ID: 356529
Sample Name: Booking Confirmation.exe
Cookbook: default.jbs
Time: 09:35:52
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

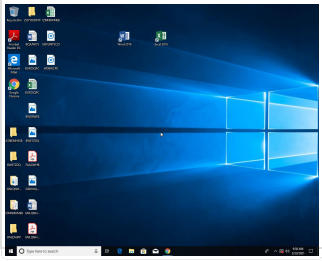
Analysis Report Booking Confirmation.exe

Overview

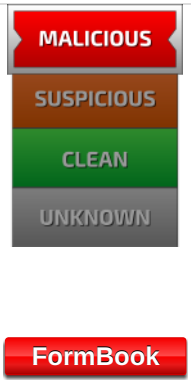
General Information

Sample Name:	Booking Confirmation.exe
Analysis ID:	356529
MD5:	78d9eadc9fcc580..
SHA1:	2bc313ca573a9b..
SHA256:	e836c2aecd7a2a..
Tags:	exe Formbook

Most interesting Screenshot:



Detection



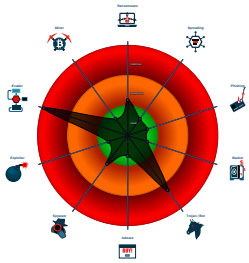
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- Booking Confirmation.exe (PID: 7100 cmdline: 'C:\Users\user\Desktop\Booking Confirmation.exe' MD5: 78D9EADC9FCC580239B360FFA2C2220F)
  - Booking Confirmation.exe (PID: 3716 cmdline: C:\Users\user\Desktop\Booking Confirmation.exe MD5: 78D9EADC9FCC580239B360FFA2C2220F)
  - Booking Confirmation.exe (PID: 612 cmdline: C:\Users\user\Desktop\Booking Confirmation.exe MD5: 78D9EADC9FCC580239B360FFA2C2220F)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - chkdsk.exe (PID: 5072 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
        - cmd.exe (PID: 7024 cmdline: /c del 'C:\Users\user\Desktop\Booking Confirmation.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.evolvekitchendesign.com/ffw/"
  ],
  "decoy": [
    "unmutedgenerations.com",
    "localmoversuae.com",
    "centralrea.com",
    "geyyfphzoe.com",
    "silverpackfactory.com",
    "techtronixx.com",
    "shop-deinen-deal.com",
    "buehne.cloud",
    "inspirefreedomtoday.com",
    "chapelcouture.com",
    "easton-taiwan.com",
    "quanaonudep.store",
    "merzigomusic.com",
    "wpzoomin.com",
    "service-lkytrsahdfpedf.com",
    "yeasuc.com",
    "mydogtrainingservice.com",
    "galeribisnisonline.com",
    "cscremodeling.com",
    "bom-zzxx.com",
    "ensobet88.com",
    "vegancto.com",
    "digivisiol.com",
    "advancetools.net",
    "gzqyjd.com",
    "xtgnsl.com",
    "ftfortmyers.com",
    "g-siqueira.com",
    "ufdzbhrxk.icu",
    "tiekotiin.com",
    "youschrutedit.com",
    "takahatadenkikouji.com",
    "goodfastco.com",
    "jtelitetraining.com",
    "planet-hype.com",
    "gigwindow.com",
    "levelxpr.com",
    "besttechmobcomm.info",
    "funneldesigngenie.com",
    "mylisting.cloud",
    "alltwoyou.com",
    "mortgagesandprotection.online",
    "monthlydigest.info",
    "senlangdq.com",
    "postphenomenon.com",
    "slymwhite.com",
    "masonpreschool.com",
    "wahooshop.com",
    "meridiangummies.com",
    "samsungpartsdept.com",
    "saludbellezaybienestar.net",
    "vickifoxproductions.com",
    "shawandwesson.info",
    "nutrepele.com",
    "gorillatanks.com",
    "praktijkinfinity.online",
    "lanteredam.com",
    "refinedmanagement.com",
    "tiwapay.com",
    "fruitsinbeers.com",
    "charliekay.net",
    "realironart.com",
    "sonsofmari.com",
    "kedingtonni.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.670983591.0000000002591000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.709997867.0000000001500000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.709997867.0000000001500000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.709997867.0000000001500000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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
00000008.00000002.912607132.0000000004920000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

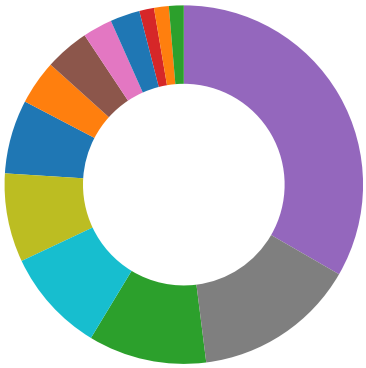
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.Booking Confirmation.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.Booking Confirmation.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.Booking Confirmation.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
0.2.Booking Confirmation.exe.36e45e0.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Booking Confirmation.exe.36e45e0.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x13bbb8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13be32:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1689f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x168c72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x147955:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x174795:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x147441:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x174281:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a57:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x174897:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x147bcf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x174a0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x13c84a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16968a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1466bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1734fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x13d543:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x16a383:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x14d5f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x17a437:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x14e5fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

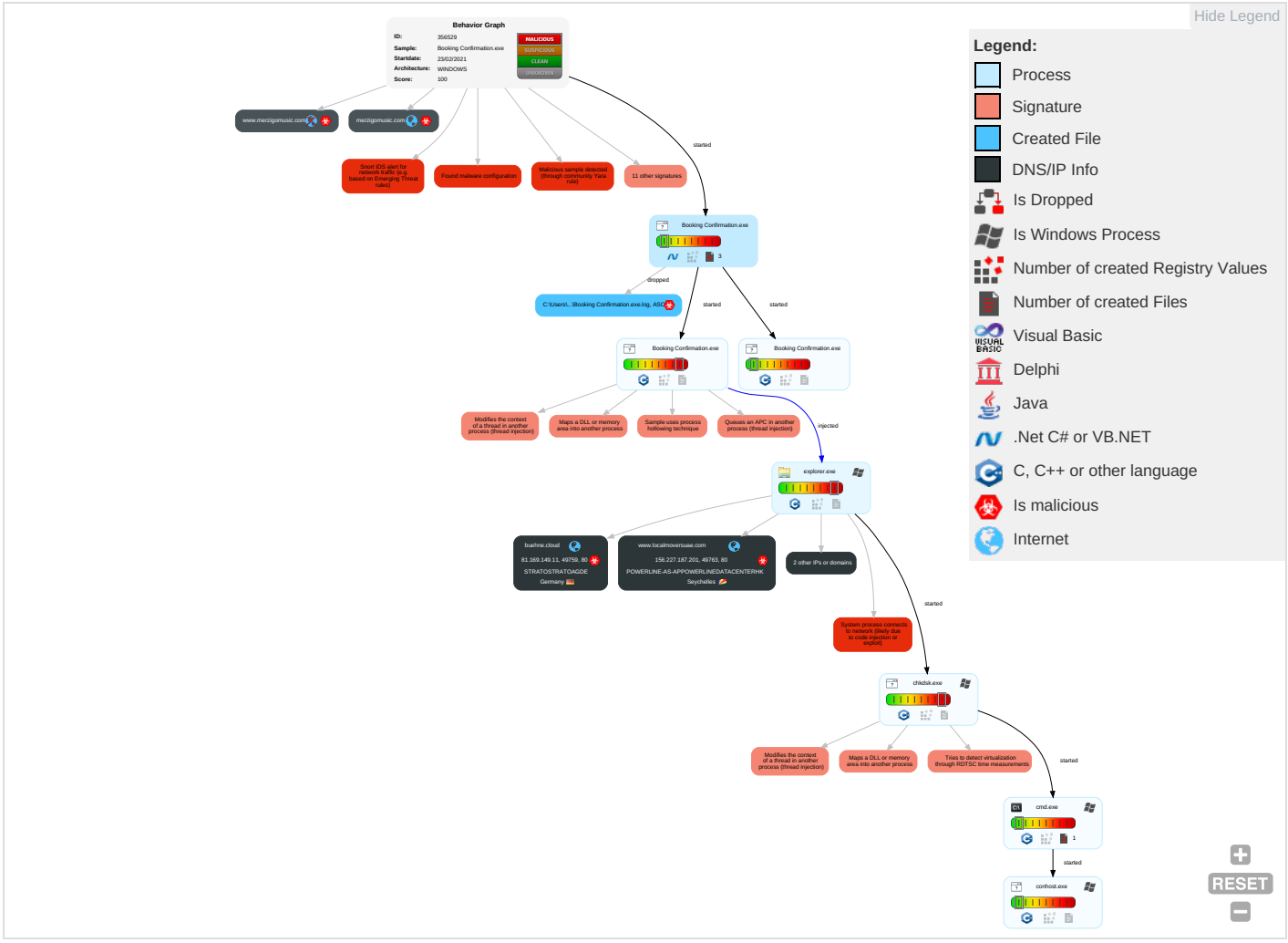
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 1 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Explo Redir Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

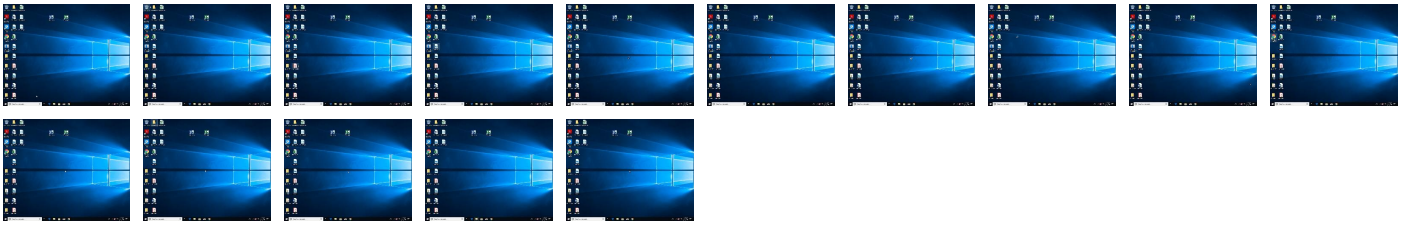
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Booking Confirmation.exe	33%	ReversingLabs	Win32.Trojan.AgentTesla	
Booking Confirmation.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Booking Confirmation.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.buehne.cloud/ffw/?MZg8=i2wbx/M7rrWGhnBeYdMUQ+oEsm11dU48NWkvE2U6RCUjjqrjMq6tqVdU8V2lO/H9m4oS&uTxXc=ojO0dJK0Hv	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coms	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://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	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.founder.com.cn/cnE	0%	Avira URL Cloud	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.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.founder.com.cn/cnht	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://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	
www.evolvekitchendesign.com/ffw/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.tiro.comym	0%	Avira URL Cloud	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.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sajatypeworks.come	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	
http://www.praktijkinfinity.online/ffw/?MZg8=QtqTw2GyYxf2WyRFtpmSmJJvhnrw03uNROtSydYnJk3JDRiYk6bsvXWgtuf5tlEJcMN+&uTxXc=ojO0dJK0Hv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.localmoversuae.com	156.227.187.201	true	true		unknown
www.praktijkinfinity.online	185.175.200.247	true	true		unknown
buehne.cloud	81.169.149.11	true	true		unknown
merzigomusic.com	34.102.136.180	true	true		unknown
www.buehne.cloud	unknown	unknown	true		unknown
www.merzigomusic.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.buehne.cloud/ffw/?MZg8=i2wbx/M7rrWGhnBeYdMUQ+oEsm11dU48NWkvE2U6RCUjjqrjMq6tqVdU8V2lO/H9m4oS&uTxXc=ojO0dJK0Hv	true	• Avira URL Cloud: safe	unknown
www.evolvekitchendesign.com/ffw/	true	• Avira URL Cloud: safe	low
http://www.praktijkinfinity.online/ffw/?MZg8=QtqTw2GyYxf2WyRFtpmSmJJvhnrw03uNROtSydYnJk3JDRiYk6bsvXWgtuf5tlEJcMN+&uTxXc=ojO0dJK0Hv	true	• Avira URL Cloud: safe	unknown

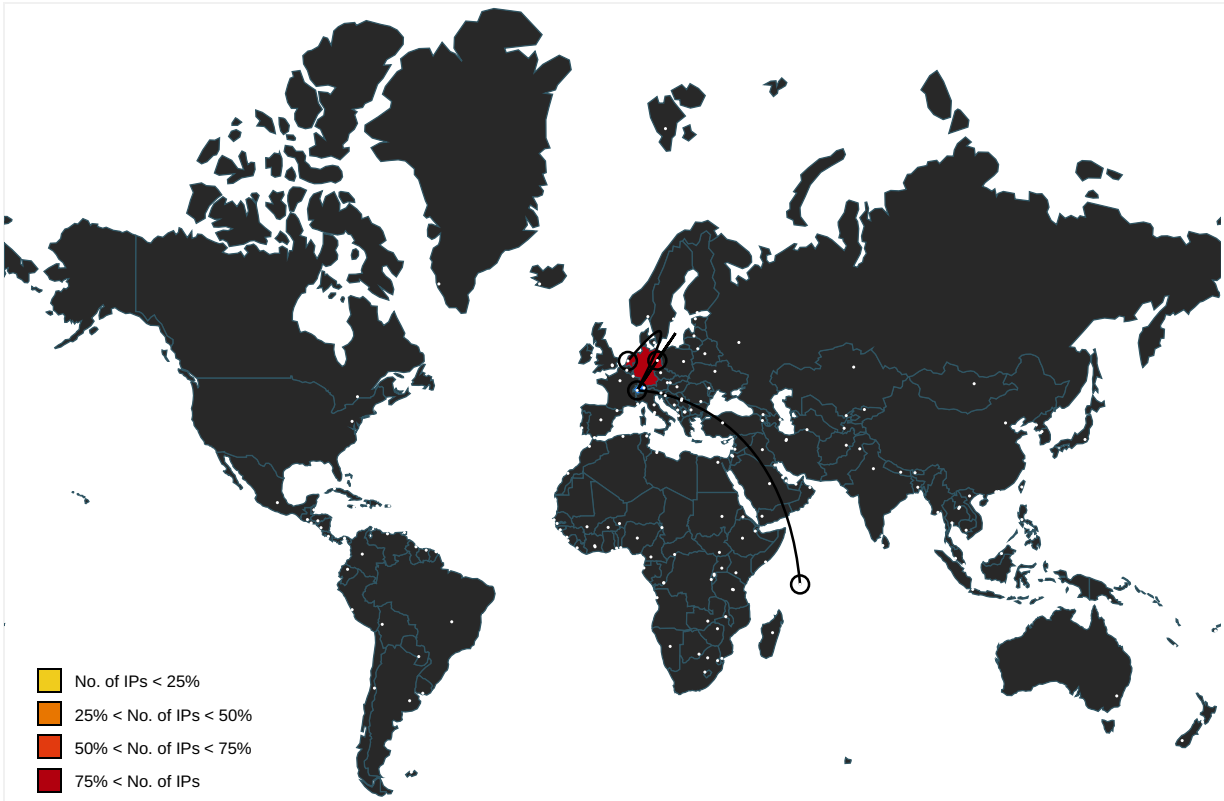
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Booking Confirmation.exe, 00000000.00000002.676021745.0000000006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695698069.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Booking Confirmation.exe, 00000000.00000002.676021745.0000000006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695698069.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Booking Confirmation.exe, 00000000.00000002.676021745.0000000006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695698069.000000000B970000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Booking Confirmation.exe, 00000000.00000002.676021745.0000000006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695698069.000000000B970000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Booking Confirmation.exe, 00000000.00000002.676021745.0000000006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695698069.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comt	Booking Confirmation.exe, 00000000.00000003.649430535.0000000005723000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.coms	Booking Confirmation.exe, 0000 0000.00000003.649430535.000000 0005723000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.0000000 0.695698069.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.0000000 0.695698069.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Booking Confirmation.exe, 0000 0000.00000002.670983591.000000 0002591000.00000004.00000001.sdmp	false		high
http://en.w	Booking Confirmation.exe, 0000 0000.00000003.650111317.000000 0005725000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnE	Booking Confirmation.exe, 0000 0000.00000003.652141962.000000 0005728000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Booking Confirmation.exe, 0000 0000.00000003.649430535.000000 0005723000.00000004.00000001.sdmp, Booking Confirmation.exe, 00000000. 00000002.676021745.00000000069 32000.00000004.00000001.sdmp, explorer.exe, 00000006.0000000 0.695698069.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Booking Confirmation.exe, 0000 0000.00000003.652141962.000000 0005728000.00000004.00000001.sdmp, Booking Confirmation.exe, 00000000. 00000003.652187363.00000000057 26000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnht	Booking Confirmation.exe, 0000 0000.00000003.651858652.000000 000572E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Booking Confirmation.exe, 0000 0000.00000003.652141962.000000 0005728000.00000004.00000001.sdmp, Booking Confirmation.exe, 00000000. 00000003.651977805.00000000057 27000.00000004.00000001.sdmp, explorer.exe, 00000006.0000000 0.695698069.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000006.0000000 2.914045803.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.tiro.comym	Booking Confirmation.exe, 0000 0000.00000003.651298106.000000 000573B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false		high
http://www.sandoll.co.kr	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.	Booking Confirmation.exe, 0000 0000.00000003.653249672.000000 0005728000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.come	Booking Confirmation.exe, 0000 0000.00000003.649430535.000000 0005723000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Booking Confirmation.exe, 0000 0000.00000002.676021745.000000 0006932000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.695 698069.000000000B970000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.169.149.11	unknown	Germany		6724	STRATOSTRATOAGDE	true
156.227.187.201	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
185.175.200.247	unknown	Netherlands		48635	ASTRALUSNL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356529
Start date:	23.02.2021
Start time:	09:35:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Booking Confirmation.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/1@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.7% (good quality ratio 13.9%) • Quality average: 71.4% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 51.104.139.180, 52.255.188.83, 104.42.151.234, 92.122.145.220, 40.88.32.150, 52.147.198.201, 13.64.90.137, 93.184.221.240, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356529/sample/Booking Confirmation.exe

Simulations

Behavior and APIs

Time	Type	Description
09:36:48	API Interceptor	1x Sleep call for process: Booking Confirmation.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	lpdKSOB78u.exe	Get hash	malicious	Browse	• 154.213.108.250
	4pFzkB6ePK.exe	Get hash	malicious	Browse	• 154.201.205.155
	NewOrder.xlsm	Get hash	malicious	Browse	• 154.201.205.155
	Order83930.exe	Get hash	malicious	Browse	• 154.215.106.100
	RFQ for Marjan Development Program.exe	Get hash	malicious	Browse	• 154.86.32.52
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	• 156.227.188.203
	SHED.EXE	Get hash	malicious	Browse	• 154.213.100.41
	wFzMy6hehS.exe	Get hash	malicious	Browse	• 192.151.233.118
	INCHAP_Invoice_21.xlsx	Get hash	malicious	Browse	• 192.151.233.118
	ffOWE185KP.exe	Get hash	malicious	Browse	• 192.151.233.118
	mWxzYlRCUi.exe	Get hash	malicious	Browse	• 192.151.233.118
	Cargo_remitP170201.xlsx	Get hash	malicious	Browse	• 192.151.233.118
	quotations pdf.exe	Get hash	malicious	Browse	• 156.243.221.75
	Project.pdf.exe	Get hash	malicious	Browse	• 154.213.241.19
	order pdf.exe	Get hash	malicious	Browse	• 156.252.99.134
	YCVj3q7r5e.exe	Get hash	malicious	Browse	• 192.151.255.12
	th520.exe	Get hash	malicious	Browse	• 103.75.46.74
	DHL Parcel Details.xlsx	Get hash	malicious	Browse	• 154.216.241.144
	DCSGROUP.xlsx	Get hash	malicious	Browse	• 160.124.66.18
	purchase order doc.exe	Get hash	malicious	Browse	• 154.201.177.118
STRATOSTRATOAGDE	PO 20211602.xlsm	Get hash	malicious	Browse	• 81.169.145.88
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 81.169.181.88
	Io8ic2291n.doc	Get hash	malicious	Browse	• 85.214.26.7
	gSvUGC0OzV.exe	Get hash	malicious	Browse	• 81.169.145.90
	DHL Documents_AWB_001173980920AD.xlsx	Get hash	malicious	Browse	• 81.169.145.143
	nzGUqSK11D.exe	Get hash	malicious	Browse	• 85.214.228.140
	FastClient_i_r756196528.exe	Get hash	malicious	Browse	• 85.214.219.2
	PO210121.exe	Get hash	malicious	Browse	• 81.169.145.90
	_RFQ_MVSEASAIL_34.xlsx	Get hash	malicious	Browse	• 81.169.145.68
	0iEsxw3D7A.exe	Get hash	malicious	Browse	• 81.169.145.143
	2021_50SG0BK00T1,pdf.exe	Get hash	malicious	Browse	• 81.169.145.150
	6gg4UwrN3I.exe	Get hash	malicious	Browse	• 81.169.145.82
	RFV9099311042.exe	Get hash	malicious	Browse	• 81.169.145.64
	MR727043761.doc	Get hash	malicious	Browse	• 81.169.145.175
	SecuriteInfo.com.VB.Trojan.Downloader.JVAZ.20129.doc	Get hash	malicious	Browse	• 81.169.145.175
	SecuriteInfo.com.Mal.DocDl-K.8726.doc	Get hash	malicious	Browse	• 81.169.145.175
	LX0950180213.doc	Get hash	malicious	Browse	• 81.169.145.175
	5j6RsnL8zx.exe	Get hash	malicious	Browse	• 81.169.145.143
	099898892.exe	Get hash	malicious	Browse	• 81.169.145.74
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 81.169.145.152

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Booking Confirmation.exe.log	
Process:	C:\Users\user\Desktop\Booking Confirmation.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94E4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.457054361780353
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Booking Confirmation.exe
File size:	510976
MD5:	78d9eadc9fcc580239b360ffa2c2220f
SHA1:	2bc313ca573a9be005aa8d22e96601c10dcd5041
SHA256:	e836c2aecd7a2ae83a5bb088780d9e7b8cd6c3a7ff6b9c3f1261bfd1f53dbef7
SHA512:	60858a1b0c966c7e2bbc5b4a86ca0023da5d4bf8d68331c8290e9a57d97e14e5c50d26bca22461301bdcbdd48ac85b2652fb0545931a43ebe0a497dd115a5c3d
SSDEEP:	12288:guB7EQbDmPXvcNGIdjKD8WMxSNyPww1rqGGRzacQA+xE6:r7EQOPQdW85yyx1eRLQLT
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....G4`.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47d6ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60344790 [Tue Feb 23 00:08:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7d69c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0xff8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x80000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7b6f4	0x7b800	False	0.765528134489	data	7.4686220922	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0xff8	0x1000	False	0.40234375	data	5.00072933657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7e090	0x344	data		
RT_MANIFEST	0x7e3e4	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	IConnectionPoint.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	IConnectionPoint.exe

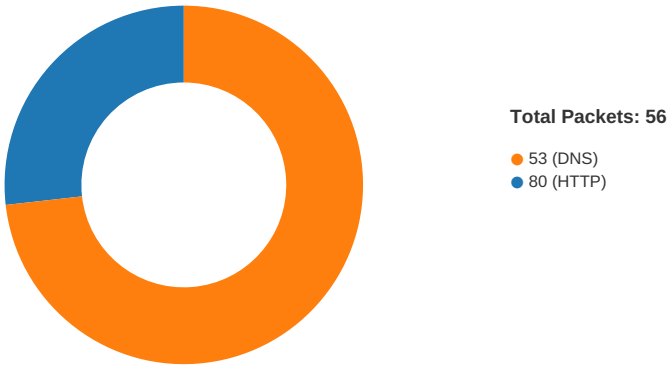
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:38:51.562647	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	34.102.136.180
02/23/21-09:38:51.562647	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:38:51.562647	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	34.102.136.180
02/23/21-09:38:51.702716	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49764	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:37:49.125511885 CET	49759	80	192.168.2.4	81.169.149.11
Feb 23, 2021 09:37:49.178277969 CET	80	49759	81.169.149.11	192.168.2.4
Feb 23, 2021 09:37:49.178462029 CET	49759	80	192.168.2.4	81.169.149.11
Feb 23, 2021 09:37:49.178663015 CET	49759	80	192.168.2.4	81.169.149.11
Feb 23, 2021 09:37:49.232486963 CET	80	49759	81.169.149.11	192.168.2.4
Feb 23, 2021 09:37:49.254631042 CET	80	49759	81.169.149.11	192.168.2.4
Feb 23, 2021 09:37:49.254662037 CET	80	49759	81.169.149.11	192.168.2.4
Feb 23, 2021 09:37:49.254834890 CET	49759	80	192.168.2.4	81.169.149.11
Feb 23, 2021 09:37:49.254900932 CET	49759	80	192.168.2.4	81.169.149.11
Feb 23, 2021 09:37:49.307396889 CET	80	49759	81.169.149.11	192.168.2.4
Feb 23, 2021 09:38:10.061094046 CET	49760	80	192.168.2.4	185.175.200.247
Feb 23, 2021 09:38:10.113087893 CET	80	49760	185.175.200.247	192.168.2.4
Feb 23, 2021 09:38:10.113182068 CET	49760	80	192.168.2.4	185.175.200.247
Feb 23, 2021 09:38:10.113603115 CET	49760	80	192.168.2.4	185.175.200.247
Feb 23, 2021 09:38:10.165286064 CET	80	49760	185.175.200.247	192.168.2.4
Feb 23, 2021 09:38:10.166449070 CET	80	49760	185.175.200.247	192.168.2.4
Feb 23, 2021 09:38:10.166481972 CET	80	49760	185.175.200.247	192.168.2.4
Feb 23, 2021 09:38:10.166639090 CET	49760	80	192.168.2.4	185.175.200.247
Feb 23, 2021 09:38:10.166727066 CET	49760	80	192.168.2.4	185.175.200.247
Feb 23, 2021 09:38:10.218425989 CET	80	49760	185.175.200.247	192.168.2.4
Feb 23, 2021 09:38:30.565995932 CET	49763	80	192.168.2.4	156.227.187.201
Feb 23, 2021 09:38:30.916510105 CET	80	49763	156.227.187.201	192.168.2.4
Feb 23, 2021 09:38:30.918800116 CET	49763	80	192.168.2.4	156.227.187.201
Feb 23, 2021 09:38:30.918850899 CET	49763	80	192.168.2.4	156.227.187.201
Feb 23, 2021 09:38:31.270864010 CET	80	49763	156.227.187.201	192.168.2.4
Feb 23, 2021 09:38:31.277004004 CET	80	49763	156.227.187.201	192.168.2.4
Feb 23, 2021 09:38:31.277348042 CET	49763	80	192.168.2.4	156.227.187.201
Feb 23, 2021 09:38:31.277414083 CET	49763	80	192.168.2.4	156.227.187.201
Feb 23, 2021 09:38:31.627831936 CET	80	49763	156.227.187.201	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:36:33.365729094 CET	64646	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:33.401702881 CET	65298	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:33.414359093 CET	53	64646	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:33.450438023 CET	53	65298	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:36:34.358023882 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:34.406892061 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:35.323983908 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:35.375597000 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:36.211026907 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:36.259768009 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:37.460362911 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:37.466555119 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:37.508991003 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:37.528747082 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:49.565480947 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:49.614151955 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:50.378268003 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:50.430069923 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:51.610858917 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:51.659547091 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:52.969223022 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:53.020847082 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:53.968452930 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:54.019956112 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:54.753613949 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:54.802546024 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:56.450119972 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:56.498850107 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:58.389504910 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:58.451144934 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 09:36:59.244559050 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:36:59.296053886 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:00.205465078 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:00.255317926 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:07.391791105 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:07.440401077 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:19.035537958 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:19.087325096 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:20.023345947 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:20.072021961 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:21.322374105 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:21.371100903 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:22.515489101 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:22.567611933 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:28.024101019 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:28.081237078 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:31.836255074 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:31.898824930 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:33.834634066 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:33.908302069 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:34.645555973 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:34.705548048 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:35.134004116 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:35.196948051 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:35.743684053 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:35.800733089 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:36.325404882 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:36.382463932 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:36.594090939 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:36.665523052 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:36.963715076 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:37.012460947 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:37.777667046 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:37.836175919 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:38.772792101 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:38.831108093 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:39.264177084 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:39.322266102 CET	53	59172	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:37:46.320043087 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:46.378277063 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 09:37:49.056421041 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:37:49.118174076 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 09:38:09.971204042 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:38:10.059891939 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 09:38:21.682096004 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:38:21.730724096 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 09:38:23.595087051 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:38:23.652355909 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 09:38:30.350929976 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:38:30.564515114 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 09:38:51.433300018 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 09:38:51.520318985 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:37:49.056421041 CET	192.168.2.4	8.8.8.8	0x589e	Standard query (0)	www.buehne.cloud	A (IP address)	IN (0x0001)
Feb 23, 2021 09:38:09.971204042 CET	192.168.2.4	8.8.8.8	0x43ad	Standard query (0)	www.praktijkinfinity.online	A (IP address)	IN (0x0001)
Feb 23, 2021 09:38:30.350929976 CET	192.168.2.4	8.8.8.8	0x312	Standard query (0)	www.localmoversuae.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:38:51.433300018 CET	192.168.2.4	8.8.8.8	0xcc80	Standard query (0)	www.merzigomusic.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:37:49.118174076 CET	8.8.8.8	192.168.2.4	0x589e	No error (0)	www.buehne.cloud	buehne.cloud		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:37:49.118174076 CET	8.8.8.8	192.168.2.4	0x589e	No error (0)	buehne.cloud		81.169.149.11	A (IP address)	IN (0x0001)
Feb 23, 2021 09:38:10.059891939 CET	8.8.8.8	192.168.2.4	0x43ad	No error (0)	www.praktijkinfinity.online		185.175.200.247	A (IP address)	IN (0x0001)
Feb 23, 2021 09:38:30.564515114 CET	8.8.8.8	192.168.2.4	0x312	No error (0)	www.localmoversuae.com		156.227.187.201	A (IP address)	IN (0x0001)
Feb 23, 2021 09:38:51.520318985 CET	8.8.8.8	192.168.2.4	0xcc80	No error (0)	www.merzigomusic.com	merzigomusic.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:38:51.520318985 CET	8.8.8.8	192.168.2.4	0xcc80	No error (0)	merzigomusic.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.buehne.cloud
- www.praktijkinfinity.online
- www.localmoversuae.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49759	81.169.149.11	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:37:49.178663015 CET	5031	OUT	GET /ffw/?MZg8=i2wbx/M7rrWGhnBeYdMUQ+oEsm11dU48NWkvE2U6RCUjjqrjMq6tqVdU8V2lO/H9m4oS&uTxXc=ojO0dJK0Hv HTTP/1.1 Host: www.buehne.cloud Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:37:49.254631042 CET	5033	IN	HTTP/1.1 302 Found Date: Tue, 23 Feb 2021 08:37:49 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://buehne.cloud/ffw/?MZg8=i2wbx/M7rrWGhnBeYdMUQ+oEsm11dU48NWkvE2U6RCUjjqrjMq6tqVdU8V2lO/H9m4oS&uTxXc=ojO0dJK0Hv Content-Length: 386 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 75 65 68 6e 65 2e 63 6c 6f 75 64 2f 66 66 77 2f 3f 4d 5a 67 38 3d 69 32 77 62 78 2f 4d 37 72 72 57 47 68 6e 42 65 59 64 4d 55 51 2b 6f 45 73 6d 31 31 64 55 34 38 4e 57 6b 76 45 32 55 36 52 43 55 6a 6a 71 72 6a 4d 71 36 74 71 56 64 55 38 56 32 6c 4f 2f 48 39 6d 34 6f 53 26 61 6d 70 3b 75 54 78 58 63 3d 6f 6a 4f 30 64 4a 4b 30 48 76 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 62 75 65 68 6e 65 2e 63 6c 6f 75 64 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.buehne.cloud Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49760	185.175.200.247	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:38:10.113603115 CET	6257	OUT	GET /ffw/?MZg8=QtqTw2GyYxf2WyRFtpmSmJJvhnrw03uNROtSydYnJk3JDRiYk6bsvXWgtuf5tlEJcMN+&uTxXc=ojO0dJK0Hv HTTP/1.1 Host: www.praktijkinfinity.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:38:10.166449070 CET	6258	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 08:38:10 GMT Server: Apache/2 Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Transfer-Encoding: chunked Content-Type: text/html Data Raw: 39 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 0d 0a 38 62 0d 0a 2f 66 66 77 2f 3f 4d 5a 67 38 3d 51 74 71 54 77 32 47 79 59 78 66 32 57 79 52 46 74 70 6d 53 6d 4a 4a 76 68 6e 72 77 30 33 75 4e 52 4f 74 53 79 64 59 6e 4a 6b 33 4a 44 52 69 59 6b 36 62 73 76 58 57 67 74 75 66 35 74 6c 45 4a 63 4d 4e 2b 26 61 6d 70 3b 75 54 78 58 63 3d 6f 6a 4f 30 64 4a 4b 30 48 76 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0a 3c 48 52 3e 0a 3c 49 3e 0d 0a 31 32 62 0d 0a 77 77 77 2e 70 72 61 6b 74 69 6a 6b 69 6e 66 69 6e 69 74 79 2e 6f 6e 6c 69 6e 65 3c 2f 49 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 90<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL 8b/ffw/?MZg8=QtqTw2GyYxf2WyRFtpmSmJJvhnrw03uNROtSydYnJk3JDRiYk6bsvXWgtuf5tlEJcMN+&uTxXc=ojO0dJK0Hv was not found on this server.<HR><I>12bwww.praktijkinfinity.online</I></BODY></HTML>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49763	156.227.187.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:38:30.918850899 CET	6278	OUT	GET /ffw/?MZg8=vCSLLgJGCp79MzLYydBa+Bsk3bm2BxHz5ofTxOlO5FwRAAdXOpMXkN2jq+v+BBk+R2pe&uTxXc=ojO0dJK0Hv HTTP/1.1 Host: www.localmoversuae.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

User Modules

Hook Summary

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

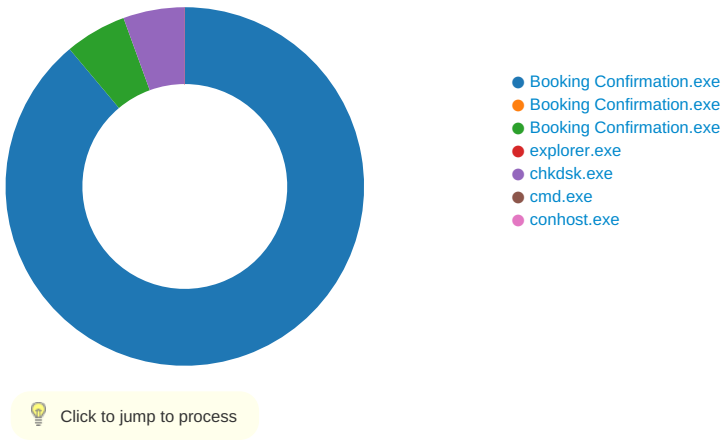
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE0

Statistics

Behavior



System Behavior

Analysis Process: Booking Confirmation.exe PID: 7100 Parent PID: 5844

General

Start time:	09:36:40
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Booking Confirmation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Booking Confirmation.exe'
Imagebase:	0x2c0000
File size:	510976 bytes
MD5 hash:	78D9EADC9FCC580239B360FFA2C2220F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.670983591.0000000002591000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.671285373.0000000003599000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.671285373.0000000003599000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.671285373.0000000003599000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D16CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D16CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Booking Confirmation.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D47C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Booking Confirmation.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D47C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D145705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D145705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D14CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D145705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D145705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFB1B4F	ReadFile

Analysis Process: Booking Confirmation.exe PID: 3716 Parent PID: 7100

General

Start time:	09:36:50
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Booking Confirmation.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Booking Confirmation.exe
Imagebase:	0x2d0000
File size:	510976 bytes
MD5 hash:	78D9EADC9FCC580239B360FFA2C2220F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Booking Confirmation.exe PID: 612 Parent PID: 7100

General

Start time:	09:36:50
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Booking Confirmation.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Booking Confirmation.exe
Imagebase:	0xdc0000
File size:	510976 bytes
MD5 hash:	78D9EADC9FCC580239B360FFA2C2220F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.709997867.0000000001500000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.709997867.0000000001500000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.709997867.0000000001500000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.709520780.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.709520780.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.709520780.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.709963590.00000000014D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.709963590.00000000014D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.709963590.00000000014D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3424 Parent PID: 612

General

Start time:	09:36:52
Start date:	23/02/2021
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: chkdsk.exe PID: 5072 Parent PID: 3424

General

Start time:	09:37:05
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x2e0000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
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: 00000008.00000002.912607132.0000000004920000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.912607132.0000000004920000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.912607132.0000000004920000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.912770256.0000000004A80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.912770256.0000000004A80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.912770256.0000000004A80000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.912146154.0000000004320000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.912146154.0000000004320000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.912146154.0000000004320000.00000040.00000001.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	4339E57	NtReadFile

Analysis Process: cmd.exe PID: 7024 Parent PID: 5072

General

Start time:	09:37:10
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Booking Confirmation.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6952 Parent PID: 7024

General

Start time:	09:37:11
Start date:	23/02/2021
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