ID: 458798
Sample Name: QUOTATION LIST FOR NEW ORDER.exe
Cookbook: default.jbs
Time: 18:53:26
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

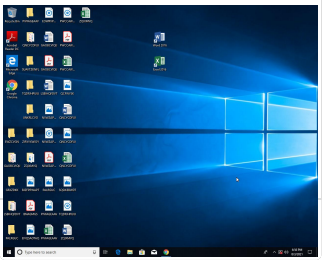
Windows Analysis Report QUOTATION LIST FOR NEW …

Overview

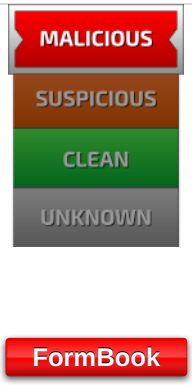
General Information

Sample Name:	QUOTATION LIST FOR NEW ORDER.exe
Analysis ID:	458798
MD5:	2a28a3e032a65c..
SHA1:	019659bb43b553..
SHA256:	317613289fb0cce..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



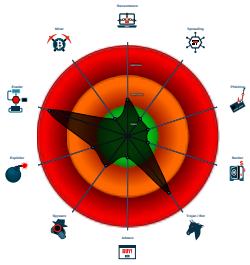
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- QUOTATION LIST FOR NEW ORDER.exe (PID: 5532 cmdline: 'C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe' MD5: 2A28A3E032A65C25B90F193621B623AF)
  - QUOTATION LIST FOR NEW ORDER.exe (PID: 4768 cmdline: C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe MD5: 2A28A3E032A65C25B90F193621B623AF)
  - QUOTATION LIST FOR NEW ORDER.exe (PID: 4760 cmdline: C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe MD5: 2A28A3E032A65C25B90F193621B623AF)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 6056 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 6068 cmdline: /c del 'C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.appackersandmoversbengaluru.com/p4se/"
  ],
  "decoy": [
    "weightlossforprofessionals.com",
    "talkotstopandshop.com",
    "everesttechsolutions.com",
    "garboarts.com",
    "esubastas-online.com",
    "electriclastmile.com",
    "tomio.tech",
    "jacoty.com",
    "knot-tied-up.com",
    "energychoicesim.com",
    "rocketcompaniessham.com",
    "madarasapattinam.com",
    "promosplace.com",
    "newstarchurch.com",
    "thesaleskitchen.com",
    "slingmodeinc.com",
    "jobresulthub.com",
    "pillclk.com",
    "shipu119.com",
    "sibalcar.com",
    "quotovate.com",
    "bluecoyotecontracting.com",
    "hc68kr.com",
    "laundry39.com",
    "vietthaivt.com",
    "ikonflorida.com",
    "xn--sm2b97e.com",
    "innovisional.co.uk",
    "spacecityscouples.com",
    "slmccallum.com",
    "hro41.com",
    "theyardcardzstore.com",
    "primewildlife.com",
    "xn--seranderturzm-ebc.com",
    "stilesandhansen.com",
    "bvlesty.com",
    "hejiayin.com",
    "philosophersdojo.com",
    "aworldofsofas.com",
    "itile.net",
    "unitronicdealers.com",
    "savasoguz.com",
    "magetu.info",
    "devgmor.com",
    "villasabai.com",
    "pipipenguin.com",
    "furnishessentials.com",
    "patchmonitoring.com",
    "michaelhumphriesrealestate.com",
    "pratikahealth.com",
    "caswellcu.com",
    "lakeportal.com",
    "weedyourmind.com",
    "cardamomm.com",
    "freshstartrestorationllcmd.com",
    "mastercardbhdleon.com",
    "ceramiccottageco.com",
    "magicznеszkielka.com",
    "casebookconnet.com",
    "recharge.directory",
    "phoneprivacyscreen.com",
    "mumbaindicator.com",
    "jumboprovacy.com",
    "streamerdojo.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.513637775.000000000540000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.513637775.000000000540000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.513637775.000000000540000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.373559944.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.373559944.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.QUOTATION LIST FOR NEW ORDER.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.QUOTATION LIST FOR NEW ORDER.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.QUOTATION LIST FOR NEW ORDER.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
10.2.QUOTATION LIST FOR NEW ORDER.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.QUOTATION LIST FOR NEW ORDER.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

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:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

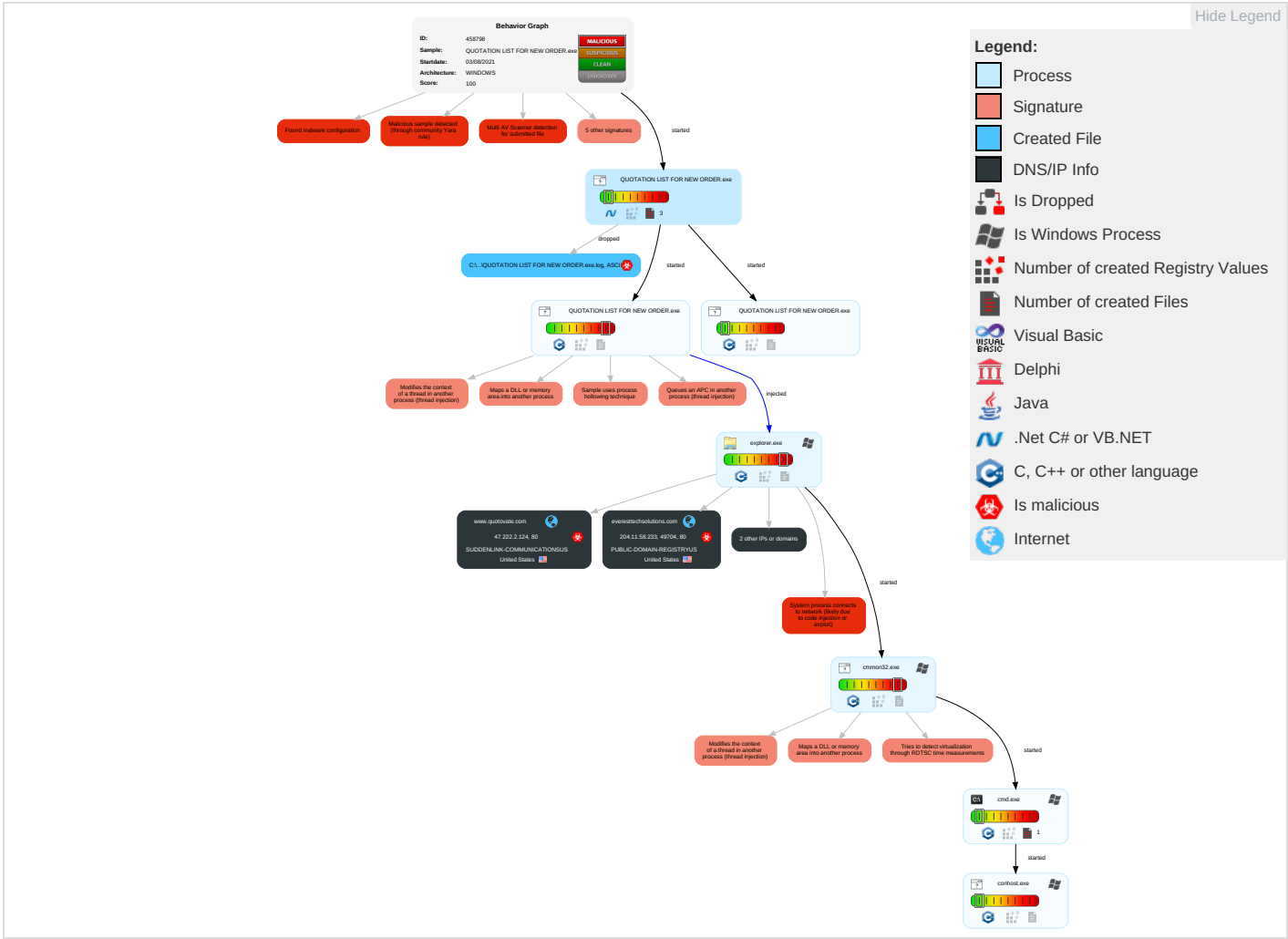
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 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 on Insecure Network Communicatic
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 to Redirect Phor 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 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 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 Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 5	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 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QUOTATION LIST FOR NEW ORDER.exe	61%	Virustotal		Browse
QUOTATION LIST FOR NEW ORDER.exe	46%	Metadefender		Browse
QUOTATION LIST FOR NEW ORDER.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
QUOTATION LIST FOR NEW ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.QUOTATION LIST FOR NEW ORDER.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comd3	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comh-s	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd:	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldF	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.fontbureau.comW.TTFk	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.com9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.como8	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Z	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmO;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.fontbureau.comY	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.carterandcone.com-sQE1s/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/xS	0%	Avira URL Cloud	safe	
http://www.fontbureau.comto	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
www.appackersandmoversbengaluru.com/p4se/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed3	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.everesttechsolutions.com/p4se/?RFQLn6=2dFdaDmhFhA0QZgP&-Zmt_=aCSsC2Wtvj0xQ8J4lkVrtXAo/y9YES1uuye3QtaBHWEeyHJ7dSrXHfQKVk1syv4zArANdeJ+Lg==	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.urwpp.dej	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.quotovate.com	47.222.2.124	true	true		unknown
everesttechsolutions.com	204.11.58.233	true	true		unknown
www.tomio.tech	unknown	unknown	true		unknown
www.everesttechsolutions.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.appackersandmoversbengaluru.com/p4se/	true	• Avira URL Cloud: safe	low
http://www.everesttechsolutions.com/p4se/?RFQLn6=2dFdaDmhFhA0QZgP&-Zmt_=aCSsC2Wtvj0xQ8J4lkVrtXAo/y9YES1uuye3QtaBHWEeyHJ7dSrXHfQKVk1syv4zArANdeJ+Lg==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.11.58.233	everesttechsolutions.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
47.222.2.124	www.quotovate.com	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458798
Start date:	03.08.2021
Start time:	18:53:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION LIST FOR NEW ORDER.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:	16
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@9/1@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.7% (good quality ratio 52%) • Quality average: 69.8% • Quality standard deviation: 33.1%
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
18:54:49	API Interceptor	1x Sleep call for process: QUOTATION LIST FOR NEW ORDER.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
204.11.58.233	Invoice #210722 14,890 $.exe	Get hash	malicious	Browse	• www.everesttechsolutions.com/p4se/?Xl=8ptXsvhhshn&j8kTd=aCSsC2Wtvj0xQ8J4lkVrtXAo/y9YES1uuye3QtaBHWEeyHJ7dSrXHfQKVnZFxvELJl1b

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	MJLkaPZomUolseU.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.MSIL.Kryptik.56a80396.11710.exe	Get hash	malicious	Browse	• 208.91.199.224
	Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Scan#0068-46c3367.exe	Get hash	malicious	Browse	• 208.91.199.224
	Scan#0068-46c3366.exe	Get hash	malicious	Browse	• 208.91.199.223
	bin.exe	Get hash	malicious	Browse	• 119.18.54.122
	IMG-20210802-WA0587-085.exe	Get hash	malicious	Browse	• 208.91.199.224
	IMG-20210802-WA0587-087.exe	Get hash	malicious	Browse	• 208.91.198.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTE 04202021.exe	Get hash	malicious	Browse	• 103.21.58.16
	PURCHASE ORDER PO09377 _093640_9307355_2 64378_88479_0E974.exe	Get hash	malicious	Browse	• 208.91.199.225
	order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ #7696679TTR6F.exe	Get hash	malicious	Browse	• 208.91.199.224
	Waybill Doc_027942941.exe	Get hash	malicious	Browse	• 208.91.199.225
	Confirmaci#U00f3n de pago .exe	Get hash	malicious	Browse	• 208.91.199.224
	triage_dropped_file.exe	Get hash	malicious	Browse	• 162.222.226.11
	oBNvb4c6bg.exe	Get hash	malicious	Browse	• 208.91.199.224
	TVz86np48Z.exe	Get hash	malicious	Browse	• 208.91.199.223
	Current Vendor Payment Application .doc	Get hash	malicious	Browse	• 208.91.199.224
	XiAn Sunnstatement 27-07-2021 pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
SUDDENLINK-COMMUNICATIONSUS	AEOjFHGJAr	Get hash	malicious	Browse	• 74.224.157.19
	uMWZeUs5ZU	Get hash	malicious	Browse	• 47.214.175.5
	LnjgWbwSin	Get hash	malicious	Browse	• 47.208.203.76
	8Z9DxqJIfN	Get hash	malicious	Browse	• 74.193.211.111
	vw23PmQlqG	Get hash	malicious	Browse	• 173.217.185.2
	psqZnqCtZL	Get hash	malicious	Browse	• 74.225.176.64
	SecuriteInfo.com.Linux.Mirai.27.23761.13200	Get hash	malicious	Browse	• 74.225.189.162
	Lv08gOEYJ3	Get hash	malicious	Browse	• 47.208.116.165
	oqG1fmow77	Get hash	malicious	Browse	• 173.80.22.233
	4dIxGwjnil	Get hash	malicious	Browse	• 75.108.75.218
	i01hLg63ev	Get hash	malicious	Browse	• 47.215.216.37
	DLGXmh48ND	Get hash	malicious	Browse	• 74.242.201.236
	Lkm548STLf	Get hash	malicious	Browse	• 75.108.170.66
	6sag2zM690	Get hash	malicious	Browse	• 173.216.23 1.112
	MJ5yMxtK4Y	Get hash	malicious	Browse	• 192.101.60.106
	EM7kj9300x	Get hash	malicious	Browse	• 173.80.22.224
	lLc1G9C259	Get hash	malicious	Browse	• 47.216.131.198
	Jp0fvo75qa	Get hash	malicious	Browse	• 47.209.25.147
	7spunOMzSK	Get hash	malicious	Browse	• 47.218.42.237
	F2PYGjcpEU	Get hash	malicious	Browse	• 74.224.134.234

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION LIST FOR NEW ORDER.exe.log	
Process:	C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION LIST FOR NEW ORDER.exe.log	
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):	7.773783545447779
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:	QUOTATION LIST FOR NEW ORDER.exe
File size:	1347072
MD5:	2a28a3e032a65c25b90f193621b623af
SHA1:	019659bb43b5535a9684d9938aa73e98682b0a61
SHA256:	317613289fb0cce8c301f63922883b30d54bbcdf1cb01bfa772244e03a07dfda
SHA512:	c6aa00f5777d5e0d2f687aaaae1ac8bb9b1689729688088fcde0707c060b8e96b46a133b47d586cb852b277f64b8ce9fd68578d9c25c7f6b702023534494646d
SSDEEP:	24576:wogS/d3ZYdke1b0AIM2Jga9lY7uEmJmwRGPoN7vdiTbnFM:YdvXl9jim/PoiM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...)..a.....P..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x54a0de
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:	0x6103A829 [Fri Jul 30 07:20:09 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x148344	0x148400	False	0.862922011853	data	7.77803780051	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x14c000	0x5c8	0x600	False	0.440104166667	data	4.16475165345	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14e000	0xc	0x200	False	0.044921875	data	0.101910425663	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
08/03/21-18:56:13.121292	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
08/03/21-18:56:14.482122	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	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
Aug 3, 2021 18:56:03.089462996 CEST	192.168.2.7	8.8.8.8	0x45f3	Standard query (0)	www.everesttechsolutions.com	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:08.939980984 CEST	192.168.2.7	8.8.8.8	0xa17f	Standard query (0)	www.tomio.tech	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:09.950802088 CEST	192.168.2.7	8.8.8.8	0xa17f	Standard query (0)	www.tomio.tech	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:11.309310913 CEST	192.168.2.7	8.8.8.8	0xa17f	Standard query (0)	www.tomio.tech	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:17.127902985 CEST	192.168.2.7	8.8.8.8	0x872c	Standard query (0)	www.quotovate.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:56:03.265300035 CEST	8.8.8.8	192.168.2.7	0x45f3	No error (0)	www.everesttechsolutions.com	everesttechsolutions.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 18:56:03.265300035 CEST	8.8.8.8	192.168.2.7	0x45f3	No error (0)	everesttechsolutions.com		204.11.58.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 18:56:12.105026007 CEST	8.8.8.8	192.168.2.7	0xa17f	Server failure (2)	www.tomio.tech	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:13.117250919 CEST	8.8.8.8	192.168.2.7	0xa17f	Server failure (2)	www.tomio.tech	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:14.478785992 CEST	8.8.8.8	192.168.2.7	0xa17f	Server failure (2)	www.tomio.tech	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 18:56:17.165973902 CEST	8.8.8.8	192.168.2.7	0x872c	No error (0)	www.quotovate.com		47.222.2.124	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.everesttechsolutions.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49704	204.11.58.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 18:56:03.427073956 CEST	405	OUT	GET /p4se/?RFQLn6=2dFdaDmhFhA0QZgP&-Zmt_=aCSsC2Wtvj0xQ8J4lkVrtXAo/y9YES1uuye3QtaBHWEeyHJ7dSrXHfQKVk1syv4zArANdeJ+Lg== HTTP/1.1 Host: www.everesttechsolutions.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 18:56:06.000478029 CEST	407	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 03 Aug 2021 16:56:03 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache X-Redirect-By: WordPress Set-Cookie: PHPSESSID=f818a483df7096bf3685fb921c9165a5; path=/ Upgrade: h2,h2c Connection: Upgrade, close Location: https://everesttechsolutions.com/p4se/?RFQLn6=2dFdaDmhFhA0QZgP&-Zmt_=aCSsC2Wtvj0xQ8J4lkVrtXAo/y9YES1uuye3QtaBHWEeyHJ7dSrXHfQKVk1syv4zArANdeJ+Lg== Referrer-Policy: no-referrer-when-downgrade Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: QUOTATION LIST FOR NEW ORDER.exe PID: 5532 Parent PID: 5588

General

Start time:	18:54:22
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe'
Imagebase:	0x580000
File size:	1347072 bytes
MD5 hash:	2A28A3E032A65C25B90F193621B623AF
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: QUOTATION LIST FOR NEW ORDER.exe PID: 4768 Parent PID: 5532

General

Start time:	18:54:50
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe
Imagebase:	0x90000
File size:	1347072 bytes
MD5 hash:	2A28A3E032A65C25B90F193621B623AF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: QUOTATION LIST FOR NEW ORDER.exe PID: 4760 Parent PID: 5532

General

Start time:	18:54:51
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe
Imagebase:	0x590000
File size:	1347072 bytes
MD5 hash:	2A28A3E032A65C25B90F193621B623AF
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: 0000000A.00000002.373559944.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.373559944.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.373559944.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.374153809.0000000000B80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.374153809.0000000000B80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.374153809.0000000000B80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.374626991.00000000010B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.374626991.00000000010B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.374626991.00000000010B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 4760

General

Start time:	18:54:56
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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

Show Windows behavior

Analysis Process: cmmon32.exe PID: 6056 Parent PID: 3292

General

Start time:	18:55:20
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x3d0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA

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: 0000000C.00000002.513637775.0000000000540000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.513637775.0000000000540000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.513637775.0000000000540000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.515171970.0000000003040000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.515171970.0000000003040000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.515171970.0000000003040000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6068 Parent PID: 6056

General

Start time:	18:55:25
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\QUOTATION LIST FOR NEW ORDER.exe'
Imagebase:	0x870000
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: 5984 Parent PID: 6068

General

Start time:	18:55:26
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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