ID: 383909
Sample Name: PO.exe
Cookbook: default.jbs
Time: 12:11:21
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

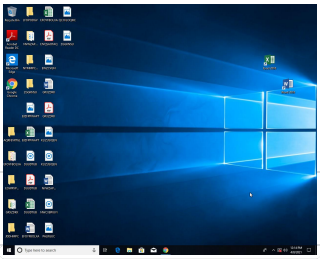
Analysis Report PO.exe

Overview

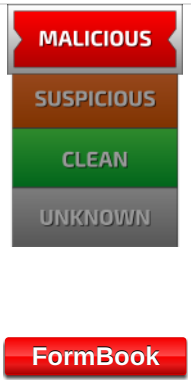
General Information

Sample Name:	PO.exe
Analysis ID:	383909
MD5:	ba83b33d39ca6c..
SHA1:	ce0bcbb882b1a2..
SHA256:	ce27bdaa30fc5a7..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



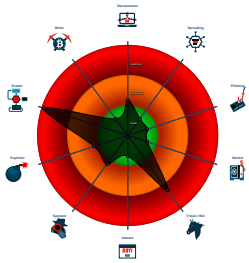
FormBook

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 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…
- 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**
- PO.exe (PID: 5720 cmdline: 'C:\Users\user\Desktop\PO.exe' MD5: BA83B33D39CA6C3BF1F311D1B6A38D1A)
  - PO.exe (PID: 2904 cmdline: 'C:\Users\user\Desktop\PO.exe' MD5: BA83B33D39CA6C3BF1F311D1B6A38D1A)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - chkdsk.exe (PID: 1716 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
        - cmd.exe (PID: 4500 cmdline: /c del 'C:\Users\user\Desktop\PO.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1260 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
00000000.00000002.240240233.0000000002670000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.240240233.0000000002670000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.240240233.0000000002670000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$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:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.495059747.0000000000200000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.495059747.0000000000200000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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				

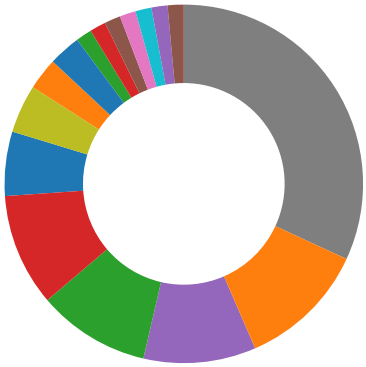
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PO.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.PO.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.PO.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
1.2.PO.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.PO.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

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)

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)

Stealing of Sensitive Information:

Yara detected FormBook

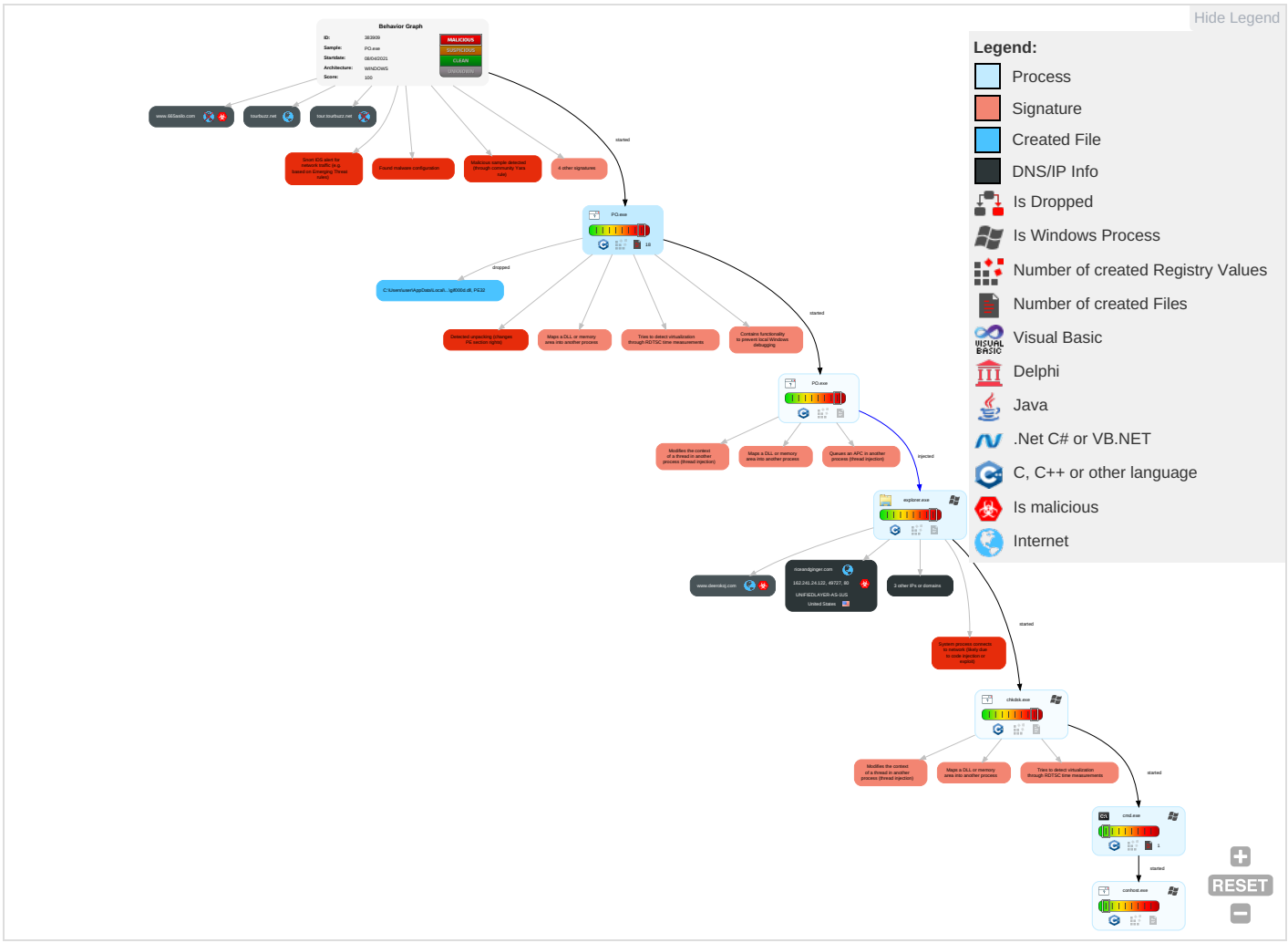
Remote Access Functionality:

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 1 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	Virtualization/Sandbox Evasion 3	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)	Process Injection 5 1 2	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)	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	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	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
PO.exe	16%	Virustotal		Browse
PO.exe	15%	ReversingLabs	Win32.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PO.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.chkdsk.exe.2a5660.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.chkdsk.exe.54ef834.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.PO.exe.2670000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.PO.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.riceandginger.com/fcn/?8p4=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&sZCp=0btLwJX8eFdTeVr	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.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.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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tourbuzz.net	52.20.218.92	true	false		high
riceandginger.com	162.241.24.122	true	true		unknown
www.deerokoj.com	199.247.6.20	true	true		unknown
www.665asilo.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ayescarrental.com	unknown	unknown	true		unknown
www.riceandginger.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.riceandginger.com/fcn/?8p4=IlapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&sZCp=0btLwJX8eFdTeVr	true	• Avira URL Cloud: safe	unknown
www.riceandginger.com/fcn/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 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 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 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 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 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 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.268129348.000000000BC36000.0 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
199.247.6.20	www.deerokoj.com	European Union		20473	AS-CHOOPAUS	true
162.241.24.122	riceandginger.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383909
Start date:	08.04.2021
Start time:	12:11:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO.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:	28
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@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.4% (good quality ratio 12.7%) • Quality average: 77.3% • Quality standard deviation: 28.2%
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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 23.54.113.53, 13.88.21.125, 168.61.161.212, 95.100.54.203, 20.82.210.154, 23.0.174.185, 23.0.174.200, 23.10.249.43, 23.10.249.26, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net

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	TRANSFER CONFIRMATION_PDF.exe	Get hash	malicious	Browse	• www.riceandginger.com/fcn/?nR-lCh=-ZkPgF4h0LuP&Bj4=IlapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwqJ/jNzuESGN

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tourbuzz.net	TT COPY.exe	Get hash	malicious	Browse	• 52.20.218.92
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 52.20.218.92
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 52.20.218.92
	BsR85tOyjL.exe	Get hash	malicious	Browse	• 52.20.218.92
	PURCHASE_ORDER.xlsx	Get hash	malicious	Browse	• 52.20.218.92
	zISJXAAewo.exe	Get hash	malicious	Browse	• 52.20.218.92
	tDuLlLosre.exe	Get hash	malicious	Browse	• 52.20.218.92

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	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
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 162.241.54.59
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 162.241.54.59
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 162.241.54.59
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 162.241.54.59
AS-CHOOPAUS	New Order.exe	Get hash	malicious	Browse	• 45.63.19.244
	B of L - way bill return.exe	Get hash	malicious	Browse	• 45.32.111.89
	RFQ#4734.exe	Get hash	malicious	Browse	• 108.61.161.76
	winlog.dll	Get hash	malicious	Browse	• 45.63.27.162
	xqtEOiEeHh.exe	Get hash	malicious	Browse	• 207.246.80.14
	nnrlOwKZlc.exe	Get hash	malicious	Browse	• 207.246.80.14
	Balance payment..exe	Get hash	malicious	Browse	• 140.82.59.108
	KEyjMfJJQj	Get hash	malicious	Browse	• 155.138.211.25
	XQ2fszii3u	Get hash	malicious	Browse	• 155.138.211.25
	7sZvYxFtN3.exe	Get hash	malicious	Browse	• 45.76.56.26
	2021-04-01.exe	Get hash	malicious	Browse	• 140.82.28.50
	deIt7iuD1y.exe	Get hash	malicious	Browse	• 104.207.148.92
	E1PyFynLfp.exe	Get hash	malicious	Browse	• 136.244.96.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hfGKHMTTDR.exe	Get hash	malicious	Browse	• 207.246.80.14
	cMOtS8JQVW.exe	Get hash	malicious	Browse	• 207.246.80.14
	diagnostic.exe	Get hash	malicious	Browse	• 45.76.172.113
	l4gLNU4NcA.exe	Get hash	malicious	Browse	• 45.63.42.1
	ekdCcEl5KV.exe	Get hash	malicious	Browse	• 207.246.80.14
	4FNTlzlu10.exe	Get hash	malicious	Browse	• 207.246.80.14
	SecuriteInfo.com.Trojan.Siggen12.58144.411.exe	Get hash	malicious	Browse	• 45.76.53.14

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\0qs5eq4gqxghkspsiz

Process:	C:\Users\user\Desktop\PO.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.999002923208001**
Encrypted:	**true**
SSDEEP:	3072:hfhva0w76JwhEkYZNjdYCSGAJG3RQ4UzWdP7NmQfey45grprDHRL/Wdy:hfhvaR6JxBZNxFSGScP7NloKFHRTH
MD5:	C76B2A549514C1B2E11142566992D07A
SHA1:	79FEF3B446A7732B091745B111A0C73F82DE5DBB
SHA-256:	CE5B3CE5686E894A949D127B10FE27382F4737E4DF7B724269D669468434ADF8
SHA-512:	70AEF1C4093FB27FB434E4A28B96E914C2A0CEE46CB9982F4E596E9D285A1DF59766354058D28A9DD73BAA3CD24AE3D4086C82AA42C82620F6039CCB36C625I 8
Malicious:	false
Reputation:	low
Preview:	..h*...U/...[H.Jp..vm..y3.L..}.....Q`;...:..p.-..2.$z..#..5tdR.R.b.IJZ.V....~...UgOa.%.....q2.S....t.+t..7J..3.....V.....AMvw.K1i...Wzk.D.d..yJ..v.@..,.N.....\E...YI.....9..Y...L/u..fF.3( ...}..t=.E..-.....!;w`...yx..k\z....//.`&.7Z..Af.1e....u?0....K.....s.JF....o;]..$m..t.^.&..H....G.4'.....G..U...q.k.d.....l...]...?...u..j_.X...yH...<...1.|.....?.....{.r.D8@..u..'9.!.P.>.s....u .N6.B.$...?.[.r.iq.d...m.j.y.Si.[.....Z"...C.6t.a...T1....l.....?.....c...~.&....A\.]....2..+..$a....8....K..)...Ph.v..u.7.MEKYN..8H.....f.=..i.V....e...}l5*....U..Ea...m.k;...Vr.T...{.|..uh.. ..gt/..r..\q...2.A>r.....Z.F.....t.w}..}A..P.{..z).<.x.&.F}.G..:..T..G.....~+.....rD|O.eO.2F...:.K..'.p.DgBkt..7.4. K.....Dv.X..a@.T.)...1{.*.....+-.16..w./..v.~.%9..?#..O...A..... ....y.'.nhU.+.*..-.K,...x .._&;...U.1.C.C..}.7b...?...G.u<._. l..m1..s~{.B.....5'K.'*O^.....l.\.d..}..e.Oj...*.._..4w.{w.K..I...&.8.....W.V....!].]...../k....

C:\Users\user\AppData\Local\Temp\4hohyb48e3wlzft

Process:	C:\Users\user\Desktop\PO.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.963332317122046
Encrypted:	false
SSDEEP:	96:kBksH+WPGZ9ImHb+KxkeDGwERGvqpW+LNd4YgLv8dYA53lmJolxQtxvz:1WytHb3ilqqpWUddg78uA+JoletNz
MD5:	8903F1E0C84D25A97CDA24636A27ED23
SHA1:	F6941D060997F540B06D6C6C85B9B56B23549DBC
SHA-256:	AE70E7DDAE9D864DD18CF6CDC1DC64C918B1FC01254C5AF6AA7DB3D1596E0010
SHA-512:	5FAE1B044DABB5E99607C4F76C8D8C661DAE754BC711074447646874CC70F179AFDB94B8770F1649197B4C118E9119EB61050A0F06184F407BE509257B09DDBE
Malicious:	false
Reputation:	low
Preview:	.~z..>.....b.T..l.....K.M.;.R1D7%.T>#?d..).....%..Q]Lokg5M.9.....hM...l...e.%i.....}.2>.LHD..U....$ ..9..bn-|xtF:.J..}TP..i."....v.6z.....V.RCO.....f..'>51-....s..... W^ea]/?.3.....b.....c;#g.....8G,..k..+.....d..ds..8...W.88.<..... ....@...1dX$h.....=Hi..%0.hT....'#.....amT.{wE..I..WS..q.!.....u.5y..E....m.QBN.....e..&e40,....r~.....A...V.d`\.>.2 .....F...&...^n.b..v..../;.IEA.u...f..!...zSo..yu.I.ia]/...F.....}.F...._.).....N$30.z.....dp..~z..n.Qb..2.....T....9<.....f./..M....5.rK..c/+.....z..-/..ok..-_[W-9...ac.....m.|.....6B..LH...". 0.....ju....<..U.`..,.....A.....G...B.&w2....7Cq.MI7.X5'..%w.ys.....Sg.uqm....b..U....T.....D.+@L^... 7..?.....I."R-..p.r...Sr.}W..J.p...q....r..|.....5..C?t.//P...As@....ows RT.__[W.....}.u.u....Y.Q.....&B..LH.@fF40,.#J....gjX.tp.d\\..\....f.....d.....3N..+?..IE38.r1..%.K...w./i.imi..\n.!.....U..

C:\Users\user\AppData\Local\Temp\nsuA1D.tmp\gif000d.dll

Process:	C:\Users\user\Desktop\PO.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

C:\Users\user\AppData\Local\Temp\nsuA1D.tmp\gif000d.dll	
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.091011953873825
Encrypted:	false
SSDEEP:	48:vpggDzDVKAxlyNHvPviTLNuLebdsbriB4ZYmRSs:BTzxlivPvinktfiuZVR
MD5:	A622545967851FAF0405E20376399ACB
SHA1:	8000D6463895519F16325B7901321247A1C84D22
SHA-256:	06A5FAD63869EF665B9E99BAEA58BCE3BB59E85D19D744D53D0E70F58738FF32
SHA-512:	939213666AA71DBE3EF9D747216A0BC959E11151AA56CFDE7CEECE6BE5EE13BBC3488F34259D6824D4B7126907A616CC172864840707619FF91B271B093C59C
Malicious:	false
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....n`.....!.....`.....@..... ....U....!.....@.....P..L..." .....$".....text...\..... ..`.rdata..... .....@..@.data..... .0.....@....rsrc.....@.....@..@.reloc..L....P.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.919251123380622
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:	PO.exe
File size:	227498
MD5:	ba83b33d39ca6c3bf1f311d1b6a38d1a
SHA1:	ce0bcbb882b1a2105138b9955c1d892e4c6f0947
SHA256:	ce27bdaa30fc5a712b41888b529f52c87f90b9d196b975d47ec9b5236b48cebc
SHA512:	e251a936be79eed23d04874324be745090919af5ab7ee95310c06d8877f943fadc9752c38db70a5f0e7d3799e4f89f471233c96d18b92c12dab9bf78f59d2b13
SSDEEP:	3072:HyewmN4skJ6MWjfhva0w76JwhEkYZNjdYCSGAJG3RQ4UzWdP7NmQfey45grprDHO:HdrfhvaR6JxBZNxFSGScP7NloKFHRTs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H..... .....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
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:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]

General

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 [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007FB80CD18308h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FB80CD15A49h
test eax, eax
jne 00007FB80CD15B06h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FB80CD182F3h
call 00007FB80CD15A29h
test eax, eax
je 00007FB80CD15C22h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FB80CD182B1h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi

Instruction
jne 00007FB80CD15AECh
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	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	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	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	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

DLL	Import
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

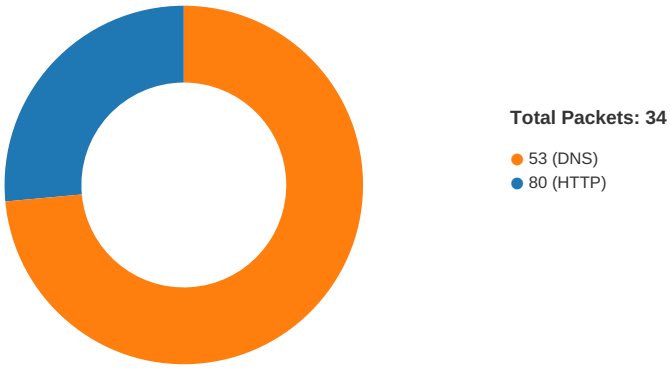
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:14:02.069664	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	162.241.24.122
04/08/21-12:14:02.069664	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	162.241.24.122
04/08/21-12:14:02.069664	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	162.241.24.122

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:13:40.544469118 CEST	49725	80	192.168.2.5	199.247.6.20
Apr 8, 2021 12:13:40.562431097 CEST	80	49725	199.247.6.20	192.168.2.5
Apr 8, 2021 12:13:41.064224005 CEST	49725	80	192.168.2.5	199.247.6.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:13:41.082194090 CEST	80	49725	199.247.6.20	192.168.2.5
Apr 8, 2021 12:13:41.595515013 CEST	49725	80	192.168.2.5	199.247.6.20
Apr 8, 2021 12:13:41.613816023 CEST	80	49725	199.247.6.20	192.168.2.5
Apr 8, 2021 12:14:01.927160978 CEST	49727	80	192.168.2.5	162.241.24.122
Apr 8, 2021 12:14:02.069130898 CEST	80	49727	162.241.24.122	192.168.2.5
Apr 8, 2021 12:14:02.069335938 CEST	49727	80	192.168.2.5	162.241.24.122
Apr 8, 2021 12:14:02.069664001 CEST	49727	80	192.168.2.5	162.241.24.122
Apr 8, 2021 12:14:02.211385965 CEST	80	49727	162.241.24.122	192.168.2.5
Apr 8, 2021 12:14:02.566215038 CEST	49727	80	192.168.2.5	162.241.24.122
Apr 8, 2021 12:14:02.752856016 CEST	80	49727	162.241.24.122	192.168.2.5
Apr 8, 2021 12:14:04.872277021 CEST	80	49727	162.241.24.122	192.168.2.5
Apr 8, 2021 12:14:04.872505903 CEST	49727	80	192.168.2.5	162.241.24.122
Apr 8, 2021 12:14:04.872608900 CEST	80	49727	162.241.24.122	192.168.2.5
Apr 8, 2021 12:14:04.872714996 CEST	49727	80	192.168.2.5	162.241.24.122

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:12:06.178884983 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:06.191783905 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:08.048573971 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:08.061793089 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:08.770917892 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:08.783648968 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:08.987853050 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:09.006052971 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:10.268135071 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:10.281533957 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:11.804956913 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:11.817466021 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:12.743650913 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:12.756333113 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:13.563091040 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:13.575824022 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:14.841455936 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:14.853894949 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:15.754436970 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:15.767277956 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:17.557957888 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:17.571839094 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:21.269838095 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:21.282497883 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:32.977138996 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:32.995311975 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:12:52.821908951 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:12:52.835186958 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:01.819839954 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:01.838418007 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:04.264900923 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:04.286134005 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:20.221487999 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:20.282555103 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:30.721555948 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:30.733474970 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:33.983861923 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:33.997242928 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:40.495008945 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:40.540290117 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 12:13:53.829301119 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:13:53.862998009 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 12:14:01.800262928 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:14:01.924691916 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 12:14:15.857790947 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:14:15.872793913 CEST	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:14:17.984936953 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:14:18.019665003 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 12:14:22.730901957 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:14:22.908416986 CEST	53	58530	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 12:13:20.221487999 CEST	192.168.2.5	8.8.8.8	0xef65	Standard query (0)	www.ayescarrental.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:13:40.495008945 CEST	192.168.2.5	8.8.8.8	0x4eae	Standard query (0)	www.deerokoj.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:14:01.800262928 CEST	192.168.2.5	8.8.8.8	0x4e12	Standard query (0)	www.riceandginger.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:14:22.730901957 CEST	192.168.2.5	8.8.8.8	0x2515	Standard query (0)	www.665asilo.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 12:13:40.540290117 CEST	8.8.8.8	192.168.2.5	0x4eae	No error (0)	www.deerokoj.com		199.247.6.20	A (IP address)	IN (0x0001)
Apr 8, 2021 12:14:01.924691916 CEST	8.8.8.8	192.168.2.5	0x4e12	No error (0)	www.riceandginger.com	riceandginger.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:14:01.924691916 CEST	8.8.8.8	192.168.2.5	0x4e12	No error (0)	riceandginger.com		162.241.24.122	A (IP address)	IN (0x0001)
Apr 8, 2021 12:14:22.908416986 CEST	8.8.8.8	192.168.2.5	0x2515	No error (0)	www.665asilo.com	tour.tourbuzz.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:14:22.908416986 CEST	8.8.8.8	192.168.2.5	0x2515	No error (0)	tour.tourbuzz.net	tourbuzz.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:14:22.908416986 CEST	8.8.8.8	192.168.2.5	0x2515	No error (0)	tourbuzz.net		52.20.218.92	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.riceandginger.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49727	162.241.24.122	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:14:02.069664001 CEST	5414	OUT	GET /fcn/?8p4=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&sZCp=0btLwJX8eFdTeVr HTTP/1.1 Host: www.riceandginger.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:14:04.872277021 CEST	5415	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:14:04 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/?8p4=IIapObjlcsmN/tTUXuiVJ6SvcAdYVsMSy0eMvzJ/vGgposGY5YkWehqMwppvssjWa3vK&sZCp=0btLwJX8eFdTeVr host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS

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

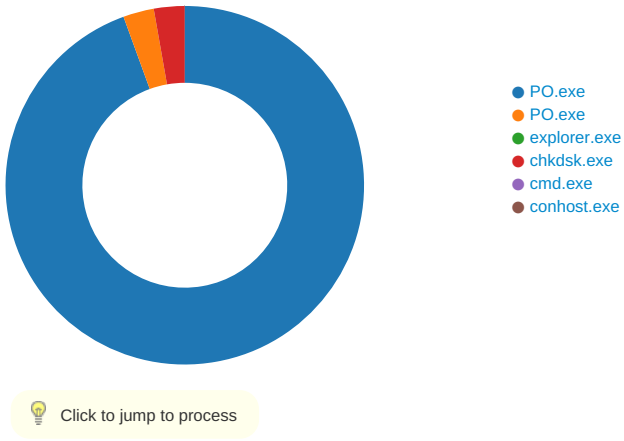
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



System Behavior

Analysis Process: PO.exe PID: 5720 Parent PID: 5624

General

Start time:	12:12:27
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO.exe'
Imagebase:	0x400000

File size:	227498 bytes
MD5 hash:	BA83B33D39CA6C3BF1F311D1B6A38D1A
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: 00000000.00000002.240240233.0000000002670000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.240240233.0000000002670000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.240240233.0000000002670000.00000004.00000001.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	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj9DD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	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\4hohyb48e3wlzft	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\0qs5eq4gqxghkspsiz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsuA1D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	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

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	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\nsuA1D.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\nsuA1D.tmp\gif000d.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj9DD.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsuA1D.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4hohyb48e3wlzft	unknown	6661	e5 bd be 7e 7a a3 c4 3e a7 b8 cf be b4 c3 62 c0 54 96 c2 6c e2 09 9f be 91 a6 a2 f0 04 a6 93 e8 f7 96 d4 eb 4b d7 4d db 3b ba 52 31 44 37 25 ba 54 3e 23 3f 64 89 03 29 fa 87 83 1f 1b 89 fc dd 8b dc 25 9c e0 51 5d 4c 6f 6b 67 35 4d f4 39 a9 b5 1c c7 c3 bf 8d 68 4d 11 02 0e 6c 9f 9b 97 65 c0 25 69 d9 e5 bc f7 f3 ef bd 9d 7d c1 32 3e 0d 4c 48 44 95 e8 55 99 8a 16 dc 24 20 1c ed 39 ad f1 62 6e 2d 7c 78 74 46 3a 06 4a ba c6 7d 54 50 cc 1e 69 dd 22 92 9e cd ac a8 a4 76 b9 36 7a ea f6 9d 05 01 fc ce 56 8e 52 43 4f ed dc d8 d4 a6 91 66 aa 1b 27 3e 35 31 2d fe 0f be 03 73 7f 8e 8d 89 85 d6 1b 96 da cb 57 5e 65 61 5d 2f 3f ee 33 a3 af ae bd b9 b5 62 a8 8f ff 08 03 99 95 91 63 3b 23 67 d7 e2 d3 c7 cb 87 cb 38 47 2c ab 9f 6b af 1c 2b 88 0c d7 cf 93 80 8f 64 f3 93 b3	...~z..>.....b.T..l..... .....K.M.;.R1D7%.T>#? d..).... .....%..Q]Lokg5M.9.....hM ...l...e.%i.....}.2>.LHD..U.. ..$ ..9..bn-|xtF:.J..}TP..i.". .....v.6z.....V.RCO.....f.. '>51-....s.....W^ea]/?.3. .....b.....c;#g.....8G,.. k..+.....d...	success or wait	1	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0qs5eq4gqxghkspsiz	unknown	32768	fa e8 68 2a 85 7f 01 55 2f d9 16 b1 5b 48 ea 4a 70 83 f1 76 6d b9 bf 79 33 e3 9e 4c d5 eb 7d 90 b1 81 d5 c5 da 51 60 3b f6 94 ca 3a f2 08 70 ee 2d f4 98 32 ba 24 7a 9f 91 23 e5 0c 35 74 64 52 d2 52 f1 9a 62 f4 49 4a 5a 18 56 1d cf 2e 1c 7e 0d b1 bc 55 67 4f 61 d1 9f 25 cb 1f eb dc c1 db b1 71 32 03 53 83 99 fc cb 74 05 2b 74 b8 cc 37 4a b5 e7 33 ef e4 c0 bf 88 56 cf 13 d2 96 d4 16 41 4d 76 77 ec 4b 31 69 a2 ec 15 57 7a 6b d2 44 91 64 98 f6 79 4a a2 c8 76 f5 40 f5 b8 2c fd 4e 0d 19 01 b4 a7 ea 5c 45 c7 a1 c9 ef 59 49 fe aa bf 9c 1b 39 92 d0 59 e9 83 b7 be b0 4c 2f 75 9e 04 66 46 c8 a2 33 28 0e f5 8d 7d fc 98 74 3d 90 45 b9 92 2d e0 bd d9 92 1e 8b 96 21 3b 77 60 b4 e9 e2 79 78 04 81 6b 5c 7a cc cb cf fa 2f 2f ca 60 26 0d 37 5a aa b4 41 66 bf 31 65 18 df 0d	..h*...U/...[H.Jp..vm..y3..L.. }......Q`;...:..p.-..2.$z..#.. 5tdR.R..b.IJZ.V....~...UgOa ..%.......q2.S....t.+t..7J..3.... .V......AMvw.K1i...Wzk.D.d. .yJ ..v.@..,.N......\E....YI.....9 ..Y.....L/u..fF..3(...}..t=.E..- .......!;w`...yx..k\z....//. `&.7Z..Af.1e...	success or wait	6	403091	WriteFile
C:\Users\user\AppData\Local\Temp\nsuA1D.tmp\gif000d.dll	unknown	4096	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 05 00 a6 b7 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 00 00 00 04 00 00 00 00 00 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b3 20 00 00 55 00 00 00 08 21 00 00 8c 00 00	MZx.....................@..... .... x...........!..L.!This program cannot be run in DOS mode.$.. PE..L.....n`...........!...... .............................. .....................`........ ....@.......................... ..U....!.....	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\PO.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\PO.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\4hohyb48e3wlzft	unknown	6661	success or wait	1	73CA109A	ReadFile
C:\Users\user\AppData\Local\Temp\0qs5eq4gqxghkspsiz	unknown	185856	success or wait	1	25515AF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	255085D	ReadFile

Analysis Process: PO.exe PID: 2904 Parent PID: 5720

General

Start time:	12:12:29
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO.exe'
Imagebase:	0x400000
File size:	227498 bytes
MD5 hash:	BA83B33D39CA6C3BF1F311D1B6A38D1A
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: 00000001.00000002.281309352.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.281309352.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.281309352.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.281955301.0000000000CF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.281955301.0000000000CF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.281955301.0000000000CF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.281979783.0000000000D20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.281979783.0000000000D20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.281979783.0000000000D20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.235598141.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.235598141.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.235598141.0000000000400000.00000040.00020000.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: 2904

General

Start time:	12:12:33
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: chkdsk.exe PID: 1716 Parent PID: 3472

General

Start time:	12:12:50
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x7ff797770000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
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: 00000008.00000002.495059747.0000000000200000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.495059747.0000000000200000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.495059747.0000000000200000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.496196901.0000000004B30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.496196901.0000000004B30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.496196901.0000000004B30000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4B49E57	NtReadFile

Analysis Process: cmd.exe PID: 4500 Parent PID: 1716

General

Start time:	12:12:54
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO.exe'
Imagebase:	0x980000
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: 1260 Parent PID: 4500

General

Start time:	12:12:55
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