ID: 502233
Sample Name: EXPORT INVOICE 2021.exe
Cookbook: default.jbs
Time: 18:20:09
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

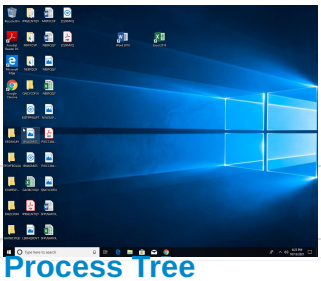
Windows Analysis Report EXPORT INVOICE 2021.exe

Overview

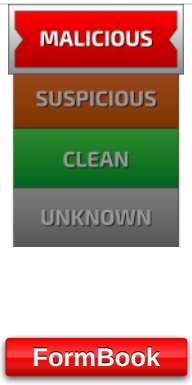
General Information

Sample Name:	EXPORT INVOICE 2021.exe
Analysis ID:	502233
MD5:	54bb8fbbfe0a665..
SHA1:	0b97e4463c76df4.
SHA256:	3bd841c6957e9fd.
Tags:	exe xloader
Infos:	

Most interesting Screenshot:



Detection



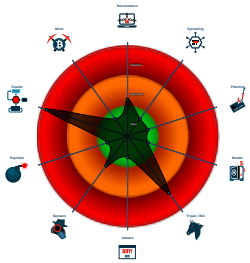
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- EXPORT INVOICE 2021.exe (PID: 7128 cmdline: 'C:\Users\user\Desktop\EXPORT INVOICE 2021.exe' MD5: 54BB8FBBFE0A665CA59579A0240CE2F0)
  - EXPORT INVOICE 2021.exe (PID: 5548 cmdline: {path} MD5: 54BB8FBBFE0A665CA59579A0240CE2F0)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 1688 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 5860 cmdline: /c del 'C:\Users\user\Desktop\EXPORT INVOICE 2021.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.vulcanopresale.icu/mqi9/"
  ],
  "decoy": [
    "spectehnika-rb.com",
    "daleproaudio.xyz",
    "cpw887.com",
    "gosbs-b01.com",
    "clarkmanagementhawaii.com",
    "taobaoi68.xyz",
    "hoppedchardonnay.com",
    "extremesavings.net",
    "newbiepanda.com",
    "arul-jegadish.com",
    "kellibrat.com",
    "avto-mercury.info",
    "percussionportal.com",
    "colorfulworldpublishing.com",
    "notvaccinatedjobs.com",
    "cattavida.com",
    "pioniersa.com",
    "yanduy.com",
    "mzjing.com",
    "piedmontpines.school",
    "sosibibyslot.space",
    "yfly635.xyz",
    "undauntedearth.com",
    "ratqueen.art",
    "docomoat.xyz",
    "themysticalmushroom.com",
    "woodbinecommunityplan.com",
    "al-m3hd.com",
    "globalglodpower.com",
    "circuitboardsolution.com",
    "zoipartner.com",
    "varibat45.com",
    "sean-inspires.com",
    "533hd.com",
    "yuezhong66.com",
    "latewood.xyz",
    "mrsparberrysplace.com",
    "shyy-life.com",
    "znypay.com",
    "eludice.net",
    "kalitelihavaperdesi.com",
    "classicmusclecargarage.com",
    "divulgesloatr.xyz",
    "djkozmos.com",
    "eazyjspowerwash.com",
    "xn--naturecan-823hqc4t8089b.xyz",
    "merchediazcobo.com",
    "09mpt.xyz",
    "zapoartist.quest",
    "vagusartesaniaymoda.online",
    "blogbynasir.com",
    "cliffwoof.com",
    "aj03yansinbiz.biz",
    "gaboshoes.com",
    "italiangomvqs.xyz",
    "safari-fadel.com",
    "diorbijoux.com",
    "lookforwardswiss.com",
    "qsygqc.com",
    "wehaveunconditionallove.com",
    "kingsmeadfarm.com",
    "928711.com",
    "saint444.com",
    "fashiona.space"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.797159788.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.797159788.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.797159788.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.936050522.00000000004D0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.936050522.00000000004D0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$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
2.2.EXPORT INVOICE 2021.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.EXPORT INVOICE 2021.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.EXPORT INVOICE 2021.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
2.2.EXPORT INVOICE 2021.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.EXPORT INVOICE 2021.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: CMSTP Execution Process Creation

Jbx Signature Overview

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:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

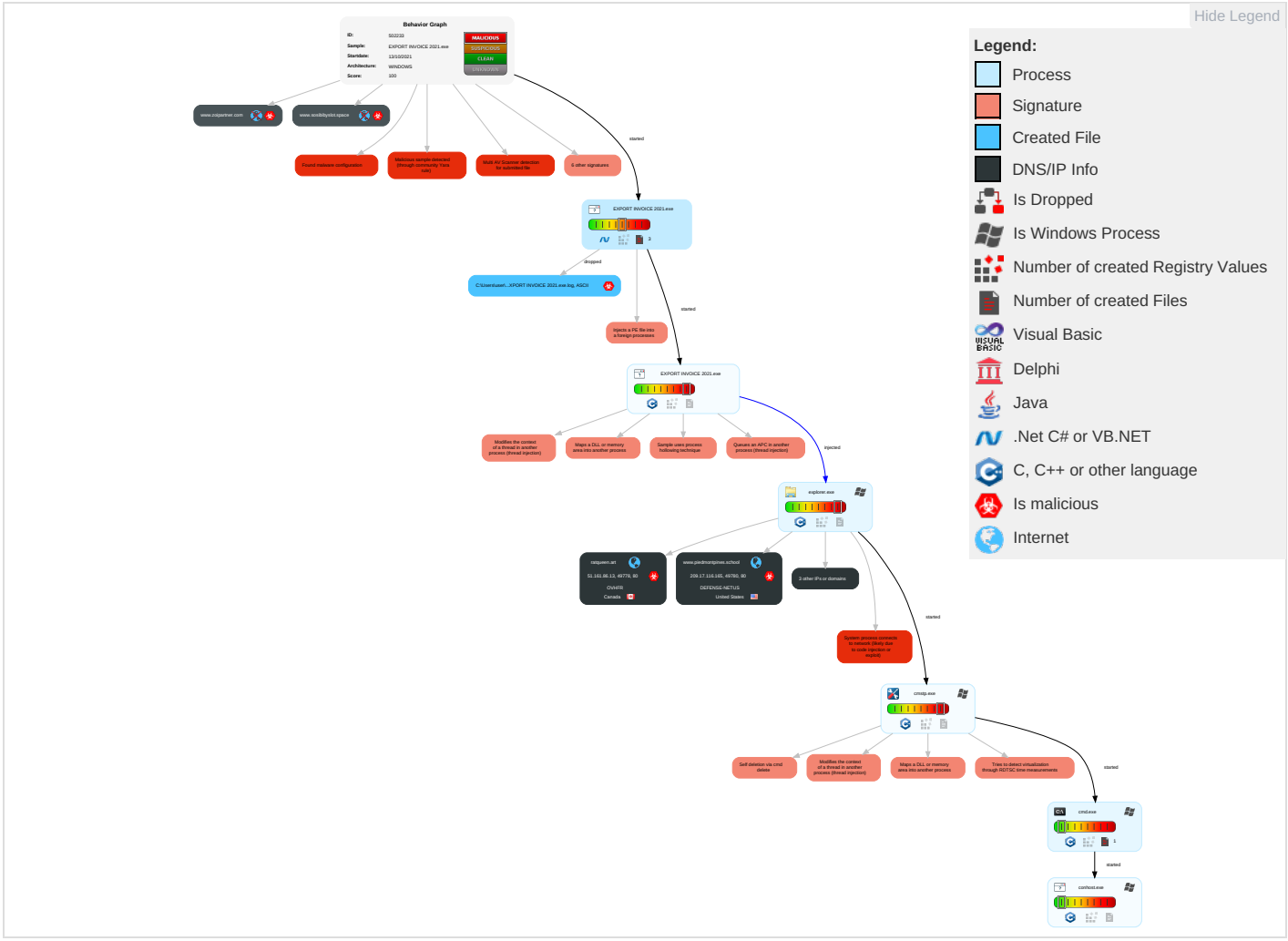
Remote Access Functionality:

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	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	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	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	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 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

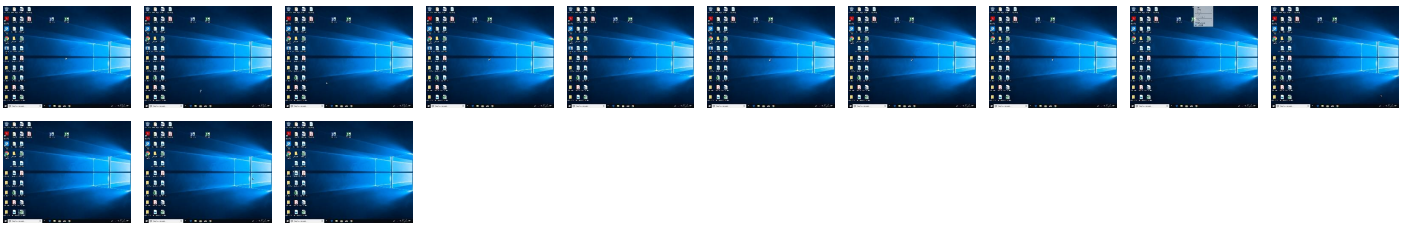
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
EXPORT INVOICE 2021.exe	33%	Virustotal		Browse
EXPORT INVOICE 2021.exe	17%	Metadefender		Browse
EXPORT INVOICE 2021.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.EXPORT INVOICE 2021.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.vulcanopresale.icu/mqi9/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.ratqueen.art/mqi9/?4heD=-Zg8bjv8BJx4HBw&z0=iv8Ag4bEJuIinTRZ0o23voggRtPwqtQ/ydF60y+S+AJP0Z2gEdIzW1gU1h5YO8GPbSLa	0%	Avira URL Cloud	safe	
http://www.piedmontpines.school/mqi9/?z0=TImHsH9dZg2P5abYftozWuM8TNrG03iNFbmWCvRDMTsTbH54OyQX2B6DGU+4mOJFrbhV&4heD=-Zg8bjv8BJx4HBw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ratqueen.art	51.161.86.13	true	true		unknown
www.piedmontpines.school	209.17.116.165	true	true		unknown
www.kalitelihavaperdesi.com	unknown	unknown	true		unknown
www.sosibibyslot.space	unknown	unknown	true		unknown
www.zoipartner.com	unknown	unknown	true		unknown
www.ratqueen.art	unknown	unknown	true		unknown
www.yuezhong66.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.vulcanopresale.icu/mqi9/	true	• Avira URL Cloud: safe	low
http://www.ratqueen.art/mqi9/?4heD=-Zg8bjv8BJx4HBw&z0=iv8Ag4bEJuIinTRZ0o23voggRtPwqtQ/ydF60y+S+AJP0Z2gEdIzW1gU1h5YO8GPbSLa	true	• Avira URL Cloud: safe	unknown
http://www.piedmontpines.school/mqi9/?z0=TImHsH9dZg2P5abYftozWuM8TNrG03iNFbmWCvRDMTsTbH54OyQX2B6DGU+4mOJFrbhV&4heD=-Zg8bjv8BJx4HBw	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.161.86.13	ratqueen.art	Canada		16276	OVHFR	true
209.17.116.165	www.piedmontpines.school	United States		55002	DEFENSE-NETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502233
Start date:	13.10.2021
Start time:	18:20:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EXPORT INVOICE 2021.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:	14
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@10/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26% (good quality ratio 22.8%) • Quality average: 71.1% • Quality standard deviation: 33.5%
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

Simulations

Behavior and APIs

Time	Type	Description
18:21:35	API Interceptor	1x Sleep call for process: EXPORT INVOICE 2021.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51.161.86.13	b5WjxiOqab.exe	Get hash	malicious	Browse	• www.scottgesslerdesign.com/jzvu/?9rq=mRzEKZUdaNl7ltH3Zt23PFVFKBVOmJl5ll4ImGRT+4jF8hnHGhoZT0nVqsAmeIAJc4K10Wg3ow==&4h=vZR8NxdxOD6xzn

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	SecuriteInfo.com.Heur.573.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.21879.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.573.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.16533.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.18564.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.16533.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.18564.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.10164.xls	Get hash	malicious	Browse	• 188.165.62.61

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.19388.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.10164.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Heur.19388.xls	Get hash	malicious	Browse	• 188.165.62.61
	Sales_Receipt 6310.xls	Get hash	malicious	Browse	• 51.83.3.52
	Purchase_Order 2586.xls	Get hash	malicious	Browse	• 51.83.3.52
	D9MmQDM0jJ.dll	Get hash	malicious	Browse	• 51.83.3.52
	A76JJinZL9.dll	Get hash	malicious	Browse	• 51.83.3.52
	8QijkUFTSB.dll	Get hash	malicious	Browse	• 51.83.3.52
	HsGBdHtLk2.dll	Get hash	malicious	Browse	• 51.83.3.52
	lPzE2YbyzV.dll	Get hash	malicious	Browse	• 51.83.3.52
	enVuNPtSQE.dll	Get hash	malicious	Browse	• 51.83.3.52
	REQUIREMENT.exe	Get hash	malicious	Browse	• 51.77.52.109
DEFENSE-NETUS	xHSUX1VjKN.exe	Get hash	malicious	Browse	• 206.188.193.204
	DEUXRWq2W8.exe	Get hash	malicious	Browse	• 209.17.116.163
	PO08485.xlsx	Get hash	malicious	Browse	• 206.188.193.204
	KYTransactionServer.exe	Get hash	malicious	Browse	• 206.188.192.207
	doc_0862413890.exe	Get hash	malicious	Browse	• 206.188.193.172
	PO08485.xlsx	Get hash	malicious	Browse	• 206.188.193.204
	5Zebq6UNKC.exe	Get hash	malicious	Browse	• 209.17.116.163
	Lv9eznkydx.exe	Get hash	malicious	Browse	• 205.178.189.129
	x86_64-20211007-1619	Get hash	malicious	Browse	• 170.158.122.60
	BILL OF LADING.exe	Get hash	malicious	Browse	• 206.188.198.65
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 209.17.116.163
	PO20211006.doc	Get hash	malicious	Browse	• 209.17.116.163
	PO_A9164.EXE	Get hash	malicious	Browse	• 209.17.116.163
	oHdx7w2YXC.exe	Get hash	malicious	Browse	• 209.17.116.163
	fmcg.xlsx	Get hash	malicious	Browse	• 209.17.116.163
	M0y2otz1JB.exe	Get hash	malicious	Browse	• 206.188.197.227
	jnnbbMX9Ch.exe	Get hash	malicious	Browse	• 209.17.116.163
	3KJ2ZgV4so.exe	Get hash	malicious	Browse	• 209.17.116.163
	cFjtsk0IBh.exe	Get hash	malicious	Browse	• 206.188.197.227
	cat#U00e1logo de productos2021.exe	Get hash	malicious	Browse	• 206.188.193.146

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EXPORT INVOICE 2021.exe.log

Process:	C:\Users\user\Desktop\EXPORT INVOICE 2021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EXPORT INVOICE 2021.exe.log	
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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):	7.068386623253211
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	EXPORT INVOICE 2021.exe
File size:	840704
MD5:	54bb8fbbfe0a665ca59579a0240ce2f0
SHA1:	0b97e4463c76df4541179880902bb6966ef3f894
SHA256:	3bd841c6957e9fdb7e9d4558fb417dca9d7317d087cdbbb270155d9a6698e657
SHA512:	fd6ac3075702fffd66df3566015bd6b2d844f28f0dfc0c638bd9198479514479514cf506bfdd56a671efa233873f9313a8b36d80e0bcb78a88624abd9f9b5770
SSDEEP:	12288:Y+zIPiLYQkt3iJHGmWG3HhY8muu8Rsni2U1Rr6s5yuuETV/O:Y+zWiLYQZaGXhguu8ai2U
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O.fa.....P.....n.... ....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ce86e
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:	0x6166C74F [Wed Oct 13 11:47:27 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

General

Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcc874	0xcca00	False	0.600356263363	data	7.07298793214	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x5b8	0x600	False	0.423828125	data	4.11165027332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-18:23:11.004606	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
10/13/21-18:23:12.994789	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 18:22:42.179533958 CEST	192.168.2.4	8.8.8.8	0xefe7	Standard query (0)	www.ratqueen.art	A (IP address)	IN (0x0001)
Oct 13, 2021 18:22:48.022957087 CEST	192.168.2.4	8.8.8.8	0x41b0	Standard query (0)	www.yuezhong66.com	A (IP address)	IN (0x0001)
Oct 13, 2021 18:22:58.514669895 CEST	192.168.2.4	8.8.8.8	0xe3a2	Standard query (0)	www.piedmontpines.school	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:03.918273926 CEST	192.168.2.4	8.8.8.8	0xfb4e	Standard query (0)	www.kalitelihavaperdesi.com	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:04.926768064 CEST	192.168.2.4	8.8.8.8	0xfb4e	Standard query (0)	www.kalitelihavaperdesi.com	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:05.927041054 CEST	192.168.2.4	8.8.8.8	0xfb4e	Standard query (0)	www.kalitelihavaperdesi.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 18:23:07.974427938 CEST	192.168.2.4	8.8.8.8	0xfb4e	Standard query (0)	www.kalitelihavaperdesi.com	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:14.961127996 CEST	192.168.2.4	8.8.8.8	0xc03f	Standard query (0)	www.zoipartner.com	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:15.974524021 CEST	192.168.2.4	8.8.8.8	0xc03f	Standard query (0)	www.zoipartner.com	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:21.774266958 CEST	192.168.2.4	8.8.8.8	0x27f8	Standard query (0)	www.sosibibyslot.space	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 18:22:42.301482916 CEST	8.8.8.8	192.168.2.4	0xefe7	No error (0)	www.ratqueen.art	ratqueen.art		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 18:22:42.301482916 CEST	8.8.8.8	192.168.2.4	0xefe7	No error (0)	ratqueen.art		51.161.86.13	A (IP address)	IN (0x0001)
Oct 13, 2021 18:22:48.464329004 CEST	8.8.8.8	192.168.2.4	0x41b0	Name error (3)	www.yuezhong66.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 18:22:58.641601086 CEST	8.8.8.8	192.168.2.4	0xe3a2	No error (0)	www.piedmontpines.school		209.17.116.165	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:09.945480108 CEST	8.8.8.8	192.168.2.4	0xfb4e	Server failure (2)	www.kalitelihavaperdesi.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:11.003954887 CEST	8.8.8.8	192.168.2.4	0xfb4e	Server failure (2)	www.kalitelihavaperdesi.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:12.994712114 CEST	8.8.8.8	192.168.2.4	0xfb4e	Server failure (2)	www.kalitelihavaperdesi.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 18:23:16.007596970 CEST	8.8.8.8	192.168.2.4	0xc03f	Name error (3)	www.zoipartner.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ratqueen.art
- www.piedmontpines.school

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49778	51.161.86.13	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 18:22:42.409841061 CEST	5301	OUT	GET /mqi9/?4heD=-Zg8bjv8BJx4HBw&z0=iv8Ag4bEJuIinTRZ0o23voggRtPwqtQ/ydF60y+S+AJP0Z2gEdIzW1gU1h5YO8GPbSLa HTTP/1.1 Host: www.ratqueen.art Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 18:22:42.997302055 CEST	5302	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Oct 2021 16:22:42 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close X-Frame-Options: X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff AS_SERVED_STATIC: false Location: https://www.ratqueen.art/mqi9?4heD=-Zg8bjv8BJx4HBw&z0=iv8Ag4bEJulinTRZ0o23voggRtPwqtQ/ydF60y+S+AJP0Z2gEdIzW1gU1h5YO8GPbSLa Cache-Control: no-cache X-Request-Id: dc568a08-0ef3-468e-b148-cc198a1a6325 X-Runtime: 0.408293 Data Raw: 63 30 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 72 61 74 71 75 65 65 6e 2e 61 72 74 2f 6d 71 69 39 3f 34 68 65 44 3d 2d 5a 67 38 62 6a 76 38 42 4a 78 34 48 42 77 26 61 6d 70 3b 7a 30 3d 69 76 38 41 67 34 62 45 4a 75 49 69 6e 54 52 5a 30 6f 32 33 76 6f 67 67 52 74 50 77 71 74 51 2f 79 64 46 36 30 79 2b 53 2b 41 4a 50 30 5a 32 67 45 64 49 7a 57 31 67 55 31 68 35 59 4f 38 47 50 62 53 4c 61 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: c0<html><body>You are being redirected.</body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49780	209.17.116.165	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 18:22:58.775289059 CEST	5308	OUT	GET /mqi9/?z0=TImHsH9dZg2P5abYftozWuM8TNrG03iNFbmWCvRDMTsTbH54OyQX2B6DGU+4mOJFrbhV&4heD=-Zg8bjv8BJx4HBw HTTP/1.1 Host: www.piedmontpines.school Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 18:22:58.906469107 CEST	5308	IN	HTTP/1.1 400 Bad Request Server: openresty/1.17.8.2 Date: Wed, 13 Oct 2021 16:22:58 GMT Content-Type: text/html Content-Length: 163 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 37 2e 38 2e 32 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty/1.17.8.2 </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXPORT INVOICE 2021.exe PID: 7128 Parent PID: 5316

General

Start time:	18:21:08
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\EXPORT INVOICE 2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EXPORT INVOICE 2021.exe'
Imagebase:	0x930000
File size:	840704 bytes
MD5 hash:	54BB8FBBFE0A665CA59579A0240CE2F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: EXPORT INVOICE 2021.exe PID: 5548 Parent PID: 7128

General

Start time:	18:21:36
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\EXPORT INVOICE 2021.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa90000
File size:	840704 bytes
MD5 hash:	54BB8FBBFE0A665CA59579A0240CE2F0
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: 00000002.00000002.797159788.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.797159788.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.797159788.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.797806020.00000000011D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.797806020.00000000011D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.797806020.00000000011D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.797859484.0000000001200000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.797859484.0000000001200000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.797859484.0000000001200000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 5548

General

Start time:	18:21:38
Start date:	13/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000004.00000000.783716545.000000000DABF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.783716545.000000000DABF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.783716545.000000000DABF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.763077934.000000000DABF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.763077934.000000000DABF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.763077934.000000000DABF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmstp.exe PID: 1688 Parent PID: 3424

General

Start time:	18:22:03
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x350000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 00000008.00000002.936050522.00000000004D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.936050522.00000000004D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.936050522.00000000004D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.936919278.0000000002C30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.936919278.0000000002C30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.936919278.0000000002C30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.937017238.0000000002D30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.937017238.0000000002D30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.937017238.0000000002D30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5860 Parent PID: 1688

General

Start time:	18:22:08
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\EXPORT INVOICE 2021.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 Show Windows behavior

Analysis Process: conhost.exe PID: 6040 Parent PID: 5860

General

Start time:	18:22:09
Start date:	13/10/2021
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