ID: 323028
Sample Name: PT300975-inv.exe
Cookbook: default.jbs
Time: 08:27:30
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

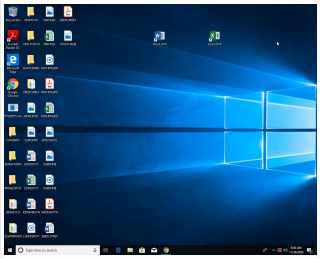
Analysis Report PT300975-inv.exe

Overview

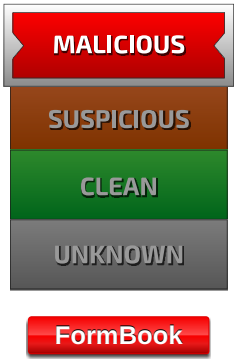
General Information

Sample Name:	PT300975-inv.exe
Analysis ID:	323028
MD5:	025544a9014cf16.
SHA1:	0123853e7960cd..
SHA256:	2858bfcb9388b05.
Tags:	exe Formbook

Most interesting Screenshot:



Detection

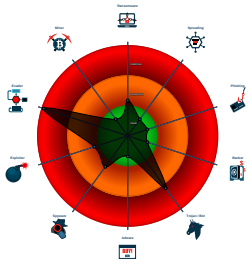


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through

Classification



Startup

- **System is w10x64**
- PT300975-inv.exe (PID: 7124 cmdline: 'C:\Users\user\Desktop\PT300975-inv.exe' MD5: 025544A9014CF1667E8A1D4FF68DA253)
  - mscorsvw.exe (PID: 5844 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe MD5: 38368FC9F84C7A27D0C8CD8E1543F172)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 1040 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 6064 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.346082629.0000000004983000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.346082629.0000000004983000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x995a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9bd4:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37018:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37292:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x63638:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x638b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156f7:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x42db5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x6f3d5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151e3:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x428a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x6eec1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157f9:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x42eb7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x6f4d7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15971:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x4302f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x6f64f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa5ec:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x37caa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x642ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06
00000000.00000002.346082629.0000000004983000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1847b:$sqlite3step: 68 34 1C 7B E1 • 0x1858e:$sqlite3step: 68 34 1C 7B E1 • 0x45b39:$sqlite3step: 68 34 1C 7B E1 • 0x45c4c:$sqlite3step: 68 34 1C 7B E1 • 0x72159:$sqlite3step: 68 34 1C 7B E1 • 0x7226c:$sqlite3step: 68 34 1C 7B E1 • 0x184aa:$sqlite3text: 68 38 2A 90 C5 • 0x185cf:$sqlite3text: 68 38 2A 90 C5 • 0x45b68:$sqlite3text: 68 38 2A 90 C5 • 0x45c8d:$sqlite3text: 68 38 2A 90 C5 • 0x72188:$sqlite3text: 68 38 2A 90 C5 • 0x722ad:$sqlite3text: 68 38 2A 90 C5 • 0x184bd:$sqlite3blob: 68 53 D8 7F 8C • 0x185e5:$sqlite3blob: 68 53 D8 7F 8C • 0x45b7b:$sqlite3blob: 68 53 D8 7F 8C • 0x45ca3:$sqlite3blob: 68 53 D8 7F 8C • 0x7219b:$sqlite3blob: 68 53 D8 7F 8C • 0x722c3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.384709518.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.384709518.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 19 entries				

Unpacked PEs

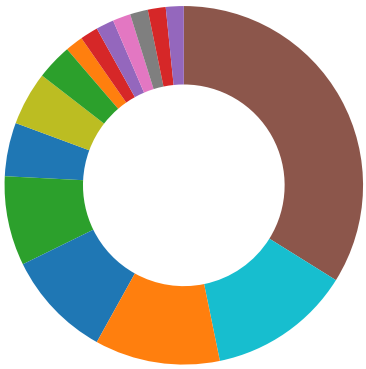
Source	Rule	Description	Author	Strings
2.2.mscorsvw.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.mscorsvw.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$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

Source	Rule	Description	Author	Strings
2.2.mscorsvw.exe.400000.0.raw.unpack	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
2.2.mscorsvw.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.mscorsvw.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
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Malware Analysis System Evasion:

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:

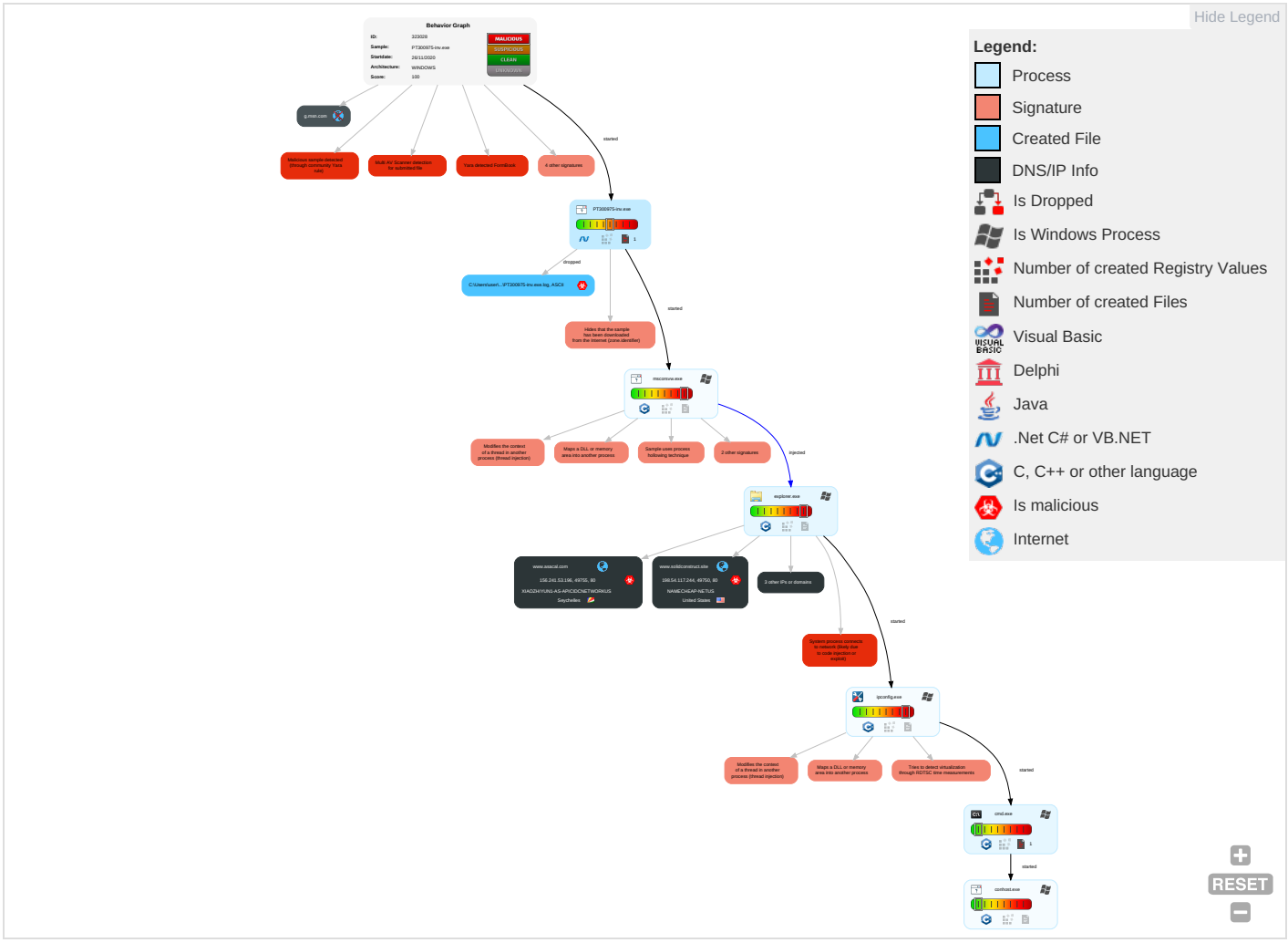
Yara detected FormBook

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 (Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

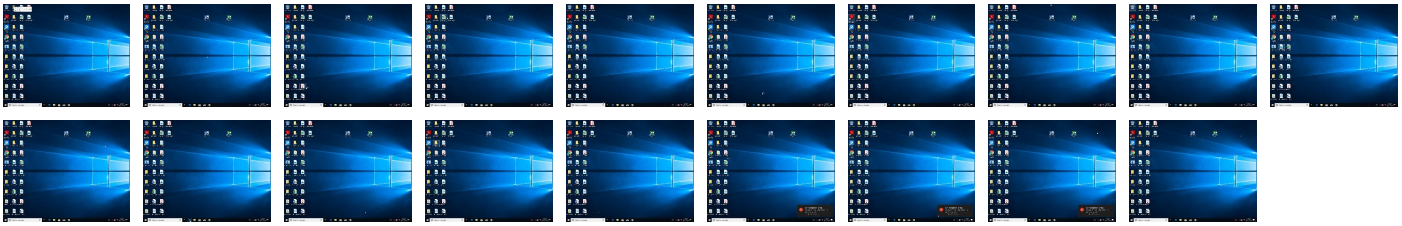
Behavior Graph



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
PT300975-inv.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.Razy	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

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.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://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.asacal.com/jqc/?JfEtEZgp=cE9UUOc3pLPT0LAdHSIP3evlMF3IBhbdmq5wG0CQLEBsctkiCkQzhS7S4EgmhhRecsIvRlsotA==&ojq0s=RzulsD	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.solidconstruct.site	198.54.117.244	true	true		unknown
www.asacal.com	156.241.53.196	true	true		unknown
www.hongreng.xyz	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.kornteengoods.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.asacal.com/jqc/?JfEtEZgp=cE9UUOc3pLPT0LAdHSIP3evlMF3IBhbdmq5wG0CQLEBsctkiCkQzhS7S4EgmhhRecsIvRlsotA==&ojq0s=RzulsD	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000002.604467265.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.00000000.367422589.000000000B1A6000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.367422589.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.367422589.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.367422589.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.367422589.000000000B1A6000.0 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
156.241.53.196	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
198.54.117.244	unknown	United States		22612	NAMECHEAP-NETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323028
Start date:	26.11.2020
Start time:	08:27:30
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 9m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PT300975-inv.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.7% (good quality ratio 34.6%) • Quality average: 73.5% • Quality standard deviation: 30.8%
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
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 13.64.90.137, 168.61.161.212, 51.104.144.132, 8.241.122.126, 67.26.139.254, 8.248.113.254, 8.253.95.249, 67.27.234.126, 51.103.5.186, 52.155.217.156, 20.54.26.129, 52.142.114.176, 92.122.213.247, 92.122.213.194, 23.210.248.85 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
08:28:25	API Interceptor	1x Sleep call for process: PT300975-inv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.244	test.js	Get hash	malicious	Browse	• 101legit.com/0.html
	dsexplrob.exe	Get hash	malicious	Browse	• i3mode.com/dbExpressversion/db87987Administrator.php?b=FKfEZOAdYedIVNeAlGKbCgFzoODmhh
	nbmvwchp.js	Get hash	malicious	Browse	• 101legit.com/0.html

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	anthon.exe	Get hash	malicious	Browse	• 156.241.53.168
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 156.241.53.195
	Inv.exe	Get hash	malicious	Browse	• 156.241.53.9
	Shipping Documents (INV,PL,BL)_pdf.exe	Get hash	malicious	Browse	• 156.224.66.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 45.207.121.138
	Invoice.exe	Get hash	malicious	Browse	• 156.241.53.234
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• 45.207.121.138
	n4uladudJS.exe	Get hash	malicious	Browse	• 45.207.121.138
	T66DUJYHQE.exe	Get hash	malicious	Browse	• 45.207.121.138
	#U5341#U4e00#U6708#U4efd#U516c#U53f8#U503c#U73ed#U4eba#U5458#U8c03#U73ed#U901a#U77e5.exe	Get hash	malicious	Browse	• 156.253.88.154
	9qB3tPamJa.exe	Get hash	malicious	Browse	• 156.253.114.216
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• 45.207.121.138
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 45.207.121.138
	RNM56670112.exe	Get hash	malicious	Browse	• 156.225.160.251
	PpCVLJxsOp.exe	Get hash	malicious	Browse	• 154.210.136.219
	PO PL.exe	Get hash	malicious	Browse	• 156.254.247.54
	1-RFQ-IOCL-PP-IN-301 BID INSTRUCTIONSCOMMERCIAL TERMS AND CONDITIONS-2020-10-14..exe	Get hash	malicious	Browse	• 156.254.221.125
	3BJGa7Xw4ugPpll.exe	Get hash	malicious	Browse	• 23.248.240.227
	y20dxdW3GQ.exe	Get hash	malicious	Browse	• 23.235.182.106
	J3ae2JBEng.exe	Get hash	malicious	Browse	• 45.207.118.132
NAMECHEAP-NETUS	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://https://dhumketubd.com/DifferenceCard/login.php	Get hash	malicious	Browse	• 198.54.117.200
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 63.250.47.200
	ATT59829.htm	Get hash	malicious	Browse	• 198.54.115.249
	PO EME39134.xlsx	Get hash	malicious	Browse	• 63.250.38.18
	http://https://www.ebhadhara.com/ova/office365/YWp1bm5hcmthckBrcm9sbGJvbmRyYXRpbmdzLmNvbQ0%3D	Get hash	malicious	Browse	• 199.192.28.206

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FxzOwcXb7x.exe	Get hash	malicious	Browse	• 198.54.122.60
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• 198.54.117.217
	ptFlhqUe89.exe	Get hash	malicious	Browse	• 63.250.38.18
	Yarranton.co.uk.htm	Get hash	malicious	Browse	• 199.188.200.218
	PO#010-240.exe	Get hash	malicious	Browse	• 162.213.255.53
	PO_010-240.exe	Get hash	malicious	Browse	• 162.213.255.53
	EME.39134.xlsx	Get hash	malicious	Browse	• 63.250.38.18
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	• 198.54.120.245
	http://https://1drv.ms/u/s!Ap6-6LFn1rzXgTxzc-81jQs8opJO?e=EhEGR5	Get hash	malicious	Browse	• 198.54.120.226
	n830467925857.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	new quotation order.exe	Get hash	malicious	Browse	• 198.54.117.216
	NEW ORDER.exe	Get hash	malicious	Browse	• 198.54.122.60
	n830467925857.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	ATT96626.htm	Get hash	malicious	Browse	• 198.54.115.249

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PT300975-inv.exe.log

Process:	C:\Users\user\Desktop\PT300975-inv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1636
Entropy (8bit):	5.344107669812469
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovjHKx1qHLHKs:iqXeqm00YqhQnouRqjorqxwrqs
MD5:	BF1A4BABF3E94AA2F0BED4C55E050B13
SHA1:	433EA392F97D828DCA9CC9C080B99D40063CDF50
SHA-256:	B74F8FCBDD8A649F2073373BD471F685A14629E7C2DE97C445F60414CBF61B9E
SHA-512:	C6D0F73205F524F3DDC9A7211BA07E28A02334AD462DAD893FFF90D5AA9723C09185B6ACF78CEF1C1300CD492FA3AF9C2FCADA18934D73C0CA87B18CC42D076
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.285704309931807

General

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:	PT300975-inv.exe
File size:	559616
MD5:	025544a9014cf1667e8a1d4ff68da253
SHA1:	0123853e7960cdae4f3ad95945b4ec86adbb93c6
SHA256:	2858bfcb9388b05049df45459ee60bf96be0b0d75a3be34cf3c00f57ec9f4469
SHA512:	a22db404c3a154339b3cd6d4a4227f319f6cb99d103346856ffd6fd249fe08bace4f528f185edc25c0672ae03b2e14c87b31b0b2d0728372c5893821b5a43068
SSDEEP:	6144:3cMR5P4uE1KMtqm/0XWJYoukAlD0o2c3zZOaoRzkZRjdnLor7/7Sr9sTFaOxSxyy:3n5PqttqmMGJYvlxzgaoG3dnG7SeG2+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... ;.F.....~..... .....@.. .....`.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x489c9e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x46D33B20 [Mon Aug 27 20:59:12 2007 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

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
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x89c44	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x622	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8c000	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	0x87ca4	0x87e00	False	0.583592671918	data	6.29806430778	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x622	0x800	False	0.353515625	data	3.65274067017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	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_VERSION	0x8a0a0	0x398	data		
RT_MANIFEST	0x8a438	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

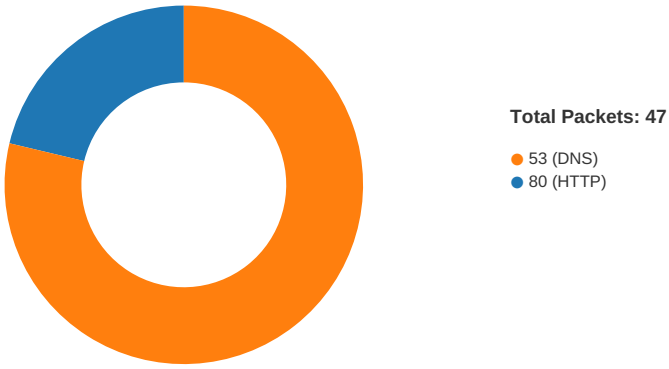
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2010 F7G5?9JAF>2=>JA7AIB2F
Assembly Version	1.0.0.0
InternalName	use5.exe
FileVersion	7.10.14.17
CompanyName	F7G5?9JAF>2=>JA7AIB2F
Comments	:6;C>4;FA4F5DH9D@88B;3
ProductName	5G5C9985D<<?=>@B5@
ProductVersion	7.10.14.17
FileDescription	5G5C9985D<<?=>@B5@
OriginalFilename	use5.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:29:26.744565964 CET	49750	80	192.168.2.6	198.54.117.244
Nov 26, 2020 08:29:26.911395073 CET	80	49750	198.54.117.244	192.168.2.6
Nov 26, 2020 08:29:26.911807060 CET	49750	80	192.168.2.6	198.54.117.244
Nov 26, 2020 08:29:26.911973953 CET	49750	80	192.168.2.6	198.54.117.244
Nov 26, 2020 08:29:27.078738928 CET	80	49750	198.54.117.244	192.168.2.6
Nov 26, 2020 08:29:27.078759909 CET	80	49750	198.54.117.244	192.168.2.6
Nov 26, 2020 08:30:08.408441067 CET	49755	80	192.168.2.6	156.241.53.196
Nov 26, 2020 08:30:08.610635996 CET	80	49755	156.241.53.196	192.168.2.6
Nov 26, 2020 08:30:08.610830069 CET	49755	80	192.168.2.6	156.241.53.196
Nov 26, 2020 08:30:08.610979080 CET	49755	80	192.168.2.6	156.241.53.196
Nov 26, 2020 08:30:08.813050032 CET	80	49755	156.241.53.196	192.168.2.6
Nov 26, 2020 08:30:09.102338076 CET	49755	80	192.168.2.6	156.241.53.196
Nov 26, 2020 08:30:09.292335033 CET	80	49755	156.241.53.196	192.168.2.6
Nov 26, 2020 08:30:09.292357922 CET	80	49755	156.241.53.196	192.168.2.6
Nov 26, 2020 08:30:09.292530060 CET	49755	80	192.168.2.6	156.241.53.196
Nov 26, 2020 08:30:09.292561054 CET	49755	80	192.168.2.6	156.241.53.196
Nov 26, 2020 08:30:09.304438114 CET	80	49755	156.241.53.196	192.168.2.6
Nov 26, 2020 08:30:09.304570913 CET	49755	80	192.168.2.6	156.241.53.196

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:28:19.663137913 CET	56023	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:28:19.690159082 CET	53	56023	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:20.626461029 CET	58384	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:20.653572083 CET	53	58384	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:21.668230057 CET	60261	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:21.695391893 CET	53	60261	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:22.580018997 CET	56061	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:22.607135057 CET	53	56061	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:23.502145052 CET	58336	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:23.529290915 CET	53	58336	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:25.972165108 CET	53781	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:25.999289989 CET	53	53781	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:27.134497881 CET	54064	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:27.161614895 CET	53	54064	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:28.241576910 CET	52811	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:28.268699884 CET	53	52811	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:29.477148056 CET	55299	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:29.504374981 CET	53	55299	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:31.500103951 CET	63745	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:31.527142048 CET	53	63745	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:34.086605072 CET	50055	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:34.113698959 CET	53	50055	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:37.824050903 CET	61374	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:37.851146936 CET	53	61374	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:38.843249083 CET	50339	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:38.870150089 CET	53	50339	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:40.249627113 CET	63307	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:40.276679039 CET	53	63307	8.8.8.8	192.168.2.6
Nov 26, 2020 08:28:49.056457043 CET	49694	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:28:49.083647013 CET	53	49694	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:05.741004944 CET	54982	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:05.768177986 CET	53	54982	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:07.180556059 CET	50010	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:07.217647076 CET	53	50010	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:11.676465988 CET	63718	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:11.726603985 CET	53	63718	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:12.470824003 CET	62116	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:12.506289005 CET	53	62116	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:12.947566032 CET	63816	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:12.995899916 CET	53	63816	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:13.324655056 CET	55014	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:13.376000881 CET	53	55014	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:13.761892080 CET	62208	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:13.797600031 CET	53	62208	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:14.079472065 CET	57574	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:14.130125999 CET	53	57574	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:14.193630934 CET	51818	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:14.231434107 CET	53	51818	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:14.714554071 CET	56628	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:14.751116037 CET	53	56628	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:15.363802910 CET	60778	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:15.399085045 CET	53	60778	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:16.189421892 CET	53799	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:16.224932909 CET	53	53799	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:16.457114935 CET	54683	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:16.500622034 CET	53	54683	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:16.675836086 CET	59329	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:16.711163044 CET	53	59329	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:21.984956980 CET	64021	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:22.021745920 CET	53	64021	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:26.549397945 CET	56129	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:26.737931013 CET	53	56129	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:47.298248053 CET	58177	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:47.642015934 CET	53	58177	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:48.052105904 CET	50700	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:29:48.095624924 CET	53	50700	8.8.8.8	192.168.2.6
Nov 26, 2020 08:29:51.215604067 CET	54069	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:29:51.255037069 CET	53	54069	8.8.8.8	192.168.2.6
Nov 26, 2020 08:30:08.060817003 CET	61178	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:30:08.402991056 CET	57017	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:30:08.407228947 CET	53	61178	8.8.8.8	192.168.2.6
Nov 26, 2020 08:30:08.430083990 CET	53	57017	8.8.8.8	192.168.2.6
Nov 26, 2020 08:30:29.262655973 CET	56327	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:30:29.332756996 CET	53	56327	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 08:29:16.457114935 CET	192.168.2.6	8.8.8.8	0xe265	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:29:26.549397945 CET	192.168.2.6	8.8.8.8	0x9f9c	Standard query (0)	www.solidconstruct.site	A (IP address)	IN (0x0001)
Nov 26, 2020 08:29:47.298248053 CET	192.168.2.6	8.8.8.8	0xcf3f	Standard query (0)	www.hongreng.xyz	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:08.060817003 CET	192.168.2.6	8.8.8.8	0x869a	Standard query (0)	www.asacal.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:29.262655973 CET	192.168.2.6	8.8.8.8	0x7da1	Standard query (0)	www.kornteengoods.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 08:29:16.500622034 CET	8.8.8.8	192.168.2.6	0xe265	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:29:26.737931013 CET	8.8.8.8	192.168.2.6	0x9f9c	No error (0)	www.solidconstruct.site		198.54.117.244	A (IP address)	IN (0x0001)
Nov 26, 2020 08:29:47.642015934 CET	8.8.8.8	192.168.2.6	0xcf3f	Name error (3)	www.hongreng.xyz	none	none	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:08.407228947 CET	8.8.8.8	192.168.2.6	0x869a	No error (0)	www.asacal.com		156.241.53.196	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:29.332756996 CET	8.8.8.8	192.168.2.6	0x7da1	Name error (3)	www.kornteengoods.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.solidconstruct.site
- www.asacal.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49750	198.54.117.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:29:26.911973953 CET	5347	OUT	GET /jqc/?JfEtEZgp=AQxPeURRQ9kC4DgOk8VME5njQ8dFSmWtzYEqQ7tz67PuOtzOYn8gv4wq3HEWg5IvV5fpD9rFbA==&ojq0s=RzulsD HTTP/1.1 Host: www.solidconstruct.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49755	156.241.53.196	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:30:08.610979080 CET	6108	OUT	GET /jqc/?JfEtEZgp=cE9UUOc3pLPT0LAdHSIP3evlMF3IBhbdmq5wG0CQLEBsctkiCkQzhS7S4EgmhhRecsIvRlsotA==&ojq0s=RzulsD HTTP/1.1 Host: www.asacal.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:30:09.292335033 CET	6118	IN	HTTP/1.1 302 Moved Temporarily Date: Thu, 26 Nov 2020 07:30:08 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=u9i0r05tpvbtv5qber0ofb8qs2; path=/ Set-Cookie: PHPSESSID=ft1su6f9qnak6jout2tis60pq6; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

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

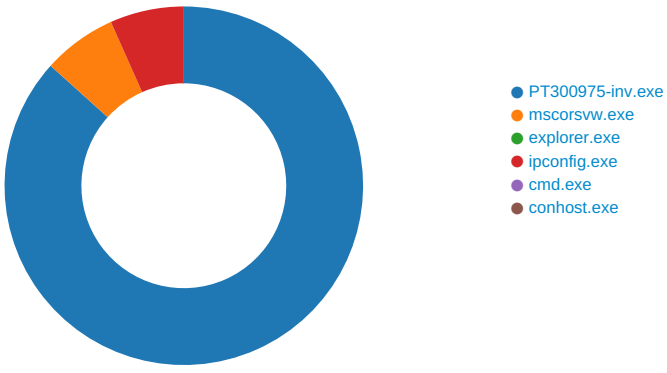
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PT300975-inv.exe PID: 7124 Parent PID: 5852

General

Start time:	08:28:24
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\PT300975-inv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PT300975-inv.exe'
Imagebase:	0xc50000
File size:	559616 bytes
MD5 hash:	025544A9014CF1667E8A1D4FF68DA253
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.346082629.0000000004983000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.346082629.0000000004983000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.346082629.0000000004983000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.345935550.000000000489F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.345935550.000000000489F000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.345935550.000000000489F000.00000004.00000001.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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PT300975-inv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PT300975-inv.exe:Zone.Identifier	success or wait	1	2DE943B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PT300975-inv.exe.log	unknown	1636	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 33 2c 22 53 79 73 74 65 6d 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DE203DE	ReadFile

Analysis Process: mscorsvw.exe PID: 5844 Parent PID: 7124

General

Start time:	08:28:25
Start date:	26/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
Imagebase:	0xc20000
File size:	107592 bytes
MD5 hash:	38368FC9F84C7A27D0C8CD8E1543F172
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: 00000002.00000002.384709518.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.384709518.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.384709518.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.384973697.0000000004DD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.384973697.0000000004DD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.384973697.0000000004DD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.385166130.00000000050D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.385166130.00000000050D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.385166130.00000000050D0000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 5844

General

Start time:	08:28:29
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: ipconfig.exe PID: 1040 Parent PID: 3440

General

Start time:	08:28:43

Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xe30000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.603415993.0000000000990000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.603415993.0000000000990000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.603415993.0000000000990000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.603938511.0000000000DF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.603938511.0000000000DF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.603938511.0000000000DF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.604508928.0000000002F40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.604508928.0000000002F40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.604508928.0000000002F40000.00000004.00000001.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	9A9E57	NtReadFile

Analysis Process: cmd.exe PID: 6064 Parent PID: 1040

General

Start time:	08:28:48
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe'
Imagebase:	0x2a0000
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: 724 Parent PID: 6064

General

Start time:	08:28:51
Start date:	26/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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