGB6x1tx+qpMzsOKL6mX4XVya54sThvMqL7EFeUWxYIJWwwUJaARTNC9BUuxdalfssqJOBdyR5lth/WdqURqv&3fiPC=E4O8TXhX80iDs	100%	Avira URL Cloud	malware	
http://https://www.coolfashionshop.xyz/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=93LycRjWm4awEovVXWVYV	100%	Avira URL Cloud	malware	
http://www.stephapproved.com/veh0/?V8Olq=q2CkvjiufJAT9gG6R5hbib10Rbp6AiWeTKlSfCVYrUP+9/ZMp3UrZ4LyF/rVbhnSgdA59VnFYN1kGAwfQYzsaV6Pz6DbznSGjFMnhMTfrtcq&3fiPC=E4O8TXhX80iDs	100%	Avira URL Cloud	malware	
http://www.coolfashionshop.xyz/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=93LycRjWm4awEovVXWVYV+IJ3Jb7LKwjIdA7aRwoOX2ozYkISvzNjnqis/EaaxX4GW2e5S3JGCYnv5+dQS5WAoQqcporDra+l+tXDBzdj1sM	100%	Avira URL Cloud	malware	
http://www.bem4u.shop/veh0/	100%	Avira URL Cloud	malware	
http://www.vnsuda.lol/veh0/	100%	Avira URL Cloud	malware	
http://www.coolfashionshop.xyz/veh0/	100%	Avira URL Cloud	malware	
www.projectlis.online/veh0/	100%	Avira URL Cloud	malware	
http://www.stephapproved.com/veh0/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stephapproved.com	70.32.23.81	true	true	• 4%, Virustotal, Browse	unknown
58777.zhanghonghong.com	103.100.208.243	true	true		unknown
www.vnsuda.lol	75.2.115.196	true	true		unknown
www.coolfashionshop.xyz	34.110.163.134	true	false		unknown
bem4u.shop	2.57.90.16	true	true		unknown
www.kahrabaonline.com	160.121.219.144	true	false		unknown
www.bem4u.shop	unknown	unknown	true		unknown
www.030332.com	unknown	unknown	true		unknown
www.stephapproved.com	unknown	unknown	true		unknown

Copyright Joe Security LLC 2022

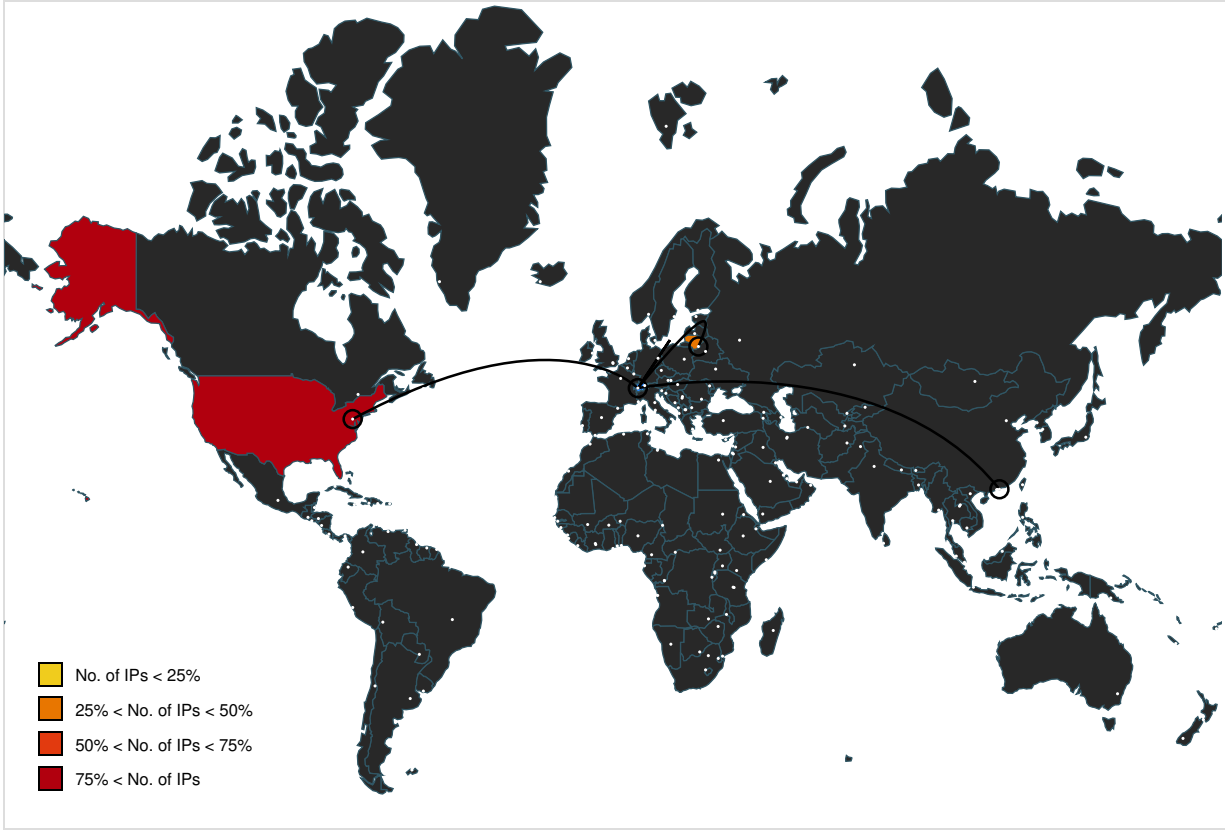
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.stephapproved.com/veh0/	true	• Avira URL Cloud: malware	unknown
http://www.stephapproved.com/veh0/?V8Olq=q2CkvjiufJAT9gG6R5hbib10Rbp6AiWeTKlSfCVYrUP+9/ZMp3UrZ4LyF/rVbhnSgdA59VnFYN1kGAwfQYzsaV6Pz6DbznSGjFMnhMTfrtcq&3fiPC=E4O8TXhX80iDs	true	• Avira URL Cloud: malware	unknown
www.projectlis.online/veh0/	true	• Avira URL Cloud: malware	low
http://www.bem4u.shop/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=4D+PWXbgB4ogRjX6fs5PVj0HGmRsMlLoTFn3Q8gXNZCg8eDi41xcCT+RlNqelGXbdrjEsGoLW5hhUyw4icMG9EbpTlbOlKjETxFqhNsrxl+v	true	• Avira URL Cloud: malware	unknown
http://www.vnsuda.lol/veh0/?V8Olq=H0phgvfvKBma6gvwGBFiiA3aGB6x1tx+qpMzsOKL6mX4XVya54sThvMqL7EFeUWxYlJWwwUJaARTNC9BUuxdalfssqJOBdyR5lth/WdqURqv&3fiPC=E4O8TXhX80iDs	true	• Avira URL Cloud: malware	unknown
http://www.vnsuda.lol/veh0/	true	• Avira URL Cloud: malware	unknown
http://www.030332.com/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=0RH+IT1kuvDJ9rkRmbuuDnrdLgu65XozQ/JOR96kX/EhF1f6QwJsxyvJPVJiAwnUlpNMH3LUUfaqGrsuBUl8TtociOaij3z8Rf/PV9bGuXJT	true	• Avira URL Cloud: malware	unknown
http://www.bem4u.shop/veh0/	true	• Avira URL Cloud: malware	unknown
http://www.coolfashionshop.xyz/veh0/	false	• Avira URL Cloud: malware	unknown
http://www.coolfashionshop.xyz/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=93LycRjWm4awEovVXWVYV+lJ3Jb7LKwjIdA7aRwoOX2ozYkISvzNjnqis/EaaxX4GW2e5S3JGCYnv5+dQS5WAoQqcporDra+l+tXDBzdj1sM	false	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp, n5335GITL.12.dr	false		high
http://https://www.coolfashionshop.xyz/veh0/?3fiPC=E4O8TXhX80iDs&V8Olq=93LycRjWm4awEovVXWVYV	msdt.exe, 0000000C.00000002.514187588.000000000553A000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	n5335GITL.12.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/fP	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp, n5335GITL.12.dr	false		high
http://https://www.ecosia.org/search?q=	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp, n5335GITL.12.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	n5335GITL.12.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp, n5335GITL.12.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	payment_copy2_receipt.exe	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp, n5335GITL.12.dr	false		high
http://https://ac.ecosia.org/autocomplete?q=	n5335GITL.12.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	msdt.exe, 0000000C.00000002.511513709.000000002D6E000.00000004.00000020.00020000.00000000.sdmp, n5335GITL.12.dr	false		high
http://nsis.sf.net/NSIS_Error	payment_copy2_receipt.exe	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	n5335GITL.12.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
75.2.115.196	www.vnsuda.lol	United States		16509	AMAZON-02US	true
70.32.23.81	stephapproved.com	United States		55293	A2HOSTINGUS	true
34.110.163.134	www.coolfashionshop.xyz	United States		15169	GOOGLEUS	false
103.100.208.243	58777.zhanghonghong.com	Hong Kong		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	true
2.57.90.16	bem4u.shop	Lithuania		47583	AS-HOSTINGERLT	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756109
Start date and time:	2022-11-29 16:41:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment_copy2_receipt.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:	14
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

Copyright Joe Security LLC 2022

Classification:	mal100.troj.spyw.evad.winEXE@7/5@6/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 77.8% (good quality ratio 72%) • Quality average: 72.8% • Quality standard deviation: 31.2%
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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com
- 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\abggklv.q

Process:	C:\Users\user\Desktop\payment_copy2_receipt.exe
File Type:	data
Category:	dropped
Size (bytes):	5602
Entropy (8bit):	6.24505051626392
Encrypted:	false
SSDEEP:	96:j7hz+pcihT7oMz55kZ1OquI8WDlzTuais2fmOPJ:rcTkMdqiquIRDlzy22fmOJ
MD5:	6D8E18D69240FFEA42588DAB287B1101

SHA1:	CEFD52A04F08EF59709DB3DDBF7F9409D0C795BE
SHA-256:	2CE4DD4327EB70E03E7D48D57BC1C46EC922B73FB7E9501C1F7A2580F19F7121
SHA-512:	0BE89301E5319E37B9C6641BBF3689FB91BB79B7CCA37034C4533FD87A4110F67D44D3130D0FDED9448251F9C6344EB1DED6A540A2F9152BD85D3E59B5F10AE A
Malicious:	false
Reputation:	low
Preview:	Y8.....jW%.....,+.....K.....zh....R.@...K...R....:..-X..%..,....<7..+.....zQq...Z....c.4.X...Y..-X..%..!.....j....."z.....R.a..^! ...K.oR7.^.W.R.W%.....,.B.R.m.%....l+. .b....?.....C..E..-X..%..!!',+....L.....[."2.*~....&.s..j...%^..J....R.....["z`.....h.%^.....{.R../.X....Jc.....[..%..!!',+.....j....."z.....+.-J.....B...B. ..^.+...R./...?[...c...c.3.X ..G..S.R2c.J.X.....S .c.J..2.c....D.Wc.....3...-^.[.....+.-^.%J.....R...R.../.X..%..,....<7..+.b...zQq.....Z....c.4.X...{..-X..%.....[.....n\.f.\.u=\.|.\.{.\.z.....J. .*.... .*...$.*... .*... .*... .*... .*... .*... i*... d*... .*...R .*...X .*...F.R...\z.M.....zet.....7.|...z.t.....zEM.....zuM.....J{...z.M.....`....zUM.....$mR...z.M.....z.M.....R..R.\..Bc.R.Qr.\..B3.R.r\..B=.R. .R.\..B..R.Qr.\..B....n..r.....r...r..r..&..r.. ..KA..nc..b..rc...B.Z..r...B...R..R.c...f.....c...B.Q...R.Qr.c...f...Qq.c...B.Q.

C:\Users\user\AppData\Local\Temp\assakziryna.z

Process:	C:\Users\user\Desktop\payment_copy2_receipt.exe
File Type:	data
Category:	dropped
Size (bytes):	189440
Entropy (8bit):	**7.998637942598542**
Encrypted:	**true**
SSDEEP:	3072:quO0aqJigCEAvaCz86Qx8s0XgLjOZ7OZyyZJ8/+UGlWBu3/2kq13Ok0em/D:qut+EAvpzIn0XgLjO5OZyAJ8/+UG4BQP
MD5:	F4A6BF70E5353725EDBD930F6311A876
SHA1:	D329889E536CEBF7E71E2BD7CB9B4F078E115E03
SHA-256:	A640DF81745A2E0EA64055877F85F6B6B5E00512018DA51AF51B85AB5FB8CE0F
SHA-512:	BC962A3C95BDC9E9C30F73C7D53463F07C16B62CF7044CEB5D06A6FA5CE96A44BFB38B02113DE92EB42D969499EF50248288E351130966F3FFD5389E31940DE E
Malicious:	false
Reputation:	low
Preview:	l.....1..._B...w..PH.....#.SL.....d%w..*Y....a.t:...Q(.....K.M...?s....F....Cb..?.1.a...W:.S.....%...}..6:...L#z.q.F.....JV.....x.....>.r=....z..(3...D.h.2.o^...N...{...?J...a...-1..../.. (.....RM..hc.]2 .3.*.}..L.....c...y...s.....N.N]d..Bw....^.t..g#..L...../.d.w..*Y.C..a.t:...Q(.F...a...dLa.n.K[b....>....Z.`..."...h...|.q.....ND,.Z...L#z+V=Pzu.{....{P..r.....?.....C.....- .W.2.o^.....$.....w.b.-..d.C..../..(.....Oe.p.hc.]2 ....*.U..L.....s.....N.N]d...w.m..^.t....#.SL.....d%w..*Y....a.t:...Q(.F...a...dLa.n.K[b....>....Z.`..."...h...|.q.....ND,.Z...L#z+V= Pzu.{....{P..r.....?.....C.....-.W.2.o^...N...{....#.b.-..4.C..../..(.....e...hc.]2 ....*.U..L.....s.....N.N]d...w.m..^.t....#.SL.....d%w..*Y....a.t:...Q(.F...a...dLa.n.K[b....>....Z.`..."... h...|.q.....ND,.Z...L#z+V=Pzu.{....{P..r.....?.....C.....-.W.2.o^...N...{....#.b.-..4.C..../..(.....e...hc.]2 .

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

Process:	C:\Users\user\Desktop\payment_copy2_receipt.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	125440
Entropy (8bit):	6.273030876874131
Encrypted:	false
SSDEEP:	3072:Ug2QMgHRT3WstYkFm/W3M0omix1RSlwTyv8/RMAIV:UEHRT3jtQ2cmGRSqT9l
MD5:	353F7D8845E3DD77D50661A00EC7DF55
SHA1:	F9AA7D4B6EC63AD64BA14E8FC9C4068204590EBC
SHA-256:	38FAD353228A143830ED3057A14DFD9A0853494BE8CD7ED62CF2676F963A0963
SHA-512:	AD8CACE8BC0A3889FFD76CCCC0EF823DC316FA4DB37F6A7A94278C3FACA26A547B5278B3DE615A23123DC6B0E2D61FDBFEA0BE5D48ED297001B080A813BE 5233
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....$.....:..P.....k...v..k.....k...m.....o.....b.....n..k...l.....~...T.~.....~. .Rich.....PE..L....v.c.....f.....@.....@.....t.....0.....@.....0..... .....text...'e.....f..... ..`.rdata...j.....l...j.....@..@.data...(+.....@....gfids..... .....@..@.rsrc.....0.....@..@..... ....

C:\Users\user\AppData\Local\Temp\n5335GITL

Process:	C:\Windows\SysWOW64\msdt.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:	modified
Size (bytes):	94208
Entropy (8bit):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944

MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\nssAD55.tmp

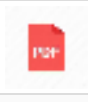
Process:	C:\Users\user\Desktop\payment_copy2_receipt.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	328874
Entropy (8bit):	7.530300700886958
Encrypted:	false
SSDEEP:	6144:jFut+EAvpzIn0XgLjO5OZyAJ8/+UG4BQvsr0em//5EHRT3jtQ2cmGRSqT9l:put+ll/Li5iJtd4WvW0eIR+RbG2cmQ
MD5:	18D5F36A346E0AEEDCB501EF671823D3
SHA1:	56E354ECEF94D44EF1B827B731B7AFCDAF9F2E11
SHA-256:	9F98ECEC18045E1B2A7C0CB27C0AF56467ED49166BD9E3E7CCD3E3C6E1FE4C61
SHA-512:	1059B83FBF865596D437C1F662A597D17F0DA2081D7E6F2ED501B33C77EA8F8C4E94B95BF914CAE99B99D3A8DD466920EB3C82CE58FDA6BB35B552F5DCC533E4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	. .....,.....e..... ....J.....j.....h....."..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.542091394809889
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:	payment_copy2_receipt.exe
File size:	548510
MD5:	9b8c61ded729ca6c9d5f7fded18eef27
SHA1:	37fc137e9aa09fc01820cd90c851ca3aee6be72a
SHA256:	c1609447bd7a2ee528d1f2145ebc3ad9a53efee61111824d22f935e497bac31f
SHA512:	d2696cf0e8b169763a1ba52211edbbc729f4f3a2aee8b6c029138d0fa180000b1f1781e777edb7328520c057c522371a698279e5ad178fda5b961d127bca27f5
SSDEEP:	6144:lBnlWGbqCEADGaF1B1XBx23XB0RQ4MXC+l1O45IDkQBha03Yljo4:wCEQGKy3R0qPHO45FQBhaM
TLSH:	9AC4FCF1C795E5A8F886AE3D41335CBB94BB997D6DA05DDE410CB4B2AF3278210A05C3
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:	214e9696969616a0

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 00007FCDF4BDD063h
push ebx
call 00007FCDF4BDFE51h
cmp eax, ebx
je 00007FCDF4BDD059h
push 00000C00h
call eax
push 004091E0h
call 00007FCDF4BDFDD2h
push 004091D8h
call 00007FCDF4BDFDC8h
push 004091CCh
call 00007FCDF4BDFDBEh
push 0000000Dh
call 00007FCDF4BDFE21h
push 0000000Bh
call 00007FCDF4BDFE1Ah
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

Instruction
push ebx
push 0041F538h
call dword ptr [00407160h]
push 004091C0h
push 00423780h
call 00007FCDF4BDFA51h
call dword ptr [004070B0h]
mov ebp, 0042A000h
push eax
push ebp
call 00007FCDF4BDFA3Fh
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	0x42720	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4a	0x5e00	False	0.659906914893617	data	6.410763775060762	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x115e	0x1200	False	0.4466145833333333	data	5.142548180775325	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b078	0x600	False	0.455078125	data	4.2252195571372315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2d000	0x42720	0x42800	False	0.17087640977443608	data	3.7167114574794757	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d190	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 262144	English	United States
RT_DIALOG	0x6f1b8	0x100	data	English	United States
RT_DIALOG	0x6f2b8	0x11c	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x6f3d8	0x60	data	English	United States
RT_GROUP_ICON	0x6f438	0x14	data	English	United States
RT_MANIFEST	0x6f450	0x2cc	XML 1.0 document, ASCII text, with very long lines (716), with no line terminators	English	United States

Imports

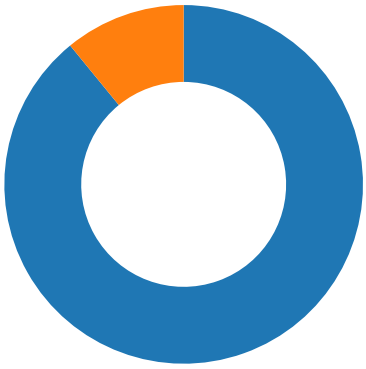
DLL	Import
KERNEL32.dll	SetFileAttributesA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CompareFileTime, SearchPathA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, CreateDirectoryA, lstrcmpiA, 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

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:43:29.603773117 CET	49712	80	192.168.2.7	103.100.208.243
Nov 29, 2022 16:43:29.993545055 CET	80	49712	103.100.208.243	192.168.2.7
Nov 29, 2022 16:43:29.993638039 CET	49712	80	192.168.2.7	103.100.208.243
Nov 29, 2022 16:43:29.993803024 CET	49712	80	192.168.2.7	103.100.208.243
Nov 29, 2022 16:43:30.383208036 CET	80	49712	103.100.208.243	192.168.2.7
Nov 29, 2022 16:43:30.383261919 CET	80	49712	103.100.208.243	192.168.2.7
Nov 29, 2022 16:43:30.383296967 CET	80	49712	103.100.208.243	192.168.2.7
Nov 29, 2022 16:43:30.383447886 CET	49712	80	192.168.2.7	103.100.208.243
Nov 29, 2022 16:43:30.383611917 CET	49712	80	192.168.2.7	103.100.208.243
Nov 29, 2022 16:43:30.772913933 CET	80	49712	103.100.208.243	192.168.2.7
Nov 29, 2022 16:43:40.625875950 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:40.645251036 CET	80	49713	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:40.645396948 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:40.645670891 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:40.664767981 CET	80	49713	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:40.692596912 CET	80	49713	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:40.692632914 CET	80	49713	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:40.692769051 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:40.693511009 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:40.706896067 CET	80	49713	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:40.706959963 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:41.658564091 CET	49713	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.678809881 CET	49715	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.697918892 CET	80	49715	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:42.698271990 CET	49715	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.698271990 CET	49715	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.717390060 CET	80	49715	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:42.837244987 CET	80	49715	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:42.837280989 CET	80	49715	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:42.837524891 CET	49715	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.838152885 CET	49715	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.852073908 CET	80	49715	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:42.852161884 CET	49715	80	192.168.2.7	75.2.115.196
Nov 29, 2022 16:43:42.857156992 CET	80	49715	75.2.115.196	192.168.2.7
Nov 29, 2022 16:43:49.040884018 CET	49716	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:49.057763100 CET	80	49716	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:49.057857990 CET	49716	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:49.058307886 CET	49716	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:49.075227022 CET	80	49716	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:49.175266027 CET	80	49716	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:49.175347090 CET	80	49716	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:49.175451994 CET	49716	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:50.065264940 CET	49716	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:51.084142923 CET	49717	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:51.103156090 CET	80	49717	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:51.103333950 CET	49717	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:51.103663921 CET	49717	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:51.123337984 CET	80	49717	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:51.221019030 CET	80	49717	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:51.221077919 CET	80	49717	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:51.221364975 CET	49717	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:51.221716881 CET	49717	80	192.168.2.7	34.110.163.134
Nov 29, 2022 16:43:51.238799095 CET	80	49717	34.110.163.134	192.168.2.7
Nov 29, 2022 16:43:56.275064945 CET	49718	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:56.400295973 CET	80	49718	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:56.402024031 CET	49718	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:56.406605005 CET	49718	80	192.168.2.7	70.32.23.81

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:43:56.531891108 CET	80	49718	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:56.536995888 CET	80	49718	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:56.537045002 CET	80	49718	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:56.537080050 CET	80	49718	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:56.537187099 CET	49718	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:56.537240982 CET	49718	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:57.409480095 CET	49718	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:58.425900936 CET	49719	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:58.551639080 CET	80	49719	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:58.551841974 CET	49719	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:58.553603888 CET	49719	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:58.678706884 CET	80	49719	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:58.679014921 CET	80	49719	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:58.679047108 CET	80	49719	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:58.679070950 CET	80	49719	70.32.23.81	192.168.2.7
Nov 29, 2022 16:43:58.679266930 CET	49719	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:58.679702044 CET	49719	80	192.168.2.7	70.32.23.81
Nov 29, 2022 16:43:58.804666042 CET	80	49719	70.32.23.81	192.168.2.7
Nov 29, 2022 16:44:03.759083986 CET	49720	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:03.791296959 CET	80	49720	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:03.791491985 CET	49720	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:03.791666985 CET	49720	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:03.823739052 CET	80	49720	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:03.823765039 CET	80	49720	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:03.823781013 CET	80	49720	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:03.823925972 CET	49720	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:04.800724030 CET	49720	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:05.817096949 CET	49721	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:05.849591970 CET	80	49721	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:05.849843979 CET	49721	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:05.850018024 CET	49721	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:05.882168055 CET	80	49721	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:05.882213116 CET	80	49721	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:05.882236958 CET	80	49721	2.57.90.16	192.168.2.7
Nov 29, 2022 16:44:05.882447958 CET	49721	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:05.882611036 CET	49721	80	192.168.2.7	2.57.90.16
Nov 29, 2022 16:44:05.914745092 CET	80	49721	2.57.90.16	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:43:29.273768902 CET	63926	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:43:29.596674919 CET	53	63926	8.8.8.8	192.168.2.7
Nov 29, 2022 16:43:40.413796902 CET	53336	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:43:40.623732090 CET	53	53336	8.8.8.8	192.168.2.7
Nov 29, 2022 16:43:48.826666117 CET	50513	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:43:49.039021015 CET	53	50513	8.8.8.8	192.168.2.7
Nov 29, 2022 16:43:56.242922068 CET	60765	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:43:56.273133039 CET	53	60765	8.8.8.8	192.168.2.7
Nov 29, 2022 16:44:03.725838900 CET	58283	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:44:03.757194996 CET	53	58283	8.8.8.8	192.168.2.7
Nov 29, 2022 16:44:10.895929098 CET	49516	53	192.168.2.7	8.8.8.8
Nov 29, 2022 16:44:11.068994045 CET	53	49516	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:43:29.273768902 CET	192.168.2.7	8.8.8.8	0x36cc	Standard query (0)	www.030332 .com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:43:40.413796902 CET	192.168.2.7	8.8.8.8	0xee3c	Standard query (0)	www.vnsuda.lol	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:48.826666117 CET	192.168.2.7	8.8.8.8	0x818	Standard query (0)	www.coolfashionshop.xyz	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:56.242922068 CET	192.168.2.7	8.8.8.8	0xf885	Standard query (0)	www.stephapproved.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:03.725838900 CET	192.168.2.7	8.8.8.8	0xf051	Standard query (0)	www.bem4u.shop	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:10.895929098 CET	192.168.2.7	8.8.8.8	0x9572	Standard query (0)	www.kahrabaonline.com	A (IP address)	IN (0x0001)	false

DNS Answers

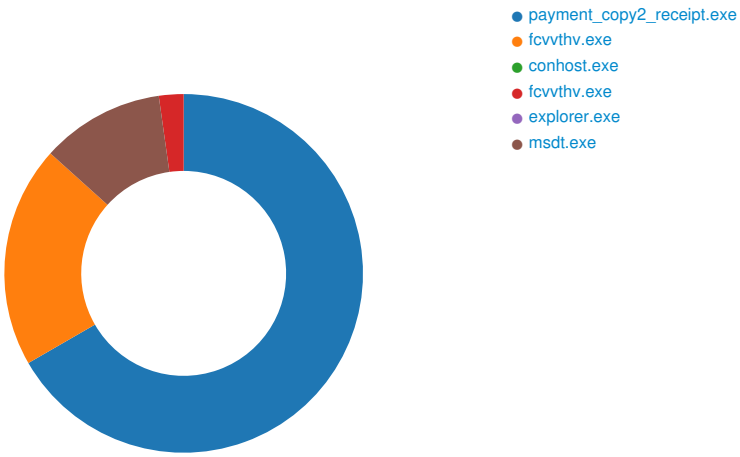
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:43:29.596674919 CET	8.8.8.8	192.168.2.7	0x36cc	No error (0)	www.030332.com	58777.zhanghonghong.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:43:29.596674919 CET	8.8.8.8	192.168.2.7	0x36cc	No error (0)	58777.zhanghonghong.com		103.100.208.243	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:40.623732090 CET	8.8.8.8	192.168.2.7	0xee3c	No error (0)	www.vnsuda.lol		75.2.115.196	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:49.039021015 CET	8.8.8.8	192.168.2.7	0x818	No error (0)	www.coolfashionshop.xyz		34.110.163.134	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:56.273133039 CET	8.8.8.8	192.168.2.7	0xf885	No error (0)	www.stephapproved.com	stephapproved.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:43:56.273133039 CET	8.8.8.8	192.168.2.7	0xf885	No error (0)	stephapproved.com		70.32.23.81	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:03.757194996 CET	8.8.8.8	192.168.2.7	0xf051	No error (0)	www.bem4u.shop	bem4u.shop		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:44:03.757194996 CET	8.8.8.8	192.168.2.7	0xf051	No error (0)	bem4u.shop		2.57.90.16	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:11.068994045 CET	8.8.8.8	192.168.2.7	0x9572	No error (0)	www.kahrabaonline.com		160.121.219.144	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.030332.com
- www.vnsuda.lol
- www.coolfashionshop.xyz
- www.stephapproved.com
- www.bem4u.shop

Statistics

Behavior



System Behavior

Analysis Process: payment_copy2_receipt.exe PID: 6116, Parent PID: 3320

General

Target ID:	0
Start time:	16:42:03
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\payment_copy2_receipt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\payment_copy2_receipt.exe
Imagebase:	0x400000
File size:	548510 bytes
MD5 hash:	9B8C61DED729CA6C9D5F7FDED18EEF27
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: fcvvthv.exe PID: 6108, Parent PID: 6116

General

Target ID:	1
Start time:	16:42:04
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\fcvvthv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\fcvvthv.exe" C:\Users\user~1\AppData\Local\Temp\abggklv.q
Imagebase:	0x400000
File size:	125440 bytes
MD5 hash:	353F7D8845E3DD77D50661A00EC7DF55
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

Copyright Joe Security LLC 2022

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\abggklv.q	unknown	5602	success or wait	1	409809	ReadFile
C:\Users\user\AppData\Local\Temp\assakziryna.z	unknown	189440	success or wait	1	B804C9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B81484	ReadFile

Analysis Process: conhost.exe PID: **5180**, Parent PID: **6108**

General

Target ID:	2
Start time:	16:42:04
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: fcvvthv.exe PID: **2828**, Parent PID: **6108**

General

Target ID:	3
Start time:	16:42:05
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Local\Temp\fcvvthv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\fcvvthv.exe" C:\Users\user~1\AppData\Local\Temp\abggklv.q
Imagebase:	0x400000
File size:	125440 bytes
MD5 hash:	353F7D8845E3DD77D50661A00EC7DF55
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: 00000003.00000002.359853836.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.359853836.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.359853836.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.359853836.0000000000590000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.359518413.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.359518413.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.359518413.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.359518413.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.360011022.00000000006F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.360011022.00000000006F0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.360011022.00000000006F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.360011022.00000000006F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: **3320**, Parent PID: **2828**

General

Target ID:	4
Start time:	16:42:12
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff75ed40000
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: 00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.325650949.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.346266084.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.346266084.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.346266084.0000000010833000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.346266084.0000000010833000.00000040.00000001.00040000.00000000.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: msdt.exe PID: **5440**, Parent PID: **3320**

General

Target ID:	12
Start time:	16:42:52
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xaf0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 0000000C.00000002.511854838.00000000046E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.511854838.00000000046E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.511854838.00000000046E0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.511854838.00000000046E0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.508172030.0000000000760000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.508172030.0000000000760000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.508172030.0000000000760000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.508172030.0000000000760000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.511779339.00000000046B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.511779339.00000000046B0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.511779339.00000000046B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.511779339.00000000046B0000.00000040.10000000.00040000.00000000.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~1\AppData\Local\Temp\fcvvthv.exe	cannot delete	1	77C8F7	NtDeleteFile
C:\Users\user~1\AppData\Local\Temp\n5335GITL	object name not found	1	77C8F7	NtDeleteFile
C:\Users\user~1\AppData\Local\Temp\n5335GITL	sharing violation	1	77C8F7	NtDeleteFile
C:\Users\user~1\AppData\Local\Temp\n5335GITL	sharing violation	1	77C8F7	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	77C8C7	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

Copyright Joe Security LLC 2022