ID: 482260
Sample Name: Covid-19 Data Report Checklist_pdf.exe
Cookbook: default.jbs
Time: 15:39:26
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

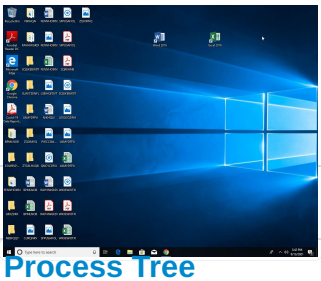
Windows Analysis Report Covid-19 Data Report Checkli…

Overview

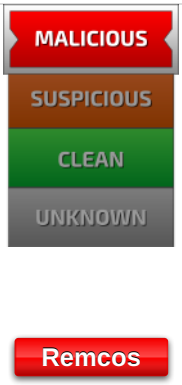
General Information

Sample Name:	Covid-19 Data Report Checklist_pdf.exe
Analysis ID:	482260
MD5:	26467941a5c46c..
SHA1:	f0c57e46d0d83e0.
SHA256:	a3f8ab3315bcd82.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

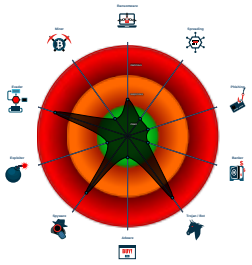


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AntiVM autoit script
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected Remcos RAT
- Detected Remcos RAT
- Multi AV Scanner detection for dropp…
- Sigma detected: Bad Opsec Default…
- Contains functionality to capture and…
- Initial sample is a PE file and has a …
- Contains functionality to steal Firefo…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- Covid-19 Data Report Checklist_pdf.exe (PID: 6924 cmdline: 'C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe' MD5: 26467941A5C46C31D4915ABD5E4A2965)
  - gajb.pif (PID: 7164 cmdline: 'C:\Users\user\AppData\Roaming\11951071\gajb.pif' wodm.efi MD5: 6BE533CF863DB26D953917024CFFF914)
    - RegSvcs.exe (PID: 6288 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- gajb.pif (PID: 4752 cmdline: 'C:\Users\user\AppData\Roaming\11951071\gajb.pif' C:\Users\user\AppData\Roaming\11951071\wodm.efi MD5: 6BE533CF863DB26D953917024CFFF914)
  - RegSvcs.exe (PID: 4124 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "cato.fingusti.club:6609:s%qDr",
  "Assigned name": "NEWYEAR",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-VHEUO4",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "wikipedia;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "10000"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.363037979.0000000004E91000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000004.00000003.368157698.0000000004EDE000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000007.00000003.394956149.00000000030E8000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000004.00000003.362785019.0000000004EDE000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000007.00000003.394845153.00000000030E4000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 52 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.gajb.pif.4efdf30.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
4.3.gajb.pif.4efdf30.0.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...

Source	Rule	Description	Author	Strings
4.3.gajb.pif.4efdf30.0.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x166f8:$str_a1: C:\Windows\System32\cmd.exe • 0x16714:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x16714:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x15dfc:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x16400:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x159e0:$str_b2: Executing file: • 0x16798:$str_b3: GetDirectListeningPort • 0x16240:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x16534:$str_b5: licence_code.txt • 0x1649c:$str_b6: \restart.vbs • 0x163c0:$str_b8: \uninstall.vbs • 0x1596c:$str_b9: Downloaded file: • 0x15998:$str_b10: Downloading file: • 0x15690:$str_b11: KeepAlive Enabled! Timeout: %i seconds • 0x159fc:$str_b12: Failed to upload file: • 0x167d8:$str_b13: StartForward • 0x167bc:$str_b14: StopForward • 0x16330:$str_b15: fso.DeleteFile " • 0x16394:$str_b16: On Error Resume Next • 0x162fc:$str_b17: fso.DeleteFolder " • 0x15a14:$str_b18: Uploaded file:
7.3.gajb.pif.3e2df30.16.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
7.3.gajb.pif.3e2df30.16.raw.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
Click to see the 169 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Multi AV Scanner detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to capture and log keystrokes

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

Malware Analysis System Evasion:

Yara detected AntiVM autoit script

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Remcos RAT

Contains functionality to steal Firefox passwords or cookies

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

Yara detected Remcos RAT

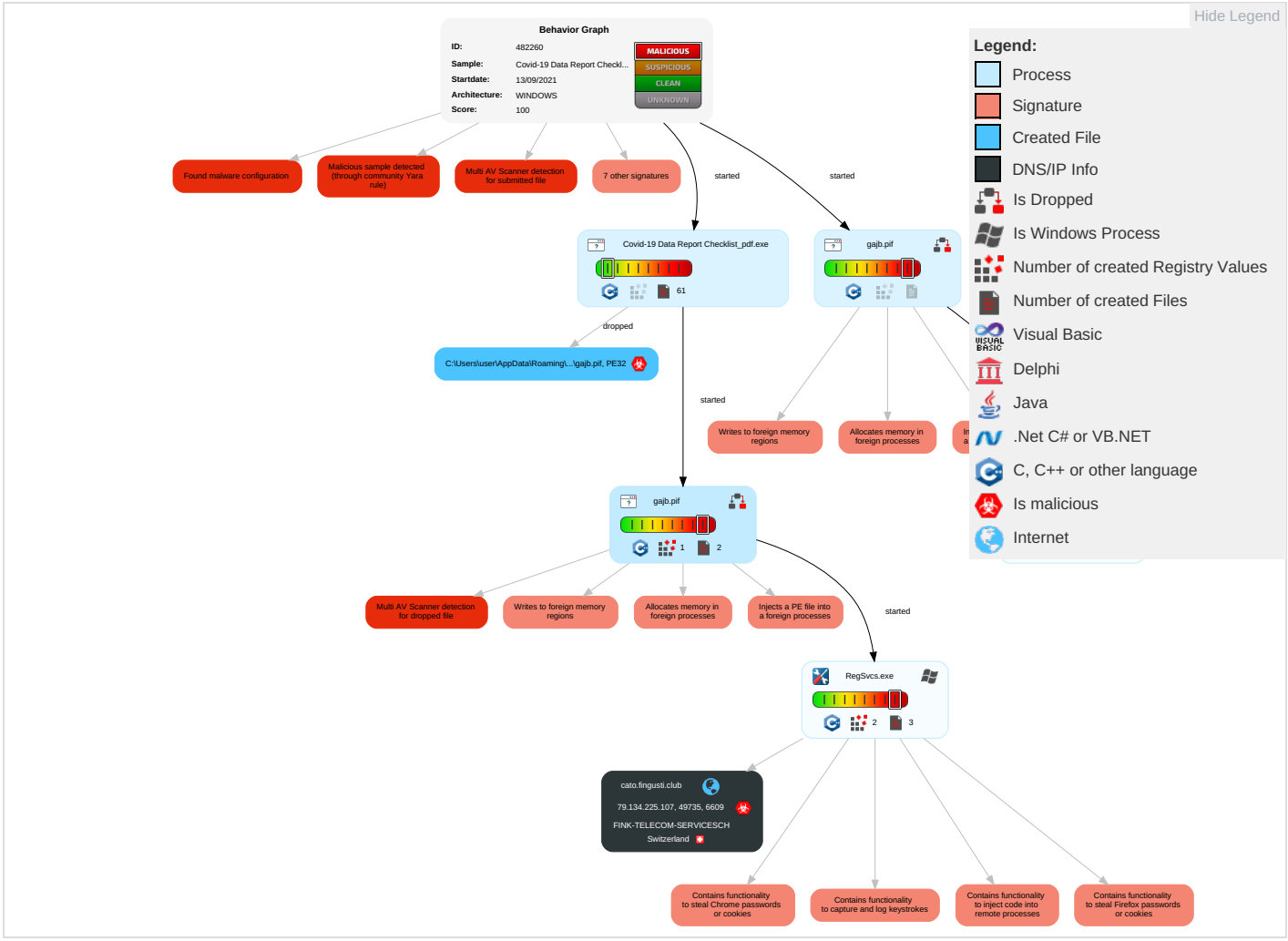
Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 2	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Command and Scripting Interpreter 1 2	Application Shimming 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 2 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 2 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 2	Valid Accounts 2	Application Shimming 1	Obfuscated Files or Information 2	Credentials In Files 2	System Service Discovery 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Local Accounts	At (Windows)	Windows Service 1	Valid Accounts 2	Software Packing 2	NTDS	File and Directory Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Access Token Manipulation 2 1	DLL Side-Loading 1	LSA Secrets	System Information Discovery 3 6	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Windows Service 1	Masquerading 1 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Process Injection 4 2 2	Valid Accounts 2	DCSync	Security Software Discovery 1 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2	Proc Filesystem	Virtualization/Sandbox Evasion 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 2 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 4 2 2	Network Sniffing	Application Window Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusca Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

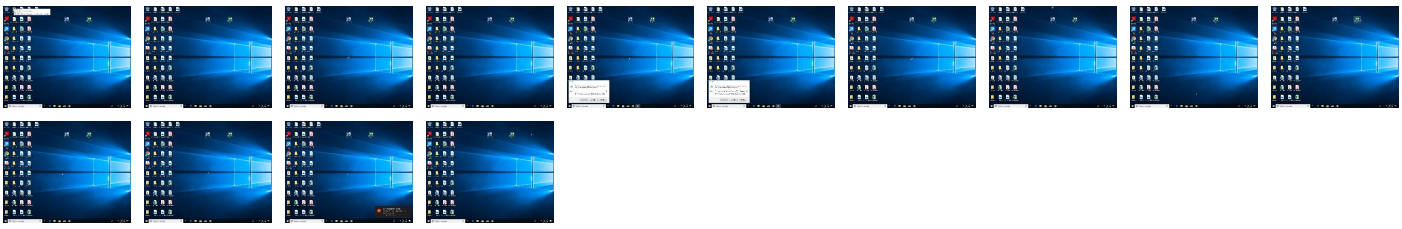
Behavior Graph



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
Covid-19 Data Report Checklist_pdf.exe	51%	ReversingLabs	Win32.Trojan.Lisk	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\11951071\gajb.pif	25%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.3.gajb.pif.30e7c20.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.2.RegSvcs.exe.720000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4eddf28.14.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
6.2.RegSvcs.exe.b00000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4efdf30.3.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4efdf30.7.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4eddf28.13.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e0df28.14.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e2df30.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4eddf28.11.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e2df30.13.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.3.gajb.pif.4eddf28.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e0df28.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4efdf30.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4eddf28.16.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4efdf30.10.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e0df28.12.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e2df30.17.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e2df30.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4efdf30.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e2df30.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.41a67d0.18.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4f1e740.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e2df30.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3de0050.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4efdf30.12.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e2df30.16.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e2df30.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e0df28.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.gajb.pif.3e6e748.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4eddf28.4.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4efdf30.15.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e0df28.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4efdf30.17.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4efdf30.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e2df30.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.gajb.pif.4eddf28.6.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
4.3.gajb.pif.4eddf28.8.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.3.gajb.pif.3e2df30.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
cato.fingusti.club	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cato.fingusti.club	79.134.225.107	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
cato.fingusti.club	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.107	cato.fingusti.club	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482260
Start date:	13.09.2021
Start time:	15:39:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid-19 Data Report Checklist_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:	23
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@8/56@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.3% (good quality ratio 24.4%) • Quality average: 55.4% • Quality standard deviation: 40.5%
HCA Information:	• Successful, ratio: 81% • 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

Simulations

Behavior and APIs

Time	Type	Description
15:40:35	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate C:\Users\user\AppData\Roaming\11951071\gajb.pif C:\Users\user\AppData\Roaming\11951071\wodm.efi
15:40:37	API Interceptor	949x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.107	Covid-19 Data Report .exe	Get hash	malicious	Browse	
	Covid-19 Data Report Google Checklist.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.26524.9571.exe	Get hash	malicious	Browse	
	O8Ii8MW7rn.exe	Get hash	malicious	Browse	
	Le8z5e90IO.exe	Get hash	malicious	Browse	
	LA99293P02.xls	Get hash	malicious	Browse	
	PO 2413.exe	Get hash	malicious	Browse	
	myups.exe	Get hash	malicious	Browse	
	scanned.pdf.copy.documents.outstanding.exe	Get hash	malicious	Browse	
	69Invoice approval.pdf.exe	Get hash	malicious	Browse	
	52Amended Purchase order for your reference.exe	Get hash	malicious	Browse	
	21PO10092019.exe	Get hash	malicious	Browse	
	40wellsfargo Remittance.exe	Get hash	malicious	Browse	
	22stone.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cato.fingusti.club	Covid-19 Data Report Google Checklist.exe	Get hash	malicious	Browse	• 79.134.225.107
	Notice to submit_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	Notice_to_submit.exe	Get hash	malicious	Browse	• 79.134.225.92
	IM0003057615_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	Notice to submit_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	Rules & Regulation (IRR)_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	wNxb2V5PKj.exe	Get hash	malicious	Browse	• 79.134.225.92
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	SecuriteInfo.com.Trojan.Win32.Save.a.31706.exe	Get hash	malicious	Browse	• 79.134.225.92
	10UNv6Ul0W.exe	Get hash	malicious	Browse	• 79.134.225.92

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	HhnZ6B5xzZ.exe	Get hash	malicious	Browse	• 79.134.225.91
	Oferta de produto 74675673748.jar	Get hash	malicious	Browse	• 79.134.225.10
	Purchase Order.js	Get hash	malicious	Browse	• 79.134.225.10
	Purchase Order.js	Get hash	malicious	Browse	• 79.134.225.10
	Payments_Copy.jar	Get hash	malicious	Browse	• 79.134.225.10
	Payments_Copy.jar	Get hash	malicious	Browse	• 79.134.225.10
	SKM_C454e20121811360.pdf.exe	Get hash	malicious	Browse	• 79.134.225.39
	kWGdFglyCp.exe	Get hash	malicious	Browse	• 79.134.225.77
	Covid-19 Data Report .exe	Get hash	malicious	Browse	• 79.134.225.107
	Covid-19 Data Report Google Checklist.exe	Get hash	malicious	Browse	• 79.134.225.107
	Price Request #20210907.exe	Get hash	malicious	Browse	• 79.134.225.95
	Quote_request.exe	Get hash	malicious	Browse	• 79.134.225.95
	tNC1w6dXQ9.exe	Get hash	malicious	Browse	• 79.134.225.76
	7PAX _Trip Itinerary Details.pdf.vbs	Get hash	malicious	Browse	• 79.134.225.27
	RRGpqq27Rl.exe	Get hash	malicious	Browse	• 79.134.225.21
	0sTLyRfo4M.exe	Get hash	malicious	Browse	• 79.134.225.53
	DecodedExe.exe	Get hash	malicious	Browse	• 79.134.225.27
	BX3RCBzzgf.exe	Get hash	malicious	Browse	• 79.134.225.25
	PrYRLweSZL.exe	Get hash	malicious	Browse	• 79.134.225.87
	Nj9MXR9ZsK.exe	Get hash	malicious	Browse	• 79.134.225.21

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\11951071\gajb.pif	Yingtron Miga Trading - Request for Quotation.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Roaming\11951071\ahvhcqjqgl.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	567
Entropy (8bit):	5.472953119060523
Encrypted:	false
SSDEEP:	12:Wd1+ofH8mHeXEcPvuWY0OYvkQgs0/yAEk4Q6QBDWmlZWjcpTwrwb:k1+CHTHdM9Xkls0qA/npBSmlogpTwrW
MD5:	3D514D20B365126A9035EAAD675ADD7B
SHA1:	8B2D8F3974C6B064A8AADB3958B732C75B74A0DC
SHA-256:	914C2F97EF3D94733628F1219968E483644E7ECEB50DC9DC284F75F32D70B887
SHA-512:	D556D975CD812034AE661A2B20D137DE5CCF71FD79691D78F218AB13E9DB5FECF1EB84AD56EDE43DBE63DCA68C78E31D9DE3096B7E093E8173743834951D5E41
Malicious:	false
Reputation:	low
Preview:	d6iZ9Z75C22t4WXA9p3k9f2I2x3W4LV41970a4g3JM5d71d93D94213jBHs5279K91720iqR5b6C9p61M4GFqFE7n11fjfQKwY3J6h6Rlu15r54A8rhA4L18l90b1o77342a24..39gQ21365C83K8z13u4g28uS4277Ks963J28W573fj2..YDIE11isd5R4A7fVEN93zCvJ396T09L3i4B70DuAUW51lD2nB..5J225D387r43R9SxZ9s6tPtQ827R3J94pGq111D12d81Mx64EVOG4jjh802x697a28vZ4l5o622o9..Q14Djdg1Q5d09828004C39u..t40H3z..67yX84z4LGL9Lg7960n859t072..231QiQ8E5ImbnAD694nuAUa8i2271ssl4bHzxrK0R82r37436om8673EOG8mF8S1o64DD75l92vtmfrxSrr20H2f52Z..m0zA0FOQyRVe1IY2Yt4yH89o3M31GB9iUKtM9xb79XSM0IHJW3n5Z02167Hi4ImZ0kIF41o25Kz86l0970D587caP0W03R4230v6..

C:\Users\user\AppData\Roaming\11951071\ankeg.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	541
Entropy (8bit):	5.473088791965721
Encrypted:	false
SSDEEP:	12:4hu2YXeKSgcCK72UcOiQEw0kXxNXz08R7XaSwVYcU+V78zsRk3YQwVVZ:mubMC02UrH0kXxNXzzXzDN+h8z4QwVX
MD5:	0304CA3C3F6E4F1EABF1103A1C62ED9C
SHA1:	0FAEE889C21E81503BB75A66C75EE76CB3014FCE
SHA-256:	9076C0E713B7FCA5FD208AB1FB6A3F761B363A1433FD030FA2E082922E4EDC25
SHA-512:	85BA6BDDD30F0EEE772F42B852E99A50CF71FBD533BE3289056866FEC69A45719FCB98218E0459A88D5B492654ADDD431706116455EFC58C6CA62F7C4D6C3F9
Malicious:	false
Reputation:	low
Preview:	e8qv0GaC893t0896l8uiM0nC8p56n8aF2mE588yrr27Q0hOLVJ13CUHhb5MQb270j9oF30F498cwEcpt7jzZ28607KGs93Y4I3T3a792C1ZD666X26160R71z5W8cS134FK31AP73Lek04Ski185r3..0Bb278u8Z49n614bX4T1O19qq2y1953s9y9py535144eik71996J02Nvl01j03f41e11P7o5279z68aA2F57QYXI9T99w9K5I2..gB07K27vYh38I22088B56Js658..jhKPS22p2r251CK6255dx45V97Xm4CstcoiW7sh74U0RB5HyaiT608Zbi29N11z023fvQX0pu94pm7Pk61dB37dnxn08381S87Pom6O3pm4o9..F06828A4SL3VUF1M15AIe0520L1X7TsZ3354lo2c85O1W020BtL63ufAn9CE23hUi2E79mFrWkcE8QXvH5d9J8J..q7I4V296a4o7152PlT0l5w4q511d6a2702p6577t123u7u0Yn068O62b78i..

C:\Users\user\AppData\Roaming\11951071\aspe.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.448670575141328
Encrypted:	false
SSDEEP:	12:qGo1KDr1yr9K7xhx3nx32QtwTjVj/fJfvQay26AUNoRbvunnpPCNcEu:ehK7PxnxGQ2Vj/fJwG6Ac2bvung0
MD5:	8F3DFFF797FAEF9B7126C0341705A2A7
SHA1:	5904788D2FD700B9772064EB2AA5DDCB6ACB44D3
SHA-256:	CC6C2875037A4BAFB688559693A670C5A64AE318E17AF9D15D75565CAD298362
SHA-512:	32A85B3BB6D2D377DBEF9A73439BCB7C256BE7B0A65D584F64FC9B844DAC43ED76F94553EE3B2C0EE7C8A49CD3B39985235B5417E9933F2EA9C536D223A3828
Malicious:	false
Reputation:	low
Preview:	975U4d62x7Dct6371xwh1b108Blhbb1k7uIkT94imBNy77629LMuy5qw19930804HsN7H3vE29V4lLE38OG51g5557tPZ37JbnIFvZ398tzy032kS5w978EG50T9v58F639RzzH3AQXSs9CqI321BNFE8R3gbf0Xc..98s47K6b4h5g5gp864..a13fa443104q7H6r1g7x522DB76d5eH3M4C7Cd42wt35poo163g8nd3a2i1DKgc7Y746615s78l4I48e7P796KjA158xAO78kE73IhN0xT4QwtjL46215Pz..43ij1U595390Cz460B4M5D95F57vv856p2zs3Jf894SDm88B7Gt4u6ClxbPaKYl49K1n7z7u4St6P390ZDGl307W5R3P7f3Ih0G009a018l80YG85S6B2Sx3K4Ob357Y0audGBw127g00886O7024xUQYy9IJg830v1R3747243z974UR6O5Z4iaB03k..m3u8X9zrdJ8PF4p3746162oIuw212Lv58211I0h155Bftd1Nd2K0D8oq39r3567c367M2RQlY6C635nO9q361s5cGiT0ql053m3386BR2x4tU43D2J3P2512B95B0U96b1PK61834KS7U0hR4..

C:\Users\user\AppData\Roaming\11951071\axeu.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.518388067582385
Encrypted:	false
SSDEEP:	12:/FigckylbUODoZX+hm0XdoqjHpBUd9SPDDq9/8cZGLdi1F:/JyeO+2o2HpBUd8Pcvcdi3
MD5:	5DB02A3E07DCB4B674F61FED65215B64
SHA1:	C94F1EF6AB519C54BBFADD958E07E6DBED84BAD9
SHA-256:	148A4E5CF07462C460E4867F6F361734279BBFBF7BF57A38F6557F314EBA1611
SHA-512:	A11E63358A4A2677345847515BA443AA3A34FD56B22D0FEDE6F2F9A8BF3DBC7B46A862A237E52ECADBECAA5FFB878BB76D8553ED251D854FCF406F7058989DA6
Malicious:	false
Reputation:	low
Preview:	74918Ey049O98SV9769otG88O95E99p..G0sg63n2hfu3u2Ms71ePeKy5A8dSJ078Vj27e8A9956v19R2l4D1K8WQB5C20Hsf05pP3y493KV15N8c30e8rBC7qM53MWee68Lw7c14d78296o8f374092e916YJ82K4u1h4rU6724ZT4YRFUE1..s9W13R1mI97Z8b7fqbhCPb066VJ4S1n04sAz..5z3Lk990NF2067JjV1l94..maD6BIo6Hf34i8469ZM51445pi7..7257323B24xmS81szUXSy43WuW0h00EhnAJ6UlH7B9N3Xz42q5n8K246EA6d9JzdF9s33w226r0bU96yiDiDi4h6R39A7qRM36vfx2lR..bhQ1qy5my2y631a9Q701pG20Qdo8n16O5T22AK3Wq6Xm53z7g03Xa91L7N075q5X..001UA803u3tbqmukRowQxX0M75257v9cj492Yowa00R481Y70p9N9A955n4B95p48566sF8zaAw863w5rd809DTuI9..

C:\Users\user\AppData\Roaming\11951071\brqgqvajhu.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.531812594516927
Encrypted:	false
SSDEEP:	12:fkl5V3vT/Wh0TSSZLBM9zNjh919jId2BFE5UYzn:8jV3vTGxSZ1wjhdjId2wPz
MD5:	547793F64A9D28599BFBCD98AFB865A8
SHA1:	473AAF492EF9FD2AE911EE139791082F5A62DD93
SHA-256:	DEFE1B6D2AD8C4398C68DFC41E2AB5DC2583AD730A87C931BAE495C9B37EE82C
SHA-512:	769D69BD70AABA5221CB1D35E2B6BD40DAC8A1262BF0D7C5D169987FD81B49FB3245FDCF4F299EBE32855439BD92F6BA17D3E49F52C2DC90A914F52090ABB061
Malicious:	false
Reputation:	low
Preview:	9LH3V96fr7B32gHuqt3BoWQOl5Lll37WCrUaWn735dN4px2qXNsnUms817p34w06N015j7WW7D44B2U9eQG0789H3WB318O210F5Mp9IN8..489ni78o64W19g7v589P0t757M3cl448HKM75DqB44a6eurf24DR487l9li5jC89Q58Lue4cp3Us178fd0A1q70JcEaS689tglzGq3F88jM208I0198j0926..8q55R29gP5plTIz41R9vdm84gKY5bVa64T1w22215cQvvZ36018LzbdBdHO7Y5VqWq5757838q64KP24g893hmBxefwI426Q4K9l99m3V54FRF081Ht58Y790XwMPy2X4kgeq38..K30E32dPF47Xn291d0QNi5CoH..Df1176A2ma7MI..630432j15k8a1nI1YcuGb51X4I4DChc9v8KJe31l5d37qJb524l29YIkaFncmN5005w053jLv462Pm13N4iS0..6chK36WP559s43mrG0X14G94AM612k9ip33..

C:\Users\user\AppData\Roaming\11951071\bxxedaa.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	608
Entropy (8bit):	5.535457072095192
Encrypted:	false
SSDEEP:	12:4R96vG4DoSosDlz455RD7F7SrUSTxj2bo2Fb8GfoQ/u55ImUXpc5v:De4DoSosDlUn5Yrttj2k25pffGfImUSv
MD5:	838C4995BE00D2A0C3DEF48C8A748A92
SHA1:	08E59C32E0391600C756903A37BD5AFF6ADE9CD1
SHA-256:	B38924B75A915F9B6FBD6D412D7EE7B023C1B6EC0F417F46A635807E2BD923BE
SHA-512:	550D748D34C3B8E77927CF1DD6488F89E657E4F5880959EA2C8501C4CF587E8621FDD78F29B98E13566FF2A6067B2552857BBEC32BCA2453931DE7134C30BF88
Malicious:	false
Reputation:	low
Preview:	f1o8vzYkf0EigXN257tHj864o19V76680Cno3QSg5AUC007b568FRc4O71l278MN605F1aYq2n14q4Z4vp3FHG..OSPq62sU..u5L1y8DBGPx6Q251cx6847Y120z79u2Owm7K25ZpM635O23wo3T3..67q3l361748TJ2DKa6cLq7lnh6PjE28901AD444U2W5NcWc27dvaN3Kd2x9m19624PW4ri6csd4x063JF2mBsM8L8i7laB76BEIy3Xgu476e3Rc36hU0X8776MXXzJ951w9VxMME85H..R0D2009x4ZS9663322tR2e915AP9cs9bD923Rc6S8e7pC19QixF3710T81dr168O306480FQ5nkO0IR209..MRj7gnW22XE7Qdv62037u7qa3B79K4HEF77814H..yV511870n8A02x87jc9899Qj58F78w4Nr8S486ti5306p3T7O9a077JB265EG392G..h2K13i9859P3ju14h89v6FLWp0v84G1mfuI5VK8XnTbue65HpZl5SB289uCkusC189GVv5923P6lHws5L4S5G8rul83664v68h2e5Pd25204v0l1o4DNH3y2o..

C:\Users\user\AppData\Roaming\11951071\cjsopd.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528

C:\Users\user\AppData\Roaming\11951071\cjsopd.dll	
Entropy (8bit):	5.465244472386269
Encrypted:	false
SSDEEP:	12:QyzOpFsLT08dyGSMcjdML9/29o3GZe8W1GOQOU:Q64F4TKTMS6LU9Mq/OU
MD5:	69572E6860248D563FB1A001771EE49B
SHA1:	2C66745680488AD4BB2FEFE543B454F79461561E
SHA-256:	C0A617A8C9299488E986836DAC89D268D0AB43EFC2C30B91DD1B2357FA3E501A
SHA-512:	37C2C9DB6078C5DBA6E8345F1ED33DB4BBE7CF0BDFF493EE367140CCE6A646C24D82DFE246EB43D228092FB3DFA64B55CCC19636695FE8265309E6D7A2B44 A3
Malicious:	false
Reputation:	low
Preview:	F3N4Q8k297ip59j2HR28KUvC7PmAh945Gv20m14u..o5nGr1203TD1nv55I4w9kZ7qz1Hu49677T1x0OB90cb973iH31r438H2FltDw2iF1V383V2BJiy829347Bne34F9 30l8H1KZ845n67Z41bj0..HQPDtWW0Txqo496t609myTT334b1PYD764U34rIs00cL992P48050OL2H0R3Wha8d698066L7rRD2DF..3yJ7Uh09g148385WB9Wv68B5n0F pd1S671K5s16OwX8fms8563NxYcwk1NSY8684ShhIP043kWI8372dGz85pOg9..01H71r8UK12967hI4S3y0jM2L2L94LhGBae1ymeQ09a8318BOtD88nZ70L2yv6Ap5aK O456dr47F92Oqpqt419lu93qJ2913..S4u0oX34wE32871epN862xn047m9uN85402G46l1w4gc9n8nLU7BZuc..7C09832uL394k35K34009F9V11X846iV69I5O562my oD0052..

C:\Users\user\AppData\Roaming\11951071\cnvmwqqe.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	550
Entropy (8bit):	5.4361391304808295
Encrypted:	false
SSDEEP:	12:UdspGuSCucrNrJJY6ln5gDAp/pb0p9IP1JHW/vz3NftXD:KspG4TruD8afIP1E3N1D
MD5:	0F44BAA43CBE2A0A9E0A53C8E54BB492
SHA1:	EBBA1E273F7E243D757065B9B798922061CB7629
SHA-256:	796F8C17101B1EE2A88D2B8899B0167D0AF238BF7F97375C3B2E715E8ABC3583
SHA-512:	0C2705C0DB71C06B36FBDEB2985A0FC5678296DC2FF3E4B30A81662B4AF4B7A7D303250E8C2F1A41F743083CE07C0C246D1BF0EA32D91D96C084EFF2CF65E6 8
Malicious:	false
Reputation:	low
Preview:	36D12Te44zyDXH5WpfvqyvJ1fg9835j8209Zp682U2UCd2J87hPid1o90dsn1Js105SlF4q07K3Eb2f..02rDr4317X8xNK..G1en49s51v2xB8HhcU401743QK0342W0x QT3tTDq4l6J334KZYUPjL1K1l5D8l6Lb34397P22y..2P991M01C1K028239w3LPf5151TcR9HiRd65787oj8V60b51U53b5oX73hd925nslk3..0O8FJO802t8256KF56 01F0Za6ta2477mr5zV166261rsA9PZ9094C2gh2lP841A9990145er070F35o21516yVl846O4t0VV108l4irgopw7B673Y5256R1P26aB8522X6044X823F69..1Cs207 Dx4QHMaD70Q1nQfYLMAV265k..5T267GZ7R2940N6D50x2L777QptOX13T2Ox7h479Xy2309xdJ7m8Qs64HD6oQ5A0yi3e7jk319V7V10kG9f9WX5TB95L7g eaP17P46DdyvV28U7O7M514xg5Wf885OEXX8ef..

C:\Users\user\AppData\Roaming\11951071\cqwk.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	544
Entropy (8bit):	5.4885706747740395
Encrypted:	false
SSDEEP:	12:p1I5e4WwwHwGri+Ch6drvmjTxDh2Rw9bVs9ryOulaJfH2k2cV:p2RhJUj1mNhqwG+ZUJfH2I
MD5:	591E706D197BD25740DAF0FA45B44D6B
SHA1:	A30B3F886D69474EB2180A67CC517A62FA5DA01B
SHA-256:	77FC992CBA890C3228F2C91C87BE15EC2969AF81851976BFBCCFB3D649229828
SHA-512:	46260D87344F57E2B3757FDFE86686F9580BD0F6DCFE2095C0B68C1380FFC3F5817A9BC76CFFB06BE361949A35D4C51235188C2688D45065B913F38B97966441
Malicious:	false
Reputation:	low
Preview:	7Dov2W9q072806J3mba4iUAnP776571k3Ttns63l3L52472c8tte41873l37jtH6D..4w54MQ7U208SH3c332Xn8Az34266558Xi44Ml5Lx4rV1W75UN7N6289uv1n253K 603MH967Fh15dJPk9521A1..BDM5K4rBS94A30b75cxE7ps90Aby2u..n28z7n9dk0rnnoMjJh7968864k0C9mLkYy6JaJ..gugZ3BHN7Zid09oLy8zHW3e8BscJ172607 j50q58N8198aos7W6mW4mL801PO19N5c5V940V348if3X9RY38S9ihL3206R3S1hrnW0w2Jw8k9F1ClA4C15dRu59GI1vW521lOVL0FNX5Id70818Q..Y75515wxW9o461 sJH36053WOq66Y4t511lMUA8kmR16N594e..9758314136572563abLTTfu66Av3RF60CXL1plcLfURV5..LeO5Q5SR1O5u5aXM31zrHQC0..09GZw5u29OyV23ZNV3237 G664837Rq37183181799V7..

C:\Users\user\AppData\Roaming\11951071\dknr.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	566
Entropy (8bit):	5.540047244594396
Encrypted:	false
SSDEEP:	12:BpBWvv0uFgr4Mrv7wZp32smjq+5LTzsXYfc8yk4x8YxI/EzOCTGrGB:BGv3Wrrrv073OjtLTz8ntQXGfye
MD5:	2E737BBB9E7AEB8C4D6E97E0E34BE065

C:\Users\user\AppData\Roaming\11951071\dknr.xls	
SHA1:	611F5EB05DE76178DC95CE856BC50D7754201238
SHA-256:	F07AEB0D6D925A00E4320E3C777F8F6EEEAE645590E093666E7DBDA95E0F6A94
SHA-512:	77F1AA2D40D4604FE6495066F42A812CF688DBE8765B959E2701BC52561A9E53B618DBE2F06A41978941449C31A024229DC4F433907FE3F7C27DD25172F2A10D
Malicious:	false
Reputation:	low
Preview:	T2K8wJe2y0fUogi91wbB9Mgb4rS9E2971LK74471CUu1863O14l00Om..wR34rP3wt74aN7ZZ2P80c636..RB2c60931cDufS89w83l7198D0894M42TY4Tk5Hd8Q5886f 15BH3r0Y1l4WS048e263x2j08oyY4sJ7fa8z7MJx16VAK11273K26pslMkT3m7L..3TJ94F6U14Kr84JUI1a3zGQ5rX7QH1CY1S134BJDM1Vrd6VG48fk1d5x66E0s8L42 9bLUw7v6P2Hf7I..e0W1DS68lE2Zq5I..7Je3L663X7Cz5Y8tuzLQb2d9YUh286K0860g5O06ip85aR43JlY47Q1..pXvg8Bee6254y02B0O5826G2R06W0z7081iox75w 4aWS4G2EJl3L5WfY984NU6zE96niO64W857O4rMAfZzTo158u543rpE1G4l06nvxd341Zq0454qbiO5KH307h6ZaD5JG50Zh782vc32Jw..0sQVy02q3v7R6l8h3ZQ05vk xe6L6i4H9376060F6Ki38xZ13PO5cX285uuD9Wz7cr7e..

C:\Users\user\AppData\Roaming\11951071\eelc.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	509
Entropy (8bit):	5.409102485739743
Encrypted:	false
SSDEEP:	12:bnbJ9pZVHUxavMuJKXZpcE83BdSOGyO8osmLobOEdv3:zLCxkMrJppyfSm7z3
MD5:	68AB60B2A078DDCD40A88CAD65D05485
SHA1:	D02041A7D4C6A319232852AFE2C804889836079E
SHA-256:	94E1B664F0902ACB7158B4A6389CE019AFFDEDD7908E299A348BD2ED7CBA8E3B
SHA-512:	93E7E38B251F6A14EAC3B0A7900B53849307F98ABB4BD0CD24B0D953C8C80E8DE8EAED23E15939550AC883FAEBDFF551AF19CD6EE4FDA2E52E247B37BEE12 DA6
Malicious:	false
Preview:	iKL89N6080AUbU4922q86Z6174By5A70623M48291rBuE62wKLY5676cGGNx0l9s83n8303EYM83xk3eutk0bS56k7b972Z3u1P0DRME43t88W91s169h0077bYa67Q18L ..94F1Hc4t4v8M41jJ5U52n4vEi1JuuC0W8..Q2QN4Y9flq9ZI39or3KD33DA8m52x7961C04482Ts309J9455J9339wPtL5BN12qx3zR2mkny3Lpc5r4f70K91..82C22 79HR8M6NS03DM7y51nqlD346524xIB9pW50Nq928L42WPu7QpZ77Z6s51kL74UF9r4t08Sn5Pfl44a2UL5f84X5QbJ37l780U64D54D..G2B405H9fa9lJ7264AY7GX744 9x3pC4y7N2NX679gS8VEe77T3414485s4wv5O1d549iJfi2c78DU0m147ZfqC30S5293Y035lf5Q9iUg43ZM8..8eP48O1s64nb556cxi3lJ38k12Vk89..

C:\Users\user\AppData\Roaming\11951071\ejimsbax.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	563
Entropy (8bit):	5.442368115657612
Encrypted:	false
SSDEEP:	12:YGKMyQvyUoskzuCrwpRmNGPGLdmVmobGwsvAvoE:nyQvosTIGPGLdmVmBLA/
MD5:	252C96B91AAB7AF290FC5E483967F4B2
SHA1:	43E9F132302CC74360F7E26371BEBD2AD27F504A
SHA-256:	3975711258AF89D69F1F86807DCE9D1AEEA28F5B9CB2E6957C9D234372959A2A
SHA-512:	6CD7CE282380498067A8D39F4598A4305E0EAB3A99D2C8E25B2D8E589F7A4C34CE7A7188D7FAD40E332A326D30306757EBEA101BBC3F1921482DE63EE25DC88 9
Malicious:	false
Preview:	168r6sMOuJ1s1N48yr269FgDkl461l0aVZFi598R5Z2P8BkVeybs6kDXBT4D5m41D27tYR20d00HN424Q99c..xgf137s03QklkA5X2O81F47pE248h3k1u0k2003T71C1 12m8W202v667s8upQK..7ZGeS9w1647GG54Q29M49W1541btH9260VK5sI7w9n07x1539n66A4SatdMs7647190R55MPiAj3e6127G9xV6PZ43124X7dH..Tc53g62HMj0 5D8HQ41q4l75jm0rfl1Z51XG6UJsjq1HU24715y6hFa527N298267dnoS05SH11..4Ciic6j05wtL6Sydx3RNFsGCh68gSk32810o7U9x4bJ437Mo31wH12a..xi63kdeU wW100xe56mYG7okx2g79klYf..l490e0ins76n1t67lW6Zbza663MhP8V182Mo32Cx147sF8194J26ZH3270fLVY80921InZM00z9B74ng49082A8999348K8b0D09I161 O0IW2zQ629H7w2d5l1464c435002168sqf02452r8..

C:\Users\user\AppData\Roaming\11951071\elkn.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.456270473889659
Encrypted:	false
SSDEEP:	12:0NKqNzvovJUSQlyzW+j+gTnbXyD8uQpgoY863kmJsX8J1:0NKqNzvyJuzB5XcBWYzXsXu1
MD5:	AC7CAEF93334EFFF75D5660793334073
SHA1:	0C75841ADBDFCD6185430F0336A1D481B68885D2
SHA-256:	C191F4E746AB50E72C19EF4AC1C58FA3F3625072B973F41A2A200C1DE309854A
SHA-512:	A3BB649BFC955B02EFF58A15E980F8F087CF60E76E218D556EECD8E79C95B1A3D11C28FD615E9C185D98B93C96F99223A05703B4D7F6A269E69F70FE9B9A777
Malicious:	false

C:\Users\user\AppData\Roaming\11951071\elkn.icm	
Preview:	a88452jE22Uef3zfiM6vN7284876G5h40Bqr0VGynbr978LB63373y4M686235Up7N9m4Cd5GV8M72193Lm59A0..E2s6B8x0673Sq3UG2rOUA815L36bfPCV93B9nIP512yqx54y9L747X1VOO1b6I429y3tl9M445z983u78wV41k3P35532Aa7En2338z9156n6876AdG98NV03E..1p1f9d7q733rZ1QP597Hj6z8x13g56i0v61XCg47w5R66G642777S66Pj774d49e0y1rFr3eqCA52437kIh669kU2Cv2..013sk40u90UlLHa000e9w94dI069r0mK72WDP3FqE89797O25L3oQj1tmy314ddsRJ68cVkX31326TGo2Y18TY64l2GRw96Uc778uno..Lw21ER92504kAz47y5164380xYcq5G3DD2Nnf..xgmB35b30XWIH5QvmS8dq7Swt7323a5fursCv2n2G8YMg48VApyayAJ88yEk85E9..

C:\Users\user\AppData\Roaming\11951071\eltl.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	573
Entropy (8bit):	5.52549131142605
Encrypted:	false
SSDEEP:	12:7JVddjOA/21uSboIhNgVymtSBQ2imanpCQ3hxyn:7bdd6A/8boIhSfSm2iPZ32n
MD5:	B76CCCB78C282303636CFEBEC260F135
SHA1:	B1E6050C8D8B13397587D24A371EA49617909850
SHA-256:	0A41F72DF06F6CFB8C1D8AA443150F02804C5C56DA4C97686A4D85A80E569A3E
SHA-512:	C39363FC8F7BCFD580DD7C54A7D431377E344D13A89403EB82C9F5E165001735481BB812B33456D3B214C90EEAD83BE21FAD1ED2F25DFA5FF4FFBE937915550
Malicious:	false
Preview:	k95jdAUj1648og5F2VOaGX8p6Lr52Ni8Dk545hTRjZT95Y8P5..mt18OTx42Wz89g96H..5c0Zw4v5B92iS81k1913EmX9y7xhk8473676a4MI9ltM300v462b3lwODRA38n67Qd0vW4..Id85c0cK741v31lPHF43t334Ec44..rLQlJ9Obr591Z7EIFVE41G9B27kgVx7l87b1M1948fF242zdY9442w..399dr965890b98XSiV5a19Vaqe420JA3s562rb600wiN1r6l87vxZE2no4dc80nxC0quTJBU752L08xhs5P6Vp89Z..0LG8QbUi9onJ3a1A5d118bI6Vh3dmz26eMW4424d4S48wsN5xF2B838A3RU59v912QPP5wjn22qKs..3JC39Cts162y715X1eoW30ZO5l6C9652w72g3541G429Z27515929HgcvW62hU6kDoEbm4759w8s3A75f11503Yn65M47Q1y45J6Fn9345v55aa70J11j3b4u17Z5lPyFJA31Te16rM7P5L9j89xle69n27YTP948Ztig8splW95m..

C:\Users\user\AppData\Roaming\11951071\fogankl.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	616
Entropy (8bit):	5.461346835846518
Encrypted:	false
SSDEEP:	12:GRFTU5R628KkIVgFdLXANIA2KPRctP0HPJi+rMHkmK:IoIJlVgFdzA7iP0RRCRK
MD5:	02755AA8BA17785155EC56992DE751AE
SHA1:	FEC47A5E88BD87AFC2D408E74D523CE62BA006EF
SHA-256:	2A91D386849BE12E4FDFC903C1EB94F220494BDC89D55E3C351671A94C94A182
SHA-512:	C0CA8F6FA4D8CEBAC61AE998FD6CCE6B1FD6703E321E63D9427FB55355A342B01814005D52AE1C696B8C6801AAACD1F4C0B9258A97380476C2BF61701B8477I4
Malicious:	false
Preview:	a1MSDYGs4MW683xb3RG676m0MX4m1IXZ01a0e9lc17Y5t9Kw9W80JSD7NxBto1636584q6Uh030J9604BLEbt..022jW70S85535973V3115J59996YtN62513247794BXpS6a..OGab7Wq78XZu9p2..3dVPmY7ESsC8QhVjh371703W2Yjg3Z2Y6Yu0B3a29B662N0C718k6M2bX7A0V06r958GHO85g545qspLi6DTU1Hzk3aY8M4T47653..2z0v432W4BF4aJ1yl01605518HpFx8E535B12q51c28829xtBWA5WxzD..38s0ihZHLnS97FE28046xv2394up2Mb5237ym5..6Z612Fl91S9R5H43MvF5Sr7h62565QdUqd3N4128750gS93B909qCol8N3Gtp8H1WZf33z0151lK86542Y2J2u51tnM28gN4q4mL6I81Xrc5s9o3jGtJq4dq7P99JP95KB355e4J1hk..z35524RP8UFi51SS2Kp7k5x3u0yxHrJ93xU44aQwJk6H33rG0895LG637zl4u26e661CR8d0fVJ5655q07NY39811WWl09g33735RgHvD86U58H20LoxK6v..

C:\Users\user\AppData\Roaming\11951071\fqcfoedv.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	516
Entropy (8bit):	5.433402798037229
Encrypted:	false
SSDEEP:	12:v6Zpn9+HqHfzYb+d8mVOU4LrNhgXPd5wkvcjxHI6y:v6/UHydJVdXVk+z
MD5:	DC900C8B8C27445E3A52FBE758B6836C
SHA1:	D2187001DFCFC2E41F22CFED2756C54D7CDD39EB
SHA-256:	3CB978889AA16FB8E198A3FE0EBB44892BF2F13FC1B9F8F378D332EB5FFE6B29
SHA-512:	9539305F49EF5DB0660356D3CE3C939C013DB4EB93109566A522407E96D394D790C9626C747998248477B6C61A17D1C77A8D220793AAC9182E9DF8AE5EE55513
Malicious:	false
Preview:	40557e067sVKg2di..S3y1K7lh8i99M3X4y6a559f3bNV4h89371CD921b312R7v94qkjud..454F0NDj68w2505Eanh156Svi0601Ha8300l3QWJW56xH4B1tav7g7DB1EtKR4s2F6HfOz4qU13t2e8MoT038O9HUirLxz8449Bd7L..i1M14B35C2nP3N0p330622aw2ApV83p49yk5aw6SNQ881sU1i6wGliRzY1Nvf0D67mNDC0O1bZ9CRNpd488Za324Y78371241eJ67tkm22TT73zI991595gt2C6764X6m5wj313v64067x2G8T162938h712jAD1993097EcVL9..koU25f18Nn589TJsK2f380g948Bp0133a0G435730w0Kb2p077EA46s3OK6D5f2hA2U45DSVdLo36D5N4M8tF1cWR8ywX8ili3At1G..u38W180l1U2W5429Th901114436w7w83K95P746NTL335eN2D5z9Vp7409qi..

C:\Users\user\AppData\Roaming\11951071\gajb.pif	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Roaming\11951071\gajb.pif	
Size (bytes):	660208
Entropy (8bit):	6.576031177867133
Encrypted:	false
SSDEEP:	12288:hBzZm7d9AZAYJVB7ii/XAvKxRJBnwvogSJ4M4G4aSb5DGDt2:TcneJVBvXAvwRJdwvZ5aSb5DGR2
MD5:	6BE533CF863DB26D953917024CFFF914
SHA1:	36BF13F22165C0997A727D828AFE8F0944F122D7
SHA-256:	85A25432737A47B03CAF3783BE66A902F0A36E70718C3CEEE765042EF190FB9A
SHA-512:	84D774033E091A5830256ABA96C0CD46EF932594C5A400A944AC4A95D0A639F762FB626CFAFE4D0C0B5B4311CCEF8F6C0573AFD81B5D9CC14E068BBB8C474C6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 25%
Joe Sandbox View:	• Filename: Yingtron Miga Trading - Request for Quotation.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g....Rich.....PE..L....%O....."..... .....d..... ...@.....`.....@...@.....@.....T.....+.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc....+.....,...R.....@..@.reloc...u.....v...~.....@..B..... .....

C:\Users\user\AppData\Roaming\11951071\gasqdiunbo.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.532754703488522
Encrypted:	false
SSDEEP:	12:41FK6k8VXRdz2fWJq0aQsdDSn9dCVkjL4aYWEEfdnVgpV6iccw3:gF/dz2ud9dCVs44jge/L
MD5:	FD3E04CF7DC1CF50DB8CAA9857B889D0
SHA1:	3F00F7EF7D05354EAF789BDCE6F73749F9CEA3A2
SHA-256:	1AD7423220B9024753B93A9CEF6A925B11E1452255EABC4761320E92988F1E0E
SHA-512:	22CE12AAF57E2B0AEC700565470FE4EC906F5F2EFCCDEF0E01CF239D4E9CCE3F600B454F21A015698B58AFE3676CEAAB7B12809302B0943E6ED9C88D600C77E
Malicious:	false
Preview:	2r232eAB9L200Tncm5b803A7T7DDr57c8461tff4g54630sGx786Q1O9E5NU323Hp2O2Wi4W7C5hJefb7101y9021UM708QytE37MoyPP03dox3G35JXG10n0s4zY..w2k3i5t384x09PJOLZoWY25L79F66..l8j9bH4qBxnO81BQ9ZF72Yw22026cnlU26342u8CQ45xDF7l8X93fb26358Z8S9B978M49s810u..v4mK844i6342705223bSbaPX6N2cy6nDP09m035CKoL947qFa34CHFUgK8t6XKY5140EC9fe7Q5vLN..IaEXwN..lMX9QZ4Yj81k46zwDZX..9k3G6w42T9nHu8J2..0529YNW7I9HJq3..2lg22466we8U0wA9O83f14K97ur6Y1EsA3ED0Hp72l89072881yyD3v2Vr5A3BzQ05w82w60791Gql7bw21567zOaF0hRJd..eR7J9F7W3PF91015z64P8NW725PQm5F9J6D78zMi02pcAN2r06Y4M82491t108yLC3995hsi395v0WQ7tz74TER1W9Jqv1..

C:\Users\user\AppData\Roaming\11951071\gnqkqriwhh.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	585
Entropy (8bit):	5.515376595397559
Encrypted:	false
SSDEEP:	12:pJlucCB9w1/bzP4rHE6GBg8gBv0v2Y4aXukUpv:TlwK4z/Og8gZ0+CXcB
MD5:	9D3534E82068C7187EA7B794F8E214E2
SHA1:	AC5ABD53835CCAB7AC50309729FE690BB999EB06
SHA-256:	672FCBBD5B7C76F7DAEEB1FD74F1710548E565A0948E70E2A7B99466F2E270A8
SHA-512:	9FEC57F21A8624BA605F03F34CD37D9938CB75AAF17E01FA785D2358A97743F22A128A93F6849A329615820BE2AB713ACCE5EF266E74010A1C78B2B5778F453E
Malicious:	false
Preview:	1153R671160y8AI0048P7p75569mXM35IpO1nfhu87D7K20W67B90w9wJJO339VcX03c22Kc4z36S3vpY0xS255rM5aVlO9me8SS5S..8G5t75eF8l7670aSEHc3BP2V465wNY49Y85qQ39P57C7xDm38g53y9226Ufsi476l0V0aR6133yhP881S5C7qEu4774617qle7j5034M1vV0752OYKO5..beA149LdH7383Vt11V1jLu7A7hC4j707T571..8Y3Rk7j69Y8V9R1Vpv5ZW84TCdb0WsOvpx43133f05zU4in43KKWY717c7cm4000421KYu8r04zOg3Y3757g8El1EJEhx9J..E12KvzSqQv5EkqWy83U8Gy0F5mK9B4nKYK2M1iNO5zw490n5K3ml7rTf6Hhh12lQg38260uAT430w4y6CA29dV46o56hn447lQ5MN5n2b..rlzt78nZCS4x0SP7jiO9e7B41O8E438Tr6kl5jO7ub69X9104W8ucRT23Sji792RS3K192aIu08935GQsTT1m010d0WpO48USR8aerim5HH66AN90gn715I..

C:\Users\user\AppData\Roaming\11951071\gpmi.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.429443779988652
Encrypted:	false
SSDEEP:	12:HkXvaNG0ysGZU3w+MqwAWuZh4l9Bj9Tonof/zhXx/LET6c+ZAVMo:HkfAG0DGqhMqw2hcToofb3LETAZ5o

C:\Users\user\AppData\Roaming\11951071\gpmi.ppt	
MD5:	64DE8DD613C278C4BBEC6127CBDB0D64
SHA1:	8470DF51799CF0707DB6ADC202A2870940116835
SHA-256:	A14C33D9B8522DB3D0ACAB44146E291C6351CB9C2B76DEA631D2B786AD25B7A6
SHA-512:	ECDA1335CFFB3D8B96682067D3484805778D6E5A74F4BFF82B03D03E8ABC52851C8638023438CDD3714030A50B9719541E9BC24D0EB7EE6EDF56C6549BA41F9
Malicious:	false
Preview:	8U681P47280..sq92ctoJN6726337419L1NZ8F377f5q42XcfxW3x6Z7VXZ53S832hO8625Phpuov5112vKEYE99024gUI7g6UqB3T1QiX3V9iXJF652P7PHK64u8xCAo5 3mAGV58E3ZC0..223l31wyQ25I602pARE2I47Cxq653f8x7L316C20567s9282WG33bd8U83Rm97M63B0u304jdwVHLSu899330t4n..Jc914W0w99x8NE1774M875cA7R js9OgD6w..7n9K2Ed2k5DgJO33HI0g721AN49k8835UN6S9KxZ24I..PiI819tuib7JR062HT61096jV1J2T09y80438I4qz22P743MT916882745k9LV6mv431qFN69j8 i854cQqAgxdW21H0Ea168XY040717Qy231u090ad8N99P08R8W2m..S0z43wE6WI0c51a1808BWO0Xy5697d294EG3l9T70sK73oYgS45oF23498X1Z05u579l7332tOcj t127987071Ytm3Yd0KO3eBYo5dbS6uq3f9vA4z..

C:\Users\user\AppData\Roaming\11951071\gxgbtra.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.480886025036129
Encrypted:	false
SSDEEP:	12:lY0/gs8YjA1QvxoAs7eMUp2rOaeZ+1U4hBiup6ZX1h8XAfeLK:lb9A+vs4QUgBpgX1h8wfeLK
MD5:	52712FF8009B874EAC52D92D69639F3D
SHA1:	72CBE9322B23C5EDC9A2547D6C3684CC1919861C
SHA-256:	787385E0CBC1EB5820F8299394DAECA05CC539CE92FD83F0DCB917B7B436C686
SHA-512:	ABC115B02B10938B2A5800742782DE8AE23CEC2CB865B67FC3057F28DFA29A48BA4796D6F383EC74EAFDA7E14D6118A476F8CAC837309B728D70EF0C7AA75DC
Malicious:	false
Preview:	3365M363Bf5HH0M61f3c3EOJr9Ya5b450893BJE174bksC22m306m009FP8LdvEiurUQ..Bf42L9R64D7yX269b8136Pf..A24K6klQ99O48mx14N8i50y0GGaZkn8700T meC0Gm6dCvRb5vaX98DiKhzxDc9622133qMtUsma58Ee3f18tlzBc059qyia95w990m9T1Tqd3P3y87Ld013pv44FiA6tz68548b3B4w1a5506Vf219G66aNJEn8419u.. nqqyli77Q66170lv94D7H3OV15VroXd31tj6sV8J13Ny42OaW80347365201n0u3M86Bd..bW5N902Kf02Vf205uY24i695M120w412BkxMXDyv..qAEolX54R8Y367i90 7qOU3sbyH4s0z1zpdq4h43a07d1802pSiah4lFn57072Si645244nGt29r289pQ7B3fD4Hsz7Rd..8239oP14hN42FMH3nIsCC26760oD3nM751b80f58Nf05MXBYs9xJ0 Jj09413XzK78V5O625Z8ME587QX2R1N0u8Z0075z78oX637Bu36Y40x919Hl924J637XG0y4Kh2232z..

C:\Users\user\AppData\Roaming\11951071\hkimwptl.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	541
Entropy (8bit):	5.457281811321593
Encrypted:	false
SSDEEP:	12:ETI/zh/VRTvMfH2RBCwHxgsII3kQJ4gEERIvk+PJ/cn:Z4FQvIAkQlZ2kyhE
MD5:	5FE60E8EBF21C837DAC74F3CCEB62F8B
SHA1:	6020162FC0FF05476B4B5BC995307C596F5E30B4
SHA-256:	354041496254728472660B11F852393CBE7BDC4470B63BC96C5546D6128E965C
SHA-512:	538EA9A3A29B7E4E91E50F7500107330FE20510C04FB011807C0D2587A684C51C0C7EE73AD41016B54E9872702C1C5B2F27A4E9F5CAC75104B3AD08D8F656E49
Malicious:	false
Preview:	6W2l8R1qt2g1craun3gB8tY745YJ2n77aK2ES6Js657zR4O054trX6N83..n734036v337oma6W6M49K24F53ZUg4rr6m6f7wm7h83985le19723v2Nle8Ts5z982978aD n461467K8i30Iu1627ikz5xjzRwXVs4..R6432AG2n90B0J67q042Kwat4FH5O2n9n8ZD5w25704G6j6i947T03510E80U896ze3634W7r1Db70OkF3kblNY8..n4YTP66 4U92N3g16tK002j0534V32j4c575e8A98BSZu3s8xi2l09nO34b1p4CwXRg386KBi4UopW9M3KqnBSY68200Sd464087pp3d50z1XAz6WTdgrI2J7TUP1126oIm4C5x399 p5GjLr15jh4W6L4PK..0i61ae97lnhrdo26494263kuqJ320K47093tV0b2387Q..41Yl65B15a36..2Di01rf8alV9rWN2326W4Atwy6X3042Ea6s9nNbRh7KGwqZn7tt DU8a2eKV5Ev58Q2835m..

C:\Users\user\AppData\Roaming\11951071\hmijf.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	511
Entropy (8bit):	5.344117767092808
Encrypted:	false
SSDEEP:	12:yhhV9Wzv4EQn+9NMUFNwFjO+uSd0zLBYyTfpSj2DFEewde:iDsv4EQn+9ZFmju1zLTfpSjXW
MD5:	0958DE4DD5AC41067148A3BCE6710EEE
SHA1:	259273776AAE942B2518BB23F51C13BA9EEE15CF
SHA-256:	BF70A6B0901EF0DCAAB906040F8B5B26F365FD647452DB017791DD2AFCDC9A3C
SHA-512:	656CEBF0DF542202636FFDB7A072777AF6DCDD1FA9DB71D9341C5CEC7B6C57514871F88ABDDE70CC08C47A568CCBE0B6B6DCCE912E1E304BAC3BF503FAAA 8807
Malicious:	false

C:\Users\user\AppData\Roaming\11951071\hmijf.dll	
Preview:	1QjZ9794h242c5X4H0Z1u6hm74rLeDYG0q6CUv62S8pr5BVX3792XQ3t65..r1J1T4362R985D45t7350I251R7997Qs5CH7789QC5P11024F661zBD31LSOX855Q5HkN6 WlZO5720..D5518e8r62w4bvr75f895On5HSJ57OUO2U01c..D1387CL9067mR115t4BE5B22089B853Ji3G1qIzo2w5Y1fPP113X3ZdqK1KoK80I8qFKaw72QSJ9..L65 9onWC48rFOnS6q3M9Gg953bRPHBc029M46gMe99I96KC9968k629maF2GB607n290p48R008cV7K94Si18O83834wV66kdwGAo75769V9JQ4..Smz4i277l8 E9C51JS7e80S644d5X4275z1U4v49631H72fm4Cn5Y3980d784H7199155f3Ob1W1q9Z2z68xu78c348255Aeq5396c7F0130xpKB59OTV8n4566J94I3U2O89oT7Q8C6..

C:\Users\user\AppData\Roaming\11951071\hvgwqd.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	592
Entropy (8bit):	5.428115068363785
Encrypted:	false
SSDEEP:	12:1NSJTNIcticRM+/bMU5zZsaD/3MClA2Bg+uBX4TukwdGR:1kJSGj/bVTND/8z2Bg+WY5TR
MD5:	4EC79460363F7439F99C86A79E5D68DB
SHA1:	25AB0A6B38D80AA5F3BB6AE3D01AAB8DAD60F71C
SHA-256:	2CA51D939562231AF6A4DC8618ED368BDBCD467363FF0B71113772F9350E51C5
SHA-512:	58FF50937D406EBB40B6B0D6BDEBC686FC524F92C02AEF1953527DCD0F7AF807CE5AD247636765732F1DF72BD5A13391D88569BF4FB5503332E43FE763174705
Malicious:	false
Preview:	8xvg0jxoJn8y1295Wy05KC69a8UN153B17xvUE6OET83y413618076g4LX4ZV1U24M3c0I8okzm29lMmKPkP03HWw326Z2944y1lN3k9KTl36G3iwc7817DGSm7g5r6K1J 07A20F..38z9j8wITVd19t8DC68y851Yx2884NDO5766P4Kf1vIq69M0475FTxu8vnZ613E0C3420y8v3i1hoa35A252jisiMz30E8syU032o2q2506D9v7s726E6WeC.. 1g9V93681tQ0Ex4AwL3e55s78Aa2I10895MH7C4u2g53B3E8L25X10a5pje2EkS093Sm4u34085014qgk8JwFP..b3V6747cOZt14Fgkil2JmM842DU2Z27d0oN26jlL31 1SA2908pg848M22j501NKd427m6k84Qs1L6wj2FrT8..91f6x052G5Z21G3r1mb82N9v74Sy9CXo2lBb03St6H1552r340V088181253g7k5i2qoO6Fu1f51157JGjx00D RI9w5N5l1N37992F167k6214q38lzRU87j9T818P0K192nD0C346tQeJ7z82K4824fP1nb..

C:\Users\user\AppData\Roaming\11951071\iqabqasra.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	527
Entropy (8bit):	5.444509179872839
Encrypted:	false
SSDEEP:	12:3HxBCp8zHIvDp3Sz2yC5VDApb+9In6DXdSyeW+8TT:3yYHoCzEuDn67heWL/
MD5:	02891A128B389705C69DD46727348660
SHA1:	9FC921BE2A902C808AC9DBC1DD248D268783D1F8
SHA-256:	BD583F76B6EC2005F55787B23896E8B4577770BBD55140BFC84A2459A56FF367
SHA-512:	AC2BE946D779B33CD292AF030B5D926F06904617FE336651770B4D6E371B34209865F931E798E37CA08A55CC55ECF8381B870291705D8B4D077E8B1C8AF1B014
Malicious:	false
Preview:	jWE19As49chFC86W42H43F7e9C05459xjkg0j3nR07I58l22t95N1C6fXTQzLH284X487..tW92T724Q36zHR690r932f5YK0k61y143q6d..04j6rNA29D1Fh8A3hO7oB yQa3278957V2DzAuLDWf6o44tG38Z7v79ET5M8R45NKHIhPd7P..mHpTM56B3K5o2RT9704xFnV6w4P89G8223g2W48h44aDTW291..S2X5f546LXb535E31BxNH..I01P yf20850kbEw69Yj2Os0g6962mco2tNe2vNg37wj9237AwYONK1c9695B4977V590..8108Byw388rZ1nV8P4Efck944u64096t19S0oV1v4a37rLJogY3v6RN6cGe6Yc19 X018487S7k0XD2wtTHI3M2PX4ORGkL40T64V9uN0nXE7940EMeO05Vc76t1Vny07915jN..k49s956428Mm38HfK8N8C3Wn6v8v10N40Vw5V9r88B6f0Z624a3w63k6459 N557A..

C:\Users\user\AppData\Roaming\11951071\jupweew.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.461863442182498
Encrypted:	false
SSDEEP:	12:qFgXOSdXtH9PCLBqSeLu0PNEfBpQj366oX0ivk7kMB:qFvw9HU2Lu0PNEYK6ViyB
MD5:	3429BF8FEDDC3BBA8A89471954AC69DF
SHA1:	D104175CDD7F5E7EE70E311C699603DF30EAC74F
SHA-256:	F159E88460A6C485D9587614EDAE6FDC9CEDA20A8CADF19F106136F4D10658E5
SHA-512:	7B005DC61DCC8A36ED79DB8DC01A7D8DB35FE0ACEEE14457CDA9E63B9C08E8A1C91F35F996EB09E6A1C70085B399477CE18DB8EBF137C182CF203F9651E63 08
Malicious:	false
Preview:	d17xwSW951126579T4hn0T130629YorvFjFNbkt82wA4399f3T4xU7639JTb13Kb841u8U481RTeSq152b62kc6bc46H4fr8a3culfn0K7u02MhuTkK2P6f9nc3GV4Y57K Oju1Hk2lYmw878o5738L25ST6C438n4..0B85070wsJ1NS9KOTDyj3z21lS240w9jl5l4f1t2CGh3RF18011z2w6x891k501hgJ1z4eSQ3995Nf56153437Ym417SOD397 hyi6zZ1C6733ec1gqvWI..m613XK6sAV82c8fNVY4Y5HiJD4839Mn964sDn8gJJ0139228z1Blj073exWSQO886Om80130936QG0r6SK1Pb8590p1Tt3Br5jQ3ZY10240T G72aRU8gQ99S39GpSwD2lsr2Q194xEH8f..55b9jA46AEp2mI0451yGQw1a7034794z1wV786f3553W627SCJn0zy6UG8U14L1o7C3D650w87cyq..

C:\Users\user\AppData\Roaming\11951071\kbcdj.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\11951071\kbcdj.msc	
Size (bytes):	502
Entropy (8bit):	5.42173294555183
Encrypted:	false
SSDEEP:	12:5J3vfQwT+mtmVXdwR7XdHe6NPiRQLiClfaNmxotwIPkRsWNMT:5nNtmVX0zdRNqRQHfaUxLIcR7e
MD5:	49C7D97423F18C893A4C49BF700A952C
SHA1:	F883BAD0E6C56D9DB43ABBB5300E01A2347D1BAF
SHA-256:	2A27BB05EF131AD66585213C1BD627FA0878A952980251CF7EAB7A71FCC129C2
SHA-512:	78B86622EF99B05A775B1D03918E2DED7A019FC9DDA18F14CA57A620C079BED698D7D91F91C61CAD891788A14C494AE04E99C2082C33F0143C50057E533A200
Malicious:	false
Preview:	j8fjId7T5l8TEf9oY..Kn61l31k1v4940xy1PzVA0qlu1sFc6nxV924F0580KnR1WG3f26cM228976F9a8zcPE1j4Z83f923nfld8Ky68bkX3tUl5Mm7j63610l0l485sP6W7kV2776040..1Jccp24n2OXzR9O2sx9Ofd5NK..61Fo02O9d7091TO36wX2phe4CPPF08S5X449ZAy96qx3N9t618Tn78p5WtKe4876YMd88200IA1kx9ILRkim54E7g641RIj638txM1M4ZL8P1..l76ECZ09w0358457273Y77wC217I89E4T..3Ps2Of44T66Bc6RHHs8ogq5I45tH406emW46k0g42MD8G6R96M02h0X0292c1z31G39911V491R3BY71n2c1c0S17x9215559lCZY133k5SSy4O6H3R1S93QkPm6g..9M6127kR4Jm33c56k07V93Oz43jP48b8T5hb7w719635DXE9FGc5Q449..

C:\Users\user\AppData\Roaming\11951071\kvoeo.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	541
Entropy (8bit):	5.449466788366372
Encrypted:	false
SSDEEP:	12:K2Z5BO0phRotrapWCxmMT9ezaIlxcS5xhuaUoP+Uh35:K+YqRo2WE5gOOxcM48+Uh35
MD5:	793D5A79CFC3B14E65BB8A1AB6B9B411
SHA1:	9D2968A7F40F9012F45FB8E3BC31AB04EC852CD4
SHA-256:	DD56FEDD79089F33A27ADD266DF713D46368950A75901828794242DEB05E26EE
SHA-512:	4297B9D2E72E6114771738212DE6E195C44AC81E39A03524D99AAAE62AA7EF8891DDAE94AF849E8AA40ED18211A40D0D82350533557E009235A88E793B02979B
Malicious:	false
Preview:	zgan8562p5X4eg8iiq3i3t48D..og4i8UQ..nI6g39c2v603Q8M0qC3p8i6Co12x218zX66..rxn6CY850sxIt849rutn0W2oC6iABY8wn3z43661IP7TakRnVJ08cr17e432022H01rQ4A081d4pf36i18HUOKvW6Hxr1638XT1fn24L6s405Hhx215..736b395Ly4Y6Ol38jbX1u6359MSy7R2HA68o..31c9l1J8X52F63W5C6xnPXT28Pljq5882sG4ZRUc89NR99x6f3A0416nDN56ciT3R9g57tFbk8B9zc694V1..55r3726xfu240B79945l0dC812c9B1854b820t17F50Om42Z8AU44Pl5308738Y0sX9T4ecWs0722071085557ZXl02S45527256J8056HU594Ad6V4siGS7e23s..pn2TrpZx1652cIS5A6A9VHms9P5y8BuiEjXK895FS9k8a11V5Xj943NhhF6w66AP5T1495e421TB75v270rQ7B1DpMa4298jfIM3..

C:\Users\user\AppData\Roaming\11951071\ldlax.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.497516285218884
Encrypted:	false
SSDEEP:	12:mnXlQb1U82sNpWHX/FkphMISNhLENXrzo1KYDueEP8vyF/EHZ4lkAhen:Q1G2sLW3/uho1KquE4qn
MD5:	BC18DF105A0FF9AD611BDA7F4241DEDE
SHA1:	C733EA2E505AECE6B76A8F7D0CE83032C662ED27
SHA-256:	A3BBC72065CEEAD8D744245CFCB32017EEDDF2682E95970C413CB1E8D5CB07DF
SHA-512:	9D82681DED35E367966B55725C1E0F64C887B64374CFE62C0E3DB7FB5CF01DA39CFA6F0D81936BD6C5BCE4874BB63305E319348A59F4AB965778579BDB49C31
Malicious:	false
Preview:	YF1cB80lC1U1OQ40uCg4p88P1Q075096973N9I76O19y0dkvHs0i8WU..f696CSJIp8J8z9z9T1cdJc6i8K6087v000509N5Ut3A4RN31nOsP6l9GM2463B89Uznv1i..XI6L3TkclwG2v467nED19I66cp02941787mx2v25a7k8m9e17wr4901Nk2t9JC28uJQ3m9V71yK15f7099u2X..4bqCd..2f52Nmy1uvC0226ECr0oc7h5fnav9CfIX0sG9N5r13zG1z36hdra2L4314O4y2D4sNBd6IO81q3462U43255FcJ8O47807ZzgNj78Bz58Nlg..131cQZaM..740CZGZ69033z8qlCy666F60h41b4fBZU4tLkN2eZ1063t0a30j1eW82570TBSh49kIvU112PV9DbP72223iW1Pw85..t235m53h7gh30O7vX73G2sy53y342TCRYXIO71BD65SeTZC887Ci1MHPp4jLUM01196G5G532..

C:\Users\user\AppData\Roaming\11951071\lomu.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	611
Entropy (8bit):	5.425879870468657
Encrypted:	false
SSDEEP:	12:YUIQhDKkzbNcyzcu9lh73WjTsCdaTMdz17gnFICnz3scfXcstBfvgZoHBdTIg7Hj:1MkzbNcyFJjW3YoF18nFVtfXc6CohL7D
MD5:	540EE0CD4B895B247C000A86C4C36422
SHA1:	7A912B95F2A69C11A6957A541C129BABC405197C
SHA-256:	4D7EBFC41957713D510B6DB819F4B4063DE7FC6CBAC4290D098F701B222C83F3
SHA-512:	29B2DFB01A8616BAD2415A9442EEB63F6D8E75387AD355D53AA81FB20DBE09CD95268E3C8EB1273849FBD83FC44861248DC660F0D593119D5FD0D1EB4B7CE8E
Malicious:	false

C:\Users\user\AppData\Roaming\11951071\lomu.icm	
Preview:	1d131X2A82ER9v849SOI8zp7o991x9Unv2DvpTi942z80oC62d0a6x1s29Y1O8Lw5e31V735w3xX5y1S..481b5K1SS2l6346uwwI149wlm76er9oj39mxz4A39957115A5vR355cz5S59t0230Ebe4W7Y7V33JP5c48062l61..96x6sbD9H14k0..30yK779d7Aylr0Q50l8M8zkU493Rq58G300F1D1Vu84b2b9d8M..033OO65VdbSv1B29EO10duw608zRqesv9y126wTDIh3DG0vI11285xN5N941f36277N39oQ33232eE1Uq69ZH7sWn553vd59wtVo8017y270rU4R1kbb08l14K7MU8G1u639821R2h81ah22cEf93557s8909052271..0z69rj86aQhoBX37KI9947a8U50hs518hJ0U0jW3972L8ng22S9152x10f4T..zp5R47Sk96k5OCO5kCG36Tu1CVM9E50iW79SYNhS4g376K6907391E32iu752ev6003r7C93V766HP604jF0khcStWM72u38oJ29736l4XsGOt18554aZJGkEIIj5r29pUDuD3AW6AMKVB2..

C:\Users\user\AppData\Roaming\11951071\lwibsqbclk.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.476440038111399
Encrypted:	false
SSDEEP:	12:QLLeJUfXoMio+mVADqca6XIDqCykicPcoXOkcF:QLLexYae36XIDqcffC
MD5:	485EB8D4C93296EF44D2E7202D70358E
SHA1:	F0F9EBB7CB5D9AC4AC1A6F46CC6E5484676D7512
SHA-256:	49811154AB7831D87102E34923AD30AE61970D76A147EA02CA143F6C1FDF650D
SHA-512:	49D7EC44583D99A78924E15491EE0F3C0A876707EA6FEAB11E77B15A03EF907D4103F71559BE7A31D9BA2FC2BC46B9A040CB091CCC4C796C8CF2874F6CE31CF
Malicious:	false
Preview:	6TWs1v4L0uwK24h3hrd2U903529m0j41g308d0l3d30M3o26l44448mC3h58zm25H718V3h83L37557e415m93Eiv6c7dDI2qSR4905CD2Wf9013H4i8sk6cB8oh1f4f5xOPU778OnAM20A93PbG36r20vCpU60dIBGu7qYfzi39cG..6by61JE5D390045A8ZH0028Q4LKB9KD13Yi77611730qOD7X9i8n6OnK749g9OCKjGDu5R89n9Kif4a464d647667N49..2Un7V5T08Jrb74YZAa4Oy0udf3T4n1l7675P8P703255V162bh8ET7CVPEGU0w613G11WLtbs5k5mWnK0Nm29W3WkPWFBQu08H22Cq13Zv86866Iahdz7s0950742l3684R91Z57pqg..KadxYF2Td598905Mgv09..0547f67a0Yh3Amq8NJbk758L8TPag807O936ZPRz11665R1STgaq40Tri79Khd7E29e533Vh2nb7X7JXX9im..

C:\Users\user\AppData\Roaming\11951071\lwmklmxx.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.502216386718625
Encrypted:	false
SSDEEP:	12:uMMurdMQhkTlmdA9ofoO6U8torIuW6OUbE3MQCTQCv:u46QyTqwvU8tBjq9Tz
MD5:	CC87607E7A24A710B5C8099AB811AAB2
SHA1:	1D55F3460BDC4C2B4320A6532EB0FFC1A2745977
SHA-256:	2678281BBBDFB92ECF192411DF7B89DF934E5850004665BE96BCCDCD08619F27
SHA-512:	C4BD91A45C8A1A9BAA2FF16EE4D88BD483CA2D653A2F39C8A7EEF0F0830300D91B2F07E22C327008EEBC94145C4F986C273C07992D511200B7AB5C43FB62615
Malicious:	false
Preview:	rZWbz4513437cHxv83g8lp66q7327b323D1QWC..5jpJ73IPts6c3V90BU7Ym76916FaPb7G6r5dGQ..93tl291ISrp5ICQ0F85t1jM8p4t0PO9v31Eh6Y5s0079q05bP70S1150TlEK3R1J27aVv66776P09H3Hs4G6GB..Y6n78v7dmi7f6p06R95w69pr42r27W9ezk0n5GN09MR5..zD2Z05F8Ho94770AJlVlleY4293lhw4acYBVOA0a9692t582f8924GQ23lV70bD..h067gVU2913cb9445Jq5oPj4i4U58oWd9N4Q7e56681clUx054g4Dq89Q69929S0tf6Q9TAojH2X2mH4DeKP2xE98xFMD92gLsP79962052som977f7DD2yX5y1WWaBn774iW43076..sSn59V2D5..XaC2gK799RRoYl10nd8o77P0Bsv02X9Tc8X9XCA3G279f523866ll4af4gvQukY3UW7V576zbbM54615y74W7F4J2WrF..

C:\Users\user\AppData\Roaming\11951071\manapvhvu.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.548352569454341
Encrypted:	false
SSDEEP:	12:yjnVmjVSbGG80QwOgdbfJvVVefOexRn3jNSbVrc:yjPXDdzemebn8bVrc
MD5:	3D9544D66FBFF28EA7667FED6F924000
SHA1:	3D8687A7B1FEAF2B39579426313A83BB78B51D1A
SHA-256:	78CF579EC95665EA07DCDA67614F88B82DA1D2632A47E5CA51130D3EF7ECC3EA
SHA-512:	FB8F3C51DD35FDDE8443DC669DBFBCE6DE99D2926BAE8F0BB70989F82844C1E98A071A259BC8F6839BFB0AA895052A81E5D5D137E1C827E0181BB79FE1D697F1
Malicious:	false
Preview:	zoC5631p4G853658S6U11U8f54132lUJ8p46q04TjzZa87c82j31bbfZYZ522vz3j4r4d78K0q605H4iq5A80i111szgaLH5w1s8I7HS429oh476x5mW80CjeZC0SDmty6e1UGUT..mk5aRe57K22Tkk4Xk9p1eDLTvs113g47YLcG285..8RG5D9X62hG2mR04bpiQ5HXzx3a3J912t8B41z7kk1152tt3P2c047us666Y67LRzH05KI690700..CRoP906phw77l6i0N0H3YhD30199M0s92s045LI..F23323xs3jvH2774534DQ4A3xv8s49w9124YZaeS34u8..E1wYa9Nsgz75Ow9uCEUT8Q86Ms8Z72r29UfKg04K7cd046CG0L15370u67ubHc29l8p8PsuxB0emxgAZ59b1i4E22kYqXJDW8a02WY8..145cPe1D92gn9ncbd0tGoTr31XVs0tYA4gA82191..784341y5iI1eX397A4r8NqkC93oRJQ3OZ98ro93vtp4..

C:\Users\user\AppData\Roaming\11951071\nIfeqelw.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	561
Entropy (8bit):	5.5815569668917755
Encrypted:	false
SSDEEP:	12:xtUFkSVsj+BG94XKZvo1ihTSiVdDVDMDwTdXf0XysERWUUWzLR:xKfaKBGyUQ8LhDYKLs5UUWh
MD5:	B1063C1A2663243D34BC0CB3C479377A
SHA1:	94A9C0705C80305162AF6F584E8B18EEBC71FC1D
SHA-256:	C36A9CFD35B72E22D5142AEFAB0235B644AA206C4E81CEB981EBA64271BAE4D4
SHA-512:	567342161AB30EDB99144F575B2168C58BA263B7169022CE0EEA4AA5F75B2BFC3B572425600E5A184B16BF3A2652CC026649C713553A54615F695BC37A2B6FFB
Malicious:	false
Preview:	Hx2N6T48OF3y132vQowN97n7ck1LF10X2bFAj5g4i236DQF3mT808611916680s64TBf51r47yW60hW304tE07473U0ZM11RT6C28kpTh61NJ3TGes271X1vD847v..z99 I1o3lySCS37NvEMJE45ROq8ZO61B564H262w05PdoaA1kyU8i820E1451MkCb8V274q3C055aY4..6vH9UNNw9sg0290E95RD9hK15zru9d7XN9608afqrm2f46n5F5f7y 4..Se9rZ92e8rhAF9ZILm0..4J2E..8c1f99l4D5LI18Sz0S32RiytdE48v0DyC43n958pDX6ihu93c0Cqn3300Q72C576108GZErz668vWpJk5pL4CVXU7..Xq6o37F60 11UvUkzO9622709P4..oW595xi1pwHwEW61aDT06MgMBa9L5fU0X8l2K481pLmaL3W2O617y08C3TLO44e..1t3k27oyd05ZUI2E7mgA5tMAVi1umci9zau36r3Qn1ULOL 05F5I2eUq30B8W797760s137M2B1wHViR4OnYe3..

C:\Users\user\AppData\Roaming\11951071\nnhnm.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	5.522447111288225
Encrypted:	false
SSDEEP:	12:k6wyMUeM0d4Oiis6IpMIyz24QliU2oc4w7A8TjvOAbqCei31zgZWWo:VlM/d4OiikWzBiiEwpTjRGM3ZLWo
MD5:	23D0FCFCFF5FF96A0249041CFC3A4CEB
SHA1:	C363E4F95D77CEF9148A8C2C7CA714FE4DE83D32
SHA-256:	D55F4E6E93F9CC987A14786A1E5CA1EBCE1A5A457E7F8C5C1AC20200B01D3E0E
SHA-512:	9CBE61A312BC09C2321CA4C06AF29D421A4955A09E328548F073A95706DC5F7015A270E9328F93F9596B7D2A7C3713020C163A5206DC4CFCB3E72E30BE8A90F2
Malicious:	false
Preview:	72YyP5T53225Fsl4Qz20V51454TfnW7Z7n2Gk5XU..23727fHaEv60ZA8is67GV82Ezr55Q7hEu6X9Gc3S06CVYX8h9g108gLM4a6Ao7O4S418b841R7..113632HsM9YV 5z964PO2UA6R8a38Ls1k8c6W8uQj99B4c62mey430r53j40N2w50766711rn30i5Eh1j..NqTl6BmG0Iakgdp8438h6608bp99l7232Vil8fX4S07j4G426FerW8op5384 459ltTdOR2y899658VtP9H9bu7V91k04U929581G91Rr0qHUPacqf9yIe2vd54eZJC..pVp4Mz2pMO4k3bOxe5M63SC4O3kD0I35181QSGYRW0G927r36c2XrSC912945Z 0032l5pAC1137l66GVtB695R2nx0v1eRqzo8D7636uC9343lt39W07Pe381829Gz5lI05WxLOMf6B1cZ9ngMW82w72pV58PaTbp0R62v..mot62608FMtb8Z61S08xtg3c 222M0331e5z4Yc4RHF4fsVK4y49Ow5X9Ya9Fiv6ykpz6g275Vf91D5jwwnOB51lQTI18660156cl3667716Z32Y35rJNw..

C:\Users\user\AppData\Roaming\11951071\olml.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	314952
Entropy (8bit):	4.513142467063521
Encrypted:	false
SSDEEP:	3072:5VK1W+OmF3OMG0gfBlM/OS0SOlVZygDDJlDxr/qdmXHJ1sod/:5M1W+OmFVgfBS/eplygLSmXJD/
MD5:	460A2D0324F7A6B5D8B9D1F3408A0FEA
SHA1:	6AF8AEA240C9719A65CE2EF57A2C2BD4E6EB829D
SHA-256:	3AE500DF81FEDBB1403D53E45890A5F5B5F8CE2F68FA1F07E6ED8E65A4A97164
SHA-512:	75038615DA6250905237645DD14F5FEFD693B018670553F4528A17BD966FE1F3258E144991FF5FEFD542635B376D3364428265DC586D5AC3513F79E739447D22
Malicious:	false
Preview:	61HcE8bX4T..7173ICm63681518J2alGkDy6448l1Y8FV33730060xjl59oxX1gKtfAN..07uC4qG4zpJXI5ZOqtM4b8K3455IpN1K4..FPAlyb1CTxiJ4927Yc..s35L77076yO42H1 D8219Wj6v78W5Pa3gQ23Z01Wwfln90p270005F62734473lIHdFdnX5m4T82M8..9q5U7rvKzT48994Dg6rC8B9269219nB3Lgan3kgSUkWPOc83Cq8..96328V041a769 4CakAcz479KX07g1ED9eS4Q4327..347e123728l6qB4s9405Q3UV5Y1V23n0WmM683m21nhiU0184a5JN49oze2Bq0yR5O..1p413K1oJ0Y14H7t0Pa0Jp462r61Q5xU2 nFz7l4wasuQU8MI5p6QY2126t..2b8497935HZ50056Z48JjvQ53F8lgE5cX44445jS5649Kf7Nb2k6rAwq2PVN40Y7..V921Pc241u52dM0Bv29e1T506e94E29X55wbI 59Ig0F0I9K1C8b25789613o8K7..J062J134k3Y6ymeWOM3035595O5K2xXX07459g..cYQVfg2Uve45P61V1904T3Wa1..8eg09c93Uy6nT3msfKl5D1JZO2g696jv5xp 4794M7..N89f978f6BKI0y0nBry3955v6K27DpUJAQ8BdvA24eZw8P548xkmypG3440c7508mC013Dx7..vf29N10eU8vMzSN7XtYdNP..i18Vcu048758Q66..vM7U764 f8SC4F8bABZ48imSq2h9RjH5U00j57T3VxP..e9UeX2Yc58Wgy074aVI286lJ8z..9PJ83a591z7hq5x911KwAl5Q055Q4G215Oa1Zd92186g8m7T4g15O2F96ZPD204ev u13v6AOP83sp3Hr5u1I97lL70L..U307Q19PI1B3T9i03G976V16e408QAEWTq81X50199q7x5Qt2iN9

C:\Users\user\AppData\Roaming\11951071\otssvuwnr.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	544
Entropy (8bit):	5.3183638690573725
Encrypted:	false

C:\Users\user\AppData\Roaming\11951071\otssvuwnr.jpg	
SSDEEP:	12:EF5hXs6YWcj5H2hlVKAiwxNfwpzZeO1RwrtdNthMqnMcuIxB6Sy:WhqW2UhPKKNopFDRstf7QSy
MD5:	175E6ED2550324F189F30F0A720AFD4A
SHA1:	A978C78F52D34B21EC7667027E7922B812E2B500
SHA-256:	2C923CD16F4CB0A90BF7E9C6481E3253658A5ED07638293BA84AA81BB6F7AB06
SHA-512:	94435C2ADB52982A31416DA2E467418F477A6F760F94DBB0A4D05731F50EF8624C2080933C621E5FBD14192A710B164A41C54C6AF831AA35080C2FE13EBBDE46
Malicious:	false
Preview:	c6149v0E32hf0OY51s91843S345800148L1g4Q8d6534C67xJOV2PNT5v8E301o40Z9n603CIf43272kR4b8132Q7p2p427LP1z5bF4ji46v8367kYE7T93436BVuv50hN 083950334L500Y358XE23Sw5468Ya1RI81Iz..5p56cnti5N254T6oeBj1Ji8E970l49g08P7lh8otKF280Tuq4N36g88WX6n15Y55r8E6050xYc2it12160z28qi0Bs2t1fro8qtz80 8320ExZmxidTR49z1hO428C4ozB7iGi3L0014X31..1405z51Ry3zEV9B6641W7c730w10FK9R5U2D2Km0h0E0y47ox5kw0yk6367ww462H1j4u7x7j9Pg9H71ae1S8i54 K2Jb9180P116czl31Q35q4g8Mq0016NG6950W5W6E5S72p13kq02941043doP..q7j8305D0v7sqH313qv693D3w5nCt59w478g8R1yZ790r2y0b715bPq31Ed239k8lu8 0MH3C7DuT645..

C:\Users\user\AppData\Roaming\11951071\qsgrrpnrt.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	509
Entropy (8bit):	5.536899162441955
Encrypted:	false
SSDEEP:	12:uCcIybHx8QOx8gsM06/no2VeVCPW99pjSSZxz2PdAjopEJI/inI:jcIybWQM8SF/o2sCI9dSSf2lAjyEeiI
MD5:	A671ABBE1BD81DA605D94762DB42C99A
SHA1:	B304C8E694908DB35B8E14C8390FA09AB7495220
SHA-256:	41C97210E8ECA03604760417132EA4F3C75DD359827102783FE00D1C75A816EC
SHA-512:	99595DFA7E64FD7369A0B0B7B919B9A2601F9363F53B2CEA0C4F97D6EEF00C34AF0BF608ECAE0C4C4679047CC12D91FA87B5AE3904CDC7BCE48F3F9C3CC00 BF
Malicious:	false
Preview:	09lMDy9C8lC637m02sR68VSI29s5lq4Lki4UY1W6Gk1j4H397mh8209006i73d7k9Ix34GH3bQtf0DFDKm79hj0s8Y53Tl18ZVo29q4nns7c5521072JS33IX3m2Y282s5 49q8ndjcnA23X..9GU311Kdt94GD78oQ3807l1M2777I6YSTLEj7U86s18BfulF10H31zGvM0i6r7o65110454r86722ERs6..Nz39260mh4UR3DJZx39xzX9P33G53T2a Tc3dw10Di5zs3NLrh4c04p1t1EAJo91w8L3m31Y595U1N557ZM50CHpgno4lACEh973XWdI5fl931R87r46d1h6lxQ48k0Ku21OF7q72U30804gt0823wLu53v86KdEu9U HP2285e9y856VSjv4K3x1..862467nCT2vKTF40m84D7Q411Fl76J7ywCgy2X9m15Cei38vow99m..J54Z968589Wkk71WV7GOT7BB..gP2qUv2vlyA6c..

C:\Users\user\AppData\Roaming\11951071\sarw.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.40867542865717
Encrypted:	false
SSDEEP:	12:rMQVZSu+rU6RzqZ0JVW6fHr0qUDnkUIttl68DmLmbVtsDfT:hQu6U422HhHhikXK84OVtsTT
MD5:	CB6DCA0FFBE7887800E5AC8BE38B4F09
SHA1:	86265A24FE8EB97692DFC61569315C6D6259473C
SHA-256:	A6B9BA1FD99226E1AD67C89774D7AA6A89114E4365A821D1D59A4FCD61D60A5B
SHA-512:	A9BB200DCB3D636106432B984C353323366C025990E886714DBD1BAD7D3253E0016EFF82BA54FCF2DE9888869359384E7BE1572908A49F9283D1CD5E0B7D555D
Malicious:	false
Preview:	7728U42FMT6E3164900yOUGO3OV9180m96z3570u5TFAxyK4RzUX97vR48yORG4Mg4g3Z102C35K2X89Tz0KhN9X0d733C1Zl67WErC7fH79H8jP6E58DEh7 Q215tD6s3Pt7A8921mT7spd71i1VX..v22g392O8vd1c59M61n7J1b7i60W9RW9iq0Zu9Is816g81Gs3EKGi8hgr0R5wO1zt42224b128I8DF0K687g15M30M606C82744 E1FC8E..YzO2mPH060IeEE3X9gi32P35f77447g86158l55hxgwj748191tLTyW20R0O6SQfSq4122p4C9k158ERci70D7NW6E3vmO3h401636c2Zu653pUX1ms76383Kp 76I..M4Y215101hb21US365r5m0x3n052G51Q1MEUS74T3676ha77CJ85954799k05jgq351HD0xUvj..99EG706nXJpA6O83dR2m8ndb..wV0s8053URI..4nXplb4q5w j30KyIHp17f14F47300K2087mT9..

C:\Users\user\AppData\Roaming\11951071\srnshi.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	563
Entropy (8bit):	5.412637384808098
Encrypted:	false
SSDEEP:	12:qJn8MkA1RvSbEtOyftIRAjETyqe2wqjtDYDuKy0AUsVB07DEkAagipXP:NMk4hOyfaRAjE2qe2Djtg6SPEkA/6XP
MD5:	E1525EC50D44A3CFBF6ACC48ADAF4ACF
SHA1:	2833D026796E36CD8B0A75483584ED11D2A759A0
SHA-256:	0DEF847DD8A5B277ED21537B8EEE9D707D5E104952B5C3E9A18458C48FF48CE8
SHA-512:	B0E29900E94685190BB545C127DF3393038217076082DCDE9C51496A73F9B9A02BB5F3FA5FA3A66721304625BF9835CE6D2E04E10B13981A0AB09F9291644F46
Malicious:	false

C:\Users\user\AppData\Roaming\11951071\srnshi.dll	
Preview:	5I1174ha6iy7cm1253285V3s604D82YoV4120eVE6I1WQlcr0H30G955q648M01y9Y557698L5LY30m3S8z65t31177h2g4xlI4l2a7Uu2zO238575BcD2L24j88FR0U4M mJ785c43XJrA..8nhN0b10N15LtFn8rMH485358562711s381yr0n9609nRBkW7l5q1achaJR942926J0r494e9xS6sDm34XJ6q1a2t15A7kv22Dd76l94a1l9dQ82297j 9UFwN360297..9i9708c61EbUO8Rx943FbPW1K3Ag4w574I9C0alEO15259NdsqEe9X2EDVM89UshDTSNEs2sP5kC0W90a8iaJ9m9r2885q2oz561X7g..1gt8co13..G3 79j737d553S4getg6Qr01RSwW574MM1f2AtNY3c3zX66Mp16K4yjjCC3aUos28977u772297z38gRu77..L7C2P118LX39523bNAd08d5f72r3D019X4s5B07jm8fmuB00 550bv38t41817980pB066u0865q9klJ49J034m2gk..

C:\Users\user\AppData\Roaming\11951071\txewuxqdww.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	535
Entropy (8bit):	5.44804165454397
Encrypted:	false
SSDEEP:	12:NHJk0GjcybZM2DCg/9YQgbGmlF7mSLZ3ZnZjQgvCsLkhl:NG0GoAZMl/luGmj6Sl3zKsLkn
MD5:	E46CC6E8BE745C9DBD14FBDAA46702E9
SHA1:	E37C3321583D56172D4B93BF6F3675F408B03266
SHA-256:	EF4AC4D936FBFF00BBF1342D3F2572748F57F577772682DB4FE6A157DDBA9223
SHA-512:	2F110B7A4B0C79C89F3B8942481FAC5A35B406E272469E860C3558493D24F1BEE4677DCD7BE22C4CEF963D3D1F540C93FF7BEC23BA5A8676341E9F1B1D6349A
Malicious:	false
Preview:	khd33w1K7489x8hc8Zh34AQj0jW1qUK2055N54m4501HKY6ViIPAJ6p42JP3FhG7MbCuwk5A166l5P9D5DO7b111518F6R31183B35i9W69014b974SpSkS7gg3lV7423b 542D9681Xp956icYw9O7715wo2r4601O064Etk..h54au9KDA583U86s3gJl6guPq7gf3fNIx44B0I73o86O646po..3tX4una03t880i7dV188p2q790Wi825..q4EmWF WI267Bq4r8b9692195xzE9b11SR..806F3UW36c0uAU8u2p3B62wh4qk06456V97Y106e..9G512ND48A5089n8dE75r4..06XpH4noY0lZ9743DD16JxFB19J451gva47 412Qtv741sTm6697F0NbCK0C88ZOq1vUyIdH26..9T95184742lQ10akBTT458vCo3n2L10u266Uq177398JM3701d300FlIB7A1AFNQQ34NveTO4816t14N6w1H0P46Kl w9nXpDSh35Ys2..

C:\Users\user\AppData\Roaming\11951071\uhlp.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.449785927565248
Encrypted:	false
SSDEEP:	12:tY66YcTF6bELQQJ6NLSuQzw8Hnhws8QIMFcg:26qTYrQJ6MnzhHV8QAg
MD5:	6412004AC3EB4417D57431BE7EB8B1AF
SHA1:	F47F1DC407FC53D7DF389542165A727C32559ACD
SHA-256:	95338AAC7A7E586791F202DF50AD930E5AD74EC0FEC785BF7D0941B72FF5DEAA
SHA-512:	8CBDC3202F5B3F795C56FB09BBE61F043D9803369B55B43E8A65FBE3BEF54319BEBB7DCF6619372087C8DFDCBEB96D076F1257829302A8E376891CEAC780858F
Malicious:	false
Preview:	40041Wg254D1dso3D6aeBWk84V92213u73XFb39695Pt2D2775EA1DkK219Y812bt138q6yU00..D17o79llOhR994p23JDYC16PhW7ly19D206Rp01620B8250XnUF0h4 eAf2fTeD2koE49H8174z1igP0j9w4KqlFeNs4x21fI66E02yh9157Q072Fo4O77..ah9XH0wos1T83472A8k0Qg19g9pdnu19I7M2a3mD3DR4V1f5Y6P7r12xJ4mQ35u1F M428B0l06eR77CNu46X2b1C9986uL0zB6vM7E9zA3AS05ot7f9t29qS2E283B9s3ATKg0Y60Kp01..p4kc930593n8FMVF44aMCi83f33Uc32sLeY..0Q3bR592R44Fu01 2J0fFBv7fKNvL149174Kj0qJzruE72386219ws7J8906d13xjxt3334k3lf45x7R5386aU67My06n5NLp4d05YI2b69V7u64719F2N1sAc82B70049cGB3dpwWQ3i11dAT..

C:\Users\user\AppData\Roaming\11951071\ukxgqfeuob.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	5.486992240221159
Encrypted:	false
SSDEEP:	12:6hKXFtUeMwH3H7RzJVcSa9W9JfOwRQOmRfBggt9gKHuvxvlQDUCR9FMVx:oKfUeMwXbkkOwRYJgSysuvjCFMVx
MD5:	BA7B1ED5D3B0DBF2664770C335F67CC1
SHA1:	F73B2D02AB94430D1DE99454BF63FFFF58BFFA2A
SHA-256:	CA171BFBB90D8D851E435C47E27CA2B983F323337FCCFE82765C868344BE6C03
SHA-512:	5BC5DFCF676CA6A18694C73752AD95FA1764FFDA535395B0C877634E1F412C19D73240BD1AEE2B82E85A14F5D61DF5DD4C1BF24F26A70F81DCF1ECD8DDADB7B
Malicious:	false
Preview:	150m28Vxcqf01EHl7T180VRp640n82f8l0Qw744f14D0F6n3HxS15p5qhXg..iW79dC9FS2oL92w65J1d5L0Wj39umCvk4V13HM1EkugulrFcZi3524484irWXnJ49o93K 79Y4s36853yubkT9bCc08899q601Kr17859351..KPV126TZ5Xf8La3o0t5g5509ERI100D63GnfT64O226..LjhAgo662NY6WR5nl0t706DVZo1XS6MK79e634W45F391 4PA3Lk3J6AI1538i1l79K51X9u7CH7U5T3D38d1B08cOeW5UY91626qhyJ2296a975pM5X0..32rzV345tS43r5389MBU61fZh875593Dz2n9ZO9kc5r0Qf13uB76tc1QF 607..2063FQWUi1N44T4u1O5423T1B37uk..Iin0FDb02256X66o9283912F3DU90r995904r383i6t7m..SA40OL7..8fa9m7Rp8ex93V332UZ2ThjM320YQ9105K1l5o 28G4G71l55w7rPfeD32XR1y0AYP33c04l0dw5i8Znp57C00t83FS0sDFgR95jF1H3J5O56wmi1G7YFf1Fx0r84232x5Ghe5uLsru2W08d6ly7QLg55..

C:\Users\user\AppData\Roaming\11951071\vbwlcsmqv.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe

C:\Users\user\AppData\Roaming\11951071\vbwlcsmqv.ico	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.517567230022341
Encrypted:	false
SSDEEP:	12:U7W9AdkxTnWtl+ldYc96Qr9IqS+AN21dXtD+hj7VTHZzUnxyZJoS:UeKtIT96Qro+MQ+h7VTHhQxuJb
MD5:	6E0A96EDF4409FB14774CD9D488F21AB
SHA1:	DFFBE80677ACCAE4B8D4FFF1A2FA038F48E35B2C
SHA-256:	195910972CB0581118051736BEE125ADB24385BF18FE39BE9E00D59A87A37595
SHA-512:	767E6C3666CE493FE9BEDDDCAF24E1B96FEA3586209F1F4C9836CB3D430CBA24B6A9CA16CAABD1CA802083984B479D83383CED2696D5A6876C8692699CB1B4 47
Malicious:	false
Preview:	CB8r5a48GVGPjm887dg3zRMY8um368J2f92cc82I1o3v2y4a8D1888236d8S75u6lN5T47..29r5mlpeEL..Cvi41848eB43o3u3H408Ospw5cQApAI5h359k93l13x9X8 0d0wP4Xy78xg2j4D7XM837O10m0022ovRP2Y1z5098f143idm9yX0sUFz3W9196Q2RT8E..rth1w6j68ysV99he7t0I0h5N75C62S8I52Apk7754X1XtGsusZbVY14my8h Bo7e62..6U86F4670N2FB8gb8zPe..G8g6O24u31f5yi1o1Yc8BKbV80Xa9qy72EsaGQ29J1577AE6m2l..kAbD51r0L9Kp8OBDoC21FyA3S6u38035f55593N079S24k2 9HQ00D83iu1P54D4a55hRV5254D1263AQA46..0EGDrPHJbH4739740EB352343k87253846aDpe0HkRehBl7v9660k..Yc59T4RT0p70eN3V0G4E2OlJQ12H96fvkfaL1 li2VICT..

C:\Users\user\AppData\Roaming\11951071\vdjiric.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	5.5471741229401745
Encrypted:	false
SSDEEP:	12:JiiRtXDukjjH1PKLUFesZ4VGPR6bfRrQ2FSKoQbJQKdPZRJ05XNhxPKA:Jiy8kj5I8sdrQ2oKbexPKA
MD5:	BA1E94BB16378F539195AAA34CBD4798
SHA1:	8B7C13094754137CA0E267C3CDEF5D6C3E0241CB
SHA-256:	18BCEDB97E69B71E13C098DEABAF05EADFC9E7C39FCAB3075340FF5CC4E1C50A
SHA-512:	775CE53067B853ED2C6BBFB99CB11D5E2B6F7D377221F8764D6CEB4D63A78D9B758B70BA0F5A0072C912337512C0F0C8CD35BA31EFAA0959EFB88615CFDC77 A
Malicious:	false
Preview:	jC52tS31t9pyq354lT5WKA9lD1l6a0..W0ha439C3sRTP06w369w99JOdH39y3128688..Elm090m7BNi42271A3G1E74N3cBvWV..mCHZhCJ8N17754sdcnL3Y93633Z7 xJ13bHnAz265wa73468uP07ZO39mf0Qi88F04OnPK8c76u8Zl4X3iCNj5tL9C63UE7W46pq7Hc45hp..0Ojzt2q0zu2n38o1BG89w04M74eUfL16go87B6LUrsP0PCo3bE VSjFJIN5M43t89F97higod4b1744225GQ13k86ocOi8240t57..1nAzm820QS4xxY1boR6O436Z2qiLMCJ79Aq62676j4m1G7EOXv6818198S4qVVts0Yt9kLkn18n3YC0 IdfApsa4X9829TdCR32x3..2M9vj1369544Lp7A0C6090l0333r5H97m5G731u32X9K0fpb153201t1JMwY26C0K77q5L8D2SJM17oNXQ75174wG0HH8TA0TfuA2779P3v 1hj3GrV4..

C:\Users\user\AppData\Roaming\11951071\weqe.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	511
Entropy (8bit):	5.551237259202818
Encrypted:	false
SSDEEP:	12:epH2cE5ayfWslBkzfIvAZa63+rESVBPTlPDZF4pYoLvGM4STWa+:epQ5a+d7YZ3+r1BLlPDDMYoLfWJ
MD5:	E770C7C03F52CE749059452E6B7CF424
SHA1:	97B4553C929C8839088025BB85C113887674FCBC
SHA-256:	6E529C6F8E96A9D004ACB7C249D1602117A34414593DACCDDB0BCF171A3A080D
SHA-512:	73C5F66A79A179FFD9EB289295E790FF68E5834F8B88A4E65C98E94F1EAB90B2A2A123573313FD5618F07415B9AB91E4619D0517FAFB27B2657C78DC9BA691AC
Malicious:	false
Preview:	VzVSLd0m2874SkU50wj4oj79sf4h97lw085k9FI47EM8uR572H0W0yxZuD8..J5be4rOA36F6CTB8A9..gg108aby7Y51upM8p43c187a701P756W68MWj7ptg423Sgx7s X84B9..U6759wAq2Y9773ZLfv5t7C796..081A2GN3Py86iZ958Tj7L1J581qdgXw2e1167H27cen3T67YJX61J23bDT506xl48wGb2xfNUS9C9607385S98foS9kj20TV My14lSo64cFgM27Szr8Gz4MnG3l3p29l8p3VYaRzB0kxw..t9EKsbz3O0W..3JZArk0KL740mkGQ0EyziW1923Uho4vP36n4Y6x3692A4W98Cwo56r34EM4f90990l5469 16129612U7998X5QI9oHe80Zh2l3u9521j5rp7Nr8c9VJcY728Mfth102Kil09d8CaQ870T2W4506deT0Eqq2158BDgh72949yG72eTKL1y88tc1T8MK281..

C:\Users\user\AppData\Roaming\11951071\wgpfxgmo.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.461517274938311
Encrypted:	false
SSDEEP:	6:ZAoVSCa8lIQGFIlJ/i+RpMIvnbr2D4XEFpjER6P0ikB+1WUoNo4R7zndTGdSUrwp:ao4QlIQGFSMl/2D40TXmTZzntY0hVj+o
MD5:	9CA2870A389E6248B4E2DAC1D0AE144F
SHA1:	CE83EC4480ADF023A450C5BD83B94FA1902E502A

C:\Users\user\AppData\Roaming\11951071\wgpfxgmo.mp3	
SHA-256:	1A62DCB6E6D3FCD65AD1BBC76A4F06CEC802085631D81FD3A41E9DCB23D156D4
SHA-512:	3672A86E4456C39CCA740D108D9373BCA9E553E482E6E3B82F5A51F9F5D3D9BD5389064437392CFEAB18452A34163B56DD57049E0649F0FD45B569351017B22C
Malicious:	false
Preview:	Ca1q5mBCM6mbR8TnM0w6kk7CT5981jsuW73PV7mw75N5q5t9u2PmU0IqOXb75x..z047up7T6QR1y86R6f895p5G788HBO7m44xh6MZ5vJ12c0N9872xkRX1 1R21Tsj6808u25437sdwhtHYc1S1s3y7VC9sY2j739Ff8R5ybP2P444Mm9wxm009ZShkw..Mr8S62XX56QY45d3p8b21QE0n075g5yV1rxfm6O07Ht4g3O9pz574TsAa4J Tl77y906vZ2279C1D77J79k2VX9BxM8pyn4MZ118C4q7..Ch01tvi29TyZ560625q86..ONaSw989eXZMAH56HG98l19bHY2Q19066A273CM19x54MC4q9vr95OfCl3301 l51MsE880y7mU18d45327t0Lng99536lW4a4KAOxK304566z29Y1q29lI20o4Fl4jj336B8lT9R655m40qr69n051b2963kZFCIMP25340Q761088Z79bqPK7R..

C:\Users\user\AppData\Roaming\11951071\wjugkdu.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.454154410319805
Encrypted:	false
SSDEEP:	12:/hG5pRSS3K2ic7mu8aKNAalwK6cSYMSSv6t0iFDnzTnvNcXSQ/fgdM:/hcnJ30haCA8w3YT6WPTmzngdM
MD5:	EE1F7542CD21E6FF8A776A42B1C6CD45
SHA1:	0D8D4D7893E2ECEA607CEE8EC8980EE1C4F806B5
SHA-256:	A67AC00807071DE56A52FE0126152FDC59F66A60567E58BFE7D1D3525D50C6A0
SHA-512:	94C243D2312997131E1680AB99A9A08DFC772FC02C463C63FB92A561281B9E7A35B8C9853CB025BA86CACB88FE6B540D2F9E16221136D67E8E3731E1C04FE946
Malicious:	false
Preview:	p58559l8HKMD38h6ds3z2YmKaZBb843eJui..3B20l16176P4v4753N7FgCV7L4D99i17043v7588Q4Y0jKky8Vq5W..9zz5J029dqCj55F2820AeS6rNLvn83EKr5X8t0 it2s36NR38931L6..q113i4u98K01a746s3hwfaK26p9qAvCsg0073k4agUG910820zCCNq3lu14fz6..Hrr3f7a..5207kGC8Wm2e84ec8bk99r9d779520Y2m4L83Db1 Fmor8L63AVfO0hv2T65ye175a5x8966Td3Q63TP16VZ24501h24109P0NW19659UU6..69W7o4256XlQ371075VsV871hlVb309z9t0119A0OV26x64N1nklGquxS0S660 7B7c785103Mj4493VVE7XB4UC48fb59RT0B44295117l952317U9d7226VV0NRlK0rlVwO0a819O1eFBscO9rKX..M03lG8hZV92b29lO87rY214UX1lmD4C16021ucqCR 28mmF8Z5f3T254sK313932pBXW5725mfRBBzS37V8px36E8g7sy2840fB06X6v90..

C:\Users\user\AppData\Roaming\11951071\wodm.efi	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	147826916
Entropy (8bit):	7.077227424472243
Encrypted:	false
SSDEEP:	98304:OKW2vV7iqLaC07rtXDedxEw3PY81ShaTk6+Gvt3SWSNW1/YQN4z0RQ30Q9puXLcm:P
MD5:	3B15284DC6879A9B5C14C1E32E1560B1
SHA1:	824EB2E978C29E6E50B11B5D0499BAA0C1BDF834
SHA-256:	B5CA52744A813B0E4E40F39D4952EEAA428873D17275F0B9AB3D03558E88615B
SHA-512:	FF517EE07864C82174C4735749739116A7C2F35293B94194DC91B19F37CD2AC29CB8FE61FE2F05EE30F60071B8EEAF5E3DE79984A51B94FE7280FEB8BAD0FBAC
Malicious:	false
Preview:	..;...;O{<.?}.hX9n..:...,sn....d{.7.{.a..5./..<..2..D...n.....u....#.c.s.J.6..&..7..h.....V.P.(I.Hy....b.+..o.r.Zc.3H.Hm.!.....M.7.9.3.r.U.b.7.4.V.I.0.D.v.8.8.4.6.6.S.e.7.0.1.A.8.t.e .A.E.I.M.f.n.8.8.8.w.a.....rX#`}.c?(=.....=6v....0,.3)D.2.D. ..K.K6...[..j..W.....).^Z.t..9.....N.....A..H..Q.:m..i...d....g.e~._.gy..jb"...XST..+f....-..].-E..,#...Xj..Zout....K..rT.. v.9Z.h....AiT.....5..T.....5A...1.....Y.$..A7g.k~t.8.....cW3.r..2xY.....z8.($.|.....{!..d3..T.84;..w.....E)}..@.~....L+2./.8..M...M.".E...`..OR.Z...../.O.`.2..S....X..Z....S....j.]I..n... .ws4l....{.o.....NQ ...={N.J.C...yF/M.'....=..s=..d.....hZ....L..$.]..X..a.....o.E.v.9.8.8.t.x.J.8.N.9.6.8.i.h.S.B.3.R.7.H.3.4.m.1.9.7.....T.....z{.)J.....m..4^..sc..f..Lj.jzI*.7.Z...f...5.E... ..".is..K-.(7.....;....wx.$..G^.....,.S.....!....P.f....ZVB.pP.*..j...T.6.}VC...s..G...'..G...U.....,_..4-v.....%....B.....I..'_.Q.....8g...0U...+..`.;....t...

C:\Users\user\AppData\Roaming\11951071\xahujdp.dat	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	596
Entropy (8bit):	5.498115964043167
Encrypted:	false
SSDEEP:	
MD5:	61A2B37830FD94B48E9B5A98F9ACDF43
SHA1:	8BEDE41E8388958EF70B93F7161DD877F537E0DC
SHA-256:	871A8514D7BB0693CEE56A6F383B26137C63C2EAB195022DE846B758D1106AF6
SHA-512:	A4E5984A4345B3515A951ECAE7B9C451DA0C15D69813E32267B88C808F0C12AE9738A4C906032DAF1D737749EC53405657E4106EB517293E4466B29FF12379B6
Malicious:	false
Preview:	6w23CXFo64Ez8Yf3oW3789d5x8f5K252n3E6m57HV937j0C4K078c5L3V1G36R24i360..T811843CfGD6x82U41ZWPzAx9xBBmHjj6735464jR124..UW8W871W8C7983 4oxDw6q81Lsh88Q7VX37nOQvH7o7512pc8K637An5D4433yN4wrIHcoT6j3x1i5T9x8U2rVbb7928v228891Q0cJC7E6M48L4AOzDDonaI732gzpF0JC3..m6525v48W39 N90f196icR5401428V3qn77xCR9M2wFI1GiW6H9999m7EyKZnA59a7GdnZ60360qpOnmy7e842f877037D3R22k4QMu31fy45QJS10K17yTz62x..GQjH83f511LbSEAFb 49v1161oqbaK3443Vc2E4637eg9x5q0q0Lm84S7955U1lHXFGlsbVsDB93E8254L2614Dd0f8Uz25a09642Nj8l..Hqff09UHmdZ5V8B4H0k3xgdtp6FoX1g41VZ81w7J5 1Ubq8Tk804Ha76eoVfB61U285J10RjDMwsY5GP9624QdO1WY2668n177m35C9pV1vfh3DZy7O4..

C:\Users\user\AppData\Roaming\11951071\xdfc.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.470137901724811
Encrypted:	false
SSDEEP:	
MD5:	76E44CBDA2BD332EC2499BA0ADCF9EFF
SHA1:	D5F493ED5EC453BFE7F8E4C14F90EE14A243092E
SHA-256:	A74C79D08611C6477D27AEE6A3153FDC2443864853760D56E94C346A7A18EE51
SHA-512:	B6BDA6BFDEF96162D8BDDD69BD290043FE1BF8E6B5872EE7B5E593E7EFAA35F5BF057FB0827D451361F29C05A360E21DDC33B2EFC5066788968837DE37FC93B4
Malicious:	false
Preview:	H0aD9141..Bmver5i474W744182S88J..ArfB49d06Q8CEmTn6lCL1535v19362w2nn63Nmo2cP742z87AlrT2742f83l595290t1D7v1178X9b3d28Ge6veCJfKn..9WFxP4K912t9536N586822E..KpnWvSFw9m1..lH9iyPzYmJxl36u9187R8sJ722fF36C28znDlw2i..82rWY53942P316b80V46so76M0X1H05Q1IBv82ut..o202V71pE2lOHC26671DAGXwlBy4g23R0dSZ5163K5wYDF9b8wj13WO4P833uDeP598L8jj6x6549p5Gt6y87dfUW1Rndo2utd4laFdkGcEP3Dsrd7S68g672662DC282218by136266674vXnAZ..d0572j3W8wtB2RhBX3f7QO79344Tqmb5Al2cVf88JJ8055962210FTC3023r3BJ..Oj27Q158AdP4VWxeONgHkO312g875Jk536yp6749201641k8p2I..

C:\Users\user\AppData\Roaming\11951071\xdvnwxbk.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	611
Entropy (8bit):	5.525547165161044
Encrypted:	false
SSDEEP:	
MD5:	F59BD426A1C191CFB0EAF760FEE043E1
SHA1:	F70BF0CE29311FEA310C527663CD72E02CA5468D
SHA-256:	D7A77DCEDB1584946370E60AA917D74CBBF76A4FC91FB71CEA907AECEE64131C
SHA-512:	C265942FCBE0102B9117637F212A75BC749D5C0C6C5B3202C9F79C91F6C7D71D4C26617D2BA2C174EBF9A323EF63B1788A80EB4FB81069FC7CED3559E83BD7
Malicious:	false
Preview:	nx3BS0A91Xw04n138TESgb4b0H8422a1B72724A1Y17i470B461f8bB4Qoym0GE6qY5r1xxX8h71e8Jk09k4PJV8gd88Lg..u23M2g0eHv4826L5nkV7hGF69119dx4410..8689cl0s5s48RgyA82usEC1X28p5jw9rL747ao55DG0630Yi616nBqRj1c753l9w0f1Ugw..Ql02Uu3R..0g7VusXoxHrl9sk1IB7IM55aB2bRY9r28kL5kdr8T86025Jx7zs26evcoV5387q73Eo07JXF..Xna16XL4d292C8n9Z57Duc763tll9iT8Ut7lS9pJid6q2qbC02G877q5ZX1q45P38rQpL7l91w3..2UT2Y0232FU034y5fGfk675j84137hFRmEOG95f8qr40444A43Vl588D681c50p8p65UQe6KCnzbS3n4w3923UuJPv2N99A39u85pN365503mC473S87L1MR5S67n11..f0eO3rKJb145xEW80qU0745cv2w4h0m6WM39h5712F5rcF1Ws6Z52l87wU3756xzf712Sfb1FE5116jsjI39Q92364J97813S6v32s64KtHf3uZf7Nk..

C:\Users\user\AppData\Roaming\11951071\xgkjrmeib.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.524354955017576
Encrypted:	false
SSDEEP:	
MD5:	90E759016061D9AE95966DA7D93D22FC
SHA1:	2458EEB7BF6DFA31C188D4B2AC5945FC04C097E3
SHA-256:	430C5FCA34F6BDB94BAD6835493278793F9C67CD4ADC28A2EE8374C47124D7C0
SHA-512:	7535ACF384A16815BECC9DB8D943594836843E52782FC5FB7BAE9BE49B01499D5A39DC2186E95C7EDD39A4BE58336516FDA9107BA6FF243236CCB9B3342D5E68
Malicious:	false
Preview:	V838ky00n6082Y66298L8m4ne7EG2l..Q8qt02aNf2EqP8d680Ex746A31018l6KYl147oKZ9cK5Z0U1tP349ASTQ87J2N9Up77jf9T26E70Ba09pByv81F..Dkh875p2Gptw7balT680o8V22D5Nf83OKx1ns5C9458GwNtE834517o45q0tZTi13Y8e4nzvEk92f71G3m5it69639chD5mZ7CkLR06k76i23RP5tXo050fb..9lzq748x0cRK70p25rlPr0349e35M8Vd0Ll84131a294SXKdn5332p359l1623lGc213JF382623ak31zea19HG76n01t346jiM3fBDFgv07jVj2md751749q71z3645lLrCl8..KQG8gqM1jSb46sVO477XrW8467g4wFykw7sU1yLE4B0jD37xcTWMAD8DT5H0k4C7S6djN5T57S706169342..9Dk98QoRrg7532w9xCk9uXTM277ina6R1eZ9x29mk2531E9uL05s6F9VFggLQ24..

C:\Users\user\AppData\Roaming\11951071\xtwebiv.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	628
Entropy (8bit):	5.410741046895211
Encrypted:	false
SSDEEP:	
MD5:	CBDB0DE2322275B28E0BE6832F74720E

C:\Users\user\AppData\Roaming\11951071\xtwebiv.pdf	
SHA1:	8FABC4210AAEFD29C10A7E539D7FC7B44585D365
SHA-256:	2A233D3F0B21B114117DA88E756505CC8FBECD5EE29C6D9405B852DEE6723626
SHA-512:	E27139A6E74FC4DD6EB6DDC460D648156B05A8B4A069700A0920850D4ED6EDD66AF7C00A050125360B9AC321C7BF63B70D6D39C3D3FC0D85BE229135C2FCE58
Malicious:	false
Preview:	DT5nn1g..872tz20y6G220H1iQv39S73376n27e4bo1R85Pj2S938133SxCn681Uk9862Ub11r634UQWiQ473i5562P5c57Xg4aACZ880516cu6F8uS32630j4P3m4723r0Fa..R346744QQ7lX8D46cF3H9hA943r3U515MC9BJ6L83V08f8r8440PK0J622a9b4e..65BBw8O0lUI2K5iS894IX4Y966C943Q29343..1h879tEXkU8lQKhODf4B8e93116836s7Esb0ZZS2BmA86V0w118hc72FI0CT5yD304280mq9mz8Y206q2FEYJ7YI..i27f4v5927N6hy4Tg0E9G4ftyf3502..7x150863P1XyR6s201tO0335J5232s00RC8L48lfY1627LE4zW1..m58Bj65urR4x5o0349370l892l8DF4IBQ1H8t0oj..Y2a7f7i6Z83C11M43GCi119liUU61BG1R6X78692v329I6z68hm2w03kcd0A7800b6Y2dD21Ogy23M2Xxow12f9J1m98Otk43Vs50pB4vkt2daHZR6ZG93fAi98P24Y17G91O562N6LB5U0256Qar272Kv0gE3r962z0j26N164..

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	85
Entropy (8bit):	4.7794780716515195
Encrypted:	false
SSDEEP:	
MD5:	980FD35CEE9960B710417687DC12387E
SHA1:	4560897A87B198C409E0D4558841A8621CBC1735
SHA-256:	6649CD35D2FF8EA2157FC9E41DAD5A6FEF7DF0CF6F3A8A8D017F673AA3108290
SHA-512:	1706E01118F6A202E69921A2875A78A516AAF80302E01555775195FB1052E6E980711C3592CD3F71EEEDC503D26071DC8CA170004996B03E3255810F8913C117
Malicious:	false
Preview:	..[2021/09/13 15:40:37 Offline Keylogger Started]....[Run]....[Program Manager]..

C:\Users\user\temp\oIml.bmp	
Process:	C:\Users\user\AppData\Roaming\11951071\gajb.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	5.006366884883343
Encrypted:	false
SSDEEP:	
MD5:	D1BDB146228653BD87FD35ED29BD5204
SHA1:	119F2AA9E91B41B33FD5F1539328BD4B92E8C585
SHA-256:	B4F5EF30DC5A76A4E7AFC226CA75A88AD638E1DA651714E94292F27D0D27CF49
SHA-512:	5317E984AD2D0825385FD4DADD38F8540CB2066325C7E22A84CE7915D2D8BF54A5121B05399473B9C6DDD9D683FD915B4ADC550049DECEBB0F48E5DAABF4119
Malicious:	false
Preview:	[S3tt!ng]..stpth=%appdata%..Key=WindowsUpdate..Dir3ctory=11951071..ExE_c=gajb.pif..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.478138337155549
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Covid-19 Data Report Checklist_pdf.exe
File size:	1112765
MD5:	26467941a5c46c31d4915abd5e4a2965
SHA1:	f0c57e46d0d83e03bc166f018fbb9d819b104c3a
SHA256:	a3f8ab3315bcd827a53bf5dfe1b55f550a21e40287d15e082e364b870d6a02f8
SHA512:	ab2a3216496b2ac1b38c710cd9c4539b9ab38d5b0ce2a6ad84ef729fad9b19e26168017c7380dc806b60fb3c530e378fd226f38211157d3e7493e26505d53ff1

General

SSDEEP:	24576:5AOcZ9ZbrLdyJ4XTn70eijnRgpPuoF+bJm:zOLdy6X/0e/Y3lm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y.../y..#...&...,...._....._.'...._f.'...._..'..

File Icon

Icon Hash:	76ececccd6c2fad2

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30581	0x30600	False	0.589268410853	data	6.70021125825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xa332	0xa400	False	0.455030487805	data	5.23888424127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x238b0	0x1200	False	0.368272569444	data	3.83993526939	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x61000	0xe8	0x200	False	0.333984375	data	2.12166381533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x15168	0x15200	False	0.214705066568	data	4.84974997403	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0x210c	0x2200	False	0.786534926471	data	6.61038519378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 13, 2021 15:40:37.834465981 CEST	192.168.2.6	8.8.8.8	0xc8a9	Standard query (0)	cato.fingusti.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 13, 2021 15:40:37.883265972 CEST	8.8.8.8	192.168.2.6	0xc8a9	No error (0)	cato.fingusti.club		79.134.225.107	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Covid-19 Data Report Checklist_pdf.exe PID: 6924 Parent PID: 5080

General

Start time:	15:40:21
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Covid-19 Data Report Checklist_pdf.exe'
Imagebase:	0x1c0000
File size:	1112765 bytes
MD5 hash:	26467941A5C46C31D4915ABD5E4A2965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: gajb.pif PID: 7164 Parent PID: 6924

General

Start time:	15:40:29
Start date:	13/09/2021
Path:	C:\Users\user\AppData\Roaming\11951071\gajb.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\11951071\gajb.pif' wodm.efi
Imagebase:	0x860000
File size:	660208 bytes
MD5 hash:	6BE533CF863DB26D953917024CFFF914
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363037979.0000000004E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.368157698.0000000004EDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362785019.0000000004EDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363087933.0000000004E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.368298826.0000000004183000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.368190067.0000000004E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363208796.0000000004F1F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.365775815.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.368263690.00000000041A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363139227.0000000004EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362829270.0000000004E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.364800207.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363109577.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362748203.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362850029.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.368145080.0000000004F20000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.367804453.0000000004EFE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362989854.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363056424.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.365073207.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362894368.00000000041A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.362921698.0000000004EFE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363159769.0000000004EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.363020662.0000000004EFE000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 25%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: RegSvcs.exe PID: 6288 Parent PID: 7164

General

Start time:	15:40:35
Start date:	13/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x670000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000006.00000002.604178944.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000006.00000002.604178944.0000000000B00000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000006.00000002.604178944.0000000000B00000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000006.00000002.605185347.0000000002E90000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: gajb.pif PID: 4752 Parent PID: 3440

General

Start time:	15:40:43
Start date:	13/09/2021
Path:	C:\Users\user\AppData\Roaming\11951071\gajb.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\11951071\gajb.pif' C:\Users\user\AppData\Roaming\11951071\wodm.efi
Imagebase:	0x860000
File size:	660208 bytes
MD5 hash:	6BE533CF863DB26D953917024CFFF914
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394956149.00000000030E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394845153.00000000030E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392597947.0000000003E2E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394884254.0000000003E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392716765.0000000003E2D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392613575.0000000003E0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.395236457.0000000003E2D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394633722.0000000003DC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392497684.0000000003E0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.395044365.0000000003E0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.395138441.0000000003E0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394775886.0000000003E0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392562844.00000000030E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394897994.0000000003E0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392774240.0000000003E4F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392430101.0000000003E0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392475891.0000000003DC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.394990382.0000000003DE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000003.392846038.0000000003E0D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: RegSvcs.exe PID: 4124 Parent PID: 4752

General

Start time:	15:40:49
Start date:	13/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x350000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000A.00000002.395200943.0000000002C40000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000A.00000002.394968459.0000000000720000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 0000000A.00000002.394968459.0000000000720000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000000A.00000002.394968459.0000000000720000.00000040.00000001.sdmp, Author: unknown
Reputation:	high

Disassembly

Code Analysis