ID: 830738
Sample Name:
Shipment_notification.exe
Cookbook: default.jbs
Time: 16:47:46
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

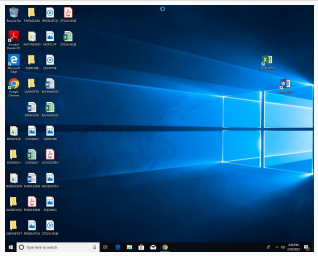
Windows Analysis Report

Shipment_notification.exe

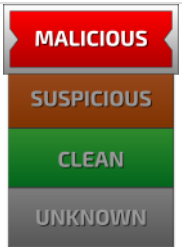
Overview

General Information

Sample Name:	Shipment_notification.exe
Analysis ID:	830738
MD5:	c310a64af890a..
SHA1:	509cdec4d058...
SHA256:	90e86051c2fb0..
Tags:	exe
Infos:	



Detection



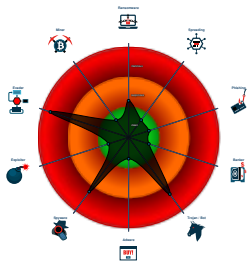
FormBook

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

Signatures

- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through...
- System process connects to networ...
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Sample uses process hollowing tech...
- Tries to steal Mail credentials (via fi...
- Maps a DLL or memory area into an...
- Machine Learning detection for sam...
- Performs DNS queries to domains w...
- Injects a PE file into a foreign proce...

Classification



Process Tree

- **System is w10x64**
- Shipment_notification.exe (PID: 1348 cmdline: C:\Users\user\Desktop\Shipment_notification.exe MD5: C310A64AF890AC32ABFF89E86CB53A33)
  - Shipment_notification.exe (PID: 2344 cmdline: C:\Users\user\Desktop\Shipment_notification.exe MD5: C310A64AF890AC32ABFF89E86CB53A33)
  - Shipment_notification.exe (PID: 3968 cmdline: C:\Users\user\Desktop\Shipment_notification.exe MD5: C310A64AF890AC32ABFF89E86CB53A33)
    - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 4412 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	**http://** blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.377445989.0000000001510000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000002.00000002.377445989.0000000001510000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae3f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182e7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000002.00000002.377445989.0000000001510000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180e5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17b81:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x181e7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1835f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaa0a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16dcc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ee2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.377228453.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000002.00000002.377228453.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20e53:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcbc2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1a06a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 10 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Shipment_notification.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
2.2.Shipment_notification.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20053:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbdc2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1926a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
2.2.Shipment_notification.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19068:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18b04:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1916a:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x192e2:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xb98d:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17d4f:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1edfa:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1fdad:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.Shipment_notification.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
2.2.Shipment_notification.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20e53:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcbc2:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1a06a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 198.177.124.57	
Timestamp:	192.168.2.5198.177.124.5749706802031453 03/20/23-16:50:29.247456
SID:	2031453
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 199.59.243.223	
Timestamp:	192.168.2.5199.59.243.22349702802031453 03/20/23-16:50:05.917395
SID:	2031453
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 198.177.124.57	
Timestamp:	192.168.2.5198.177.124.5749706802031412 03/20/23-16:50:29.247456
SID:	2031412
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 154.218.155.8	
Timestamp:	192.168.2.5154.218.155.849704802031453 03/20/23-16:50:21.020230
SID:	2031453
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 198.177.124.57	
Timestamp:	192.168.2.5198.177.124.5749706802031449 03/20/23-16:50:29.247456
SID:	2031449
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 154.218.155.8	
Timestamp:	192.168.2.5154.218.155.849704802031412 03/20/23-16:50:21.020230
SID:	2031412
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 199.59.243.223	
Timestamp:	192.168.2.5199.59.243.22349702802031449 03/20/23-16:50:05.917395
SID:	2031449
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 154.218.155.8

Timestamp:	192.168.2.5154.218.155.849704802031449 03/20/23-16:50:21.020230
SID:	2031449
Source Port:	49704
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 199.59.243.223	−
Timestamp:	192.168.2.5199.59.243.22349702802031412 03/20/23-16:50:05.917395
SID:	2031412
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Machine Learning detection for sample

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- Performs DNS queries to domains with low reputation

E-Banking Fraud

- Yara detected FormBook

System Summary

- Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

- Deletes itself after installation

HIPS / PFW / Operating System Protection Evasion

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

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

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

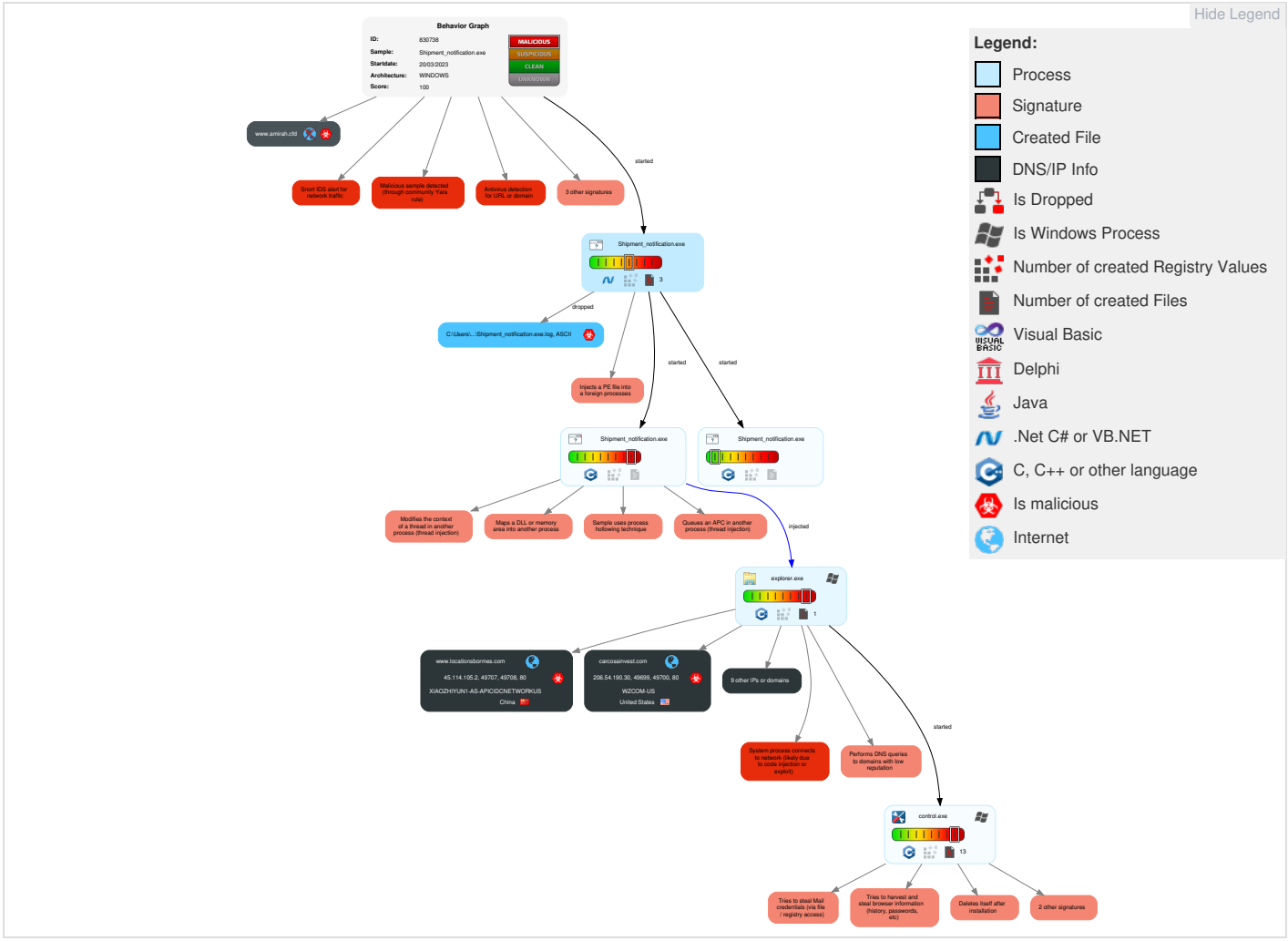
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Shipment_notification.exe	39%	ReversingLabs	Win32.Trojan.Generic	
Shipment_notification.exe	43%	Virustotal		Browse
Shipment_notification.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.searchvity.com/?dn=	100%	URL Reputation	malware	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comz	0%	URL Reputation	safe	
http://www.fontbureau.comzana	0%	URL Reputation	safe	
http://www.carterandcone.comn	0%	URL Reputation	safe	
http://www.ywtxsm.com/rs5b/Pr	100%	Avira URL Cloud	malware	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comx	0%	URL Reputation	safe	
http://www.searchvity.com/	100%	URL Reputation	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.peramid.xyz/rs5b/?uyxvg=pPgXS4BiopaVkxB77nB8m5BmJKRgxbtyTgQ51TCNvvWiqwh2ZJ0SiqT/1xVf5TTVOW5skWvYLryZyUzfOZLrBqpWBEotOTgmwg==&L6HRe=HinkmsLDjhA	100%	Avira URL Cloud	malware	
http://www.zzxiaoyuan.com/rs5b/1	0%	Avira URL Cloud	safe	
http://www.zzxiaoyuan.com/rs5b/	0%	Avira URL Cloud	safe	
http://www.emagrecarapido.store	0%	Avira URL Cloud	safe	
http://www.isabellagambitta.com/rs5b/?uyxvg=CsXC0bU6YgbK4v/ikU	100%	Avira URL Cloud	phishing	
http://www.drkathleensanders.com	0%	Avira URL Cloud	safe	
http://www.notebook-rucksack.com	0%	Avira URL Cloud	safe	
http://www.drkathleensanders.com/rs5b/	100%	Avira URL Cloud	malware	
http://www.rubyidentity.space/rs5b/	0%	Avira URL Cloud	safe	
http://www.notebook-rucksack.com/rs5b/	0%	Avira URL Cloud	safe	
http://www.peramid.xyz/rs5b/	100%	Avira URL Cloud	malware	
http://www.piergitarshoes.com/rs5b/	100%	Avira URL Cloud	malware	
http://www.amirah.cfd	100%	Avira URL Cloud	phishing	
http://www.amirah.cfd/rs5b/	100%	Avira URL Cloud	malware	
http://www.starauctioneerspro.com	0%	Avira URL Cloud	safe	
http://www.ywtxsm.com/rs5b/	100%	Avira URL Cloud	malware	
http://www.locationsbormes.com/rs5b/?uyxvg=5nmvRd2KsNrJ1ILohWvWv9G51OYC+JQySj/wVW5HrbzlASqN8826SlrC1uxl2FZ0KA9XHqewj3KetP3L0XT9wGstOg81NIph5g==&L6HRe=HinkmsLDjhA	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/b	0%	Avira URL Cloud	safe	
http://www.locationsbormes.com	0%	Avira URL Cloud	safe	
http://www.isabellagambitta.com	0%	Avira URL Cloud	safe	
http://www.notebook-rucksack.com/rs5b/%	0%	Avira URL Cloud	safe	
http://www.kaj8tfjcmkn7.xyz/rs5b/Q	0%	Avira URL Cloud	safe	
http://www.rubyidentity.space	0%	Avira URL Cloud	safe	
http://www.carcosainvest.com	0%	Avira URL Cloud	safe	
http://www.isabellagambitta.com/rs5b/?uyxvg=CsXC0bU6YgbK4v/ikU+FR3ZDcTynpB6gZNcuxnLmHu8DrupdLy2Rvx2rp5ka04f5VlwEigsTcDnoyRb/ht4uYCIEoQzcZzfMnw==&L6HRe=HinkmsLDjhA	100%	Avira URL Cloud	phishing	
http://www.sajatypeworks.com.Y	0%	Avira URL Cloud	safe	
http://www.zzxiaoyuan.com	0%	Avira URL Cloud	safe	
http://www.starauctioneerspro.com/rs5b/	0%	Avira URL Cloud	safe	
http://www.kaj8tfjcmkn7.xyz/rs5b/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cnv	0%	Avira URL Cloud	safe	
http://www.kaj8tfjcmkn7.xyz	0%	Avira URL Cloud	safe	
http://www.emagrecarapido.store/rs5b/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cni9	0%	Avira URL Cloud	safe	
http://www.tcatelier.com	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnx	0%	Avira URL Cloud	safe	
http://www.piergitarshoes.com	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno	0%	Avira URL Cloud	safe	
http://www.tcatelier.com/rs5b/	0%	Avira URL Cloud	safe	
http://www.ywtxsm.com	0%	Avira URL Cloud	safe	
http://www.isabellagambitta.com/rs5b/	100%	Avira URL Cloud	phishing	
http://www.ywtxsm.com/rs5b/?uyxvg=CESO3iylK7QUfFCiUFLwHXxmSIHW1gBrGCjGxLpE4g3q3SI6yIOiTvn7qrQa9OdkrAgYihNybI2hWOHGXNYRIortSIS8Lcg0Kg==&L6HRe=HinkmsLDjhA	100%	Avira URL Cloud	malware	
http://www.peramid.xyz	100%	Avira URL Cloud	malware	
http://www.53876.world	100%	Avira URL Cloud	malware	
http://www.drkathleensanders.com/rs5b/?uyxvg=Sr3AwP9Ski0v59cQ3JwcPDLo9I+EFZxtPOrHknZVg/8QV/fIqaYOT5hsTQMwMe6TSfps7iDWaOg2o/5pI6PYy1hDK243b9ADKw==&L6HRe=HinkmsLDjhA	100%	Avira URL Cloud	malware	
http://www.53876.world/rs5b/	100%	Avira URL Cloud	malware	
http://www.locationsbormes.com/rs5b/	100%	Avira URL Cloud	malware	
http://www.carcosainvest.com/rs5b/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.peramid.xyz	198.177.124.57	true	true		unknown
carcosainvest.com	206.54.190.30	true	true		unknown
www.piergitarshoes.com	199.59.243.223	true	true		unknown
www.isabellagambitta.com	185.27.134.217	true	true		unknown
www.ywtxsm.com	154.218.155.8	true	true		unknown
www.drkathleensanders.com	66.96.161.158	true	true		unknown
www.locationsbormes.com	45.114.105.2	true	true		unknown
www.emagrecarapido.store	unknown	unknown	true		unknown
www.tcatelier.com	unknown	unknown	true		unknown
www.amirah.cfd	unknown	unknown	true		unknown
www.carcosainvest.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.piergitarshoes.com/rs5b/	true	• Avira URL Cloud: malware	unknown
http://www.peramid.xyz/rs5b/	true	• Avira URL Cloud: malware	unknown
http://www.ywtxsm.com/rs5b/	true	• Avira URL Cloud: malware	unknown
http://www.peramid.xyz/rs5b/?uyxvg=pPgXS4BiopaVkxB77nB8m5BmJKRgxbtyTgQ51TCNvvWiqwh2ZJ0SiqT/1xVf5TTVOW5skWvYLryZyUzfOZLrBqpWBEotOTgmwg==&L6HRe=HinkmsLDjhA	true	• Avira URL Cloud: malware	unknown
http://www.drkathleensanders.com/rs5b/	true	• Avira URL Cloud: malware	unknown
http://www.locationsbormes.com/rs5b/?uyxvg=5nmvRd2KsNrJ1ILohWvWv9G51OYC+JQySj/wVW5HrbzlASqN8826SlrC1uxl2FZ0KA9XHqewj3KetP3L0XT9wGstOg81NIph5g==&L6HRe=HinkmsLDjhA	true	• Avira URL Cloud: malware	unknown
http://www.isabellagambitta.com/rs5b/?uyxvg=CsXC0bU6YgbK4v/ikU+FR3ZDcTynpB6gZNcuxnLmHu8DrupdLy2Rvx2rp5ka04f5VlwEigsTcDnoyRb/ht4uYCIEoQzcZzfMnw==&L6HRe=HinkmsLDjhA	true	• Avira URL Cloud: phishing	unknown
http://www.ywtxsm.com/rs5b/?uyxvg=CESO3iylK7QUfFCiUFLwHXxmSIHW1gBrGCjGxLpE4g3q3SI6yIOiTvn7qrQa9OdkrAgYihNybI2hWOHGXNYRIortSIS8Lcg0Kg==&L6HRe=HinkmsLDjhA	true	• Avira URL Cloud: malware	unknown
http://www.drkathleensanders.com/rs5b/?uyxvg=Sr3AwP9Ski0v59cQ3JwcPDLo9I+EFZxtPOrHknZVg/8QV/fIqaYOT5hsTQMwMe6TSfps7iDWaOg2o/5pI6PYy1hDK243b9ADKw==&L6HRe=HinkmsLDjhA	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.locationsbormes.com/rs5b/	true	• Avira URL Cloud: malware	unknown
http://www.carcosainvest.com/rs5b/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.starauctioneerspro.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	control.exe, 00000004.00000002.578430894 .0000000002FA5000.00000004.00000020.0002 0000.00000000.sdmp, 10W12dX.4.dr	false		high
http://www.fontbureau.com/designersG	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	10W12dX.4.dr	false		high
http://www.fontbureau.com/designers/?	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.emagrecarapido.store	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ywtxsm.com/rs5b/Pr	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.zzxiaoyuan.com/rs5b/	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zzxiaoyuan.com/rs5b/1	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.amirah.cfd	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	control.exe, 00000004.00000002.578430894 .0000000002FA5000.00000004.00000020.0002 0000.00000000.sdmp, 10W12dX.4.dr	false		high
http://www.tiro.com	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.isabellagambitta.com/rs5b/?uyxvg=CsXC0bU6YgbK4v/ikU	control.exe, 00000004.00000002.582622308 .0000000005388000.00000004.10000000.0004 0000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://www.drkathleensanders.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.notebook-rucksack.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	Shipment_notification.exe, 00000000.00000003.31626 7483.000000000557E000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.amirah.cfd/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.sajatypeworks.com	Shipment_notification.exe, 00000000.00000003.31340 0358.00000000055AD000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.313431498.00000000055 AD000.00000004.00000020.00020000.0000000 0.sdmp, Shipment_notification.exe, 00000000.000000 02.351857642.0000000006782000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com	control.exe, 00000004.00000002.583265968 .00000000073D0000.00000004.00000800.0002 0000.00000000.sdmp, control.exe, 0000000 4.00000002.582622308.000000000583E000.00 000004.10000000.00040000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	Shipment_notification.exe, 00000000.00000003.32268 1699.00000000055AD000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.322630345.00000000055 AD000.00000004.00000020.00020000.0000000 0.sdmp, Shipment_notification.exe, 00000000.000000 03.322651512.0000000005577000.00000004.0 0000020.00020000.00000000.sdmp, Shipment _notification.exe, 00000000.00000003.322604070.000 00000055AD000.00000004.00000020.00020000 .00000000.sdmp, Shipment_notification.exe, 0000000 0.00000003.322780036.000000000557F000.00 000004.00000020.00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.notebook-rucksack.com/rs5b/	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rubyidentity.space/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/b	Shipment_notification.exe, 00000000.00000003.31594 7840.000000000557F000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.isabellagambitta.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.locationsbormes.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.searchvity.com/?dn=	control.exe, 00000004.00000002.582622308 .000000000551A000.00000004.10000000.0004 0000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.rubyidentity.space	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

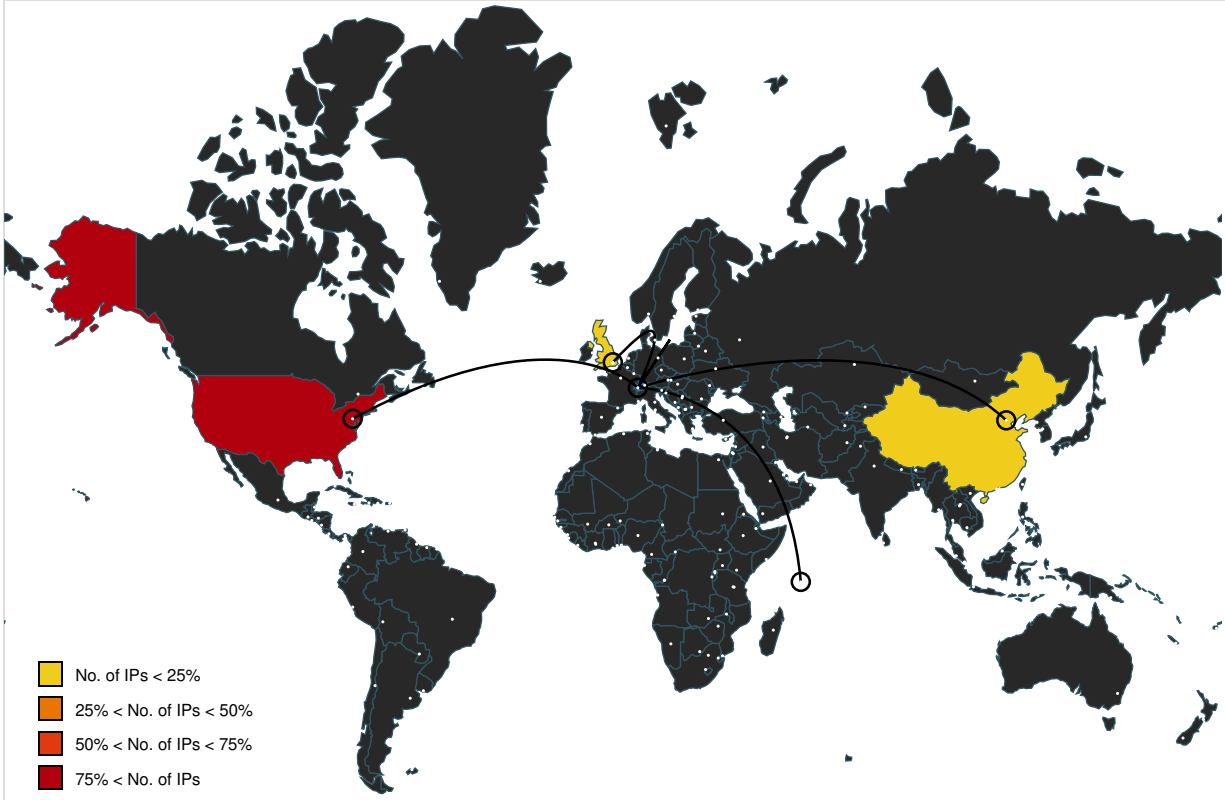
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	Shipment_notification.exe, 00000000.00000003.31621 0305.0000000005579000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000002.351857642.00000000067 82000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.kaj8tfjcmkn7.xyz/rs5b/Q	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.como.	Shipment_notification.exe, 00000000.00000003.31626 7483.000000000557E000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zzxiaoyuan.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carcosainvest.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.notebook-rucksack.com/rs5b/%	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com.Y	Shipment_notification.exe, 00000000.00000003.31340 0358.00000000055AD000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.313431498.00000000055 AD000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.00000000.33941326 0.0000000000921000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000002.577680371.000000000091F000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Shipment_notification.exe, 00000000.00000002.33676 8528.0000000000C67000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000002.351857642.00000000067 82000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.starauctioneerspro.com/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	control.exe, 00000004.00000002.578430894 .0000000002FA5000.00000004.00000020.0002 0000.00000000.sdmp, 10W12dX.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.kaj8tfjcmkn7.xyz	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnv	Shipment_notification.exe, 00000000.00000003.31621 0305.0000000005579000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnx	Shipment_notification.exe, 00000000.00000003.31621 0305.0000000005579000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cni9	Shipment_notification.exe, 00000000.00000003.31534 4428.0000000005576000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.315357516.00000000055 7D000.00000004.00000020.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kaj8tfjcmkn7.xyz/rs5b/	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comz	Shipment_notification.exe, 00000000.00000003.31340 0358.00000000055AD000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.313431498.00000000055 AD000.00000004.00000020.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.tcatelier.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.emagrecarapido.store/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	10W12dX.4.dr	false		high
http://www.zhongyicts.com.cno	Shipment_notification.exe, 00000000.00000003.31621 0305.0000000005579000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piergitarshoes.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	control.exe, 00000004.00000002.578430894 .0000000002FA5000.00000004.00000020.0002 0000.00000000.sdmp, 10W12dX.4.dr	false		high
http://www.fontbureau.comzana	Shipment_notification.exe, 00000000.00000002.33676 8528.0000000000C67000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	control.exe, 00000004.00000002.578430894 .0000000002FA5000.00000004.00000020.0002 0000.00000000.sdmp, 10W12dX.4.dr	false		high
http://www.carterandcone.comn	Shipment_notification.exe, 00000000.00000003.31626 7483.000000000557E000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tcatelier.com/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ywtxsm.com	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	10W12dX.4.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	control.exe, 00000004.00000002.578430894 .0000000002FA5000.00000004.00000020.0002 0000.00000000.sdmp, 10W12dX.4.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.isabellagambitta.com/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://www.53876.world	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.founder.com.cn/cn	Shipment_notification.exe, 00000000.00000003.31534 4428.0000000005576000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.316084822.00000000055 76000.00000004.00000020.00020000.0000000 0.sdmp, Shipment_notification.exe, 00000000.000000 03.316210305.0000000005579000.00000004.0 0000020.00020000.00000000.sdmp, Shipment _notification.exe, 00000000.00000003.315510968.000 0000005576000.00000004.00000020.00020000 .00000000.sdmp, Shipment_notification.exe, 0000000 0.00000003.316267483.000000000557E000.00 000004.00000020.00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.31594 7840.000000000557F000.00000004.00000020. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.315357516.00000000055 7D000.00000004.00000020.00020000.0000000 0.sdmp, Shipment_notification.exe, 00000000.000000 02.351857642.0000000006782000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp, Shipment_notification.exe, 00000000.00000003.320065711.00000000055 AC000.00000004.00000020.00020000.0000000 0.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlP	Shipment_notification.exe, 00000000.00000003.32068 1722.0000000005578000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.carterandcone.comx	Shipment_notification.exe, 00000000.00000003.31626 7483.000000000557E000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.searchvity.com/	control.exe, 00000004.00000002.582622308 .000000000551A000.00000004.10000000.0004 0000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://www.jiyu-kobo.co.jp/	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	Shipment_notification.exe, 00000000.00000003.31621 0305.0000000005579000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Shipment_notification.exe, 00000000.00000002.35185 7642.0000000006782000.00000004.00000800. 00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.53876.world/rs5b/	explorer.exe, 00000003.00000003.57362528 6.000000000884B000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.peramid.xyz	explorer.exe, 00000003.00000003.56196023 0.000000000884D000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.552948713.000000000884D000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.570252381.000000 000884D000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.573625286.000000000884B000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	10W12dX.4.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.177.124.57	www.peramid.xyz	United States		395681	FINALFRONTIERVG	true
206.54.190.30	carcosainvest.com	United States		40824	WZCOM-US	true
154.218.155.8	www.ywtxsm.com	Seychelles		62468	VPSQUANUS	true
185.27.134.217	www.isabellagambitta.com	United Kingdom		34119	WILDCARD-ASWildcardUKLimitedGB	true
66.96.161.158	www.drkathleensanders.com	United States		29873	BIZLAND-SDUS	true
199.59.243.223	www.piergitarshoes.com	United States		395082	BODIS-NJUS	true
45.114.105.2	www.locationsbormes.com	China		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830738
Start date and time:	2023-03-20 16:47:46 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 12m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
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
Sample file name:	Shipment_notification.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@10/3@12/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 66.3% (good quality ratio 58.6%) • Quality average: 70.8% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:48:55	API Interceptor	1x Sleep call for process: Shipment_notification.exe modified
16:49:00	API Interceptor	838x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Shipment_notification.exe.log

Process:	C:\Users\user\Desktop\Shipment_notification.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat

Process:	C:\Windows\explorer.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.2414849034866355
Encrypted:	false
SSDEEP:	24:Yq6CUXyhmbmPlbNdB6hmYmPlz0JahmNmPlHZ6T06Mhm6mPlbxdB6hm3mPl7KTdB2:YqDUXycSNbNdUcVNz0JacQNHZ6T06Mcs
MD5:	4816271302882BDFB06EE40F624169D1
SHA1:	A8F07F0A5940C4A9D4DAD112787FE109CCACA869
SHA-256:	26D30DFFC5E2C493FF97B32C775C98630F0466D49144778BAE2688BA0716C760
SHA-512:	3D46AA6777AF386524E65D8D158201B699F766A5640A3E917CFA78E337475F910A839B93E0097C6651D2FCBE02ED7BFAF9EF8274C9632A88D06985168087823B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"RecentItems":[{"AppID":"Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim","PenUsageSec":15,"LastSwitchedLowPart":4155601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.WindowsMaps_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":4145601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint","PenUsageSec":15,"LastSwitchedLowPart":4135601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","PenUsageSec":15,"LastSwitchedLowPart":4125601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.Windows.Photos_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":4115601904,"LastSwitchedHighPart":30747926,"PrePopulated":true},{"AppID":"Microsoft.Getstarted_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":4105601904,"LastSwitchedHighPart":30747926,"PrePopulated":true}]}

C:\Users\user\AppData\Local\Temp\10W12dX

Process:	C:\Windows\SysWOW64\control.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.287139506398081

Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3 1
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8691620331810155
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Shipment_notification.exe
File size:	772096
MD5:	c310a64af890ac32abff89e86cb53a33
SHA1:	509cdec4d058011fb55535a936e56d3158f3f05a
SHA256:	90e86051c2fb04a3f6fda85273580abca9a9131fb5e32065f620c4410febe1af
SHA512:	095334ee039c7c70b5459b16f1e8d66b56cb7847d3769859182ef5764a8fcb6720cddbc20fc7b5a2c87a6ec4141a70b537e59e27f7fd2ff57c0c325e1b803fce
SSDEEP:	12288:PIrmYMUnFW/NObV55FbasbtrKnnRy50vHKB0otonixVtd/FmQSBhVa8i6NFJHKoR:PIrUUj5FbfVoy5hB0hnixT9FHI04qooW
TLSH:	1AF402206B975636F13523BD85E46296A77EB3A62B13C54D14F212CE1B23F0349D1A3F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..... .....@.. ....@.....

File Icon

Icon Hash:	209480e66eb84902

Static PE Info

General

Entrypoint:	0x4bd0fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6417DEA8 [Mon Mar 20 04:18:48 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbd0a8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x1110	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbbc98	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbb100	0xbb200	False	0.9291656229124916	data	7.877600970637655	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x1110	0x1200	False	0.7309027777777778	data	6.633661427958474	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbe100	0xa79	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbeb8c	0x14	data		
RT_VERSION	0xbebb0	0x360	data		
RT_MANIFEST	0xbef20	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5198.177.124.57470680203145303/20/23-16:50:29.247456	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49706	80	192.168.2.5	198.177.124.57
192.168.2.5199.59.243.22349702802031453 03/20/23-16:50:05.917395	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.5	199.59.243.223
192.168.2.5198.177.124.57470680203141203/20/23-16:50:29.247456	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49706	80	192.168.2.5	198.177.124.57
192.168.2.5154.218.155.849704802031453 03/20/23-16:50:21.020230	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49704	80	192.168.2.5	154.218.155.8
192.168.2.5198.177.124.57470680203144903/20/23-16:50:29.247456	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49706	80	192.168.2.5	198.177.124.57
192.168.2.5154.218.155.849704802031412 03/20/23-16:50:21.020230	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49704	80	192.168.2.5	154.218.155.8
192.168.2.5199.59.243.22349702802031449 03/20/23-16:50:05.917395	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.5	199.59.243.223
192.168.2.5154.218.155.849704802031449 03/20/23-16:50:21.020230	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49704	80	192.168.2.5	154.218.155.8
192.168.2.5199.59.243.22349702802031412 03/20/23-16:50:05.917395	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.5	199.59.243.223

Network Port Distribution

Total Packets: 61

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:49:36.752985954 CET	49695	80	192.168.2.5	185.27.134.217
Mar 20, 2023 16:49:36.798513889 CET	80	49695	185.27.134.217	192.168.2.5
Mar 20, 2023 16:49:36.798667908 CET	49695	80	192.168.2.5	185.27.134.217
Mar 20, 2023 16:49:36.798851013 CET	49695	80	192.168.2.5	185.27.134.217
Mar 20, 2023 16:49:36.846467018 CET	80	49695	185.27.134.217	192.168.2.5
Mar 20, 2023 16:49:36.846508026 CET	80	49695	185.27.134.217	192.168.2.5
Mar 20, 2023 16:49:36.846534014 CET	80	49695	185.27.134.217	192.168.2.5
Mar 20, 2023 16:49:36.846668005 CET	49695	80	192.168.2.5	185.27.134.217
Mar 20, 2023 16:49:36.846815109 CET	49695	80	192.168.2.5	185.27.134.217
Mar 20, 2023 16:49:36.893564939 CET	80	49695	185.27.134.217	192.168.2.5
Mar 20, 2023 16:49:47.305160046 CET	49697	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:47.408058882 CET	80	49697	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:47.409275055 CET	49697	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:47.409413099 CET	49697	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:47.507940054 CET	80	49697	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:47.522320986 CET	80	49697	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:47.522334099 CET	80	49697	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:47.522448063 CET	49697	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:48.911513090 CET	49697	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:49.943849087 CET	49698	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:50.047447920 CET	80	49698	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:50.047601938 CET	49698	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:50.047743082 CET	49698	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:50.153841019 CET	80	49698	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:50.166798115 CET	80	49698	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:50.166841030 CET	80	49698	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:50.167016029 CET	49698	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:50.167174101 CET	49698	80	192.168.2.5	66.96.161.158
Mar 20, 2023 16:49:50.270334959 CET	80	49698	66.96.161.158	192.168.2.5
Mar 20, 2023 16:49:55.218449116 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.362806082 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.363044977 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.363253117 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.507684946 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.599078894 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.599138021 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.599172115 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.599205971 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.599205971 CET	49699	80	192.168.2.5	206.54.190.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:49:55.599307060 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.616341114 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.616391897 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.616436005 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.616446018 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.636303902 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.636338949 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.636357069 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.636382103 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.636410952 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:55.638071060 CET	80	49699	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:55.638227940 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:56.865391970 CET	49699	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:57.958993912 CET	49700	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:58.106313944 CET	80	49700	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:58.106503010 CET	49700	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:58.125310898 CET	49700	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:58.271821976 CET	80	49700	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:58.301676989 CET	80	49700	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:58.301717043 CET	80	49700	206.54.190.30	192.168.2.5
Mar 20, 2023 16:49:58.301903009 CET	49700	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:58.302017927 CET	49700	80	192.168.2.5	206.54.190.30
Mar 20, 2023 16:49:58.448338985 CET	80	49700	206.54.190.30	192.168.2.5
Mar 20, 2023 16:50:03.352196932 CET	49701	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:03.371409893 CET	80	49701	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:03.371604919 CET	49701	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:03.374115944 CET	49701	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:03.393213987 CET	80	49701	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:03.574099064 CET	80	49701	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:03.574167013 CET	80	49701	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:03.574197054 CET	80	49701	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:03.574322939 CET	49701	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:03.589508057 CET	80	49701	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:03.589802980 CET	49701	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:04.881839991 CET	49701	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:05.897761106 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:05.916883945 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:05.917094946 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:05.917395115 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:05.936451912 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:06.120157957 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:06.120187044 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:06.120206118 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:06.120223999 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:06.120419025 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:06.120467901 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:06.120614052 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:06.132888079 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:06.134841919 CET	49702	80	192.168.2.5	199.59.243.223
Mar 20, 2023 16:50:06.141745090 CET	80	49702	199.59.243.223	192.168.2.5
Mar 20, 2023 16:50:17.256160021 CET	49703	80	192.168.2.5	154.218.155.8
Mar 20, 2023 16:50:17.533209085 CET	80	49703	154.218.155.8	192.168.2.5
Mar 20, 2023 16:50:17.533366919 CET	49703	80	192.168.2.5	154.218.155.8
Mar 20, 2023 16:50:17.533485889 CET	49703	80	192.168.2.5	154.218.155.8
Mar 20, 2023 16:50:17.810214996 CET	80	49703	154.218.155.8	192.168.2.5
Mar 20, 2023 16:50:17.879627943 CET	80	49703	154.218.155.8	192.168.2.5
Mar 20, 2023 16:50:17.879694939 CET	80	49703	154.218.155.8	192.168.2.5
Mar 20, 2023 16:50:17.879858017 CET	49703	80	192.168.2.5	154.218.155.8
Mar 20, 2023 16:50:19.728488922 CET	49703	80	192.168.2.5	154.218.155.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:50:20.743052006 CET	49704	80	192.168.2.5	154.218.155.8
Mar 20, 2023 16:50:21.019658089 CET	80	49704	154.218.155.8	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:49:31.670409918 CET	58648	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:49:31.692192078 CET	53	58648	8.8.8.8	192.168.2.5
Mar 20, 2023 16:49:36.711066961 CET	56894	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:49:36.748585939 CET	53	56894	8.8.8.8	192.168.2.5
Mar 20, 2023 16:49:47.181622028 CET	60841	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:49:47.295319080 CET	53	60841	8.8.8.8	192.168.2.5
Mar 20, 2023 16:49:55.184149027 CET	61893	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:49:55.216954947 CET	53	61893	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:03.326172113 CET	60649	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:03.350786924 CET	53	60649	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:11.142652035 CET	51441	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:11.171879053 CET	53	51441	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:12.181365967 CET	49177	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:12.202626944 CET	53	49177	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:17.231201887 CET	49724	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:17.255079031 CET	53	49724	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:26.343081951 CET	61452	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:26.362843990 CET	53	61452	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:34.530338049 CET	65323	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:34.561840057 CET	53	65323	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:51.235682964 CET	51484	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:51.260627031 CET	53	51484	8.8.8.8	192.168.2.5
Mar 20, 2023 16:50:58.838778973 CET	63446	53	192.168.2.5	8.8.8.8
Mar 20, 2023 16:50:58.860341072 CET	53	63446	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:49:31.670409918 CET	192.168.2.5	8.8.8.8	0xa49	Standard query (0)	www.emagrecarapido.store	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:49:36.711066961 CET	192.168.2.5	8.8.8.8	0xb396	Standard query (0)	www.isabellagambitta.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:49:47.181622028 CET	192.168.2.5	8.8.8.8	0x30a5	Standard query (0)	www.drkathleensanders.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:49:55.184149027 CET	192.168.2.5	8.8.8.8	0x94e6	Standard query (0)	www.carcosainvest.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:03.326172113 CET	192.168.2.5	8.8.8.8	0x35e6	Standard query (0)	www.piergitarshoes.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:11.142652035 CET	192.168.2.5	8.8.8.8	0x86ab	Standard query (0)	www.tcatelier.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:12.181365967 CET	192.168.2.5	8.8.8.8	0xddc4	Standard query (0)	www.tcatelier.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:17.231201887 CET	192.168.2.5	8.8.8.8	0xccf9	Standard query (0)	www.ywtxsm.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:26.343081951 CET	192.168.2.5	8.8.8.8	0x51a6	Standard query (0)	www.peramid.xyz	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:34.530338049 CET	192.168.2.5	8.8.8.8	0xcf32	Standard query (0)	www.locationsbormes.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:51.235682964 CET	192.168.2.5	8.8.8.8	0xdeec	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:58.838778973 CET	192.168.2.5	8.8.8.8	0x1301	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false

DNS Answers

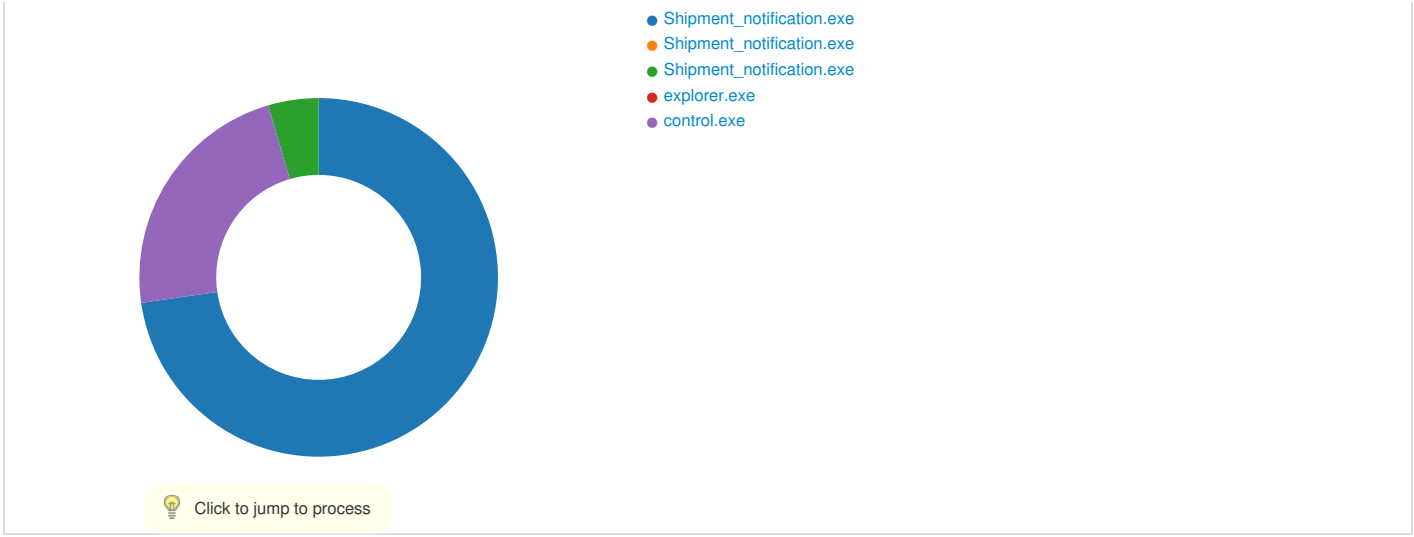
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 16:49:31.692192078 CET	8.8.8.8	192.168.2.5	0xa49	Name error (3)	www.emagrecarapido.store	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:49:36.748585939 CET	8.8.8.8	192.168.2.5	0xb396	No error (0)	www.isabellagambitta.com		185.27.134.217	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:49:47.295319080 CET	8.8.8.8	192.168.2.5	0x30a5	No error (0)	www.drkathleensanders.com		66.96.161.158	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:49:55.216954947 CET	8.8.8.8	192.168.2.5	0x94e6	No error (0)	www.carcosainvest.com	carcosainvest.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 16:49:55.216954947 CET	8.8.8.8	192.168.2.5	0x94e6	No error (0)	carcosainvest.com		206.54.190.30	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:03.350786924 CET	8.8.8.8	192.168.2.5	0x35e6	No error (0)	www.piergitarshoes.com		199.59.243.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:11.171879053 CET	8.8.8.8	192.168.2.5	0x86ab	Name error (3)	www.tcatelier.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:12.202626944 CET	8.8.8.8	192.168.2.5	0xddc4	Name error (3)	www.tcatelier.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:17.255079031 CET	8.8.8.8	192.168.2.5	0xccf9	No error (0)	www.ywtxsm.com		154.218.155.8	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:26.362843990 CET	8.8.8.8	192.168.2.5	0x51a6	No error (0)	www.peramid.xyz		198.177.124.57	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:34.561840057 CET	8.8.8.8	192.168.2.5	0xcf32	No error (0)	www.locationsbormes.com		45.114.105.2	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:51.260627031 CET	8.8.8.8	192.168.2.5	0xdeec	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:50:58.860341072 CET	8.8.8.8	192.168.2.5	0x1301	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.isabellagambitta.com
- www.drkathleensanders.com
- www.carcosainvest.com
- www.piergitarshoes.com
- www.ywtxsm.com
- www.peramid.xyz
- www.locationsbormes.com

Statistics

Behavior



System Behavior

Analysis Process: Shipment_notification.exe PID: 1348, Parent PID: 3324

General

Target ID:	0
Start time:	16:48:46
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Shipment_notification.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Shipment_notification.exe
Imagebase:	0x1a0000
File size:	772096 bytes
MD5 hash:	C310A64AF890AC32ABFF89E86CB53A33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Analysis Process: Shipment_notification.exe PID: 2344, Parent PID: 1348

General

Target ID:	1
Start time:	16:48:57
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Shipment_notification.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Shipment_notification.exe
Imagebase:	0x300000
File size:	772096 bytes
MD5 hash:	C310A64AF890AC32ABFF89E86CB53A33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Shipment_notification.exe PID: 3968, Parent PID: 1348

General	
Target ID:	2
Start time:	16:48:57
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Shipment_notification.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Shipment_notification.exe
Imagebase:	0xfc0000
File size:	772096 bytes
MD5 hash:	C310A64AF890AC32ABFF89E86CB53A33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.377445989.0000000001510000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.377445989.0000000001510000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.377445989.0000000001510000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.377228453.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.377228453.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.377228453.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41E69A	NtReadFile

Analysis Process: explorer.exe PID: **3324**, Parent PID: **3968**

General	
Target ID:	3
Start time:	16:49:00
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **4412**, Parent PID: **3324**

General

Target ID:	4
Start time:	16:49:14
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x880000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.580922850.0000000003170000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.580922850.0000000003170000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.580922850.0000000003170000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.578168386.0000000002E90000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.578168386.0000000002E90000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.578168386.0000000002E90000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.577613473.0000000002920000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000002.577613473.0000000002920000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.577613473.0000000002920000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Shipment_notification.exe	success or wait	1	293C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\10W12dX	object name not found	1	293C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\10W12dX	sharing violation	1	293C947	NtDeleteFile
C:\Users\user\AppData\Local\Temp\10W12dX	sharing violation	1	293C947	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	293C917	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly