ID: 756334
Sample Name: PI & PACKING LIST.exe
Cookbook: default.jbs
Time: 01:54:10
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

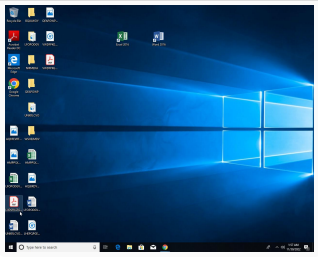
Windows Analysis Report

PI & PACKING LIST.exe

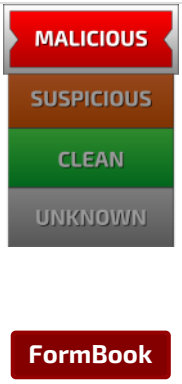
Overview

General Information

Sample Name:	PI & PACKING LIST.exe
Analysis ID:	756334
MD5:	36fbb21511e87e..
SHA1:	eda2fa3fe4b62fe..
SHA256:	937c7c476bb363..
Tags:	exe formbook
Infos:	



Detection



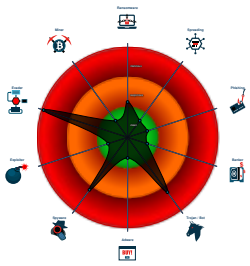
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- PI & PACKING LIST.exe (PID: 6140 cmdline: C:\Users\user\Desktop\PI & PACKING LIST.exe MD5: 36FBB21511E87E8DDDC8916CC2DC9367)
  - PI & PACKING LIST.exe (PID: 5216 cmdline: C:\Users\user\Desktop\PI & PACKING LIST.exe MD5: 36FBB21511E87E8DDDC8916CC2DC9367)
  - PI & PACKING LIST.exe (PID: 2352 cmdline: C:\Users\user\Desktop\PI & PACKING LIST.exe MD5: 36FBB21511E87E8DDDC8916CC2DC9367)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 5228 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.singglostudio.com/m5oe/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x100a0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x8df7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C 3 8B 17 03 55 0C 6A 01 83

Source	Rule	Description	Author	Strings
00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8bf5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x86a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x8cf7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x8e6f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x78ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xee17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xfe0a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xb119:$sqlite3step: 68 34 1C 7B E1 • 0xbc91:$sqlite3step: 68 34 1C 7B E1 • 0xb15b:$sqlite3text: 68 38 2A 90 C5 • 0xbcd6:$sqlite3text: 68 38 2A 90 C5 • 0xb172:$sqlite3blob: 68 53 D8 7F 8C • 0xbcec:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000002.512821683.0000000003510000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 24 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

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

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

Remote Access Functionality

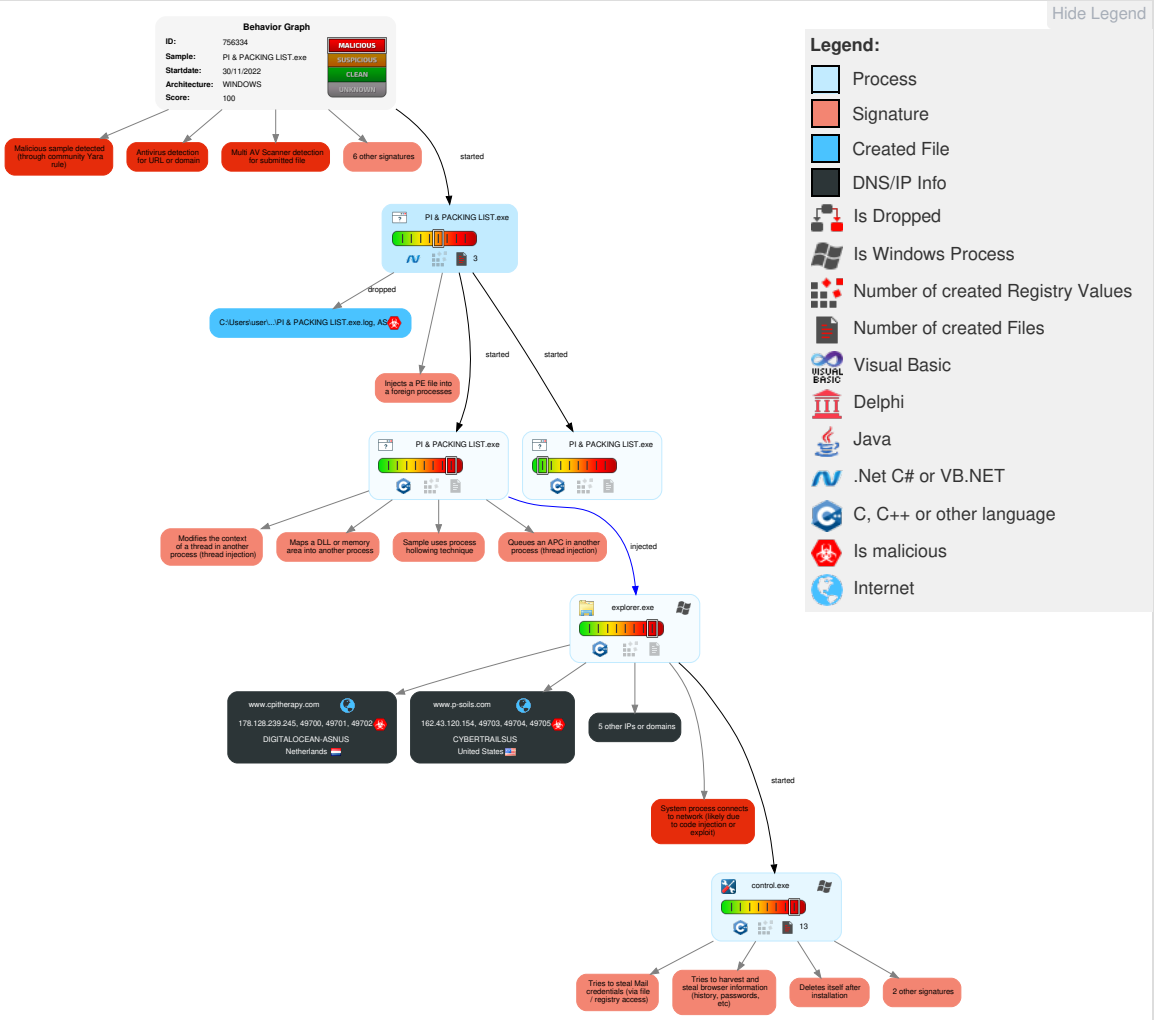
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

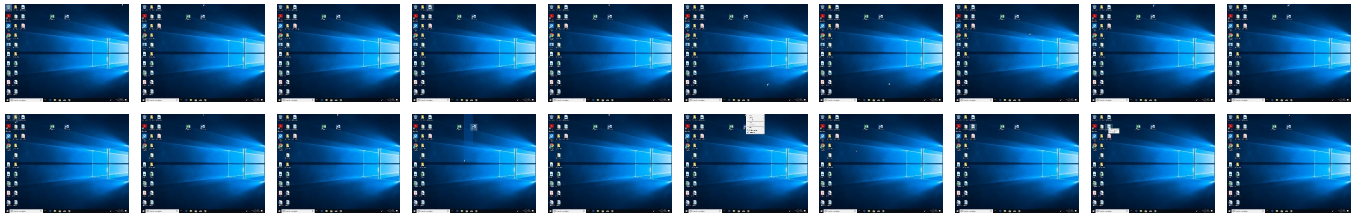
Behavior Graph

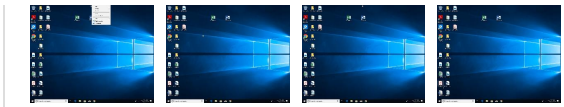


Screenshots

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
PI & PACKING LIST.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.FormBook	
PI & PACKING LIST.exe	57%	Virustotal		Browse
PI & PACKING LIST.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.PI & PACKING LIST.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.nu2uresale.store	1%	Virustotal		Browse
www.p-soils.com	3%	Virustotal		Browse
www.cpitherapy.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.fontbureau.como	0%	URL Reputation	safe	
http://https://www.bengalindex.com/m5oe/?l48xl=yrQlZi/yeQekXtziTibn9LfL5FHN0Y47PbY	0%	Avira URL Cloud	safe	
http://www.cpitherapy.com/m5oe/?l48xl=Kdt0ttn6jBvm5dVCPGsq4sF6gZwVhJORDr+IW0q2lJvFs7kzNd/E4xjIZ8hkWN2nAiXaUCaRapMtLMo79OBUYLpofMwqWu/G3g==&y8dt=cR-TJP3pr48	100%	Avira URL Cloud	malware	
http://www.zkjk888.com/m5oe/?l48xl=lXL2hA4gPGXGkrsXCHLs63wEyc6+ZxTcosJkE7OlAbbgzBCGQ1RLZhLXXwLUr0PxIclnwkI7OF+QM6Klss4VWWvRg6rabD2uNg==&y8dt=cR-TJP3pr48	100%	Avira URL Cloud	malware	
http://www.bengalindex.com/m5oe/	100%	Avira URL Cloud	malware	
http://www.nu2uresale.store/m5oe/?l48xl=U9+cid+ik5YJF3jF27GFdJRqVXeG7FP+UvbSj6ZytGipCLvwOYSuUs/u1hqVfurTuH6/pVSyY1dCVh8DyPcg4wzd/AwTcksoYQ==&y8dt=cR-TJP3pr48	100%	Avira URL Cloud	malware	
http://www.nu2uresale.store/m5oe/	100%	Avira URL Cloud	malware	
http://www.p-soils.com/m5oe/?l48xl=OgbUJyD2Cs0iavfQBCvIOQvZdrfaRUMlkbnSDVoQDO79KZkwY+JyOZ2XW8xl2hee24/cs1yqqL6PnYlAwwwxD54r6/lzPRoMsg==&y8dt=cR-TJP3pr48	100%	Avira URL Cloud	malware	
http://www.bengalindex.com/m5oe/?l48xl=yrQlZi/yeQekXtziTibn9LfL5FHN0Y47PbY+gegrHfqcLEwJAZ2lhKdA1OTtZbcFcNKVJgIODn1wmw2XGX+PWpMZIoldVyV5wA==&y8dt=cR-TJP3pr48	100%	Avira URL Cloud	malware	
http://www.p-soils.com/m5oe/	100%	Avira URL Cloud	malware	
http://35.78.89.117	0%	Avira URL Cloud	safe	
http://www.cpitherapy.com/m5oe/	100%	Avira URL Cloud	malware	
http://amh.sh/	0%	Avira URL Cloud	safe	
www.singglostudio.com/m5oe/	0%	Avira URL Cloud	safe	
http://amh.sh	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nu2uresale.store	209.99.64.33	true	true	• 1%, Virustotal, Browse	unknown
www.p-soils.com	162.43.120.154	true	true	• 3%, Virustotal, Browse	unknown
www.zkjk888.com	35.78.89.117	true	true		unknown
www.cpitherapy.com	178.128.239.245	true	true	• 3%, Virustotal, Browse	unknown
ghs.googlehosted.com	142.250.203.115	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bengalindex.com	unknown	unknown	true		unknown
www.gebouwpas.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.p-soils.com/m5oe/	true	• Avira URL Cloud: malware	unknown
http://www.bengalindex.com/m5oe/	false	• Avira URL Cloud: malware	unknown
http://www.cpitherapy.com/m5oe/?l48xl=Kdt0ttn6jBvm5dVCPGsq4sF6gZwVhJORDr+IW0q2lJvFs7kzNd/E4xjlZ8hkWN2nAiXaUCaRapMtLMo79OBUYLpofMwqWu/G3g==&y8dt=cR-TJP3pr48	true	• Avira URL Cloud: malware	unknown
http://www.zkjk888.com/m5oe/?l48xl=lXL2hA4gPGXGkrsXCHLs63wEyc6+ZxTcosJkE7OlAbbgzBCGQ1RLZhLXXwLUr0PxIclnwkI7OF+QM6Klss4VWWvRg6rabD2uNg==&y8dt=cR-TJP3pr48	true	• Avira URL Cloud: malware	unknown
www.singglostudio.com/m5oe/	true	• Avira URL Cloud: safe	low
http://www.nu2uresale.store/m5oe/	true	• Avira URL Cloud: malware	unknown
http://www.nu2uresale.store/m5oe/?l48xl=U9+cid+ik5YJF3jF27GFdJRqVXeG7FP+UvbSj6ZytGipCLvwOYSuUs/u1hqVfurTuH6/pVSyY1dCVh8DyPcg4wzd/AwTcksoYQ==&y8dt=cR-TJP3pr48	true	• Avira URL Cloud: malware	unknown
http://www.cpitherapy.com/m5oe/	true	• Avira URL Cloud: malware	unknown
http://www.p-soils.com/m5oe/?l48xl=OgbUJyD2Cs0iavfQBCvIOQvZdrfaRUMlkbnSDVoQDO79KZkwY+JyOZ2XW8xl2hee24/cs1yqqL6PnYlAwwwxD54r6/IzPRoMsg==&y8dt=cR-TJP3pr48	true	• Avira URL Cloud: malware	unknown
http://www.bengalindex.com/m5oe/?l48xl=yrQlZi/yeQekXtziTibn9LfL5FHN0Y47PbY+gegrHfqcLEwJAZ2lhKdA1OTtZbcFcNKVJgIODn1wmw2XGX+PWpMZIoIdVyV5wA==&y8dt=cR-TJP3pr48	false	• Avira URL Cloud: malware	unknown

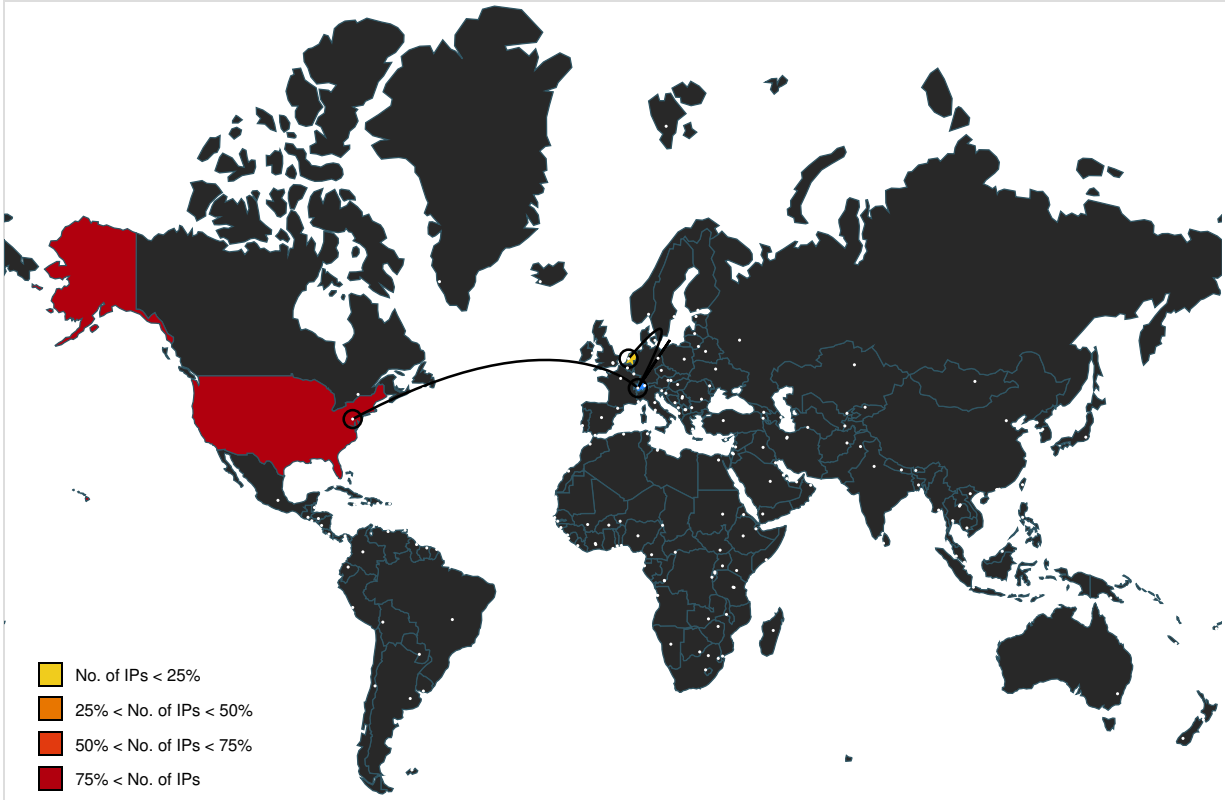
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	control.exe, 0000000D.00000003.438741340.000000000118C000.00000004.00000020.00020000.00000000.sdmp, 71M40-2OQ.13.dr	false		high
http://www.fontbureau.com/designersG	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	71M40-2OQ.13.dr	false		high
http://www.fontbureau.com/designers/?	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	control.exe, 0000000D.00000003.438741340.000000000118C000.00000004.00000020.00020000.00000000.sdmp, 71M40-2OQ.13.dr	false		high
http://www.tiro.com	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://amh.sh	control.exe, 0000000D.00000002.517236136.0000000005748000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.bengalindex.com/m5oe/?l48xl=yrQlZi/yeQekXtziTibn9LfL5FHN0Y47PbY	control.exe, 0000000D.00000002.517422506.0000000005BFE000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.29229480.000000000F270000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.323770993.000000000F270000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PI & PACKING LIST.exe, 00000000.00000002.261208049.0000000000B37000.00000004.00000020.00020000.00000000.sdmp, PI & PACKING LIST.exe, 00000000.00000002.277482683.000000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	control.exe, 0000000D.00000003.438741340.000000000118C000.00000004.00000020.00020000.00000000.sdmp, 71M40-2OQ.13.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	71M40-2OQ.13.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	control.exe, 0000000D.00000003.438741340.000000000118C000.00000004.00000020.00020000.00000000.sdmp, 71M40-2OQ.13.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	control.exe, 0000000D.00000003.438741340.000000000118C000.00000004.00000020.00020000.00000000.sdmp, 71M40-2OQ.13.dr	false		high
http://www.carterandcone.coml	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	71M40-2OQ.13.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	control.exe, 0000000D.00000003.438741340.000000000118C000.00000004.00000020.00020000.00000000.sdmp, 71M40-2OQ.13.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://amh.sh/	control.exe, 0000000D.00000002.517236136.0000000005748000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.como	PI & PACKING LIST.exe, 00000000.00000002.261208049.0000000000B37000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PI & PACKING LIST.exe, 00000000.00000002.277482683.00000000065C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	71M40-2OQ.13.dr	false		high
http://35.78.89.117	control.exe, 0000000D.00000002.517236136.0000000005748000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.78.89.117	www.zkjk888.com	United States		16509	AMAZON-02US	true
162.43.120.154	www.p-soils.com	United States		11333	CYBERTRAILSUS	true
142.250.203.115	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
178.128.239.245	www.cpitherapy.com	Netherlands		14061	DIGITALOCEAN-ASNUS	true
209.99.64.33	www.nu2uresale.store	United States		40034	CONFLUENCE-NETWORK-INCVG	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756334
Start date and time:	2022-11-30 01:54:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI & PACKING LIST.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/2@6/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 44.7% (good quality ratio 39.2%) • Quality average: 72% • Quality standard deviation: 33%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 93.184.220.29, 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, cs9.wac.phicdn.net, ocsp.digicert.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
01:55:06	API Interceptor	1x Sleep call for process: PI & PACKING LIST.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI & PACKING LIST.exe.log

Process:	C:\Users\user\Desktop\PI & PACKING LIST.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\71M40-20Q

Process:	C:\Windows\SysWOW64\control.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.599851542938325
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:	PI & PACKING LIST.exe
File size:	1030144
MD5:	36fbb21511e87e8dddc8916cc2dc9367

SHA1:	eda2fa3fe4b62fe3d564cf492cc31a875e8f1922
SHA256:	937c7c476bb363e55fdf1ff275c87de91ec0f550072e9a759387cc95e6c78c83
SHA512:	85aa4905d89f42acc75d9a31806d16a84ffca0bbd4aaf9b9605d98adc8ff66544616afd8705c9c5295a9153930f1be1d58c6556f9c244e1be163218c42336dc7
SSDEEP:	24576:s1uqqdOC2Clep1Vtcl6gIGVfeSvopbGCh9XV:sbqdO+IAInVnFCh9X
TLSH:	06256BCB2F300E84CB5F34715C8D1B8861823DA149F59CF22B756A786E564FFA69227C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...>.|c.....0..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4fccde
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x637CBC3E [Tue Nov 22 12:10:38 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xfcc8c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xfe000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x100000	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
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xfae0c	0xfb000	False	0.8133160716508964	data	7.603845618377083	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xfe000	0x388	0x400	False	0.3818359375	data	2.865449669398995	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x100000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

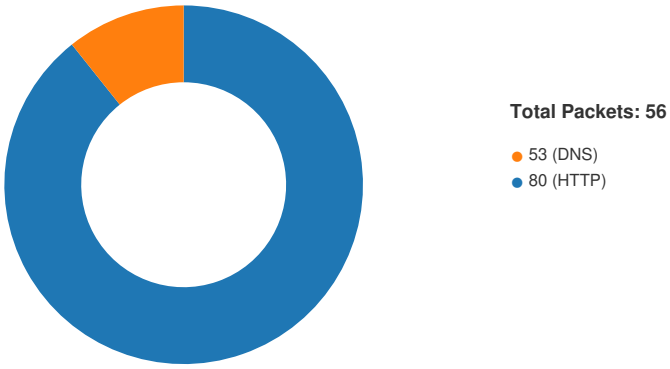
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xfe058	0x32c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:56:30.435599089 CET	49699	80	192.168.2.3	35.78.89.117
Nov 30, 2022 01:56:30.690313101 CET	80	49699	35.78.89.117	192.168.2.3
Nov 30, 2022 01:56:30.690747023 CET	49699	80	192.168.2.3	35.78.89.117
Nov 30, 2022 01:56:30.690953016 CET	49699	80	192.168.2.3	35.78.89.117
Nov 30, 2022 01:56:30.945398092 CET	80	49699	35.78.89.117	192.168.2.3
Nov 30, 2022 01:56:30.945488930 CET	80	49699	35.78.89.117	192.168.2.3
Nov 30, 2022 01:56:30.945538044 CET	80	49699	35.78.89.117	192.168.2.3
Nov 30, 2022 01:56:30.945661068 CET	49699	80	192.168.2.3	35.78.89.117
Nov 30, 2022 01:56:30.945851088 CET	49699	80	192.168.2.3	35.78.89.117
Nov 30, 2022 01:56:31.200309992 CET	80	49699	35.78.89.117	192.168.2.3
Nov 30, 2022 01:56:36.075532913 CET	49700	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:36.203886986 CET	80	49700	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:36.207110882 CET	49700	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:36.207313061 CET	49700	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:36.339452982 CET	80	49700	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:36.339534998 CET	80	49700	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:36.339648962 CET	80	49700	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:36.339735985 CET	49700	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:37.213046074 CET	49700	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:38.230366945 CET	49701	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:38.356884956 CET	80	49701	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:38.357409954 CET	49701	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:38.358261108 CET	49701	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:38.485125065 CET	80	49701	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:38.485260010 CET	80	49701	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:38.485310078 CET	80	49701	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:38.485519886 CET	49701	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:39.369651079 CET	49701	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:40.385653019 CET	49702	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:40.512706995 CET	80	49702	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:40.513171911 CET	49702	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:40.513289928 CET	49702	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:40.639802933 CET	80	49702	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:40.640072107 CET	80	49702	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:40.640115023 CET	80	49702	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:40.640268087 CET	49702	80	192.168.2.3	178.128.239.245
Nov 30, 2022 01:56:40.640450954 CET	49702	80	192.168.2.3	178.128.239.245

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:56:40.766827106 CET	80	49702	178.128.239.245	192.168.2.3
Nov 30, 2022 01:56:46.443892002 CET	49703	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:46.717799902 CET	80	49703	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:46.718111038 CET	49703	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:46.718338966 CET	49703	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:46.992011070 CET	80	49703	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:46.993747950 CET	80	49703	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:46.993794918 CET	80	49703	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:46.993834972 CET	80	49703	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:46.993962049 CET	49703	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:46.993962049 CET	49703	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:47.730102062 CET	49703	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:48.746025085 CET	49704	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:49.020411968 CET	80	49704	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:49.020566940 CET	49704	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:49.025969982 CET	49704	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:49.300954103 CET	80	49704	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:49.302470922 CET	80	49704	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:49.302534103 CET	80	49704	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:49.302563906 CET	80	49704	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:49.302881002 CET	49704	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:50.026726007 CET	49704	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.043955088 CET	49705	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.317914963 CET	80	49705	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:51.318133116 CET	49705	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.318274021 CET	49705	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.593318939 CET	80	49705	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:51.594609022 CET	80	49705	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:51.594669104 CET	80	49705	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:51.594719887 CET	80	49705	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:51.594772100 CET	49705	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.594810009 CET	49705	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.595088005 CET	49705	80	192.168.2.3	162.43.120.154
Nov 30, 2022 01:56:51.869878054 CET	80	49705	162.43.120.154	192.168.2.3
Nov 30, 2022 01:56:56.655076981 CET	49706	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:56.672187090 CET	80	49706	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:56.672312021 CET	49706	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:56.672535896 CET	49706	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:56.689588070 CET	80	49706	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:56.798434973 CET	80	49706	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:56.798474073 CET	80	49706	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:56.798841953 CET	49706	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:57.683523893 CET	49706	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:58.700560093 CET	49707	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:58.717950106 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.718117952 CET	49707	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:58.718626976 CET	49707	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:58.736681938 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.736748934 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.736793995 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.736835003 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.736877918 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.845972061 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.846035957 CET	80	49707	142.250.203.115	192.168.2.3
Nov 30, 2022 01:56:58.846225023 CET	49707	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:56:59.730948925 CET	49707	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:57:00.747503996 CET	49708	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:57:00.764229059 CET	80	49708	142.250.203.115	192.168.2.3
Nov 30, 2022 01:57:00.764373064 CET	49708	80	192.168.2.3	142.250.203.115

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:57:00.764707088 CET	49708	80	192.168.2.3	142.250.203.115
Nov 30, 2022 01:57:00.781295061 CET	80	49708	142.250.203.115	192.168.2.3
Nov 30, 2022 01:57:00.891392946 CET	80	49708	142.250.203.115	192.168.2.3
Nov 30, 2022 01:57:00.891453028 CET	80	49708	142.250.203.115	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 01:56:25.364172935 CET	49977	53	192.168.2.3	8.8.8.8
Nov 30, 2022 01:56:25.383728981 CET	53	49977	8.8.8.8	192.168.2.3
Nov 30, 2022 01:56:30.406841040 CET	57840	53	192.168.2.3	8.8.8.8
Nov 30, 2022 01:56:30.430402040 CET	53	57840	8.8.8.8	192.168.2.3
Nov 30, 2022 01:56:35.953828096 CET	57990	53	192.168.2.3	8.8.8.8
Nov 30, 2022 01:56:36.071085930 CET	53	57990	8.8.8.8	192.168.2.3
Nov 30, 2022 01:56:46.184161901 CET	52387	53	192.168.2.3	8.8.8.8
Nov 30, 2022 01:56:46.442496061 CET	53	52387	8.8.8.8	192.168.2.3
Nov 30, 2022 01:56:56.621620893 CET	56924	53	192.168.2.3	8.8.8.8
Nov 30, 2022 01:56:56.653685093 CET	53	56924	8.8.8.8	192.168.2.3
Nov 30, 2022 01:57:05.922028065 CET	60625	53	192.168.2.3	8.8.8.8
Nov 30, 2022 01:57:06.161883116 CET	53	60625	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 01:56:25.364172935 CET	192.168.2.3	8.8.8.8	0x79b8	Standard query (0)	www.gebouwpas.online	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:30.406841040 CET	192.168.2.3	8.8.8.8	0x2c63	Standard query (0)	www.zkjk888.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:35.953828096 CET	192.168.2.3	8.8.8.8	0x2c27	Standard query (0)	www.cpitherapy.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:46.184161901 CET	192.168.2.3	8.8.8.8	0xbf1a	Standard query (0)	www.p-soils.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:56.621620893 CET	192.168.2.3	8.8.8.8	0xd877	Standard query (0)	www.bengalindex.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:57:05.922028065 CET	192.168.2.3	8.8.8.8	0x7a2e	Standard query (0)	www.nu2uresale.store	A (IP address)	IN (0x0001)	false

DNS Answers

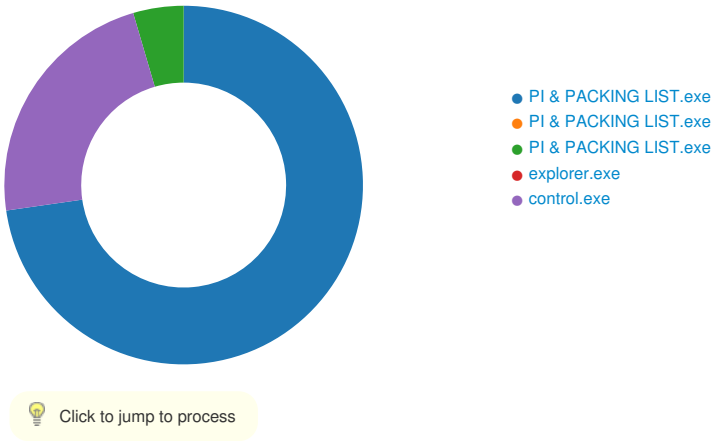
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 01:56:25.383728981 CET	8.8.8.8	192.168.2.3	0x79b8	Name error (3)	www.gebouwpas.online	none	none	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:30.430402040 CET	8.8.8.8	192.168.2.3	0x2c63	No error (0)	www.zkjk888.com		35.78.89.117	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:36.071085930 CET	8.8.8.8	192.168.2.3	0x2c27	No error (0)	www.cpitherapy.com		178.128.239.245	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:46.442496061 CET	8.8.8.8	192.168.2.3	0xbf1a	No error (0)	www.p-soils.com		162.43.120.154	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:56:56.653685093 CET	8.8.8.8	192.168.2.3	0xd877	No error (0)	www.bengalindex.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 01:56:56.653685093 CET	8.8.8.8	192.168.2.3	0xd877	No error (0)	ghs.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)	false
Nov 30, 2022 01:57:06.161883116 CET	8.8.8.8	192.168.2.3	0x7a2e	No error (0)	www.nu2uresale.store		209.99.64.33	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.zkjk888.com
- www.cpitherapy.com
- www.p-soils.com
- www.bengalindex.com
- www.nu2uresale.store

Statistics

Behavior



System Behavior

Analysis Process: PI & PACKING LIST.exe PID: **6140**, Parent PID: **3452**

General

Target ID:	0
Start time:	01:55:00
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\PI & PACKING LIST.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PI & PACKING LIST.exe
Imagebase:	0xd0000
File size:	1030144 bytes
MD5 hash:	36FBB21511E87E8DDDC8916CC2DC9367
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: 00000000.00000002.264428315.00000000029D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: PI & PACKING LIST.exe PID: **5216**, Parent PID: **6140**

General	
Target ID:	1
Start time:	01:55:08
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\PI & PACKING LIST.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PI & PACKING LIST.exe
Imagebase:	0x3a0000
File size:	1030144 bytes
MD5 hash:	36FBB21511E87E8DDDC8916CC2DC9367
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PI & PACKING LIST.exe PID: **2352**, Parent PID: **6140**

General	
Target ID:	2
Start time:	01:55:08
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\PI & PACKING LIST.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PI & PACKING LIST.exe
Imagebase:	0x720000
File size:	1030144 bytes
MD5 hash:	36FBB21511E87E8DDDC8916CC2DC9367
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.353618597.0000000000C60000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.353260864.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.353260864.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.353260864.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.353260864.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: **3452**, Parent PID: **2352**

General	
Target ID:	3
Start time:	01:55:10
Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.345082941.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.326684434.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.326684434.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.326684434.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.326684434.000000001030A000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **5228**, Parent PID: **3452**

General

Target ID:	13
Start time:	01:55:49
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x1360000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.512821683.0000000003510000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.512821683.0000000003510000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.512821683.0000000003510000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.512821683.0000000003510000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.512567942.0000000001330000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.512567942.0000000001330000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.512567942.0000000001330000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.512567942.0000000001330000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.509273886.0000000000EC0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.509273886.0000000000EC0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.509273886.0000000000EC0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.509273886.0000000000EC0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PI & PACKING LIST.exe	success or wait	1	EDC8C7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\71M40-2OQ	object name not found	1	EDC8C7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\71M40-2OQ	sharing violation	1	EDC8C7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\71M40-2OQ	sharing violation	1	EDC8C7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	EDC897	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly