ID: 479070
Sample Name: Covid-19 Data Report .exe
Cookbook: default.jbs
Time: 15:39:27
Date: 07/09/2021
Version: 33.0.0 White Diamond

Table of Contents

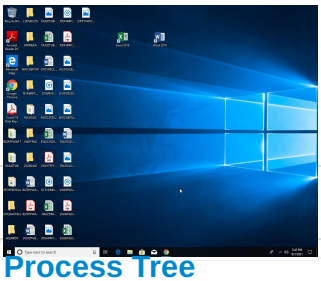
Windows Analysis Report Covid-19 Data Report .exe

Overview

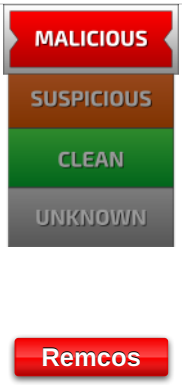
General Information

Sample Name:	Covid-19 Data Report .exe
Analysis ID:	479070
MD5:	f7b7d0144665b03.
SHA1:	2a8d08e5189f564.
SHA256:	6712498150d5e1..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

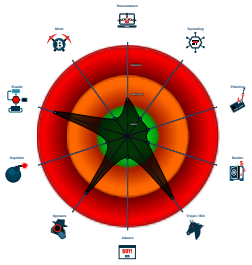


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Contains functionality to steal Firefo…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Covid-19 Data Report .exe (PID: 3296 cmdline: 'C:\Users\user\Desktop\Covid-19 Data Report .exe' MD5: F7B7D0144665B034190E826E035F9C98)
  - glpmruvjds.pif (PID: 2436 cmdline: 'C:\Users\user\53280493\glpmruvjds.pif' otggkjoob.bnv MD5: 957FCFF5374F7A5EE128D32C976ADAA5)
    - RegSvcs.exe (PID: 3508 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- glpmruvjds.pif (PID: 6556 cmdline: 'C:\Users\user\53280493\GLPMRU~1.PIF' C:\Users\user\53280493\OTGGKJ~1.BNV MD5: 957FCFF5374F7A5EE128D32C976ADAA5)
  - RegSvcs.exe (PID: 6688 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "Xhpvfingusti.club:6609:s%qDr",
  "Assigned name": "gogo",
  "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-WHOQYH",
  "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
00000011.00000003.317794056.0000000004800000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000005.00000003.270724186.0000000003C71000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000011.00000003.314903867.0000000003AB6000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000005.00000003.271079064.0000000004010000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000005.00000003.269314350.0000000003C91000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.3.glpmruvjds.pif.47bf208.14.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
17.3.glpmruvjds.pif.47bf208.14.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
17.3.glpmruvjds.pif.47bf208.14.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:$str_b18: Uploaded file:
17.3.glpmruvjds.pif.47ff218.6.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
17.3.glpmruvjds.pif.47ff218.6.raw.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$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 138 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)

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

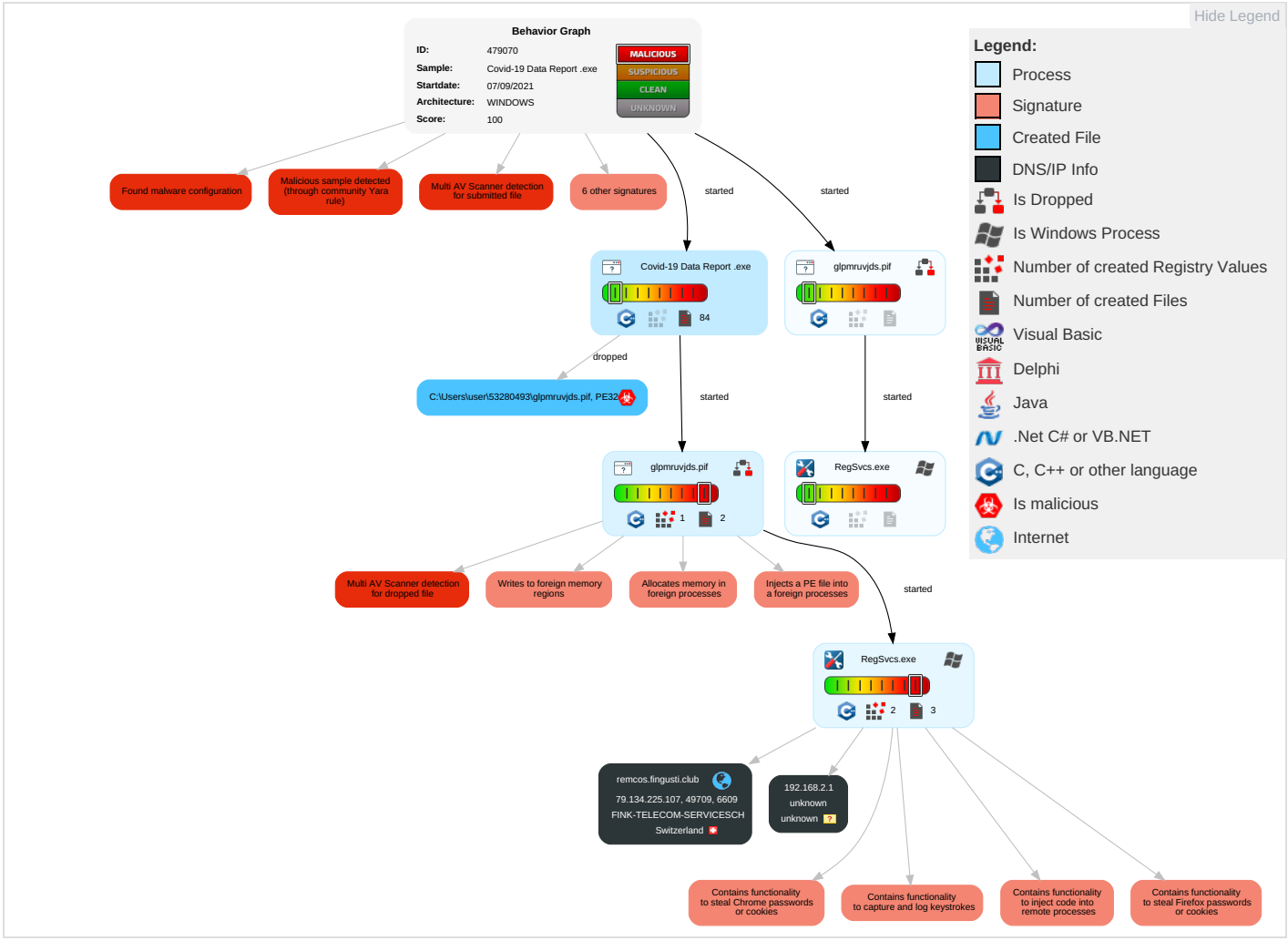
Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 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	Obfuscated Files or Information 2	Input Capture 1 1 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 2	Windows Service 1	Application Shimming 1	Software Packing 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)	Logon Script (Mac)	Access Token Manipulation 1	DLL Side-Loading 1	NTDS	File and Directory Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	Masquerading 1 1	LSA Secrets	System Information Discovery 3 5	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Process Injection 4 2 2	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	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	Process Injection 4 2 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)	Masquerading	/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)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate 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 .exe	53%	ReversingLabs	Win32.Trojan.Woreflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\53280493\glpmruvjds.pif	31%	Metadefender		Browse
C:\Users\user\53280493\glpmruvjds.pif	50%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.3.glpmruvjds.pif.3cd0a98.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.3.glpmruvjds.pif.47bf208.12.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47bf208.14.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47bf208.1.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47df210.11.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47ff218.6.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47df210.3.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47df210.13.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47bf208.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47bf208.4.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
18.2.RegSvcs.exe.930000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47df210.7.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47bf208.10.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
5.3.glpmruvjds.pif.3c90a88.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47df210.9.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
5.3.glpmruvjds.pif.3c90a88.7.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
5.3.glpmruvjds.pif.3c90a88.6.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.47bf208.8.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
7.2.RegSvcs.exe.800000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
5.3.glpmruvjds.pif.3c70a80.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.3.glpmruvjds.pif.3cd0a98.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.3.glpmruvjds.pif.3c50a78.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.3.glpmruvjds.pif.47df210.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.3ab5f28.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
5.3.glpmruvjds.pif.3c90a88.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
17.3.glpmruvjds.pif.3ab5f28.15.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
remcos.fingusti.club	0%	Virustotal		Browse

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	
Xhpvfingusti.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
remcos.fingusti.club	79.134.225.107	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
Xhpvfingusti.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	remcos.fingusti.club	Switzerland		6775	FINK-TELECOM-SERVICESCH	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	479070
Start date:	07.09.2021
Start time:	15:39:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid-19 Data Report .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:	29
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@8/81@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 43.5% (good quality ratio 31.7%) • Quality average: 55.3% • Quality standard deviation: 40.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:40:47	API Interceptor	868x Sleep call for process: RegSvcs.exe modified
15:40:49	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate C:\Users\user\532804 93\GLPMRU~1.PIF C:\Users\user\53280493\OTGGKJ~1.BNV

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.107	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	
	Le8z5e90lO.exe	Get hash	malicious	Browse	
	LA99293P02.xls	Get hash	malicious	Browse	
	PO 2413.exe	Get hash	malicious	Browse	
	myups.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	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
	TTCOPY.doc	Get hash	malicious	Browse	• 79.134.225.21
	DetailedBooking.js	Get hash	malicious	Browse	• 79.134.225.10
	DetailedBooking.js	Get hash	malicious	Browse	• 79.134.225.10
	etat_comp_du27082021.xlam	Get hash	malicious	Browse	• 79.134.225.73
	2dnUPJR1kl.exe	Get hash	malicious	Browse	• 79.134.225.61
	secondupdate.js	Get hash	malicious	Browse	• 79.134.225.10
	update.js	Get hash	malicious	Browse	• 79.134.225.10
	secondupdate.js	Get hash	malicious	Browse	• 79.134.225.10
	XTziUJe6uK.exe	Get hash	malicious	Browse	• 79.134.225.54

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\53280493\glpmruvjds.pif	Purchase Order_7789.exe	Get hash	malicious	Browse	
	Covid-19 Data Report Google Checklist.exe	Get hash	malicious	Browse	
	PDA_pdf.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\53280493\acecvl.pdf

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	565
Entropy (8bit):	5.478406599321546
Encrypted:	false
SSDEEP:	12:5Z1IZ+8ue0DB4fb4JM9zNXkTARXqisyTWPSQvDqu:HV9e0d/JMpN08dqUT8S+F
MD5:	0EE5752210ECD6F4162E40F42D4F055C
SHA1:	3C2EE9FB50E437DFC73E014BA98C255EFE8DC602
SHA-256:	3C0F9A370E7CCFA079430006509FB10F47A373A9819E2D098AD860A73E83CB9D
SHA-512:	5272D26352FD0F0066E349ACEFF61184491F077B5C327751AA10152D5C1698167DF478918F32031EF1BE1B851D266CC7592CC2D4A845897B62F6104DBC425211
Malicious:	false
Reputation:	low

C:\Users\user\53280493\acecvl.pdf	
Preview:	9AvnH8u43E98Y91SJosO79784c2f51xSoon8z4GEpg745DVj5diqMu29B0375H115661701521l7Wtunf550426W03X11ywJ81HbT6pOlT92k7NjxGy060G077W510928P0o576B4AX54d21jz5Amc17n64T..m0ZkAmx85A374a22jov9yz29799095N23GHR9kE21g3F154932V8819h4j9favBKBx36ob0935723dKI257Q3Frlb5PX8A0uR0Fk8zJhQ2Th4P4IBz1v..62s7EG67700g85r422607X293m1lB8DC72BmZ6I9l6v8y60QkFxKcH7M60..2tm5337c3pENG1Gse1iQ1eGH9430i18Gu6PlXeX3dNE41a674S19QlZ5075081m0q0SaIpLbg3Aos..38154MJ0048ujA3i5aYChF1P93006pMUlA0p5j782dk8m730d4E09jCOHJ7495255x..ykO077D60061BXjiBz8l275R7AJ8fMxL0wY236y6l7C011dz8HCXJbr5nU0h7c6s5o3049s27130J8Vb..

C:\Users\user\53280493\akvecmiek.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	538
Entropy (8bit):	5.509745113401239
Encrypted:	false
SSDEEP:	12:IT6khJtEd6l+Fh54Kc6yYM0Lq5812YmnyJt8hzSEcxaw8n:ITr7l+/xM025kWnyJt8t878n
MD5:	4FA4F8D73EB9034E737CC2ABBEF5A0B5
SHA1:	9CAF83137A5AC6F1280687655674392FF0F68C7F
SHA-256:	E0831979E3EA0F600A2D0D03B75F7A369B2BCE04FEF7AE8A98350980C0D02C1B
SHA-512:	8EFFC2DB704C7A1A2C26ED77268DA06DF246FD78F7B195C5E4F272F06F0BCE7E4225E296B4D559DB555C23F4FBE25604DB3189338486ED3C1FDAC8826ADA185
Malicious:	false
Reputation:	low
Preview:	0917U9B189aag2DA4F4W8YE4C825OE2x4576k99myy6rQc52TddnXIaDG16c7oIK5joU1424gT9s2lYA98d..808849Chh6AoYAGKB90P625Nf28953L525l0jheXj2iJ6n11v..ztf024252286A6t31EkcU9rDB40g4tk9a1D67gDb6246796v439j..84G2v0gX082XW15KAc76PZ7c8mD23U43mV47bq4..3E1CpRDX7z0fk6qu7u64GN8Q8Y0l5d8aN37eQy0HK9Y8HNT7F371r42Gj9Q6o2P5r37416GWT292U..lD13ZMu69cV5Q3PwcxZqG7b7977921Sdap37C6P99LxIf4EU6MQ8mR99T865C5o81p94024065r71Uy9Vr2l7PJ5jdrFRn51p2e7MURe20q706B4OX594Hi7c625w896a464Z57FaL7I23v8s3yXnUu..2SCK765Xec9q9V4zBcSkR6aK7..0m795oS48l49La7xU5L338637YyT1CLZ59Pk6825sTb725..

C:\Users\user\53280493\anbk.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	568
Entropy (8bit):	5.387839099663672
Encrypted:	false
SSDEEP:	12:eRQlyyAiSdYTflOvNCl4SRd1qKk0bt73JmBamBJmIoq2v:eRky0vTYD4SRf/9J75mRHmkI
MD5:	345FB0178EA77012BF243744E215868A
SHA1:	928C8F4B6D442E30275C465AC7E584C7FDF568F5
SHA-256:	7A5BC012B472DE9BEEE42FF3E8A8AFB72009FB650EB306FA1DFAAA1615AD00EB
SHA-512:	D52A8BE4F5B6B6A672ED0E7635813858E1D464B1AD36DD5B50433936E7F969528358BC8C6D7299B075C8B8E118A8F21B3B2F289AE2E2EEA39854C8E34ADE922
Malicious:	false
Reputation:	low
Preview:	9eY6472mdSNjsa1A3716691VC2Q0559Mq0r17v9Qx0u4QG7Q414517t..XG8t10b7LJYp633MxS968SR8505Mr9IfaqGXh8p7Yo924XfvY1q82Rsv799X446P3m09C9E16eA9Z26J887yJYPx424..1jX1QD66B1b8rRG727b46MQ1c55317996r673LuNr7N3Qqb6v..075jDD1RIIau8m24X725806L60tCE4E029qI06e77e468800UUMuQ88n15e0316u8rcVS2UYI3K4945y0292NW..Pwf6V982in86ir4g64WL1S97LtX587zsser646cZ0EroW7089fI8a572..50K070gM6l7rF7391O4R2aL8n9Rz10HPjd0ar8W97g7vZG4JxXdi3672n49875d75788o7AxgV4S9t03J3or..lh78h5m9hR1pM313..eBn86568omu644coU44nf48E0Uu89z24I504XLK44l56v76P4Xa51e457LN91Z7ByRT8m3c133oh6978u03544U1S2Xx05B4W52h02Z2702h0MoN817..

C:\Users\user\53280493\aplwr.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.584416913222413
Encrypted:	false
SSDEEP:	12:ODroWZHs8ps0pOZkE5dW8NYI4xkmWAOuDGDozDEQrl:OYWZHhpOZkv8CI4WmTdB
MD5:	6B212303634B7C35A3A9DE35B847245D
SHA1:	91788AC719034019327584C0B71875E69E8E2539
SHA-256:	DA6C18F1385E348AF00E7865DCEF4D00C8DD7EA09FEA8E5EAE79468EAC6AD52A
SHA-512:	7D68B7CE44732C0B5C8DDC281AE68A65FD105ED05F319F2B37D410B39283061DFC456CB9650A0F88F30C555F8369D9423D84B496B61C53EE07CA001A92DEC9A
Malicious:	false
Reputation:	low
Preview:	t56m38ZF1AH9Rkc1cO97879v6auvjNnG2i3O706S26HRqlrGByY070i89vAf4FsZ7zE4i68..k23N9J69Ht3iLr0..23MXF3o45mh9WxljHs77kl473opZs33044854p9mq1Lsyk662y586142..73139h3WY958racTL592L5bsv8OK472SP2p316YN118dCFJMv0mTccYG55Zo29s1mDCS871..78149JmlPJ9TZWB93O7hs48Y49511RQVU4j4296m6Y7J5c..f22RM6919Z6E74G15NAeKX18Dx414yVaw214d00rU3C299ZY839X4cH7WbG5cfq646XW1Ma8vZX97AKA439G3V2342a7V4O6b5r4..TU8iH9Gnl5LMKNw2v8072ClN71j166U9jeW501j91GHEwd0v5C7Qk75Bj05oTS1A326QCs2a45feM3AgxPVm46T387s82YKHfzuVRH74lETCdl8872hSX..H7eRj1zmWXXqnuBY93..

C:\Users\user\53280493\apqmcl.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.432363612345915
Encrypted:	false
SSDEEP:	12:WNn5SdK/bOdiI8c3Spcb7zOZx3YWAZNx6eqLBcqZQYy7p0:W15SdtiI3GcbeYBBUcZYgp0
MD5:	2CF908DE879EC81C53CE52D5835DA491
SHA1:	79B0E5FF758F3DFEA3F42344497C080AD03D6977
SHA-256:	D14E55C478B9E2B3CB6531BBF1D939BE3C1A0C2FBB92A1CDB8F759FCEB541063
SHA-512:	78935D0770DA382D3BF87A9AC0F44A66D29846C68CA5FB1B3CB93669C9B5A8F3F02F8197DDE82C0DE37C42A17152C4406B950D2B7ABF2E2BB61F158CA77D6A9
Malicious:	false
Reputation:	low
Preview:	2900161B62M8CnBZQalPO6ULd4Z9eV2BS4e68afMr936V51198rs306738W1Uw258D58004X0JwRmB96X85N80687t5g10o0x6AngGN00To63ATWzK..8Uee 6TE490L4Z9489CWOo2fhjdvG8aUOJXv1p8lzUT452j0zjF0sDKIZiI4MpEI3R6..938EkXo3x216l37d35nJQ18g8329D90Q79wa63uK98Zj331w..me25z74a4ALHMh71 516f31d4T7816412fb0ju2cKwn34b..7nD2jhJ5ImwF21D0097d3yn80R651j90..64J6z..Wb71CQ95JF6437b4CZtX4z16qx417951056M47V0RE2332NX9go31hh7I1 2OHDjhb135W2f6K58U213936x75520628fMOY55436QQI18Iv919A7661d5..omR5X2OdXf8nU2n7Bqf682hG3I38037dq873R9M2d41g9..r5C1XE13jHc3J0t86X9Pn1 ZB8V2W2AC6EV1G1n43u0890nd363023m447teN8ma3L5Z48C2gUEc806hXd..

C:\Users\user\53280493\cidbwvj.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	546
Entropy (8bit):	5.489386917483217
Encrypted:	false
SSDEEP:	12:E4jmgUItm5CESHVZmEtmQ8y1CqxT/D6CJl40uRgr9Dm8OOeRC6fH:rjmgUIRE2FmLy7TbpJq0uRQeR9fH
MD5:	D58212ACE99CD92FC388DE4527C286D1
SHA1:	CC470D7858889E42FAD4DDFA92627687F733DBFE
SHA-256:	A121F09A3EB9F90FE216B6D87FAF58724D897638148BC78FBE4A930DB8F2A741
SHA-512:	93370ED05373D717350847C7CF6D27EB767DF10059402B1ABA32F7F05B7E0E523C329AA2BC11B3A556951E70F15EDD9F2A6B42D4BDAF13F0644E9EDA5217A6AE
Malicious:	false
Reputation:	low
Preview:	2747wVukuF300z8XHf0c5Y9S8Y14f..36Y7FzC40G105awc71c1010XqgP5eXpKf920zXGw6l1A425G757t4q92g66coS5cx9p1L83..9a5n6R02q4oO8Tw0A3w5L681Y4 T47b6m10n1520065l43ZUBobwzD5n4S36F42q07D50oLIJ00Or020KZEQ9QcRC9740364i4530l2Sgon5t2IgL..8F6Oy8566Nd1UB447g9V2C279680Mek2079Y3V9k19 9..pG4f4QmJVe6QqZUU76iCr8yPte2Qs224zPRq19u9nw3c17YP065Oc9iT38a97Rfj3tGUg0745f33589VV7..oQr8G19gQX5Mj12QWmAq4r7YamkPWSSA5X53w6eKF6r 2Y0syjLasxeHl740119925B6A16M4Zv6vCH03SM8uD6Bp8LCm06508fjlpfS07Z5w0800388j99LtQ14938s04th9..Vds1C320D1uPP7681G5fw47c15G1790YsfCg833 56S1V58Uu0hl3837d9K64cFX..

C:\Users\user\53280493\ddrlreh.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.442170680355698
Encrypted:	false
SSDEEP:	12:VEBX5jCl/68dQ7o7AlWswCjgjnEzJ2BV9cc969JsZy85S82:qBX5jCl/68dQ7pldVMjnK4BbASQ85s
MD5:	0A80E4BBBBB4E93436F14D8CD7F9627F
SHA1:	91E0084EB12898226287B8DE210B0FFC7016FDBB
SHA-256:	513A661ADFC9AED45DEC1336F77866092363FB7604960688FAEEE0EE3D5916E6
SHA-512:	E9988A7377ADFD523B03984EE4AAEA7AECDBDD7B2A374E6B17D9C6E6E25E12A1062AFFA4F3C9FB3B82A494DFE267369D994C2457E39813A15E0FEE57A8448C9C
Malicious:	false
Reputation:	low
Preview:	U2r6BCWo24vL8752y26w09uG003t8M4h7zq6UA80fv35s51p9Zp32BK9k1k6E65Q6665x40b9ZTC46U06524..7o8r0vD1GYTDOQ92O5VJ7BK08vo6z6Z4md3r2a49B9Ax x634LQaztz5Ra556Y66C2eo4h0VVh15203v0tl771Bze81VSw942..4W6G3aGT9q2B2jk89J1JY154f2Y1m07D9Qbk08l350jUy27r157wS9817mYsI28K5..084A45e6N 0t6k7u12X7F2di9ML75g4Z24I6210Kq9BW23rh89WZX4plhMd17C9MO0G52eb3C0GR5zaIRm2u9vXH..8aH5G22A579f1GM872b95DI0r9Q2707K4r86p4N99GV1g5P..1 sh9167w036b6z9Sc4wvCN4of6Q9yxvXgyr60M4GF5c3Tw4468BW1031k2204W5SUP5fv0P22kN709I5d5S88u2408v8El5IP334V9lz7..41o75vx86515kS28Wvakj254 TP0685935J9X2i..

C:\Users\user\53280493\ddxecn.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\53280493\ddxecn.dll	
Size (bytes):	555
Entropy (8bit):	5.412945496744946
Encrypted:	false
SSDEEP:	12:tW2LdJsQ7QWa69RGGfJ+OjPVMPUNXbDRQpaA7dmCM5j:tWkdJspmLVM6D65yj
MD5:	7EB36716476C614B3DED13571C2F32F3
SHA1:	97751CBA734650E12E058FFCE5C05E8CFC16371F
SHA-256:	417B4B4E94894DBFF58320C5AF2C776204FF95443C9A0E684813A77BAB9AE483
SHA-512:	3FC11576AB58960596FD85C4444FF70328CAB333CBF71F3B55DC287734EA9A4A34FECACC21967E8A0DF21AB448F2999FCAA9A8048890B9075FACD2E59FD3786
Malicious:	false
Preview:	17Lv4QsK50P677ih39w91J9Q8N018Gp64fy53xUD017GJmXs9B6WqK8G2k2J4824104v818k597z6O1n8MEkKh900K9M1q94849370861J7B36S0pM..y6b5j18b6xu95R 0n5y35Q8Q8am239zv0l5Jdi8969D1Tt5NqwMGl10L6897682M8BB3vV0ccWr051JWnA6199m..40Z37989mO7358qd1an630lS131f672A2gcK684W5U0937HPXib0dSBT bl9793Cy298i00Y31dF3FVcY04918S0s2487912Q07qU9jv73612xUtSwrL4b0x..0uo62974yt6BtJ422dbiXj62e5CG1..x8619v1XhLW017903m03CD89eko336T35z 2b0A3EZ54h58iPH5NVO766Y3..4r8U5xH6Iy45c57700Z2V363gth5wXk4866N33S2cH1Xi00vyx3I136B435E58d4e6d4Pa9732xAJX840KMGg65lAp3296w0yV38M24N W9CA5599liPP88p4S09O172J18GU1Drua..

C:\Users\user\53280493\dxdgejcic.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	501
Entropy (8bit):	5.510975344748129
Encrypted:	false
SSDEEP:	12:2RAxY7dOZVXwB3hxhcUNQSdL6oMSL+/HpJwwHj9za:pY7OU3hxhcCHdO5Htm
MD5:	37EEFD2B53EF18B9911FBF4A71F15B57
SHA1:	7D9E409A484DED1265C37E12DB439E782559ED9A
SHA-256:	B34F5DA8CFD9EDECCB1BCC8EF21C83629FF7F13A6333E1A025EEB01C6B9C84D4
SHA-512:	16DCD59330F285E4606C7D9288EA00F4D5A7F762AB742D30CA9D62F74D6A400720EDE5BC980D5986A484091BF44BFBD606E05175320EA6086107B89A9A1699F5
Malicious:	false
Preview:	f0UwQ9fI3e14JZV33BkDbA202inA1II7E2X8M1lV3WX6801Jk6iu1S5NACygq88BpD3Q05IUvQ06Tzpk4Ql4u5I98VhC03BT0p..60q0f7n1Y497P0Tae069Ki8U0mk6Ny Km4IQ0JCA0hXA0agv32pi258i81OGi41u16738P04464351XM3K56ua9L548iU..691iCk8a881o4W4j78L0002MCc8zOL31bKysv3l4X4Od6..r701973gre18P374G6f Z92e39FU78v2M9135wu3g2y7784433MV759N17uO471ggqtAQ66eL4b20t6Czp0d55aKs4..j6ddcF787OatE5266213R1uxYP8ex2n9Mk03r534..G64Aa8x3g4O5l801 vs0F7R719bb09532Bf77Vk74j5fo6522i5bU0Z58i71Iz5yD03gCv4M6462Hy0s8l0884sFoa0N24BlUoWA303Q7XjGkx97DE4JrSr4Efx76P..

C:\Users\user\53280493\eiqluixotc.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	598
Entropy (8bit):	5.491195002496309
Encrypted:	false
SSDEEP:	12:olGlTAciJnCmBtGQ574RLo3cI5gp596UtMwpUzpRVeTNTD3WQ5lbud:oUAcinBpOLJIW59xMwpCApTzxNud
MD5:	13EAEDEA153AB5F5D46C0512F5BCD3E2
SHA1:	B68C1283BD49D6B995CF593E528734736BB74161
SHA-256:	3F6223336B8DA656BB11453B776EF1432B61447C996D0D558AF89BB303A25FFA
SHA-512:	25D4BFC6C5B8249FDDE8D0BC3F09C3F2BE1397CF00EFCAD4EB66A9F7A9FE3C720AD449D5CE9560382D0A49F7C66629B403ACDEBC8F258A8A74E4C1F14CED CEF
Malicious:	false
Preview:	6uJ8g725xV92jirJ4sV02V0qHFd82Ka3gH9gPOA5nG978Zbe9PiN2g61655377c5Y9KO73f40wx4J4K9298899mDF36Y414377174352ZtU73592A9W0u2670491Gix4Oc qf..u3G6Z715B0T845yZ85D25Ke71ZzG4m6..93mX3pK7cfp26a03..1450l151j9jmrwLg3Nz0ns0G9vNnbriRm347K3AQE3PYLZ6MB465SQDpN9391Y1f4PR224m6S68 Z39OKuI7951okg0D1OE9112Lj567w7YCy2X619w84ZfB7fRXmMG264IT4YdH96GA04Yt063V3..S75U0Ey97cI681g3R1l5Pt4q..cVw746SugO1b00d8k4277l8Yt9eFp Di1M7Mg9DK7W7z1bo4R0m..m35W630l0a8rW4nnZIT5958..7Q6tz50qF5W99L240496..F45Y4P71711..YmpFMX6pjQj014C00If62D7b9fT20O050cuam43P3lmlbVD ojCOn3932Cur685U71292m14KF7to7bv273a8oWq68Yc911Yq4nZnCD94li190r9v1E9oDw6q08t..

C:\Users\user\53280493\elmw.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	575
Entropy (8bit):	5.524653923114035
Encrypted:	false
SSDEEP:	12:3qeE1J7npOz675/85K17GSqEdsqV0cTitwZWFNdxaim3:Kvm675z5bsodEHbu3
MD5:	0E7F736E72EE80004C9AC5764D354181
SHA1:	47DEA8F5F65E4D1981F53D05835199981146261D
SHA-256:	C59F6E58C514AAB047A2BF594D5AF0CBD22A5DF31662435523885B3CDBAFE52F
SHA-512:	F017843E53C319282EDA88272900ED3152C3928A67599794385233B8669B36F79BD81B7591A3D9D92045A1D1D4211E242C89A0DC5684C967A2E223CB67BAB7C7
Malicious:	false

C:\Users\user\53280493\elmw.ico	
Preview:	GGvzk57dGFjRln7G1OXIY4w42M80Wu2T9G9JlY5q8o166772Slx116393kPu59m6L3d4yo9cCg2tm48s9i15373US5..04cG4m657XFVf58018WYz6X8o5e4e53UG28wH56A814788x0HF6q3rl049xqHOf2t7g0Q7VlvkBI9Z4S4Qcyuwn7yhLYw4230l10..1StS4ai5Bcu3yl7i2860dmr111194qriGI8308X7iAP15977kdL3t47018M8d417520H..7Le4T4058009dgV6n209d7w4L1593P7d35Ap3g3z7T34X5Ac1270QSpp96S754ga..9G6uIqVG8OeiWzH014sRa8t8tJQ6QY3b742078p9C..gaN40vL9u7g47MwNXG0r2fk37..8Yx9G7HrF8Ge1Zy41QBD8Az9h1PC18Hd6TZ905t96I9BE6M5AK6LzG515vg61z62MBP..3LN9R33mW02f2W7d7aee956w0h20w4r2bx3ZsPbh2070DZ3q5483KD090vY5fI5J94WjM6t3Yhl32R389Y03UW3P2uZ9R6tgS892100Y..

C:\Users\user\53280493\fflkirjbw.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	543
Entropy (8bit):	5.421168252399577
Encrypted:	false
SSDEEP:	12:jzxkKhSaPXbavQNtVUrNpCZtpxr5UhX2JX74oo1xUlAKYDWvv:CoPXvJZbxr5UN2FomlATOv
MD5:	3DAB777F126B8DEAAF5F40C548BE2DC8
SHA1:	6C843E42C9081FCA0F7937C4100E30D87AE19969
SHA-256:	9831274A9B61114349630CE86AD164B5F6F8FB9F5BDA380F1E1780DC909BF478
SHA-512:	6D3D3D0DBF6750EF7942C33588F16CDB35E05B82F8939ED467E3C5C3A7B08232C4032437C1CF9B0B88976B7C8D79D6E1805B382433DF3ABF1D5F64359A6C673
Malicious:	false
Preview:	81z8WRS5x77q927H16wn1L18dlU3C7597K069017QSf9wXWx777151JP569Ld9q..zFB501CU3o71cRog1TSRSqr541M4q6CE63451f8x6fKojB0r8u05E0J0530dPUX4G8h1Q838iG06s7523q6iaT3a6Rj0QgP1DR4a6gMcvydJ5h70QQn0iWh191HW71K4D93xDn19eQC6P0i423WQ45Zbg62vNA5J1FCE908Ls312539wo9W40z..E00a7zGP1619t16f214Y660Q3FbT5C5UO24j0kL30x898b1R69H030YRik1X31cL4..L4505QZi79Om450q0Zvcxw873oju42tj1i522DQH20O19565J8CfwFF3OE095P68563CRv6228u731Z8Y2c04436..zb1i282WUW3KS486S9kP895B70c4Eq8Pj3lbF6Y8cTgb511ei95GIF70c920Z064zf6Q624s4ftf1n4o3t2IoU80V5s45n6ur8u57v44p0P28zj93s3e765kV612U0dt7zu5433..

C:\Users\user\53280493\fmvnisu.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	515
Entropy (8bit):	5.5476656687734645
Encrypted:	false
SSDEEP:	12:rJASYRUTwoBRUx5ea+7hePVA8Pt5wSc/MlrjEv:iSmU8QRUxkX7iV3zcl
MD5:	D03F886EFB4F4A27FE02AA849F654E3C
SHA1:	90F79CBCB7E5A872ECCBC0B3074751E6BE4A682D
SHA-256:	DBBAC67934F3CE7402D6CBC73714E0EC78FD4B23BB296093363DD134119A7539
SHA-512:	6606FB3EC0539FDC0940DD704EE46D727EDF0D55A384BECF8F51CF4AADBBA330E5BED75CB074CD592913D6A54894FDA4217FAB020B35EC6D50FF5D698F78FAE
Malicious:	false
Preview:	3G8kbpW5v38rn7o64E5ZOm0669756Ppd0Yf5k4a1nFWNQ932XC4K1hE522897KGCg7aE7R..XX8Z1W8XZdTlU4F0a14w337L336U2E4sx9WIX3hk6f1aB3QDn79P3zOpHCC1sW..33t6r8w80W26qPMuq1XUr3sL79qA4hB1Y1552855880l5gsH7008xh154Yg42bSeXd45846l91fv9211351BFZ..004e66XC15239eijMG0f8OK4642Hf14812DMuP5sS68BZ5D0..8AI41QXIP1m258Ss9vkFFI2D38669pnWGC6K7n201q41SUgV8h90Dz3y5V00G07MkaCv0pbcn9lK9z3149yJu729u4grv615RsTr7bt67530sRm7rZ0q1D04j2896WEVV7gaCs3wU0714tXLz36..t04051l608x7p5lJ8fskNd..V82gl3x67g2xKUr244GX52JyD94gfdw5x..TRPpAV25xyXU4M348B525DG6107dKKP..

C:\Users\user\53280493\glpmruvjds.pif	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	661744
Entropy (8bit):	6.575295279326677
Encrypted:	false
SSDEEP:	12288:mBzZm7d9AZAYJVB7ii/XAvKxRJBnwvogSJ4M4G4apo5DGDt2:YcneJVBvXAvwRJdwvZ5apo5DGR2
MD5:	957FCFF5374F7A5EE128D32C976ADAA5
SHA1:	72A4CC77337D22B5C23335538C62BEA7ED9CBB93
SHA-256:	699534A988A6AA7C8C5FF4EB01AC28292BE257B0312E6D7351FB4CACAA4124D5
SHA-512:	E9DC65FBB964CB64CFCBB1C9B5C53595B0F0304A7179710DDAC5AEFA2F0F40BB67271B7AEB39654254C2FE68FCD62B77A94674B8E9C3A57AD3497197EDE87CA9
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 50%
Joe Sandbox View:	• Filename: Purchase Order_7789.exe, Detection: malicious, Browse • Filename: Covid-19 Data Report Google Checklist.exe, Detection: malicious, Browse • Filename: PDA_pdf.exe, Detection: malicious, Browse

C:\Users\user\53280493\glpmruvjds.pif	
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..... ....@.....p..... ....@...@.....@.....T....._1.....D.....c..... ..D.....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc..._1.....2...R.....@..@.reloc...u.....v.....@..B.....

C:\Users\user\53280493\gwuqk.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.511651848817459
Encrypted:	false
SSDEEP:	12:RcXcP6666epK6Q+WrDvIZG8h5ToSgHmWsUTJE25WNlqyK8ZHU991DLb:Rmz669E3+WvvIZ5h5np23WayKY09zv
MD5:	895A5E0AAD40F37E9602C2397B7E2A26
SHA1:	F8CBB2D3B6DF120F5AD01C55B5D605711981E308
SHA-256:	6691E86EDB494A310CEE5D081D8A386C3C416DA8D3E45B376FDF81DA9BA5E674
SHA-512:	64878C96C4B4E81C8BE8C521A7A0E3C9C54151974D9825925669FBC0F2715727086BE60100E5507F0AA23C79C7EC7EA68B77A7BAC881F10476C73F79D98F7AAD
Malicious:	false
Preview:	40f76IhNaA6c7B5l3H5227Ig3Hay8ef1897Om53Xk5R5F8757E36o4mk1..n10Z5Z3V7KRKN3U725LaN6235Q1w1Rj6Zz6y5kPba387717a858Lwb3N82BY2Z2BY8mI997 7t1CSd18a671274fC40llw804n0248y5h8799Xc8ta9g0xJt26L779O14mse7wj..93F20Uh83kWs..8Mi1n069mS1..Tm7q4X483..qiR5LW9d79NV946C3zXSHp8D94P 7757O9Jm246Olw9Qpw8CY0Pxq40X2WCbo536oTvz9cR95ypkPc5aJ86p74enOf2IS520Uw13mW99E1V..41Z3Km525Y..Im4a16h8c6wfq3C5a8cr9369U5513JmuR1H61 e25..6r435U77zL8DQE90u70iEvu52OX44eT3a4..6Ca0zlmyL8kt8dM31819y1ZKOw3MJz9686a55F0s50h3rxCw1SWP16VjXlifQ6IQ3H58W9lTdPq3SVh7A9090wVcD Rt6k04917Y2hxt210S36VK9K97af981yy359528cZ1c7UF7Li01wkYV03Q298nBC92516c8Zq7WjBeX..

C:\Users\user\53280493\hhbng.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	541
Entropy (8bit):	5.47191970301225
Encrypted:	false
SSDEEP:	12:C0+bxmNh+xL7gnevlmUW1s7NfU8K9Y1nMGP9ivu+mC:cCh+xUeN0W7NfvKC1z9DC
MD5:	0FA2ABA321D800998053E99C8C107C4A
SHA1:	1217A91F7BA8054B16D72D89CCCE5ED121E909E7
SHA-256:	D4DE0670A590E9F21FCEBB07A0A5D6AA1880FCF75F076416E7ECF948709A7B92
SHA-512:	92A3C48D6DC345EF6457FE5A0CBB90EB73817F600BF1458C80C9B1C5044AD91BA105B2131437EA51FF50ED03918F8F0EAAEEF91E9956FCBA53292300B409EDD 5
Malicious:	false
Preview:	2la3P2438aVFV7JQ7502Y3q4kf67Tgm40KzNHQ669gi38Vj128Te7D3Qx08P923975le07IMgS798t26l0r7w..Lw00lPY8r7Vu185Pa185mckgUi89El06XekW15SZ7d. .27z4835kza8Br7d9KJ20510Z02785507nzR8i8IB69kjFj243K98593ZM115zI6979Ji9ON5J6nk578Y5TU9F5D1UGaZ1CY32f544x191l2a41PkZ005se96Qqc7mi5b4 2ot11zDdn6W176q06eiuWl..jTF32uYEl0cGmXii31ualbU2T2176s13xueY718t1C8x7O2R6l2103E81SG2a90m209e52GBWRyhaz97546t22Y5616mf826152W8SMBUU 6V26QiDQ94bt18z5o8kml5ALv5R1lfg..Q6f7j035ia77oW33u9855y0cW3G995XYnfX62C97DOU07x81R..T6e34Wyysrb1E632DN8Y2nXf3r8k0Jk8CNZZ99jS899tP5 695MZk38o279gP73g4q..

C:\Users\user\53280493\htrdshaq.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	5.456145489533924
Encrypted:	false
SSDEEP:	12:W37Jf4dlV315+VJeT2t6UM5U5Zd8HyiX0VZfBs/TOEx56:KJAdv1kVJeu15ZCHyFLBs/TOE2
MD5:	259ACEF98745DA1F89D2EF9EDD9DE742
SHA1:	4F353688E7AEFC94B43E975FC054E196BC445F77
SHA-256:	20091CBF527FFF4E2F600F758FB556261836B32286BD56706BA1D8F99E75A7CE
SHA-512:	40045C5DE6B2F9B011CC6DBCBF2E8C612FA36BB4829F81EF8A9C323EC6554866D1E2ACD83F4F6911D068E28842E7DB5F8F540717259574C2229D63CB70B3110
Malicious:	false
Preview:	p69Z820W0Cc11NA0W2fNkn77s6ZJF61e..Z4K7150rI93U67ZEoq6T3u8Sn3P618VjX41aR2yCaUPJ3sB2p7..sn0l155fnorQ0jZ59o80155W23g2y3357z39e90ae6io i14j74S35a365ZMn2XDj9LL1Ba6173n31knvB..8q0002Xo3HAZn66dnt74L02w7W3j3HV1zB2870ApdPFc5t471VX28..08j6M9A053W7nbP3td189Hm1z7Xn327ta7Q5 Fby6Sn4dBuxfr95L17270966mw41G7J5GbJ25..WO88gy22W090Ttq995835YK0f7z85nhn91i3..0s9c07L0blkH27s0whcR79L29W2Gi96Ua18w78U5wS8T0M3q14J20 Zn7Z509389o8m2gqZV2o7lJ463U0Sw6y31l..44PMV8tn6w740i857842pG479yPI71i9v6gT5355q5qM8chrGz58MQ16Ca4053uR1o5624w617knqvrkHC8d65gtI62v58..

C:\Users\user\53280493\huvtexmm.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\53280493\huvtexmm.cpl	
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.502174989427254
Encrypted:	false
SSDEEP:	12:rCnwlyUKWIrwANfPzGi40aGQVyRYb1ixvHAFR8wfZS:rCMyUGPGh0aGH3fOZfo
MD5:	C1E1C8940A45DCD2C751D1B8582B9C0D
SHA1:	BA98F4148F0E34563BE0EBD267A311A39692CF28
SHA-256:	2CC43765F27CACE82215DCAF5B74710C5924E75877E88C6563B778B8FB1BAEA0
SHA-512:	270A092BF3CAE6C028DEC1BA89B953E2A57000DF726D7F19F372373D53946C3CE4E957616BE07AC275E79297A0144535E71699055A16C2BADD3487430E795B64
Malicious:	false
Preview:	i5s3Ef93v..203bnSJ65CwE4NrOUX4M55qJ8Rb39xg..Dw6279wo6g9RRupE1X53533Lfd68fszph51e51..xo79aD4t6369GjvZvD362ez7d52Gs0o3nh73t05Kc123P1 6EQh26c80g81gnI6R4EQ1b6728qc9x..77H1603H32sd99R53owT1jm8c422Wj71p7beeSO5ja3O3VPUx2h633g25r327539qm94s9ln9S18BpE3nBf9X6zL22J7529N02 F9744AHgHZE68Ig2r43X0VOKo50KS8846U2E6oL7qcd1f..e3AKB03nS12m4YUp68x6OVx19j5c0..716cLc86J312MS7xZR473bdVbC4696Rog2b0YFk01cg6Gp60x83C Y3m6V55d4JRRxY..0sK4787wI4Nh22A099TI3J1707S2BT7xA913iug26B0a6qdj488f8786uW7fiFWhq08mTM062hc5770440r941n1E339O1Aw85BGZr2pSTm79106qc v1Fvn9Q51U..

C:\Users\user\53280493\hwlfh.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.481972864360933
Encrypted:	false
SSDEEP:	12:6kwwKRgl4RXIUR8UG/l93KaUoW32YEsDAXR9pYIXtdCd4TiCYZzDR:pURghFUEX3KaTWaiAXRHtdCdIYNR
MD5:	889AEF27132FEEA803DCCC122B1BBF59
SHA1:	F3801103C8BD5384A278ACEB493E68E6C9CD7BBE
SHA-256:	6B5F564CDD9E7C111C4B2D336A4A5D89B5369083A055286D2E1015C7084CE109
SHA-512:	DF539EB79B6FF1D4F796B2EC9ADD84ADFF0E4CD5DCC8D6654E022B2CE014B5506644BD081F2E200FE9535FC2968E75C80FF6CF0E91C37EED319181364DA33A A2
Malicious:	false
Preview:	7iZ852fZZG2Z29gH7GvY487P7x89..ApUWWr1921r0ASF754iL339BjG33W4406eUp4HA1eK0L72W5T779g0X0A6Q15M3py61D7680T19Ws05r086zl2..v08KP4ULLY8V N229u53fJii07ob990ZCJR3401V31544Qu2S7hh2679MN60216X17xCj4699pPs6BQy7t6118P16FX22i2y28091dQp2rLSu911c2h1iE60Rm6cJ25b4yED9RCC4id4o57 oV6QChD5856JYXY..E6689l4MI0eFx61iXkB1WBW3vs3ncGsu4..P3gPBqOqX9kaiWd166156EE01X3xSZ27h4T2X52400v270b90..nsji6874lH8TG8x261R16Ppx5.. dp2nI98fdAh1rpk247K89a3LDS349818g0098H84a20Ehz4K4X099382H7CC6tBH8F6djLS87v51569Q4QTWJho019Skv4tXSH..OgedL536F3PJH8478n16B56bHTPK74 7sc6A595E7JcDT0pg94F47La6578704zy64bTy9665..

C:\Users\user\53280493\iccii.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	552
Entropy (8bit):	5.550120079524096
Encrypted:	false
SSDEEP:	12:5l/vILq7xC0RjhpdTYkASC1kEUAqepNglqJWwgv:oSY00Rjhp9XREkMlq
MD5:	6A0F61AFEA053D369BFBEE14C797CE06
SHA1:	11FA980D0BC58C645B5D8698B6FF2CD98CA1A5DA
SHA-256:	1E8801549DEFAC8FD207AC3548644D49D54BA1C1F9645EED444867A9CA2CF923
SHA-512:	7168F6D491A52A1EAEE51452181D4212CCFA1E5A87B2B3F68C165B7C4BEADD38F08319F435F47F3FA7ECC3C7C8A077EA9A89DDE6432555DC922852BA6D6264 7
Malicious:	false
Preview:	x07F4Vf015MI676lk2FJ72V80Z8X38Sbv7B..jjtPZia5osV0Z1452ljC6C8941V0flJQ2B42p705cN77U76L98RdOr98GY07U91N28D6011a1mmXLWTA9oUm7Kmo9V2w. .713041N2rX979L5C4bCya3n65T27F83bU9w3w2o1r7SAkoqJk94g8UVQX5RW9kJ49OVDWHFC99T5g72956OpX691PQ7TQ45Fn2jc938N0Bh2WX4cOz2oM.. Q81Caa2K3y6HO..as1677J3P9eJq53VE4o1TENXDM4p15R47h6neLy926d91w777MM2V7N7ly4Lr6cPL5Drs9u06bP5Aha477E2kzl9O4k..61Fkc9WC7X1..5Xo21uC70 RpN6MC1922cz702wW3unf760jw5Gr840O0X7DbV05z4O1D3v6T5V6G4qB1AID310gO7zaJ5D8pjiWoQPe228gQAHo3vm186Si7ll..CQs35861532WK36R57c44J31Fu0F 8Dh71c1TVQm853T2HD2uQ1p1767nx06k671vu656..

C:\Users\user\53280493\ihgiaxcv.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	503
Entropy (8bit):	5.533715493588028
Encrypted:	false
SSDEEP:	12:omuhXH01Dh5pJrShF9Hnp+6y0f2kmpvsD5Yv:qhX01lJWp+6BukMvs1Yv
MD5:	F13603D8CA811E3EF786F6BD2673F3DA
SHA1:	30A1025E6F16A7D24F65D53800D3481FDA6C8F86

C:\Users\user\53280493\ihgiaxcv.icm	
SHA-256:	616A174C8D55DF50CC44357B97CD239B39B00F2EDFA5D3FEB63F022C1031531C
SHA-512:	8E028F7357FF034AAC799F69DD96E1D19143C929CA17433454D8F7C6A01079F72260BEEB467F7F61562C237C9DB442B004C075A62FDF5F9294E0FE263F29C58B
Malicious:	false
Preview:	7j6FSvE5unMpWNw58a3SxOMTs50eKx750W7w36f065FK2iZd7HxABc4EbIW8G99U4q7cSD74pz7Z9VRt0h3Kp5nM2b9xu5q01O26lL86757o30uL2z1v7K5749P4P389tN I082S8X573As5I..5kb2HvV80Vu0R63W0d2wC6NEPJSuJ7ag8wwQ67Qz91792R3262R7129Q9zW4ko3y3FcPA983q1A3rfgcqZiA6P4L9499h189B8Ab153266p84580PH 6Cv6Q888w5FC4fmNKHV3D52Q83v103Q..E5Aj183y036aYZ52jbn9v6596Q6Z35YZ0n22jk72oRge8y3MIee94q97NrVH..gbhzzk3A..vH4JJiS8n2VAEuO15g0HJ6k6l mICOKD7j1344q7Zx791C6X548150DODK83Z203Ii53523W50Ot65WY542g48M1gi06..4qc7V1p0DXX889042voyzc3j927Y5tSz75M5o9529k6..

C:\Users\user\53280493\isrjlttjqq.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	526
Entropy (8bit):	5.4992757067928695
Encrypted:	false
SSDEEP:	12:rFONtRzP+FoyAcMbeC3PdoKNVVrzCfPt9qH7rH1:2t9SotcMbffOKlsmbrV
MD5:	9B8EB335C287CE22FE803A22A8A1F46E
SHA1:	33E3D74274DBC23BAE37FF270C74E300D5A887E5
SHA-256:	840BEBB8CF38AC999A7C2032286063341A4036BF3A4E8D3F5E621A9EA1109155
SHA-512:	A7A66C24C20361ECD7E0AB3DAAF05F8222DA022449F5CBC7B31E6FBF5B32588377FCE0AA2CADC86D5B864342B67094062E854421BB4C65B99F67BC0A681A7F D
Malicious:	false
Preview:	29A40l31fx4nJ9bHoP3J060o104i88816072Pqq9s7YZ4ya5Z4DVgyN0W9D640G95dT56jPOXP50c3j8D821p11l34819vh72DxuE63p6X06m8fdWB0457T65SP4UX894A a..zrg955c8j95q668vH63xv7781cjj73V4C0y2b88c953uF6J1bq64964VfNV2eh98mo7ZB1T8i499gPv5M10oLI..K2K6YQ16y55064Doq81374XJH52u16M02K14XTr ok1RF22g39529WD4C415OJ14nP2jxcO6W6uXS8U1NC9j5G4ONwVp620WN5179FbIteC57BagsFYt284C6ce44g13K68u190oSpJAU369GYVS38Uy70L894eZ yQ73RYR96l24H1O45t5..muCpMz80qCwXBclG7ibG2WEB40qD68nGKK531BBRxe0N8r9G34A5pO91327GNV3I6i923OxSg0q662KcS16C12b536T2738TNqP 2y44c799uvHI1hg7501ey9Bo..

C:\Users\user\53280493\jbprcjxwdo.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	512
Entropy (8bit):	5.444049773069389
Encrypted:	false
SSDEEP:	6:XNM9dRkOUqkWL7h3Bl5UmwRTUIdIvziQBfl0VsevcxWlZcDBOWetCV1EvImrQEAN:deTtbPUmkTpyrzBflEzBOvCVoImrHa
MD5:	B6AA213A3CACAEAFC0E7462CE288CAA6
SHA1:	C6F2DABB1B3CB1D80F24D22C2935FF9FBA986E28
SHA-256:	DE9463814F32F3673934093F565F68DAAFF9C92B5833408B4258F4E250A33C70
SHA-512:	5625516A38A0E8374BEBB2A9F3CF59BAA13DE764072BE3322FB91BDCFCAA320206691CB45783D1871ED024170F7238A8568AECCCEE786FC8D83BFED7E47B80 B
Malicious:	false
Preview:	EO7ih0b5n773gcI645H2i602E7p484szBu4NJ29072l8z78Z2VB7i94430C5H54b9Ca7zKj7d..j0WHynV9u35OWqe72L926544Dot030x62gyQ99TE0dxA7nk7he842W8 1244662S2xR9G049j66xg2TTG4Z431t1Ub7ov81Z28..5p2E7skvOHn3k6aq649W08Z11381K1an2byq717l71SVAJilNQ3l376uQ869865es9..9024fFLo4q5M113l64 2WCTX3wK5Dh59K0U9OEz132qS5ZJ86Jy5WDB90W09Q0cjq7kc94dgqzI5jg..z91noe7S395Qh3767qLe6BSVll19d67t380D46HV9yro12063Rj0262209e51i5f06t9P 3qi24N3MY10V3812233QL33lU2URj6xOY52E3736s8208Qg5m..5CAQ799996yv12qx822Od4S8KV631DVs0e0D5r77iwHaM9873fl9fcgjr9pV9i0412F79..

C:\Users\user\53280493\jqleufphfj.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.438508288765481
Encrypted:	false
SSDEEP:	12:kiBN4gAd1HzhsaYgn4VBzn2xQgWu5R2Y44MGeV:kiMgAj1saVYZgX9eV
MD5:	A3238F109720CBBD07DB14FF70E036D5
SHA1:	0B1DEC4E8EC666CE04ABC097D78E45C5DA8D04FB
SHA-256:	D2C8E6435A7E18D2F76EA63750FE7FB69FE241DCD3458AB44756B66D2D554EEE
SHA-512:	2ED36767FFB7A9F9E202C040BA3DD38794E4B25D8F2207EC30A67BA91A676C6134022AF5678173B4872AA72340F4962B2D9984838C1823172AD8B74E55DEECFE
Malicious:	false
Preview:	ed4038585EbZ82A7Uqn9OOAwx8623lo30gV5684g6o7nI32n28x142VNCWTp0hnVB721c82191rB0C9jeP6j43..C10hW98227C7VW5xh1635D857BR9Y20117i249L2RL yNtL7rz0tO4v1564q45Do991sw..J4MiEI7r567LRS40P0u237Owx695p7y87alf50IaVD1168pDEd6o6Dvo721o8Bv3nubD70U3Fbv6Y7c4ILne7Na4IfSq3634485nh7 aQeY828jEF505pod05T09700j..F5238444U1P6r77447R81Mwk4X1a2D694bgp12ZK31w1iaWAS7h31362G1..1h5449Ck934pu04V7M39Q2Eo87f7C7y958wU657Zck9 53m08..6P6gw306C9z5lYY49jV1KgKw69nP5re78eK69C9r4935i2q152iB60zRt3aTbpJEm0611098020D46W99rEM32u19438R7xBZy3376D527w9Z1CUQFqc5O7y62y 4r1cHeLlF0..

C:\Users\user\53280493\jtdfgk.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	512
Entropy (8bit):	5.580811322761355
Encrypted:	false
SSDEEP:	12:BmqOQ5LrT5MWYn5WCaPnfc9xDxlbXa2B54y9BFSpvHtgD:iQhrK58PwDxlbXJBx6uD
MD5:	1EADA34B16367E428610B818458ECB09
SHA1:	F6326BEDB790614AFE1EB941A26323C88E1466AC
SHA-256:	8C506335D68047FA0EF6CEB6C12245F4E84FC98783094C144FCE296F4D346B5C
SHA-512:	BE713983250F72A9B3EF53EB5D16DED06F7B352D2B197CCFC30436870458F2C73E777F415B7635BA8303A9BC5490352EE7A0879E621BC2404189F406DFB978ED
Malicious:	false
Preview:	2ZW6EaZgucpN79AKG6Pe526Z7Z52AX20ZDc3111Qu77U58FMn170QdB5sbTa5d4J103Ts925EWZUA8Hcz983FSZR856le4..958Um3vb2N85194h77qza7p98oqlur6g0f y8TIx8dtf1i5LN36537..75reW56wD8s7H8705A6hl5CZzz49hN0S6KY4M83mAvqp7RcS2gHA4fY2v5Yoaqb521A46cb749Wcrk9ot4w40l7j992M5l7x31kb990Qra8j2 Hw2D2kZ2o329S7cbb6nk0Hz57R9Vd19M5xnB28I3F5wC1OmYr7Zp..e7Edk6EnJn504Z5alP603P4P1125Zlar8vylgf1N1Cv761L070513MHB4NR5k32L3K..0140cw6l ..4K01eNflP5..qj1357725r22F7b87EU2Uig8DjL4Rv0f2kl3jEW8jFK..46p2i2g8F833h398rrqdHC36M42v4s1xH1..9IilH70Q6YSl4Rih401i1y790..

C:\Users\user\53280493\jtkl.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.452326565866018
Encrypted:	false
SSDEEP:	12:MA5vB4lWFQafYLE4mW0VfucGHMGfyOUrPr0AD:MA9xLEx5t/GHMGf3UrFD
MD5:	796E81E2A9F1AC68D7F92B7D011A6B3A
SHA1:	25F529A9992D91A965384B235117DF98BB47CA1B
SHA-256:	1A0486157F99812630995E1DBEBD4220E91A154B87B01DC353758478FE615A28
SHA-512:	2BE117F11DFAAB62B1B0D758D503EA31BADF41EACE7D5A30DC454400359C9BD1371ED8206F0DDB1BECF28A2A03B7594BB3A79AA8659B5E41119B79ED7C118 24
Malicious:	false
Preview:	J76xH1g64Qazf283A4666CW1ku0ZykY388O16Ki6j245T499Upd1nL8l06BK95KjTWm4m9S969Ji8T92H6rmFON..97LN4Dh4167S370003u60a1u7s5y6v955qtdY4aF9 6G5la0VD98..011s421ud1Yf5n47mP5578b9DU7lgB5idM332iUy466y6036as76vv07S22..3Sm0p2sF5A3V38P43fBF6Y63u2sDv9110p18eX83182157239Efq1ulL7 3y448N02Y13qoAO14h2Ao884mtXp819e554H318Et093Pl6l5Whg2R5F..iVsce402C98sRRclZ62Byn5k8q6..Pa9766654d3fu4X8Q71NzA5q347119R3sJDeDl28KKi fetv0o7..2UQB4517CNO213..K4IV6ohC6g51B2w562W4YS33Ll41923Ka4O38Y5c76Vt0KfV..16z3UEin476Gb6Fl6B6j3f3pRs3Y34w937408G5BOt7M65Dj92222Om 0879i8zN20..

C:\Users\user\53280493\kfloojbqsj.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	579
Entropy (8bit):	5.532046473649814
Encrypted:	false
SSDEEP:	12:qvqSBFFa8HUwyTPjeDC1CK7X8OuApLW05RomWab+mkkh8w7L7BzF5G/MDMfLf:qvqWY8HUwy7jhvMOuijb+neHFF5GkwfL
MD5:	26A254A25B7D1B4806BDF14DE45B72AB
SHA1:	8CB70B7A600217F3EB8B218C6E63A90D9561B86C
SHA-256:	E2F5BC174E6EF0803F0E9700508251A269BDDE3B3696C530E32FFFABDB6A2993
SHA-512:	C535911BE7E34D84579FF91082895F4165A65645553B9B6BD375816457316ABA157BF1BC19B8411333A3F6FF379AEA3239DB3629781927653F3F2F0436346E29
Malicious:	false
Preview:	i5TEQdEBc3X0296gltvl0T55z33KIg26lqhxtoUrM1jQ4Aid3t448C..d25ag9dj2U09V2f584iw8yME8z28Y8Y00l..5515tJ473MZr036..T09Yx03j3yzy9VIp1N868Xk5R739S.. W1lvcQ29337457922xyl184v3w82..2U5T0500x545W4TNC5Y3D5Y94f0E52D5F8qB..S29V16jf7gS08qrCVm2o889Qf8HHk34729G..0EnnugS3K75I0swa44M8KCBNX uKaV2qP2158u8O124Pf621c5q34314B1Y20J14753N682OZa39MhJy9Q8a93at6n1u55945..3em8aZPI7p0rk23LrHA84Yy66tfb65J8o64Ri6e4M3J8B1J5950S1edzt j9207uNxJdIFD8Tc151h7a93Q3of..75C078k1x49078aK2341fl7G2Xs599LDXCY7rNM48Jik1..e1b4396B77dW5E3D95VN386G9192o1vqO6eflYt17Ay4F2xbH607z B31BNLX7322lu443somh7fm81Dsd8vS3hWz9m73Fl122vg9..

C:\Users\user\53280493\knjndlimwp.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.4706631738348745
Encrypted:	false
SSDEEP:	12:TCoU/cEGoCvH374EiRdi3huSQjyc1MM1zE:uyKsX5ux+xM1zE
MD5:	437752EC160A63BA1D154F3498395C3D
SHA1:	110179CED16CAA1209A62380B75FCFFE7A666B33

C:\Users\user\53280493\knjndlimwp.ini

SHA-256:	6FB7615586FF1124E27AF8ECF198F73D0294B398D42D59551D1D7B3224639C70
SHA-512:	6789E7BC1C25B4BB7BCD562BD7ED1E4258F385A6F808A04AEADCD1F368D80E0F7C4A58B305CEAB7ECB66905E4F2FE797B6077E7B657375F941C7C50D6B7BC 6D
Malicious:	false
Preview:	3uf7xq6Wt7E81n0MJcnfPh1LLs..v9974dX3i5SdfknlyMtLZT50O8q21L81i9T2YP4WCkJ5480bAY6N5u0382603n8401C93KO83FDMy2SQ37miwpNG481L8tkB6nLUL1 z51BgTI7h5831qi895o1G..Kq07EyE4Y80t83mi7TG7A7A1mG..43o0z4qI3214561q2oF39g4HD7H6Y02562yJ5tK9rv7V37Jz1..1H3faqiZ101TMR760QM61mNBz76S v0Aa9ClH0OOsE5xB56S6e4R97u752IDqliY5F40oHtzLs7m8822r626270U6..Hz6TOD0wiM7rWE4gN1q8173972277..1NIKgc5594Zuq4Zv1b88s1H054U820747NP6H 7905XO99psE8OJ0GFD94yL96Y8a948N8177nS7Z342Vm93763h73ONk5J0gG57Pnr3Ntn47608Hn290092iU4..Vr305Lw8838G6O6310C1O8W54..

C:\Users\user\53280493\krjplrktd.mp3

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	597
Entropy (8bit):	5.5041724313549505
Encrypted:	false
SSDEEP:	12:LTIgwes1Wx9GGGLpoR/FK+4cXlNmpruQ02RXkKFsBjMfdTHaOlv:nIgwtlGYaK+nNwrXsA7
MD5:	76EC7556C4DE989C776565D02455A82B
SHA1:	273A3AB961195E0C630781018445A55F22C936E1
SHA-256:	DD6D107332F32FF6E4A6A8DF04FE54A6EF512A887C3587BE1073367406A9AAB6
SHA-512:	C0D1F32C5817D7AB33D26402933AAD06AE1B7D5491F4BB06B5A5868B9A32034EECE332459DEEA686007ECBB41EB19803A329A16AEF82D52A5123038E7DB87EE C
Malicious:	false
Preview:	2ZvT1699cF681725aU048Z475..2M61l5025f2n2UR6iD35Eh84x48076SOa170783W0T7PG53fA1N44Hh46yz1T416L2b9203tY14z75..x5B3916lG5ozroK3OrS6922 24G2yMU71..0YyY4fP01l08FAU99b9Tf4PFUrpN42Lw9OM7..i3hJf5331BI7136O400xX0TWXVt3G4El273fUc8c46SKxRJ5TJU26P0kgZ5K24lTG..0754G5Oyjd1oib 117O3RmQ96765R5C0m61d9iK9Q0T9K193A17j29A0I6X6SA4NRJ8u91ej4uS1yu3b30K8v64k2FpzJ70zaF0930F3vcvge4lQ9472MN3EFzePf4L7..4319928w226r997 o5v834p9Os4uJw1IK0Y5L9040hFydc7YJ3O0QTkU3S6GYq7tOX3hJ81oF1..8fp1t08H46wWX4u3I288y530R..978kJpL505O598369p169s07jziY6E9912T39f9jqS1 Q2wX02y9BxZh48m7naO3ohKW70kB3632v6w2YL7S62b3qSXDLvqkK2GDlUMz2618xXzj20mbTLe..

C:\Users\user\53280493\laqcdswu.msc

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	592
Entropy (8bit):	5.459464564526366
Encrypted:	false
SSDEEP:	12:hbfTA0aALELl5PdhtKHSYUmWysh/U4JqMtoe2YaEqMSmXxwBN3h:hb0ILUlnvKTnNy/UqtoerVSmwR
MD5:	8060CA1022ABE6DD6BD8F726C0A92AD6
SHA1:	F51BA09E2617D48E4F72E5FBF82537219C04D38E
SHA-256:	2A164FC6A5A479EF4E8EEAEE1F1C824F1F7BA9D45720D2ED8A87E1D1F5C3AE09
SHA-512:	3FDDC44A13639412AF7C0E21E0C2997072949A0A1990D9BCCF015C4E91541BA7BC2FB91DC241537A4609DDAD1AF28EFD6A1D996EBBD753695B04312E187669F
Malicious:	false
Preview:	ePQa351ZH4rISo9788T63730936u1BU7b73RI7eXE7zT2H6S6h..G3q3dN0LE5z7PT688068E040843N1CI27Kt86EKCa6lXAH57nD7038Ft16ILe0eI766a3zIabf8IZX 2Wu49KZ4tWJOtq2xYP1W1SqkYEx5Oat6Y292LkSzy8E..E08w462..K95Fr21N7pI19268sak5hV78Td96WRXNyFFnACvn5Qx47W8MIkzl6270LU9Z114ZT5SfN1r5eYcJ 2nGY4FOg3q47I23Q17..2yop12148qn6fx4SD5Tk11P9Pf8c6xCpM0NM67Sb7t2868vG8l218wj891995ud..7o2fZ..95581cEky2845fp3l77E11776395T778097gsx48RI166a4I w221Q819ZDkZG363kcF1k8B6r071255y2506G80qngq4r5N9aXXJ85649jL6pq160..0rLkKV802zk54850cn50Jlc591In01RT1YE15S166RJR21C37e255xW980b98UX q24992V6M6l58CSRBZ06vj5B78S84B1En2y8YXMZ1NWf5S25Y0b811q054jq..

C:\Users\user\53280493\lekcfklpqn.xls

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	5.417949855648765
Encrypted:	false
SSDEEP:	12:VwS62aONmups6sqiUEbh95psAAvhSwVQSWgHv1+n6V0GCUFYi:VwZ5wfQbU8rbs7P2gPnVeUp
MD5:	EE18BC5F6C5B7E96B96F8F36B1A0A0EC
SHA1:	640DB76DB36D11ACED09B8D276C317CB2C7FA880
SHA-256:	D391070B3F37102CAF266D3EC651314A68D373290C4B2BE3A02529A29DF02584
SHA-512:	90CE018785C27A299E38200DCD8FA7CCE6E87A6741B4C964720E54F8594605F335854A34EC12843E652B932EC9611AB59FD09849DA8991E03F9F7227950F5A3F
Malicious:	false

C:\Users\user\53280493\lekcfklpqn.xls	
Preview:	RD85w15s6l555s4d3p96WT3J6Zn8oA2Mn16xs6ne4VFRbp4762P9S199Iw0fG44X19C2937I..48W9N91147K6238M68u40..9732Wu80322Vl32nB12uNFBd39iQ8m18I 57jP60J36lc6Qt4..9tr2LIrZShL58eUdyVc7K264tLSL1Cn1h2a84QY3v7mh9k967497Sl5h192540d386E404G32GW365kTv58S0G1..2vK62yn22q13qY8..16C4iD6 d4a6ZTyJf5888NC46Nv96T668F3F3z3m8KmERwD8U3AFhhS0oPq6Lk428Nh1762c4MQ9N7WX68..D70oF7g83RR7Ct72l1041PC1K0cS3f92E8l2lJUehsbkuMmlDc47LE D7M30H788uiN7604D0Eyhfn633X335BSfZy..73x9F9330J2T94X60w3wP3DYW878Qe9Z357C1F55YWR78071211z0o2y6vn54845T43P1SW728UYm7S7w9V 7EL6d3B5ZH2y482T652En00i2w13S05I2y3876Q22887V4B73174hTOy8Eh3..

C:\Users\user\53280493\lnxwq.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.4584643021742245
Encrypted:	false
SSDEEP:	12:MxaTKved2/y26wbKahZ1nbm2yw/DyQHsFXCwAxdNPHIShEcl8:MOGH2aP42yw/D5Oud9eca
MD5:	B9E58CDA95273B262AC02376514F3BCD
SHA1:	87E810AF614AAAC71030F3DFE0622E19FDE1FC3F
SHA-256:	0003B65D0A20251E744C1E994AABDBEDDEF0A852F8EA6688B8CABBE36B61DD6A
SHA-512:	F0839C171BBAB66A3B679AE5273CA94F6BDC2B87BCEE89A9A3D0AF04E5BD57E33B30A9C2AC7870BF56074691966E960C62B04D101779D9B9DE36A06134F5C6 4
Malicious:	false
Preview:	1i4g6s44A8TG10pIu11854Bc5W4C45uPPXP6hq11P56383t64XjSo185kz319X30c9B3O4Va7B5gg84tS7mkH8892vh4Ibb0z115GaT368QEWp166u3rVG1Cu7e644032R 08k52u7443KFxm..3P4059Y09i3f085nPbT8e4800e85LHpMQN0N370B2572OZXZlU2J2mN8e9635tx21X4TZbl4T2WcGU8LB3..2KI2a497fyM487..54W3z54147r07P C62D35n09..Qz47O3oa34LwI9979ULv01gyF2Z0LDUh7L11P8wWKq4A2e3Lgvg3hI5bIXT55509y2PQE349c6F2..5sR89z92V518Xw1Oh9l032Qf307ZDa6lS82i5Tg3l xXWefOr8H..88pF0304729S6E7H3Y964DM54BOF90k285i0I3gzoOd87hGK7fozU18w009819dl34Vd4..F7F87a02969X99363k17811n6NT3LWc8a3ES7U285JZM3044 YF2c30pY2M36P61794233q2q340t5C2bzyEG4Km5Jsk079M87Bd3i1v6z3Gh759SUP07L8u93..

C:\Users\user\53280493\lwdpaxi.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	526
Entropy (8bit):	5.508401628260195
Encrypted:	false
SSDEEP:	12:ECw64tc2srNeTcaNYsMT7CqLTviYqVjOiwSrBe7xj95n:ELLt/sr8TcaQ7Cq6Y3io1jb
MD5:	C68200C6D6259819849C3F5A49C81A5D
SHA1:	0B823B06CB13CA6F741CCCD42430A7F9BB243750
SHA-256:	435427570C321348E79510EB18A485D4E5CEB794EC2DBD0B235954CB08712F33
SHA-512:	7C3770173A8A60E1A61DC083E90665D7EC9B683E78903A354945499E2275C78E1EE1014A9F28DF583C01DB7EB29D74C334A27802A39A45A37BCB70D2719CB3C4
Malicious:	false
Preview:	4l4S17bU2342651TA7269071i530fq7hbf6F6Gw5t8944X1k75s53j37tn0h596F359Y74iEL75b0FBNp93k7Uua3v47jYIh..4J1BIC27q7273O4OlEU508kZ347Nk9c1 m72761x593kz4P578Gi6H9806vLRb6f..4Mf70T524jzm6TwR9nY69c1eFP8tS9gh84YZ492uiQ2tB4692375SpascJIWOC16jw6f554cheY0lHEBCNmn8f3448h4beC3s xYM7cXtF6FL5165Jn96LDZQ87t7CM5Q..jn43i02M8P98NiU038R9ndG004386F1187Zrs9i47r529OD84p14002w3V25k78S7n37tWG3iaX67nk3V31l4u88mP59RY82K Vf9d332w3..8kL3iZYqm22BCYJ..J3nXh62ocZkl99T0z38Gf06262DhFmb5bE6DA25w58C2NlSJDjenSe02E5p..999TdZh4aojFb6GOr1y16x9b19b059e6T60XD7La6NNP8..

C:\Users\user\53280493\mclr.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	676
Entropy (8bit):	5.530268978577162
Encrypted:	false
SSDEEP:	12:XRwc6d+bxM6ge4/EfdwiUQaDgjPrxbncdqh51TGw67sYJdVayoktpPn:X2PqxVgP/ESitJbnxasYJdVay5tpP
MD5:	D4C88379AEA75BC1ED9EE361298FAB7C
SHA1:	CA96B87B086232937445F1DA6D8009A2DF526843
SHA-256:	F418E67F0F781D55556ABCA93A9E655C0433EF2CBD151C26C6AFF270DD88153E
SHA-512:	5780D56BAD904AA22B39CE9529C6F1344E81C5F63935799F39A4A81BA05B7C1468DBF50736D39B462804882A69168CBBCF6B95A46A9541C4ED71015D5533BE32
Malicious:	false
Preview:	W75kGK2ux6e4z37xq5w48BU9PiN7i455TB54DuZMt2817Bb7KbH3GrZ39WEp062d8YYX8wl4F23q5I3VG3le4d402wHoW29cnkREs2mtw7IryJR15oVp4fL1giEm1CF460 N0ft21803337gl75g439X..o258vT58s8B3i34623j4e64iFJ27g972117k74535b..9A7eM7f808zP550T3vqj0O6af604wn578QI2TD839..YLn0pfr2Vwf0t9Amf216mR1Og10gk7 57a19e0e98I3FjqE5qD7Iw94824eeDw16Lu4S2jXK1xC8c5f0Mkywt2I6l6d88Q..t6Hj062122qSt28NnTWzS6klg8xs9mFN2531H5z869HCmwX6689K2VS..378u6rO9 w76tSARc72y2080rX958L1196l0W8032l909E6857HbE8l229E4R8R7vB0lk5p2NB099605..FL6V0653Gq..l3zK9G06gT7tR47H7L761I7Q9P9yE762wD2r4U258Vno1 34Toz1kcWW1Q9849p36ux33g9ZM0715h05G4VGJr31kpZ0o8CjjRB031NCwfm1MYkRuXPX0933fBR9F8qi77RTd7u928en6RG8TaJ435WA6C6wDs1pT61Y47 28927f70yv4y27Lv4789S8kj..

C:\Users\user\53280493\mdlphmkbq.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe

C:\Users\user\53280493\mdlphmkbq.exe	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.46650019048111
Encrypted:	false
SSDEEP:	12:Y6bExPCzxCwvjHz7B3yHchn0g4EbwD1gEWaeRHNqXoX0AuAtI:ZSKkw3dC8hn0g4NDoaaNXX0MI
MD5:	1532D6007BFFF31371E95DAE7B5A86D2
SHA1:	23D733FC3E51591D863E95555CFBB1024E3CB2CC
SHA-256:	DA76154F5A433BA239B2AAC0DFC5DEE3CEF924CBF23276E751D28FC8FF779A9F
SHA-512:	FE6A2F5D61FB3A04CED51D09B965F55613AEF7FFDC004365C90CA0C6C2EC6381AF0574AF8DC75F3AD10BE14CAA42910CBCB09C557EABBD731F5709B115AF1D4
Malicious:	false
Preview:	A4Gr9ch47j91car5Kh6L9n3Jd3ok8d..7nX50n80N95FW34B4uIQD39uP4t4M2V8nMPWIsA7..22K1ZuR97805fihHzc9C853Z1Y1Z38840416y44W1wz40Tx20W455k89Y82FC2FS5P43jF71w5Fp63y5888l098Az9q0yW3c908xXb7L4MA0967jMb9A4br04jl6K7Qhz9G8Q0QiH36040l34RY53245Y0G17JFrAn6jd0488CLGcZ1i43W4S3N0q..M2D3T6NQEKHt24R2azx4k8142sOljF3l8G4702w28q8129s13J385Y6bC6Ej6O4A3d7t7j74g2LO0np0vtU1nJ645z9lnv3F13U2bM49L85G01A1b6v183G3N6o51L..Cb99..04n0fzN8tO2mgsN05j313387p471A39Ka94i17MmokjaO1cO59084p2xv9212ES0fQO2ZiMM5971L8r0Q4c4R9Xxin5bhnnk8E7IDn9UL7D99wXoG86Gx717..

C:\Users\user\53280493\megx.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	513
Entropy (8bit):	5.4491890231029
Encrypted:	false
SSDEEP:	12:tZB4EUQB5ctoWwCQkdhuxSsi9aJYhqfny+RUFfi9Ycn:3Bn5cQCTuMnmy+RUFf25n
MD5:	D7B1B7F65123A1C1EE083056EEB76244
SHA1:	E3F9A9DC898687B87FF38D09FEBC40CF1206276C
SHA-256:	742563AF417558CE8E5BCF8EBAEFAE0B5DE79CE2F3C489FB138E9A0AF8D2AEDF
SHA-512:	B25724A91B6E86C6E395C8BFF04E833738E790CAB3608200A52C6C88FD43D1DB855B6AF1349FC3977AB87F79D4DE6EF42C1674A4FA1B60B56A4BF43206398C3
Malicious:	false
Preview:	6629833QX23E5U1K1qkx5ckdVPud3zKC6PE6c9J4QF04ryCA411j9154wK1h2W35D75fVoS307RA17w27dW0Jt9d3U6..12ARpft1321lr768p722T3wHe0pB2Gn4DD9244h970bCD50173BFI6c0AbtBwE3658a2AL7205w1nv77bK6DBu095841R0M09q0698sW768mO7sIb82w9Q..834GGtCJ1let7DhQq35g51Rc35hY2KKkW8AK6o3J55O0K424yd36R6C2JJ19OT749U471547nm01J0AN96mU77wcU1sIJ4W8h1P665n1E1409R6493RsS767653tZCT0gf5112y8vn65c15GZL3O7r2lr297I2Y2T8N9x8thE235CDks1V9..tw1QJD6S2s9T81531z47j2J39065713Z6kz5b9G7TzZ5b1000LaQ655Fp2WT7f21s466KPJLK0086V9FoJk1G5m6xiivQ20h7Pl9lw277UoGMZ06abfRL..

C:\Users\user\53280493\mfqo.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	580
Entropy (8bit):	5.499952066599516
Encrypted:	false
SSDEEP:	12:yP4E+vKexzCxTQzVhs630aJT0lzr8zqzMuXio3S0fpc7W7O7dymtm5T:s4yxTQzV6c0aJT0/7Xioi0hc7WMtm5T
MD5:	1A428CC86613B0F5565620EB63783862
SHA1:	3801473CC683286F407D2FF6B708665F096EA778
SHA-256:	0EC4B97B84DA77B741918E925924EF5AED155EB485F5B5234FD682D032E3A897
SHA-512:	751F26FC9E33D761FBF8BB9C26F5BEBE5C590E1A76625DAED85B14934BDAFAE9987DFE9B42DE7A587182F1CC701060672CE3723A82513F7857FBCA0CAB43FFB
Malicious:	false
Preview:	dhs53262t78ShU6y35595J5t34OtKNl1kl694Trr4gV1D7myH2246eJrs48g8TsaBasuB15O2lQm7K38vXqoyo2888..4UCS0F072m64843s62X8394pSWt3b7bOyQpzHTD1C2hu3a6C3e5ksgz028fMA9g0214N3gKoF302..uRBk239744uH45WNk04O37x982IR010Res594..L92UM6m3jokX2XO31Tu4638g92N2NJw0E286663953MxyY7S32mtxR91ov8PArOL139nL76otb0Ts44AZx06p15BPAi2..sj9Hz7lmOD7z02AbEyWXJeKOk4Zr90k1o61t2pyZq523P13cZ61kxx2lN2XErEEArxXXkQ35k0598lvN9n9oMT72Pj6AU5b1aN3RUEzJay60xU67H9755nL582l3Z22t6553..7978542de224WY6bUOLM5K7O0H03350y898USx6973PFR9g2142TD3Z6X7E1P5x4L3qs70b152vV8d25VZv5gr8117GRmx838002jS3qJ46Zr392455NX6R6386y89nRC432jp4Gm0Z38..

C:\Users\user\53280493\mfupqiv.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	547
Entropy (8bit):	5.563157742411892
Encrypted:	false
SSDEEP:	12:Wj3TUmRVTEcBCDbwVBWBcNUMj0RYvAOHl20vGUSav7mRy:WLmEG6ZIRYYozvhSavSRy
MD5:	BD63A4A4C0746EE32B5FE37D743F9694
SHA1:	17E4AAC658C895F21E3D43379B06F4169EF53F42
SHA-256:	9A506BCC0245FBAEA31655D332A3070C5F1626C107EAC6CD031E31FB06F60026

C:\Users\user\53280493\mfupqiv.dll	
SHA-512:	F9243AAEB5A8FBBF75AC7E63890E508B1CBECB9E745F304233B13DA6F51F241632302E0FACE626C57F529ED7A6D2AB99623F8BE1056D973DE269B0BFF0734E17
Malicious:	false
Preview:	P62Vxn1E216rCL8z5w3IBIM55vT2h042v8g93rM3820orA115I40uG0066H97SZo1z4dsOVE9IC49e36wY5p310..7RsY3V5lN662qv99jsdr892pULFz5Wsix1kH80zn1 Z3eV1Fulk81238T0Jj9L91Ip38p0EF621zclZ380f51kVt26Z54c67678KE..OW8E432bX3X7Iat3U408..5sPGqrvO5U49F963f..X1Y3MH80cQ16K12s3Qup0ygBj5py o5uFh8NN5772388997VAhU19dUo7yIJTqsA6jT805WDWm04bd9W1K44A941z3..0v29a025l8ZS47CY1B71yKj145Zv8kszpE9095t7987P477Pd5wYL023zpU90..jGwv 85rGGxl9M5f3db2gjeS0j379if8d..J79Q30S7f7187J7g8e280H47bZ09e3R75y5395dbna379D06vDilnn0P4410a6A738h1o167C7d2aEd379Uf1c6eY2vcc2dk5196 KbLNu47A4qM3Jwx0DMb1aj8Bt..

C:\Users\user\53280493\mibhghdc.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	608
Entropy (8bit):	5.516235749905406
Encrypted:	false
SSDEEP:	12:MArUc4TZVKbSXnToAFAURiOAhs4EVTzayEJEc4K0wYENBUon:M3dTm2XnMAFLiON4EV6J14JwFNT
MD5:	72AF226CB969CEBE5220748E02B471AF
SHA1:	91E78B461AEF172E677FA33D1A1E407DB9464CC3
SHA-256:	6AA00870083F233D29784626331399A23E4535632C34960CE14C0D8EF60A344F
SHA-512:	092F38D14049ECBA9A215C594C653DFD1A9C78E93F84D11E806BA7F46342E32E5604656A7C90BAD566C7F73C989DD802AD2A91B525DC23D446B1CB9ED64FF2E
Malicious:	false
Preview:	y65QF49QHygK..1E6E95oK3N1f13kvb9XyrD13qP2S3Vm51y52H079E149sl0UYH9N3DRNxzW664Hw8446qF8nkJ7lcZqtU6782I2V7022WniR0639Dl58YK61Op84Yw51 oklp176237M77208r897P520CNU7..1P77278Z7Z0F1I372b8WD361Z753f79iY8Gue8Sk19O36n7twaXFG86L0mM4510u06F1Z54wQ56lq669A60601U1z694l6reT11E 4t9O3v0U..v9969ZA64i0w2Fn21u50hNct36Y5c9b080vCQo68KieFh72V8Ct04P4e2HHG345p9930SaZS0f52vT25h4e521S1i72Bqh7sAU0221..pz9PnY67h2k31326 kn24pQ858519h4faKrCb6IMnkLQ90yT0705D4j12i092f81PfMcI2o2oYj9t4A..2786ecx062z8Law..3P38jtaElyqRjdJ9tyq3NKyIIuvBYkY69Tc895tv1PLu16i741L9MNwMPKt vA5OpN2a3Qxwf1T08e430n7h080875463643HOmHJI4g8F9d43398w7V0uLS5432910Vm1zFf08C..

C:\Users\user\53280493\mjvutjqat.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.44271366245259
Encrypted:	false
SSDEEP:	12:puVQ9FcV4qIqbVuBonAXGDcNskF6+QaW8PnXLzdCZM0wgU:puTV4usBkAXGg+GiT8/XL+xTU
MD5:	5BEBE5E5B79555C59F2F99C794F95B05
SHA1:	13B530A6DFCA9E18D1EF3C32B1B9EB76E9163D9B
SHA-256:	C3228C005895DC94D6B759BFD0FBDBFD46BD661B96D1E239E137AB3B3F20B527
SHA-512:	521AA907A19C762DBB6C143C4EB03219D2402A8FC492D8C47203AE16E5EF30BFA635CE3CC4D5E86AD7EEC7775A78854C1CFD57275F5F847EF6031E649A0E261
Malicious:	false
Preview:	5Iq0430EQU6S30..0DFSwqB32eH8N48f7s48w8lV75a25sb6bN4c44116QN0H1I25EW8Ih55fNPQCFf038326i91552G65A6B8v3X8rb7o2884qawe2kT16192B8K5a..o 23mu90dr29g7348d4gl3yK85i13oT1z39GoHep42BKGe3ls3lPN85181PSwQS705J8UrIt4W8C63U05Dbx7x672703s8x6PuNo76y..V5ke8028ePo488tUvrpE3SX0IYK d5f8J7uk4h51l07U2H5K1QL1eb3W1AVz8867QdmOy2GI568tr57i10f6I6n413tW8U8L4Wc4IFQ0384p2m6IV35L38Y6154..Qw1N2SlB55Lv8P52jj827..sWAZIAOoGx 08EE19i43p70r8038usN544H75LMrluZd34199078286eb13FE0NLMy6Af1646W6o657cH121K896ICAe0wt36253B6043sAXx78wZu0Mu1556DmoX1t698ca08Ix48gh0 C862y25W5R3f5c192Yk3U5643T979452kA4c8b7seURuf698a..

C:\Users\user\53280493\oavaapsk.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.482053799631562
Encrypted:	false
SSDEEP:	12:SgU/5M1K1iEG+SKE4CDvZ0wr6px2ONDUkUx+qMoEXSnr3m9dOiNN+TBZ:SgUm1WG+Sl4CDLGxukLXAr3Od1NgX
MD5:	839C4548A6762760588638111586A7F3
SHA1:	5F87746B8054CFD87BC147AC5C0F261A36D85026
SHA-256:	64800D1F700AA3850648417AB93012941E2DBF78549A94EF3D74D56A15762953
SHA-512:	56BCD4DA254B18EF49E0B583DFEA163FE4B2766E663B028C3C784B826140C014DCFC86A424FA4277D690D885515067F408C404BD2E8B1787999DF5F30E7A0DD
Malicious:	false
Preview:	pmtYn298y5h2Qy98sd24Vcd697Aa1921ZHI9Lict9Ry8Zw86pb5yhu15I976KUeUvxp65VEzjd3k7hWYh93837..k346yD4bs7ivluC15810oU4t9r221ZN217UY9Zg7uu z9t75238138Re8Z3823QRa3qH53mhy8Nk6FjiEsTvev602..A2u6wRyQ4H48C88o9ZKq6l64202qr531a6hk8K587k3X6W33J6232E663QIrf78D46r2605hc1bE79kZOt g87201u7jm58Zin44t9anR7k72y9RPsP8Tar7n538c5iy08uy616gd8945ac9fDoB8y5V4567j8E7y1pG9..Y75LTne2363YO7Hx5k6Z16NX747Z49xk4528uUg9t7EK13 e9t236k99J01n5Z89E74E165F9ex513bzr06w2MX62vkSQ0M9891q1Ru06Hhl09l471s1K6906..5ID5M0..32l3t9wXK4a84M12D442k06i0WUO8983OxxW7q5Q2a4Es6 3N960B15uK53255cI09ld4Y64S1Ql4z21MXf3W9N3685OwyCIN7hzjmYH5xi3tB59S58K84gzjF4d6J92IHin7207BD1GVQ8776..

C:\Users\user\53280493\obrdvagh.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.488510060065238
Encrypted:	false
SSDEEP:	12:uI4kblj5JORvfDGzADfTeh8g+RFe0rsQdCxylRID:quIjofDGzADr0uFJ5ggwD
MD5:	7A3F1164A63866111E3524961999C141
SHA1:	BEF6AE74FF830B73CE5274DCB981B30D5FE59E6C
SHA-256:	369AA9D94D69E0289D3061474758092778438896D5FAEF37F3C03CC7FC422863
SHA-512:	01501DFFBCD003D2447CF46A68EAD82F4531C1217E7DA422887A5EB6857B9F2355199DC913F1A31FC7C594B7BD74B66A74A9EB5052195D53B7C9BCC287E3295
Malicious:	false
Preview:	dC311u3uemY69H37O333Z4Bd94sz730U22163J5GbgJ7d2n73Xi2rH50g10r26VEawSA0O8Q7rgE25ruDTEODbC9H5453B97Q9RJi5wi28h85zv6wJ8SA3..4NB4ch57rh q6tc0V6p14kJm3XX4UBq84mz9162834cK551Ui2RE916oUh5JvQrk328S01m1y5n7j23dW7iM1m..Bbt2Xt7G8idQ9H279VM4aNt372vE4v8..ixEYq3U34k635m14B3e. .bR44IDlRT0u48m0L6ug4O8A1av9M388O43xp305F46467eE0SZGu6l1WIs2GD6U1CLm21Rc1D8k178v1B540H..7573i7poiM462l931D0190p3fOt832fv786C4ull75 aCc30VT1cY4k3554uUnV2008qM67gS82rS7708d0R0WUY6Y0jll8692N0p7g681NP96472t2837FFej8qtwY39Py03Lbd423D3viMJ92D43TS78131l519J32659b9c0i0 J9o393K93K6..

C:\Users\user\53280493\ogtukuwqh.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	594
Entropy (8bit):	5.521313456654463
Encrypted:	false
SSDEEP:	12:gTcbR9cJj+6/wktBVORsQbc8+aST2jp35MNT8HyNACJN9UgBhEH:KqR2Jvac8Xj55soH4lNYH
MD5:	76B07301B2BFDA118E26669513376568
SHA1:	F44AF1077D803E801827BE26511BE15A723D5019
SHA-256:	D8B8430A7665ADE743DD755D2F77D6A66465AF3DD42EC972A2E6DEC9C6F84BC0
SHA-512:	1D9525188BD1D1A5E108B40C7FDC72263C68B7A2A956FB3DCE0532AB0879715031FEE0624054E7908311B329A81E08E4B074AA39B6C08779C5AC4FE2E7F7DFD
Malicious:	false
Preview:	7440TQr6r1GB9Fx1K822bV75Vbi2Sv8BL785p674z7F462OBMs4x22vtnG63x9kvg898..7Bn539793l56V8TC8XJH9i1k6xix4h96C1b5y292B9KbNmSHMmG56H00Fe2W H831681s4SD177BZd6NB60a384cn1m577dm91c33O5G715222y8Sl3..300014di49n16y797ls7286G155S483H7z4A5X4OsC6OiFL6Mu75q538En0of90jdgQrbmY4y5 9d7u61tbZ0GD679g51u9xF5z64lXu0hqH33GTf7w833XM29o2FS..AZ79qjh1V9l5627xzW1T469ik28287A705HVtiwpHaR35z25Ut21RbV8a6K33672Mm7966tUQcJW5 3g06..a904e6xS43uS9L0l80k44IIOYUyP5eZ3kJd12p5F0P01CpD4j4Q92YNa9Poyl6a5neQeX0649r28139w2562K7M60D87..c1tEr650CCQoVKG718jLUo56402yQ6 V701699E3t3c622j5P453E181cNuG4BM4095z37XCVIT8v7W5ISS00fjwH8b2Bn9knxrYhQk..

C:\Users\user\53280493\oiebljes.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	570
Entropy (8bit):	5.433706935652008
Encrypted:	false
SSDEEP:	12:MfQSGqK8pJod6V0trJjAITslcdA+YPJ2LFp2Vyfo0XhW0:MIfqPpPiXAIGsA+YMLF04foC
MD5:	2F1AD0E369FD291C9C76790527C86284
SHA1:	9B68CCE9CA0C8FDD89E0CFC2D2D006C0E109954F
SHA-256:	CF56308B7DA42F2A05C8C9E0CC76F11BBF9A3FF4F9BB086B163A1E1501E1FAB0
SHA-512:	AFA00CD9385B043993FE13CDB495326572A15864947DF9A1EB9CE58DE4FD35BE945996501AD173B58CD1970E8B84B09BE30AFCFB671CE0C5C61DFEB35C8D9F 9
Malicious:	false
Preview:	M6ON25nrAe3l2n80wYEteOXG1X36w3733839451395Lm83B7J6Y9v3C00l6u6304QXAh34C34hbBXONb58jk506779hpwOg01350j6KV63909Q1gPw70l0Ch5kBpfp2Z38 bO9Tjct164830747Y93ql..t7U2i36281xQaRQ..tFbJ12105..Q86qI6f87p7Ax53K299o1Y5ttJ3OaG02198d656ofJ64F0..tm49544j2X0i4anGBEZ6Kama6q23Z8un9472lmHO0 p6V264ZK87h64751C832795wl278P002I7a1S..90Wh8450MBVI1hF649719l257Wud0n49g4Wo44F86PQw50Vp88lkW7335V37qsVT63u244j90h69HW2Q4440jqs6CZ0 44xfTomz81A5zj59j1354oQL0nx092Vg9O42w486YF9hu..3F467685Iy6xKAv0Z27v..8pM3J61etinBE1VJ4xuVXgP9Z69c6uf5wXD271V8p2lV07a32y98KU7snk59J 34299mKe75l33b876VXSWA1mpFmfWT07E83T4X..

C:\Users\user\53280493\ojmc.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	587
Entropy (8bit):	5.460977625432686
Encrypted:	false
SSDEEP:	12:RQkAbo1ymHoyqgPMRTEHMH0UBfiUWQbrJQV10c0HKya7/TIMzkVAm5uieOy:S30Wyqg0RwHU7B/bI14pa7K/uT
MD5:	983663F43BF18EE575F8EB63E9019446

C:\Users\user\53280493\ojmc.ppt	
SHA1:	3D95BE18141C9E7EB7DFA72E93DF61C3440246CF
SHA-256:	248F6485FF9B52AFDF7088BF9CB03864072C7C06E68F9F44B354783B55267BAC
SHA-512:	036087736EEDF763AE1F944C73E450EF78E3CD080E1CCCFDB1D2FFB82B021E36B00CF6BC89ACBCA94E6F710251A8D0E011F5B6B230CA9B3188919F5B1508E0 7
Malicious:	false
Preview:	J557eq98scLeX082605TD252y66T3acIz053A7JPYsQ25Wdu8agPgU1CRYXOY71s6VtBC643iI73Td..7092Xa3e8HbzlS9Kpo2X229H5571uT7d958Mo80G5F45UE8Wco 8gM27JA66jzxZkcA8iX1797437KCfS73..841X2Zugcu9t042c6XVN48I66q4tBs7c2N606o12y1u379gLG6pe00240Edjk8Od51GizHA5485X4MzHp1757r25s29L5UYo q966R8bos9qU9oo399aF8877..f355zPqsPF13FyA5p9788roN15yXE4vQ17900o3I1e493R1540h580E58zP5pa50338JH1Rx6u4387O4R105LKjMb3s199n9v6E130b8 5Lww491413s213qFILI854067v21W7NWVl0wO6D5gIzZ2677z11V5F..4rY10803XYp0364Z6lg6t95Bg8Hwn85OS5755LFQt1oDh090fzbqj7z76PU519T478660QrDI6 Zl018v52lyt8g02T427I938CWlML74e27Lvn8l5Ym88051K5nlYyD5q9X9477540Q..

C:\Users\user\53280493\omlppm.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	538
Entropy (8bit):	5.369449597133576
Encrypted:	false
SSDEEP:	12:nZDQ+USguS/YkUTAmtdT3tcZ6E7a/38E3THNGeHyslD/Scwy:n9uSgd/YkUTAUdT3tcZ6Ee/fjt1HycDX
MD5:	38D7DA18EECEFD097985E2ECDB6C1BA6
SHA1:	EE674E02719064D08447C9FD1C3CB77B696A218D
SHA-256:	0838958D5FEE44179D6279C26B9FCF5C2085D3F128ECC875478EA42951539765
SHA-512:	5A0E49F7FF3B835857FD20E290EC15C68FD27FF4E6DE2073E5154CCD01658C3772991FDFEA3AB2FAECD06E9577477BDD1213D71B5DE7491613FD8C9B95E972 C
Malicious:	false
Preview:	27l831k9MHZOq030a8E481Wh4Zk136C740Y35C31Z45tB20K3T712KP3i3P4Sq6D564413gU4060cL49sg65D415F4O9231ku42017M247XUi9L3A2OXW..A6d27573c81 ..d34126OB6099Gs2397i637lNf5EQ74lVn64I2NT61uY1XahVu3j289tBI7263cD70x8818ImgQY87..3A29P1425XC0Av05Zq28TT1Jp96En7396375..35EG6N7c7bx WO584ehn677w881H2jyp1t4911V50l0yrur6z819434HH3Z1TD7C3q7cRc8f0S58d..9B1pKV362..DgP26304vus6AeP241V1904N3c5lcu123o76TJcFopkUV354057E dlGJH94P820V7OMoME131374y4o370K2721x364l6J3Pc1V404KPI035Ej7Qm..1As9w073V9NJN383YQ8a4u4sPQi4S14300T788L54N74vgJCn30X685lF8vu2r190RS P15m02hD5yqK724c..

C:\Users\user\53280493\otggkjoob.bnv	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	225944084
Entropy (8bit):	7.080014992811793
Encrypted:	false
SSDEEP:	196608:wzHvuoKrb6DrpKawWiHwsZF+qdxgLUjahTXPmAmjHjAH4u1tY16hkVWZtoUXOKpz:8
MD5:	55E9E6BAF1C8FA40595A3750A7B3B4AC
SHA1:	3A544B30A4B942A29486973E35DB94B139A8F08B
SHA-256:	EC5FCE76A76D9D58902329AC26C4432A0665D1B8A9FD978B5901239A3D613672
SHA-512:	65978165317C7599A4F1FB3778D4675230AA4D6DE7D0F55DFEA3605208BD8ABB52F7F4DE39551C0C5127CE72304690D534523572078772A8EA4EA8C581BE8EDE
Malicious:	false
Preview:	..;...0..q...dY.l.g.\.#e.>,..EJ+w...._T..i.a....NI..~..7....]&..r.M...c2.us.+t.Q....".s.>...=U.^.a.q?...u....4....r.[:.;..8.9>D....P...e...u.C..&4..x.n...4zh.:.....O.Pn....#.c.s...XTfAD... ..h.y.M.....lB..m.....Oi}...d....Wr.....~3...m..E.Uw}.K..).....1.....Q..B...c.....g....P.H..S.T.XrS..M5/.OQ...=.r..i..-.....+..GY.$.}...Z..1.E..E....2:..x.v.].xm.....xK.Ns.i....Y..#....f...; .J;|...qs...V....v../.gI.!ziW.=^*A....7..'..;...".*.....:.F.B...<.....J..d"s...1..?.=S....Uou..f..-.....,_.[v.IR.S.....e&3U9.....p.`.....).../&..NZi>=;B.g...,G..wc...-.....a+%.zgD.{...i.x..X;..&. Vr.Q9..(.U..?Nu3...`.k}<.....0.....a/na0.....8..~`..]q...&.c..4d....'...X.U.4.#...SR{.N.<83D.;..P..%&w/.L.:.).....8.1.8.3.C.7.H.8.0.5.....{.4.}d8.g.....%..D..h.'..."qk....3.}v_..%.. 9.Q.tO.J...._.....r.gI.8..n.....w$..V,p`.m....c.....\.J.'.{D.OV.ZZ..3....w.w.G..".E8.....K{....g....[.../.p.^.S. ..j...X.&.r..Z:.....vT.....

C:\Users\user\53280493\pdxc.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	511
Entropy (8bit):	5.461388938504073
Encrypted:	false
SSDEEP:	
MD5:	D5C7D095E84209B1BDCD8861ACF52292
SHA1:	884123F47D1D3C8815E618D14D7CA012DC3C2C1E
SHA-256:	65A3EC4BE4DB3FEE0739AF5B53D1FACD042C3467BECF7B61EEDD2FDE636E10D0
SHA-512:	4C5DBB3ADB2A646BF3EB207B0A1D5138550C659EA8467C5E24D744EF7316D2D3A9FA5217904AEEA681561F339367422BA358D6506EB7DBDB19CBB27ED864CB A
Malicious:	false

C:\Users\user\53280493\pdxc.msc	
Preview:	99Y9eELoZF34A3M18FDlSWhh0xSJ0JP25d3285Hp2708U986ey8j6N..p3e7U3blwt8l18mx19r81376650jlw69lV65gha3Yy9606q08dxbK295P99z8UeN3nm5m13WO. .3V17K8Q957L32u02CkBv53AA8z80qHH433T01A47l7baYKMpT4V88y9Wi3ViO6I4IT6Na8h9w7KK460Av1tBNQ81Zh2..35fcH291k30yTy075R5aa890QaO798G77712 eUZ4hwl8Z869Y7u83m45..Oc721I4aM6LZ925j8f43Cy131mt8mjf14O7n7945wQr0drm732R0p7Y7tZ3657v8S5b11474qV3ka04..814060N17Xw02i2Cv..NpE140Y7 n2VZe374673xLo6W4KFAe8a2904eLle0450685EVs0F31387Pwv6dN2670k6Tfvf1Z80F9..15U9lauHN0X6c44JHQm67o0t94952eeK0ZwgEzP62z47T9a..

C:\Users\user\53280493\pgjbsik.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.545598248460607
Encrypted:	false
SSDEEP:	
MD5:	30EA58AF0A625A583582E2C1CA986BF8
SHA1:	236290C2B6D9937825A500F0BB5C1468DDE0B287
SHA-256:	6ED7BA21338F0CDA3F1551A0B680295F64B967753C603DE54D35EC7EA00A432F
SHA-512:	669CCD18AA08EF155F1741656EF8135D67CB8F7BC28B5F562A259CD435853B820952CB0E4B4CECE079AE37048438EAA9A87A0FDC0A5455A6111F385420B28E1
Malicious:	false
Preview:	83i1A61BDLKt88oV0Vul7Umqf6R2sVJ14l7e90l4P38Y25Y5JO5SMSqRFm..1197C8tT6e24Ljb3i130UQd57140S1258x9N6ZQyLc4cS07pL80..467dhx1ENoL7tn92V qa919b2v19e4g42P2EHd0Y578J0260536l5re3F5l6Tp99391C0O9F4Fm9O40l0x2M5F6748mP4437Gab04e43s5789252LsRGjX99x4z93Xg91Keheg8DYs615Bge4ErK w2H6i9sB50o8uv9nexZNPabB768E239O..pP5Y94Y2V33o916db9zA0lfr045Y6OZF0f2cI01l30VxE0e..K3D1aOJoT7R5oa7EdDyWk2z450iA57jC80Rv596FsD3F01J 4PZ3j51s7sELY7T3e07K4niU5qaM8E0676G2zlb050rl8o569k2MNU263UH64B8KOlFg6XIt2h4660h52Ik0o4314H8i8w184y9dyZ58bw3D547gA3FYGHcb7R77g4..

C:\Users\user\53280493\phng.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.476053326109192
Encrypted:	false
SSDEEP:	
MD5:	DA9A74323C3AB27BB4ABA33E0F7123F6
SHA1:	299042235B3D1B108F8DD22D6432654C0EB05146
SHA-256:	563192AE0E59C4CD95F3BFDCC857FCB23773D46AC933D3919C73153B5CB51BBD
SHA-512:	A63E1715A20D5BF73FCE92A31C859FCA8D7743E1A6FA7A733D577460A2B8D5B8FBA81EF08DA6C97884454B3643D95E25449C27A8A34469397A50BD4262A3C955
Malicious:	false
Preview:	m4N2l8d1Z6T76404oZu7DVNv769OY2rE29i385cbp0psG79l5fqju9..6MGc337w9Z5HO440zjS18..FJS5s7g6Xua17SAoM4I239A4y054iZ7t4s9a3ML320v125XzJ88 iTi4LFc361448Hq4XG7Z7ykea14734Z87IT51sN9458a6552SQ..nX7b7w1wF5N5t937i8k6ohd26V5F77..135M4d829Z2WAXZMq6K5CM91x31M14w5331S34O5d..20F h4j385cTu40H0jL2aiAW78SY917030q8lx23f17446Lmw1132K0aa..B2JFgz28W6s5b4yo12Bw3r495tqJpNaXupH0WTP6dEf2LfS098x36gJA9C83A7330l1728n30ht g7V87fd2t677Coy83gHE882363co99ciUp14D1d53K0aq91kD25555yF6CNFV963ScfhFh66u4dB..97M1ky21SQ2czC8R3d3oPGl95u9t39cUi163E511V257b2q7..

C:\Users\user\53280493\ppvagipo.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	638
Entropy (8bit):	5.525924213145048
Encrypted:	false
SSDEEP:	
MD5:	0A0C0302E61B847424F667669B66E805
SHA1:	0FCDA410642D633F0067785D61A3103000D06409
SHA-256:	BC251C12B995539E9CB9C475585904ABB54F8550393C77522C4AF8E102F044AA
SHA-512:	8206CCD27C6D987504916675AE8CD7747D371DA82016B1B1E655379E304ACFA79F8D6B0A855FBDA6292E0A9EC518BE982E0A1D0D87E54942E7382E754D46F03
Malicious:	false
Preview:	5Pz62v8qWdLxZ29f3JJck268h..N7uy8BwPl7g0h5336Ry11N5c2hv98I8he6W8H9FZhb25bz687X7Q..RD033xv593R2f3GOOF9GI3qrehkIT5ZtT0LmA33R1y837Wauj A57o4Uj7zE2Eac1684t02V15TH9O533OZ6..N7xlhOWAwQ597704xR54..14Riy8Fj505X55712N93IvF78R3BE21859yBK60G5R6bO2pNELW7k3fNX38977aGkO12Vn0O r6z2l8akz4F3CMD5es2F6mwB95E7jIQ52MQ880B0j0..c2338f66U8523e51yCkOOP0YBq5iP6jUUEpx52W6739yOwDiVuSYo831g86B7239QR0Y5o88n8k8F13c581380 8453T7..S38I1BPVdrU694y494H0d076Wn91K913l181w2t1uG28924MXMJ34..b72J58N8dWc189T1e8u5wqL902YqG247M4962H4m8gn243g5jl2IbiLZ308k768z3oY k5N141R7gOK4AWqvh1r1l780HLE10PCaV7533Lp4im7yg0Pq2D77E327gWE93844fG634838g2MA216kL6K9578LoBS5p5nm6Kv147bdH110Ekf9X1z7..

C:\Users\user\53280493\prwsqqdfl.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	534

C:\Users\user\53280493\prwsqqdfl.dll	
Entropy (8bit):	5.589817193140979
Encrypted:	false
SSDEEP:	
MD5:	0D9D78973059BA306870193A9DF1AA57
SHA1:	FCAA46E89899D59285442FECC77883F506080E86
SHA-256:	16FCF86BC97B14AD65B15C96A18F52664E1814E7C3EC85B4F6565EF038062FFF
SHA-512:	88B41A2E8C4396E99A1C92FCAA997A736DDB93BB0F17D5F881AE8F35D07ABEC98215F470E2A32E3EA01A8B959DF24B706786EF90E19341981393B6BA68C6A4B7
Malicious:	false
Preview:	08G0WuL86h2ZQzr5Q6gzsp6783672m2fuNx77t436C2s978bp0F9460s554EZmY2Go7mC6A0eq37lRi5x1zGiG692olQ98J81e3FtUS150CN9FCtwR781W7Y90x2O199x06i02iP1wY99t41EDh646i4HhrMZ30q1hK1x54Q02Wd6kNmn36Mk74545237cX..14Ws2q9PXAOq..b17c65..95da475VFmvWr376vFP4Z3F2vqvm899716317503..n3x73igB6F3s5O02o35Zr56Y5JBW3l97Z7mn8I1zT9636HLr35j0VhMVK5f546COB1L23Nh89yya1PBm28r5gG18b9VN0b66kb..0jT2NQYS571g4JE0w3exfvNBu5WF9J9vq6Sn43wsSABx6Z8Hmk1f1d3P7luEX91J1W3B7aH1dSB6..HuiA667V1bfY56Z5678M28EC00oh80x33PD4M90Vd..X2nlpr4cTK9b3q6h49joLT63wpYv95v2q1aK9trNe7MixXWwI99s62..

C:\Users\user\53280493\pudrgncexm.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	556
Entropy (8bit):	5.468541741555916
Encrypted:	false
SSDEEP:	
MD5:	164D689D65F0F08D794CE45FB8DADE22
SHA1:	1C1A98ED4639AF1368F24D221A0C5CD09794C977
SHA-256:	3478D25E6070A41A4E70BB9383D7271E39B4D406887D56A3FF8066D2A3ED6B7A
SHA-512:	6D373528FA4AF04F7807C10ADBBBB2B0E0A6BB1031EC35F719100F2BD6665E35AF1BDEA3D4A5308AFE66BE7F92DB307380033E184B7398FEACF8CBE1228BDCF1
Malicious:	false
Preview:	R1s8044w9Okq6MCqU2NMbDx47Y19c5H573b50wG4Lc4826o56M6o6MdC15NT5ZUI2R16xr2D1w3lBEOs4Vto2HCKyP190XU6h7949cdW0059B02B8200..WT6m83s554sqOd45A80698C65q275pieK45a14c4pKoy3j8P9562J5Q0721dC1SsS27Y9k49B0f095B88q97P2..jZR0w54g050J8J582J8FM0AHQydeS98PR8N97Y5X80mgE7VM055G5QH1nPf1jTHe0775N4x7RNz0YRT1PCp13204sS41vr2Eo4620UFq13uR3F4Xaz3hU8lK4Tc2zbd2ah7YA7056..StpV0Q4xx19728a9S0Jr14WoP55HX51y9T5bBKI4BY42Pj5537j53VCs0485sLn1mv7jq49n85XyaOxl9a996m5v444o8SEq..8dX853t90LR68AdA1u4Vbp60v20H0O5c0i9AYa6Qb393UV0cByt834M10641c2lN5738lzs1nACEt23lq5254928858g2tdX0j2043y95a9y044..

C:\Users\user\53280493\qbfgf.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	555
Entropy (8bit):	5.4633742846429145
Encrypted:	false
SSDEEP:	
MD5:	0F7BD07950B27F6F2EBC0FEA1619C4B9
SHA1:	3A3581F4805EBA80D48638051724EF565960C137
SHA-256:	1C319011D22BF8DC2B1D7990CE02B538AB0444269E5CF73F0AE9A73607D2E8FF
SHA-512:	87D71154B92AAB1BD99AA104A8D3DB6F2AB552B3054379A9632C86D054202D218C297DD4D85E9ADE2815BF20B297361A3A49BFEDF4346D3119A4517731413AD
Malicious:	false
Preview:	I198H1xe1aYFbRqDh1o7000dmGkkcV..13c4..u4RQF8Jx9strQ434jgy77t5wivd24CJ07Z1SD8kf45713814hcK1ql5ok8YU53e8BLmWAmX57339TzTn..9391v778t486689c2r07ry3124h04hQUaX0Eh7..fUqi1YIULXWA8sAJ473H3Ym6G2n22331829vCvo00B0Y5Gk471z10mMRK4i4o0c516760895K227f70SLM3..61qCB63u1eO75rkoK666b36Ri67TYDb5LptZ206X8350M..e3180X67WHm1n3B12JkvS5948JV43M93Wc425746JO67k00G71224j2q38YIN4X655R9S0l12z7G1D9dQF941pE5667nqv6L69QZJ21yP08D6z80apqON0t66037Y1Ja9a4956..s2685932304jRE7980E06600072KDiJO7119w9vxwiw8VtC094nw50QN97C76492sF77x1C8116y3bd2w06340f8i4gSO20BWz57X3jFa9wN614LP38NVoifQd212..

C:\Users\user\53280493\qckuffmko.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	532
Entropy (8bit):	5.52118510470627
Encrypted:	false
SSDEEP:	
MD5:	B5267C674B91A53F75CDC3FC75B5CD06
SHA1:	07FE473FBC8C6EBBAB0B573C2798B5AC10DAE391
SHA-256:	438BA7805C90646C47C904B88BAC417EAE08373DF07833A7D6572DB0C3B55D81
SHA-512:	1809E82A51B5133267C5541331F3BE510BA65FF40BDC9F74B19B7FD8DA77FD4C36EBB599F14B081FB419B7404C76E93823946EC0C4F6F8796D6EB7563FFC489E

C:\Users\user\53280493\qckuffmko.ini	
Malicious:	false
Preview:	53adLpYssI41h8BkQEA5Xbf4XF30ub697E58TL6p94U1D9150HXFo32Yc06w8467K919XcT54Imj3B8i5A0794399c5649d737g4RlmyFfeB881k599z641j6wO1pw351y62tU7Es8sx2hi460I6x8X9iHsNh34z42581oRH..i6A7Q8R9D653u2wsn49ww9oT1d7I4274711bQ2z6ZTShoDYKH27gX4g390803QiFhkr8pq6QnpNU64S5Vwbt4rE6X1Ug17A92e952T0651IZNHD2hFi8mR439Z5vl32L908fDd98R1Yt6D88OviS36N5w7K6ADPD5M..1WZm192Yd369r06atUc9c159uN0n4MO42H8j1R9ZZw31o01S7I..S63q2kY9u0ogA1q8B630Sd3KMf2c826x26S1FTQVM3Vt4v8p1793QC3s0gfttM262ExO754t5m284G7Of886AUcv1060uRa97S0677U0..O02r41b7y4l91B9PHo1Eu8XWe9G7YTY3qQ9o70..

C:\Users\user\53280493\rsel.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.595852162517942
Encrypted:	false
SSDEEP:	
MD5:	3C3F2D6CC41237D1D53B8A5E56B14812
SHA1:	CDCBB2B5266544754D7F20665814E79B074C47EA
SHA-256:	1ED0F1C1CB52D1697777D71217CBE57A861C624D75A880FD39579A1E12F9CA52
SHA-512:	7DECFB1CC6776CECFF4E55C9A0EC6F6653D4056044BAA94770C133927F5E83B56003468B44EFFCB142DB669B99C2D1527352D4BA411E9FEE0FD5F1563DD8CBE
Malicious:	false
Preview:	6Bdu887UWL25QOXiACs1Wn2871K5QW6wqM0y8A78m01O5721ZF6i51h4OB3Aom2623R2oL905b34cTC7w1b9G5S1y3tm..UVM1zmx4h74t8C79B8B6s6075f44oN57Fq70261Th6h707E453mARO0lv3..6e3Fj86X91N0084Ks72N9WvN3yv03B..QoGj381X693d..jf9Rat18tu72Y476723UNsMkR89Uv3qDT9XV6MG3a7701N1xq452kG0P..74Ac6c2eeSB811xpeT9JF3NCEh0k0dDb5xJ4FdJe0HI53OF..aZuO571i1FEs58450RhuxfT1h26f9zr340N0mfoHA0F..qr9Xb7dFf2bmBgPFYii9QaZ7333H6Y50L9tQ2UV1r4Ds2sXk98WfMt5JDY71e..H0184b53GihZ456TP98cgNcoG7B7M..vM1F415242N6C3nti6B9Xw338gD2d3S3Yx42Q9xZW9z1lc1D4640zet5cuY6MWZC3Q464s67b1q4N8H7v3w4gAu2y8GvV3W59N94wkPY5224Z277..

C:\Users\user\53280493\ruosgms.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.564668029740761
Encrypted:	false
SSDEEP:	
MD5:	074D9A50218E92CF16DF3C24F3543AEB
SHA1:	7A4C0F19E3B4619EA06825E65568F1B428575B0B
SHA-256:	5336B6FF5B226B67A67FFCB4D3DC4DD76A1B525D6959C0754049C2F5B26B9819
SHA-512:	88219C7EEAE581CA9B4773AB0282C056C041A1F9786B5BBB6F9EA82BE4B65FECA8F41753EABDD5EC64CFC04D880CB8B6E7C88A314DB6E3253AED49480B1CE288
Malicious:	false
Preview:	25wO94SV89R2n8C4gl620724x6Rl085X05hwKb8..4JfZ3GTp1201yM0l923f00SGXD7Z1Ex5gJC09p57S61..803Y7s8kc02LT0C84UFJ00U9N2I317db61D7p483Nz9sSGvqR25Sa59ZN1Gk9616K90IfWM6IK6g52D7t61i2DKYVr8940xw76VyZzqu3U21129xs43c1954f..mMAeMhO79VkB2Smgw514320T436le8S2k02fE05oEDQ..yokh539FZxMBj3z3bL2fL8004dEu2dmE6d5o4O4..97rdCcC3B3A5dHWp500B7QpesfJ694O489g6X4L50MnNla74002B5vP9dwe898S19R782lWA70033WS15X0Ls..62ae31d38p69A52lW6T0Q6IUGit907WRs1VL33aKx6a..64l2Prj98mVtC2tTHbr39KuFiY85nC8HQVOUzb09ae6060117W81zDu01..zl176O2i4bvi623443fG8M7Drc10g1501SX7..

C:\Users\user\53280493\smgabf.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.468899586118615
Encrypted:	false
SSDEEP:	
MD5:	21C5F086D29010FC81497ABB34D8280F
SHA1:	B56F7696F207976A2B87032378E3119F07DB6CCC
SHA-256:	7AD043C39D6CD81C747604C0D767110422522DD917458D6E8A201E66FA2A226F
SHA-512:	C9232624617BC83B655E8AB221E5407534D6B054BC00E27D4EC3367A6526DCE9221A3FD6EFCD8F0DD9A87C92D09604808105F08F2DADCFBA653EBED989767E5
Malicious:	false
Preview:	RNZ96GSO506k924J4Bx5A72kYMy7wY18py8..80985ia0Ax5e26m8483Z8047ZV0M208T366va1e3Rb966w06V87J5Wk5aN6f65rq552X7v178C9..ne4Xe26t0Jy36kY94eiIT7h3225e0ljf507W92O79AiEU7KwWD353x9Na5x8J74O8SR7U2T7Y4S798p69GCWeG0H44F0h104N5..O0jrVweYOl97X808KI56710Q163cUt1tE8564868764Y5a..101JlS4yr2l3Nyza8EclVwT0j6I6d584r07frD296oLwbWyQz2w3u9653H91F6ip5OdwMC45rM28U6aMv7j9202z1TIY333id100hDXuC75Dh511A06r90xbomZ1tCLlJ6328987Yk36SXa66b5gUB86W103..5TYl7y64U9b826jwOc57NGWC48682W4M8R14D37lN7SI60f05g0ggA190w3lx3Hb256tAuqj8i90hPFeC359zl3H00hirp0E788335Q2W9Rc3PMXr732TpA7v6FlK8h..

C:\Users\user\53280493\spihfhp.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.549917502461049
Encrypted:	false
SSDEEP:	
MD5:	9293CA6F766D126DFA35E15AAA6887D9
SHA1:	F588ECF173FDC0E40570DC8A8E77D4808295D7A0
SHA-256:	1F0E008EA2051FB524385B262D5D31A282A641A1615C5F0BBBD93999F5EDC907
SHA-512:	E63E148FA578EF019FB3F1D830307A0DAF1C41EFE828E27824B2AD7E073F41B91D58440A579BC7A43AF4095666B5D43C3278AEB0D425A329C2DCF9B73C918A0
Malicious:	false
Preview:	NxmT7Kl18r5o3oI4zvmbb67WC8Ge12829G7195uC2YV048374099s7P33c83WqSd7Jy362283hu9452sZ9q0xdZBr1P81Ar58LD6alt21YKRg8qY6GXb83xp4..615dzFJ jl4..5o0hWx09P12W0QJ4i46KFvx18Vcgy414Fl5TR1U1x0R7c52f50m3AF78z..9ABm21zR703tG056wA7bDo3U1sPv86..M0g23068H5y4XU9j1B1G2GjSuCe5crm8Rm ym2774VTDoX52..RcsOp3W46171aEy4m864CtV1k5714c1Fk2361p123f2qgRgXlw52Yjl5v671UYNHUmPfB81C48TC24jnOtMfnR3cMLYlmdy0o..09DQ6uYsNX5A7826 Mx6g20us209DViU24LZR913e2B470df489a7Dl747g9gS8pWt3K091DPkRcG..V22xs9x3rxu8e8oJd3cRw..g941i83T973206z19020S931Sk4V741c0V3910327tWY7 16e3dhtl2139pXG2k2R74Bv3005xn909M5o14QBw7799ck240y8n90Dye26rQdE11R6hgLR6ib01O0e72M1JWj97ElM2e9kHC255O12K663m42j7u2WKG595h33g5..

C:\Users\user\53280493\swrswi.dat	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.465290266761089
Encrypted:	false
SSDEEP:	
MD5:	D0636B424A1A9DAE69352F6A58F3B454
SHA1:	3F878015BA653315AC29F572D8FCD08E58455E62
SHA-256:	0B1BE4C7CF9F2ECFF922C50EFC39DF2C0A2FF426AA5477C02F9E9290009D6F77
SHA-512:	3743470B72342217291702232BAC3F45A005275A806B555E9C19FE3D2305F1E3D24F41BC5F5F60C7B38013305D5125CA0DE1C4928223EC451E8C2D5775749B4F
Malicious:	false
Preview:	0g61625Hm46Y4C1i5iK89h66Y1F112Gd0T3j6w1C8SwAL086d56u2tZYYK02If38u612UtuT3783K237vS..Ev31K3220572e9W90x960HSw2J45ByR5yO69rW2..5758I 2445O66Tx3R06dDU1s6r8080lNAv95iKhb2RAc0400b4eC218Zi3C3npMKaQv1D806v95i3960n9BWahOJ7Jwc905MzKs2s3Vf03ZtI99UeZ3058x52q978YI86r0OYy7p N33mL1s53f227MvJXfY6k08XEI74c7K7Y21TD9WCy1..qdH8s10EUrw8Q5w07w2J63K8SyYqd875ms8w25rKU3M9Y3036s18307V0e030Qa43O8wr5Sh64..7y845R3r3p 5gr4d50490z54ek6n2An6TAf8K8B0Tck5204M00xHb3b1FP3m869kV864x3VT61XvJb7S8863P16YOZGH17p3Ccr071T..Ts8qm33K9z1wJC8c1YQ3e94O89jlLE4k9W5F zyk64p6sia7CHYw794..

C:\Users\user\53280493\tlbbmigtfe.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	5.624046523503253
Encrypted:	false
SSDEEP:	
MD5:	070E3D41FDD45A91592EAFED8B8755AA
SHA1:	41BBA7C0C24D1FE2A2D7A4F4EC54173CF1194D80
SHA-256:	E459B8674EE9B04CB6E136639A212BFFF0E46160BD3CBE5FC9345C92CF5459F9
SHA-512:	FFBE60229F187AA9C83177CF377CBB6F026D31673A29D352730592A1CE5182872520C6154E46B7DB7D43E81E7130D657ABED20180FD18128D9DA862305F941F6
Malicious:	false
Preview:	y24Abh41ebmtWG61pF4ZA54ou0ZGBcDsOvcn03V177cGojWS5PPmh3kH4W..Qqf0580HxjAot2Ec9EEuksM31ZUC6U909us2t156pcLg5lLDD666CwH5691414i9I7201H BmUZeW912h4yd1D8O4OWk87f2UV99Eir41q45zk02uE86qE623oSSTqN..oyN8V7E6Mv62Ct859EeR9p0C7URVsjnkdQj1J1y35d25e5zaT2896QI50K8Mn3F3S20RCc4T 27y50xRS6195H599a2309K2ne6mT44nV9Ink4wC5lIN1E2i6x74Cc..7gnjp72wO604utF480s9r211786l3q..D7Ht8783yH1658747F9IT5I..ptoz7J6M4D4bT0uA5K1..BjL26d7 0E3qpdbwV2H5066286K866l4..56rDW20WNMuvfd6515d0N4BSu480Ce..6Rhhz0A77Hy2r2ZA0dmgC5MboENyRNQFy1X5EY1..3pf60M397K932Q5j6f2f03JiJH6wC9d Pn5W77I2Pv89SO0fZW17Fe43y3E4917Xc6FJNaP1n75xw72h9f90j1tnE4Tj9KDT6p5024016uoxX476w56iQyx9Fe803l4v6O7frT2mQ..

C:\Users\user\53280493\tlodellh.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.496853173745706
Encrypted:	false
SSDEEP:	
MD5:	2150F9C19D44255E8A3AB337B49C3E3A
SHA1:	B653516E8A4965801D67854EBE17C17B4FC3E387

C:\Users\user\53280493\tlodellh.mp3

SHA-256:	BDED7F628EE7EF7C6CE14D92D16C8CAFB1B1ABE4E91796851F09585B54E856E4
SHA-512:	C25E44BF7730ACA9FA1D6111299E46263E1C921F4715F12F5AE06377B7A7C35D716BC59B06B24766DE5E80FE5DD58728A97A36E2233719132074E03CBBD31155
Malicious:	false
Preview:	la4TB4F2ZD7z9S6f84w2Xx9wW0p54MxmfF55MS0594876H372209SF369O5RkTw18272P653x3l5Q00j54BRnPrsP9v1T76Vh5mTuWp344cS822M7O78F23lo222..g964 5r5u00vyf4544x1ToXRc9y01k2S0x16Z3K633YJq3l784Fo83Co5iBU7BJm102E3zKh4Nz163yS53W4J8H0oto6Lhl87Y9xYS7o..26A3Gt879b89Ul0c0F25g2a24FURX 9Q1lo8v7Zm2OD94j8t4fwcsNuX866320P311p4Z7L4p35Yw178RJ8s5j4498bFL..glXAt5e1d068e0h2i1TyxuiJ7V6Jtl5RrHA1YopD3n82h3Co45P302tA347Mq99e7 16H5o9N..nO973f1B2KwfFGh89i29C4l5GU1l5kW26Ek6zlZN46862991L12K2yCw6l8vJW0F3a26s494ns1g22jZ000kl7T8X0t2Kt9287oh217H40A90x6Hq17h21p22 726Ht0tHXZVeTJh1srM4Q7F746j..

C:\Users\user\53280493\tnpmcqahoq.icm

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	516
Entropy (8bit):	5.495027560631433
Encrypted:	false
SSDEEP:	
MD5:	9327EB426AEEFC9EF95BD0E4F1664D1A
SHA1:	98F689693509E69C58A6D38DD63123EFF958C665
SHA-256:	48758C7140B9A8FAFBF660C4F9B168C52B0F1A08F1747703E46576BC1A29E3C2
SHA-512:	2E2CB72AE606623318268CDB5E7F86164BBD4B97E33CD84C4ABD55367DA57652199FC05B3042D61C2D48AAB8795B9F82D6FC254C5505B9D95FD26A5B08067BD B
Malicious:	false
Preview:	a84X9rS77T0T6D2082p9uMRf23XJ882zUq79HW5lg67UpG2h87y2Q3297Zy31f189lxo3j913r712k8rx6g846sV75x5X480Z5zYACoj4xjxP912A46oc6T03H3q70pg04 IN430X5X6Qx9zP7Wr8h8L..37n08Ozp6s05L3hE954C0eUyP0o54YK813kR7aC323R65W6Z573z52MWX6f2TYYCi6Vu1yyU149XM96W7L3D4..3DcxkbDIJnG579T41jN5 cy1V4g4piCJVl51Xkb90KF9pY5911md4k772zN42O83882eNbin6663l90RfE1ccNuzxJt0NU73w5X47526aksy07a1..2763ug4LPJ92w0c3WoVE33az65q740QM8mG4E y20gYq2790s36e315..d51ib792lc4G1354GaD7bEVTy31yd334Gs587t4f220M51g58ySW..0Gw7Lh7u92SQVnFB2YU3J6FV540gl0PVN7149F067z424BgWq17..

C:\Users\user\53280493\txsc.bmp

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.53924566990092
Encrypted:	false
SSDEEP:	
MD5:	F25168C5066E47269CCC038D8F742BEF
SHA1:	72D05158070C8E0EDD28794AC3269C895018209C
SHA-256:	A9CF554D28B98155C4BBB9FFC6ACD36DD6164F998EF11CF63E7845E5381610CE
SHA-512:	0CFF49549A86609C5445E8598AED9338A74EF2F2E779D408E90C6DC5E699F84319EBAA4ABA0879910921EFCE759B4FC3A4AD234BCC9E111C82A529D0FB83A60 C
Malicious:	false
Preview:	o5YhPh127a58xDeC6391YS7909R2I91yfYgu930212kD3W3b5UM3668nW1etglt19fuB0Sniu81F17D1650Qc08H0Nx55Uuz04Z1yL4J8NGh3jmQ..4Z7vpK8i3yn4U3Dk 5hG157tYG5fy0Nc56Cal033D190h4IT986X63F68j1ki795S7qZEv374yCQ8aJIGN61s8s46Qt659YYv64aSP88r4dF..9MCAidF831dsa9562zmm11ves19DWe7W9d030 B1G7ct53Z31U13145q8095W7hAcw9A7IQ1ob529V60wJ2C3h3HqUa73t2OE1l5S91QB60l5938u5pqU05ILS92ILY787e53Q9p..45CvfaAsh1xRPrL604f32n84G0vmfU 43h1F3..x09f9f5Itym1iD94K4BC3222D22383Hk2a694l616cHi27QW1cSa2Ef5ob4z4g0Z235q2r2916f1NRf9B01KyR7F68AHJPexy8360qMUjQgwj3lcS57uu1n9R8 Zh45Xa4k8P6n4UKr5..

C:\Users\user\53280493\ucoowohbq.exe

Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	616
Entropy (8bit):	5.493766122193799
Encrypted:	false
SSDEEP:	
MD5:	C0AEBE6E03935F6B85CB7EEF89453147
SHA1:	2A6379103563D54A9D9546E78C7AD86CECD4B723
SHA-256:	A7429F442782B19B930EA759E893B90093B24D5D0DEF8DA85A3FD607FE521EB0
SHA-512:	B18268942AFDB59542C3FF6759E0D10B450E0AF6C73C661D3F97FD126F925C5D5FF5E0B9A684B912F31964F9159EFAD9B148F28753F26D02F93DD3550C1AC793
Malicious:	false

C:\Users\user\53280493\ucoowohbq.exe	
Preview:	01Xtd58DS081I6B3m15U771nO4O0Izp150mi8hSu0..aCRA9G926mJ0125rXM7cbyWnzOz6uWYl69Mx22ilK3a3M6T3Ne1D682038480DGgQ50d14U0hb7tkSlO521T8446L68141N17i2733a63X1q38Ux20Jz484071wmUiKC7Tb9671W0o0xZ..1Hpu2Bwn6xLHTb4FTf7u9wRI13x87x3KpKP2M2m9K651fe9594HA8A200k91s708J3990h8z530n894uJSA47Paj40rcj49g5AnxY614g7..15492JH8Rd03eT184RS12MH3VIcb659ZYtd8v8l3g545bUdi1i4OH673C38939p8t4yE5Y051os1mfjBtQ776960NK1m01m7w5RNCJ24382vq5HoF4536A8fc98l70Hxz1lgs3jp0G1F31tD05Gf3Xb8fkg03AUpoY882395L5A..3W0GRlH10ZR65Ukj2wXJZ31Z6NN714d1zE548Zp2D8rT10MQj17xPH8KzAZ6x1HKK854T40w948a6Q012oi5X2r1h5m0gdws5hH3HSa1F8y4332NV41IfM6q6aW7J131m511YMm5mki4320b8H4..

C:\Users\user\53280493\udvbltspem.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.468632584984932
Encrypted:	false
SSDEEP:	
MD5:	B9F1CA80D78B554E8A835625127EE854
SHA1:	776DD2A97C0CDFBBA63AEAE0893E314C22E540E5
SHA-256:	99D9C7964B9F5129ECF368CFC532E3974743309061CC209CB7BF77FDA7A1667E
SHA-512:	C6D0058037D9EB160122E8A4E5687AC48804C3BD408D64D2085CA527348B67C57BDEE0B586EF14E55714D92D99441D9CAE85D0C511F1C29A0539B4B72B0B35F
Malicious:	false
Preview:	57475DYl63k6t7w62VSmKjy333E1OrBmYebtAwHou5v2209B3q14829c540l09H6xjmzLWO9n69389fuPW53jl29W2NdWEL319G88410nrM7s2ljw1b46q48Zt7r2544w2Dg89hi67R8690..6Z7030p64l629zUU6F363nS1kV9v34hVdX7m3i038lF2A8b5s4Q4v861YLt8DX4I13880961dK109542c93M3y77p0C..0d7974c200dv65J94ruG6c618f9Z529k48Qb1o0Kk06cm9L9inmhb3Xw3J4qZ2xq6d36038ac192QSYu9Cl688..u553fX12d4BX9QLKO3439496xwuBp2dQd501413guQogv884GFxSZ7b8E11e4c23311g9hus6793TQyj3i..PgN6oW49533b3309j54pV529w6O14mLs24A8vV2mTV..bRm213v4G60337ExI..0t5wCr0493k57a66861W3d3Xv2VK0Rt97a4419civ4cmTt5Kzy0K3UA5p05BX7325Oidt3ONhZr4rdk2WK7KUH2BX8EQ9dCn23Ez6d6eHiJ13z81d6D11PlQnRY81Tm2XB1659q958091w5E55..

C:\Users\user\53280493\uikdqjn.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.465628136046867
Encrypted:	false
SSDEEP:	
MD5:	C79ECB2577BFEC280DB0B39CA7DCC184
SHA1:	241E664212EF919030E140C37E12F95E6CDCBD6F
SHA-256:	3A94F6C724AF99C5B8E766E2B4BC307724FE8644DE6AB129615D187F4050FFA6
SHA-512:	5B742582D6E3B4AAA89ABD811F99A75096565BCF1B0DA6C6716465C4963D10E5E274CA9AD69A0E89C461C66AEBDCD2C14D851AD95007ADAAF49AFAB5486C4CF
Malicious:	false
Preview:	YdBl23C04hQi64K2l71Srr7rpyW8luX6T29..NsBOKA21h5445885Ge98l1N7AhWp63nn06p57l3s7cI4pS3bj0Pw776401y9h620Li3dLVEfrWyNV402Z8821mJ52u16lm06187hJ07U4JLER3GDO5Y55D23630ggd76bC8pNJCAIJ302Ihp205g604..UMu99mH56..7Dj8lskpkd7VB584uvz0W286NX588l4E12fi58x55J4BQX8aerOmyveEd1p3xPrul652c5GWr2Z63aJj43..v7Z7qf4p08j5b2BpNk30z14on306DEe45mer9V2y9876HV60gcYU9j71m89Vh180003860f310M3403V01lwu4392g88dg3Dy6818608er51YF8hW5bi8l9m2p39MO09nxi42O..S649ZB639321Wf0d6e5yIS566rada5PK5Y101DXW0sc77mfV66BBj4X22650MC68x22o5SW2d117fi0g65kg1nS7CZ04ZE70mt0b2kP13345998y603O5g08M01829WTe11lwc4j2E8R36X8Fc2635C2164Ndo8WXX6n7F1x0LH1..

C:\Users\user\53280493\urmf.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	515
Entropy (8bit):	5.460298121883905
Encrypted:	false
SSDEEP:	
MD5:	0EC0F35D03883D8C357D9DB4BC8BE6C8
SHA1:	105AD9DB9F9D70AF6177A28D49F426FA50AF9E63
SHA-256:	0C7434CDD338CD8CF06E122D5388CBBA0B3BC91AD6170BCDDE3A9863E0CC25CB
SHA-512:	F01905A596546CCB30CC0788EDF193300E2D11ADF05D3F57A1DAC00E0771A787BC70861FF2C0F75531CFE0A25492B9CC6875635313ECE2F76A55D7E180D4C89
Malicious:	false
Preview:	K813q..4Pa0N64v6h48736Xp1jSh90qd44Gz1b67EU37w79d84NQcEhfUtC41yQm2L8r7k91k766U450Fq8716C7S53Nj40nTk..03R7l154Z4u833C921907by0z8QRlE3HvcG17Jd1Q9B78m..993obSg6CK42sr7874..s3H15V82781do88StGK5do7P3Rv67g26Zj7yzou4a49dQ5uT2K0oo6Uz9061h6YWrr2x5VB4g48pEH8279ovw9G580r2R9MhaJ0I56W7QGf4532c2W54104W..D0Xr63MSU79T1c73c52JZi9HS827ZdY7D40456N2300N86729415lDi329O0NHnv..4gALPk1Cd4U30E137o23l5D477T96kQ8n0371yKS90wow8Rll17yFBAQ8987vPro39P0614hBfEGH17MSW2U08BtX68D08337ua5236e3r44oYt82l2P179AyH745s51WMWHh..TmG5pce91J591L5y03Gy7l..

C:\Users\user\53280493\uvnrlp.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\53280493\uvnrlp.ini	
Category:	dropped
Size (bytes):	501
Entropy (8bit):	5.489948348418101
Encrypted:	false
SSDEEP:	
MD5:	29805AC1FAFBF612E971AB670706EE44
SHA1:	74FEF4A8AF1C4C83E1AB78FA19F21C9101BB5D9C
SHA-256:	236B2BCEB937E5ACC7433A77421F934EF63BF13C42ECFA28CAD99504E35DDDE4
SHA-512:	5712113CABB3EEA0FF74D662C4DE77184686D05DC6332C144FF7F4F922E2DD9996A0673846465F46B4253D2EFD870132DE3FA7ECECB5F61A982D665F5ACFE0F
Malicious:	false
Preview:	rB4oGw4g38acl29Ph4x0T8BNAlh8095egaB6f982n2i1j0ODKg5Sm59f3w0Q09Zo3o1wej018KU4d85MjEOujgb51hXT55XsTpzxEc36D0st2W..4OZ4Fi737V0724X4Dr zad66W199c66710K58Gy5531hz0q8x671z4WU60999c89..aWZ261Y38N9Nnl9V6b73ZJc4n6Sanro0946nxfVz1T7nC2Q163Gl665m5C1C2sM7024p..x16C992f67w41 O1F4k88490RAv7DdAs3J981226S60377p23D1j85UM4562..my281T2a43G8K030yC0rrYijBMD2N3ZWh70lx4a1u540JwBP7tV662YtR208285dQ19916qlA88Ig14i0N 539t8y3K3j6eSS..24x04413SM2693344E7F433N8O2..s0PXL9Ca4pvE397L35wCOSr4Q7XW0N75Zn187..B3olzcvdis95Q5508L6v741Y9..

C:\Users\user\53280493\vbdetvhl.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	556
Entropy (8bit):	5.394314134995018
Encrypted:	false
SSDEEP:	
MD5:	4EBAFF68BD9A242D84CB8AC6A6EE625B
SHA1:	872671D1DBECEEA94EC4BE8AC26CBB6DF6307F09
SHA-256:	638A948CAF431D677547FDC116CACC2821E05DB7927A0C75BB2EAF552280AE78
SHA-512:	A6FB36F09F885795C9B3C2BEBF27E3393F2903AA69425868FF7C8F9A258E5BB0BD20F5A4C2246614C5DFD2949BBE55D60FC0E13EDCBC951718F99A8D1183F13
Malicious:	false
Preview:	cTX0U75mx8635ycM66Jr1ESE..PvO14v4r11Y..S7G646344O46LXr4SeHbDk72ocm63474Y9cC83nkS612i3r4o1888E16Yw924D36z1i4A1QIeEg5w9j76E4pn39xO15 Es157782X6..1KGv3j87msnd76A7I58a190lwASp1OA9058P0k31c3H189325va1fcBV5jEJ4911b0r387Ax97WSiLl3451393NudBP83975F17B4G0AYZL1m039J174oB b63572CW..80s4826..uE4fi2Fn9YB92Q687O7H40l4639D111d4n75R8k06wOX9J8F1E8j6En3631g7S401575D0862aH2tY488Ndy64z440MyoS59Q8NhFYfQ2A8L1p5 77Z44m97A44cm9R49K8S..z3ou3096J63y5nn0grWCt7D5KF12Ys53kGF3TrG7mv80V3Z6Fm56rCyzl595gViwoB8muz98c979293YC9VCmX88eR0S11z2iC99r41F03no 53l79L4g137r6w9oA9y07547611Wbt1ur6..

C:\Users\user\53280493\vssereuub.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	606
Entropy (8bit):	5.478899422944322
Encrypted:	false
SSDEEP:	
MD5:	0E2F1F160F79F6731E1FDFFF5BB3C984
SHA1:	4024F5017576ABFAFE3FD89F841B6D438410DFD7
SHA-256:	27287C33A1F2B84F26BC36AF2594B0308F71F6C6742CA5A28E3739962E474804
SHA-512:	7BA3D9F2217739D6C452B75F0EA41761C488C701417CBBBA20EE7DB7C57277D964CFD313C1A61C9B7FA5CF55A3E1447CA5627DC4C104E5CC576E0B0A5CB15A 36
Malicious:	false
Preview:	qhg0n9HLw429WO0n0DfMSua2pC45oB94vU42lc1g3296YD0K507wOW73669UGp81t7818T4CLm..K8q5Mi49lZ93cM0H51Jtzn5t306mQ2j3e72812v475tY9X97o9m7Mp WJDc0XOfhg61lf8s5ltY1X5TE6836MXSF0C47B2ZXCj9AAY284j8q1pnE4..3f8ndc51G405Np6C7u0zcD6l4pgem9We135JW78..a5j0nC2663bi8hH6Q2V3706mMbTM0 Si5rC435587353J0G147P984945g9t2mP2IruUpX2b140XZr7PFzc41W47U2Q6CLhs2T57R786M0JunY69781yNQ13dZ2Iz8R6336O87U073WQ2Y0BjU7710300mFDat8l 5..hZ09qc25Akgv7932Fq5z09I7XAZPdUO67u491x1024h31f2TBG69429i8E3vcp4CHsf38141..6w9064Wi554G3mc519w8J64j63y43q72960b2sa1N04ia45oJ05L2 26e097i4l7k9K13w06C707333N6s8gK44t19p560463jno3s018i94n1xh8X30Q7P7LVf3Essk67GkdzjO74..

C:\Users\user\53280493\vvhedbw.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	5.4631666208701954
Encrypted:	false
SSDEEP:	
MD5:	EA9635B14DDDB493A48ED9A5E16CC245
SHA1:	738B38A1C33F96FBF0BF184BF8A7BA4489EAB202
SHA-256:	CA2C618115C4FE03A73FAC3A9F883D4C1B5662619C7380A4DD40501956F61403
SHA-512:	1A96A0DE7ACB871DE3D84EE41D2B42FC4BA6CA21D5078AB6B4395DA4A3953D9240830F5B3ACB8194253675097F0FBE48479543B46F093CB5A3D67C43468D285

C:\Users\user\53280493\vvhedbw.msc	
Malicious:	false
Preview:	760X319a68dh0Wz6az97h3N7Y817i69o1xDld1k56JF898o5Ut5369f123TL9..9xg09d53I1s2862UN4QZ87UiVO771E9gHvx8nNCJ47XGs3602UHWj1D96K716aN4591 Z298hn6G02A..pf90u34F..5GyG9a0815BF47E89sgW9sn372ybGw9LwV5KqY6PI7273yFL84Z3ml1zP59S77502o7mY903px..tMC7LulEW70VpSs8i3dTrq5s7BU79P5 60qYs63075JR73E45n58A4457I77i3N129O48F98583u9DUvyWgrL1sn80Um..9N0Cc5U0ms18467Q4014w3858n66pC568WyHlWzbXT27e1pPEk8icQ4VS27QX9KNt1cF 819J9g42R1fRmsjc172QD16nK813B1b8d6jfn1NE019ypDc9519V4K3W..7H9VMoBWt40E31G635esp375q5GPv1541hgy4Qo6NYzS9K2IiN7A5W1OoH7t34u60086W753 5126fx7X98E60HvvA2L7809w931Opn359258fnu9x83oGyz08751Y919P45668f2L044Vz4jiaBmi8Mk39Go68b40689I17C1PG20S02936zW6N5t07..

C:\Users\user\53280493\wmnfoflxo.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.534487418668525
Encrypted:	false
SSDEEP:	
MD5:	DF019C890665BB6A529628046B36D49C
SHA1:	11323608D200148629265F27CE085EF983989C2A
SHA-256:	50D8324C0693494F9A97FB2D9ACACC36F6214E66733F1280ACF030872CE9911D
SHA-512:	C1A7AB3E432F488E6E6F83413B1C155FF78957EB423A8FF74B001B186186637DFF07719AD79056DBE7F257A2EDBF1B21A3E3F2088A2F12A8B08F7F20E5DA53F2
Malicious:	false
Preview:	64XpQP73f6J969Oij9l5131G9nt3d7uV6y8e2bSp4kD3hF0PZw74I1M3Y9QvzZrh7170r4S21HTUI7F1365aDk938q9r..716lU..h689lv86HS5Ue355AK77k3Cw3uul2 481y202..sc30594nub057zx50E3BJimNGCf58trydgp8if1A93Li1M94BRSja33127zQ1FI70Yh2m84BIqUum0M7G7T88w5778f23036J45..WqF66XBQ6VS9s91xaI6O y03H9I4Q8691AwN5l7b642OSHit9pZi16A5ZLw3yo502a5L857S98LpXE09o4d8d2yZBii5..9082RN5dC44b3IT51t4w25m47672tUb733280r7Vd40SMYV61iNm9BZ48 07HA8p0M3HYoYxDdUPb630D6x64s25..bf03hiFJ53X4A8A2m93489J6VT9Z4WV9X047..q47e10176xF18t578u8x9L8VWAt773r26uFa34U9X6zb68d2sTaEb73N8lZG 5i39N9470i9g06390Us54ug42B06lIHoo3v9x4VQ2tF98rr4w7uSx1Pu7FEs9UgfyBnYSrR8e76Y3mb..

C:\Users\user\53280493\wnjjt.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	554
Entropy (8bit):	5.464808247913593
Encrypted:	false
SSDEEP:	
MD5:	141CD4BB4A06BAD43C65351B317C80AF
SHA1:	B313F5594788BE3EA4CF66BD687E5D6EF7022253
SHA-256:	A029214B3A57946559FEA897F2C70EEE41E5F17D285D73039483C2948142BDEA
SHA-512:	C65263D4CAAF91D49E53198F8734E32C78A1357DDC781860D90D605C66CF65BA7BA75E59A6C601C4FA08262E488ECACB0A640BD22DD69972279899E1A4097B1
Malicious:	false
Preview:	FE3M16W61e87101T4F38b9m4XW732QN0x3jt3w6lR9U6a13BksYeB7u95i0o7n3m95o1rwId3nB92177Qrno9414l5V04894DK..f0L94tTn..6skzF85i8dP67iTF9885 8901W163lo3qg3vQPCbg3c0jJe24D8m4fX52778U8i669Q6Nw1a6z23b367W..h0s8998g57UbEbWmYj814379Kd01S1..361WFC1016FEW3A941S64t09..QzBZC79640 919378z133mNKpriJ81D678zj0D8yE1l3qoyL18S69m2Lr0ULL4uv454N39p53623ks10wnnCe776NvxhQ93d60eHL5UIU8vF74IC5X45M5Pjk5h2wy1pF5yS3Uzr2..Uo 7853lw02vP90DU43y1QPE8xYt53YRku6S4L1eVxAZ887S9L58PGy6..A19k863t3Q02P4836l908eIT7XVEH6dw80076aj3K08P93m6If1Vz7Ub63d0s062yjT0DCbbep3 w4b510I920Nb5Fxy9f5WS791A31OP36Q..

C:\Users\user\53280493\wuavvoeqs.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	319776
Entropy (8bit):	4.544380095743814
Encrypted:	false
SSDEEP:	
MD5:	13ADBBE59EBB4DD4F192C5D8606C4CA5
SHA1:	EAE40399AE5C1C7082DC967F3BF6F02453F4BE23
SHA-256:	AA43CFCBF121D2F385971D09DC61A1E44B40DCE9A3ECA8AC345EEA35FEF228A7
SHA-512:	41D758A709DEB6A43D9514D5D7C7CB13AA8B565FA04F21950632FF154D82EB37EE4EBDAE3C4EA1E49DBEC9D9B37FDABE802EBB7F6CAE015C1A16C78A6E00 398
Malicious:	false
Preview:	Ed4L4iDX92dj29CTn3IdC6gbJEBj8..7jHP6H7WQ4fMQO19V8hVyC1x6JlM45CvD43146rPb00Cz42oM8q74PJ504VV2mzY..09449AsywS2fx8pSr4ZuIQMGu96Xx3751 P1..0I52lT586545IcdJ02Yi5qqKw4w5Z97926318pa6pLAO9Jo979jvOY1lz2VGe..8r751f4894uI58184GtHBUPo6E2YuiOT0r0518..K2Zok6t8Xv8rc0uF2Ef114JW4w1L2aj9w 3MsnEsgy5N1U6b347..7617y21DRB335P6M5177Y3g1497d9317tpIi0O2V4n477rsd04zXC56R4IS02b5A..vbq0cGo6W1L4w9QF9zWT5664V67P..G84r6Jt44wM2c0z 550023Y4p5Fi1lD60MbxnQ75r0hy20Bm54z775pN88365Q3jcnR1R16Y5oK703tly77BeSbO2n4..rW5e311un9F2pFGO25tB9qruiy07g3F99512E30qGj994Na3t3951 s3X8KnU19759..Xqi8vT3lK8cHVb15447651lR4WFrzrBEQ6E..57vS2j12U784Q570SH2338Hd86n99C161TWNvPFE61Ns69Z6PdG99421r45C..069238zT7M0Dnt5vV x0838zEC45gs8g1VLBdXU1y374n4s92dpc..7naa56Gd95285U4J8FA9r2A497Q48Xd943ojO7CzuZM63Z7q834I9F1T25..6RDs3WcgIEp71730fNjzm655614e6m5om6 2O6Q6205c44lJo4916H0..hM6ty7pSo03377qwvdM859AkN063NdGt5718QsSY3hZXCtm7P3pFjE6OfBn9qkukJmh925y8b20771r..0TE1ll607E0s1GKK6zU265Zd81L 92F814P179549q..QV7UiR0348xMV37o7L8m32J0x14S5V758OWh31650k795F36d346..191XmS29E2

C:\Users\user\53280493\wvxlnvkod.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	577
Entropy (8bit):	5.496968821741932
Encrypted:	false
SSDEEP:	
MD5:	1943F1C57614689FEDE64CEC2AC168C0
SHA1:	E0CB756F99501495F6350E4F6C058786199C969E
SHA-256:	033A558FFCA03DBDC62CC1B45D9469B4D48A1DED91615FDF1B7E5CDFA5DCF652
SHA-512:	80F8E1A9351C874D7417B380AB4AD679EA983670F15F78D4FFE50C1B93A8FFE4E589DDE73B431C15C4ACED8A7128A688EB0B0121885315637A353C328622F40E
Malicious:	false
Preview:	DMYpb4ZW5s7SXz..102t8N99JE4Q918W8f55yjt8Cr0832y3f024r4J6254R459m451g6885964ATX5..1X389zWso9sx418Dj8k2gZ58zclep710N88q9fFToH6AaF6sG zQ2kksg5W2I35b6Q6Pf0vz7NI4K..X76f60bx913315BmTubb0EA109293kg3ZW1G62PiD52e5z8WN8079oM24PO88NEoaI8290TZBjg98v28153orqhNpIa49HzFg0a99 q79IW82..2g5389915643js022SPLNJ217NF1706CjD0F1Zct62CI69EH0Nl103gW47Xr1624O86T61V7867DHIIv11qtKgytV..XwL263262ZV8XwLbKR134S0wFGZis2 7Vj2Mapv72m6ncvrMX7i64BbXJBR800Jh4..4qDt533CzTI6Zc3P0GnPBF8g2z2jd5d41533i5H65v3828b05wrLX1548F5906W0432MZY89K2CX53lqy343uAf70Hrw0w J89Wq803ju7ysR2cz76D4228H5Q1Li2b88HWsVVe507k875M48k7L87..

C:\Users\user\53280493\xevwfe.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	5.529298013546283
Encrypted:	false
SSDEEP:	
MD5:	5E0BBE823D622BA3802DA972503A79C8
SHA1:	8A730EB30C5E3D099776ED45801141913A16B79C
SHA-256:	2D0583FD7CE6ECA5EC331F740FF7F90997248BA26F442658E4DF36326C79A22B
SHA-512:	4C3C91ED6EBEA18E06DD682E4DA470A6D11F1207E6A9606058FF55D3AF75D62406EF68A55C6213A7B22F926813EC6EE1E7D2C42C22DCDCDFEE07FAF99EB01 6E
Malicious:	false
Preview:	98b670wSC9h3k709F6GjtEG3HsB8Oi..4o60r54b027gVG02t6dfr6t64heYx59P5t951J0d4EWqqMZ9B9W5s9G08VTvx0KL7NlB8j9u9rr7H2j020q22Eo535h4t8nk.. gZmj4dD8SH8n853o8L31SXk4di5vM29v49WCfJ0J70lkeT4x4gI765G734NQB..28e8844P565s293M1nSazX5w7X3Lt4d2sn48en137Odu904A8w2qKyP1..13UkNp76t 3n0el64s0ccA6..kD8GGQ81Y851h3ct757B0SC87CAJ2atq8o2pIz1Ua37YKg36D6Gk856X3b2zd40b3886n31YW95gXA13W9AN..9DRM8789bN5Wi850V4g12wG086G9h 901CZH244j46Rr9pY50w3q350i470K1U4jM7688baN85594870Ri471wgk898ZMQ2oT3wTUCY25rVafa..52o0424237s1c6L0T80W9HyN23149Yk13kyDVQAO0EY4645FI..

C:\Users\user\53280493\xlcilbc.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.514247336546518
Encrypted:	false
SSDEEP:	
MD5:	A765209477192B224C838B7081EBB180
SHA1:	F3D04985D9769DB08BED5CB19C580021FA9DBA85
SHA-256:	927CCD338A70A2CE3B9C6F24AC98AFEF3B6883E50A9FBE65362656CB8205C880
SHA-512:	4B0A19239BFE2F0576EF3CF1592E540EAE8B64461E949FA750A7F47ED2020CC734CBCD43FC0258B3B928973370754D0AA2C131CC9736CEB085431FFD67D10F3
Malicious:	false
Preview:	E785980jrdODr5621Z05t61El4NC357fC990345A1PvC73jQ601168..7xnUM8u137207yl31x81VdJ7Ez724L9xc25510Yx9GiQrV82zQ43u9R60HlC9999cde..Mk1E2 6sNl4L4O94tG2u01X0i31i1r3tf3xy0f1bWnt3A7629HR1S70EUZA8210jTC2E59092p275g3Fp1G50Wvo020hr7g50mj0h3TfE787K71FqRD9..5Wl83gdUwv875H86w2 O7B36EwC82tb715XSL5MAda97gWhmzxT07o77CAo5002k..MIbBYpv81z43CJ8ktnw8Ve7189j7M5sRtO9400n3640p2mx4851p420mu..vUD0jS5b8ulHJ74J7Hc9..05 9fU61BQdNfu0H3547C18Vb02xs8t5t2C4MO2641xa4oPF4392y805p3R5l3Oi3YR8oo6v1mw33nWKnFW7..1U7M84288YlOH41745959aUd0786CGks7pMs9aGJpx9XJWZ U5BZJ60UX91747u0214s9wLrnTT69C85v58190a05Y191s2eGk3C61l0e69Q2RGEq2bg1mJY7451ik656a99aeh3BE75YVK8476h2WcJ7414k7mCRNc1zrvXo4C99c..

C:\Users\user\53280493\xvpumsb.dat	
Process:	C:\Users\user\Desktop\Covid-19 Data Report .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.512186453909894
Encrypted:	false
SSDEEP:	
MD5:	A29C8E93AAB79341495980E7BC075792
SHA1:	BF1C1C448EE2031F0473DFE62C1658322B3BAD7A

C:\Users\user\53280493\xvpumsb.dat	
SHA-256:	C05BB438AEFCBCF1F73F22ADC85A33FB6E3E2C49000BB680EC2F58AF8D66EAE0
SHA-512:	CE0A5E7401C38C65484589552BC1CC17E5137A631CA058E764C068E96737CC86EBBAF50451FDA309E74A7C96A919E73CDB47FEACC168EB81789F6AFF1AFFB22
Malicious:	false
Preview:	6127w02902g7Hgwm662455xYJa95a35jc3r5h7WVKmW633Oh3152zuR7zbJ8j62f7d43q5315o22q74961N8FF20804BI1629IwXyFu30Gcr2eD1I8uNu5x243vHV3..wL44SS2Kn6P8A4g4uy0r0sH8Lo0H76o8436S7d6oq44chY9Z00ws9Kd538086hKiYN5HF21K4CoBNjAP92042Map260u41UIy61A7Dg5J17Fi2a8xmQ40bgaQ6M7HEnF9zb0JZL7d1nUm73G24XLrZROj8919Qy0vd9s7q49mv90Y05JpPeti1C9..28gp5pO89gp63uOz9I21o8MA12ZVr1G7474Ug6TI..zDuE6Co2d32092oy9s04Dr23JUm0yQRXnN7AA397P9e2AH5H3AT26R092As2a27887j439o3h15vbOJ48j9w9z69Hw9..u1R90XMa35gntp3u6LTn7OKP84G702p039S216SYi8ybm3pMp952NBZ45P7G36866Tapg9707oRx1MZ4J71Du5818k7J59xu6FPs..

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):	76
Entropy (8bit):	4.727851362978713
Encrypted:	false
SSDEEP:	
MD5:	8271D9058A08452A68221D45554D76D8
SHA1:	4F5495446DE321A39722F1B60C8F60AF10F9C6B3
SHA-256:	87C881D774F6CA8793DABBE0D5F3FB9B26ACC0540F65ECBC80C2008E701A9A42
SHA-512:	30928FCE09392D559255E46FCAA8F2CAF06861A2C201D2A64686803E571DEF0A556CF5930C56ED79C6C1D04698FF71993E494EAD68C2FE1C103EEE29CBD8950
Malicious:	false
Preview:	..[2021/09/07 15:40:47 Offline Keylogger Started]....[Program Manager]..[r

C:\Users\user\temp\wuavvoeqs.pdf	
Process:	C:\Users\user\53280493\glpmruvjds.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	93
Entropy (8bit):	5.147136102437051
Encrypted:	false
SSDEEP:	
MD5:	17F4362D04C8C89EFB461B1477BF32F9
SHA1:	351B5570F52A1405B3E76EDF752BF3FDD6FFDD05
SHA-256:	C9299EF6C7D3E9EC4D82A4239BC617206F57F9CD6E7DD1C098B07450356C9B7F
SHA-512:	27288FFC117A6CD35711DA106614D1B7FCAD0CB03F3F95CAB891585DF0A4C34DF73F610D005ED8AFDDF731552C2B69D6A7E2DE62EAB5FDCD2D107458A041DE0
Malicious:	false
Preview:	[S3tt!ng]..stpth=%userprofile%..Key=WindowsUpdate..Dir3ctory=53280493..ExE_c=glpmruvjds.pif..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.433413370714196
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 .exe
File size:	1260641
MD5:	f7b7d0144665b034190e826e035f9c98
SHA1:	2a8d08e5189f56453424b3e2103589ae44d6db58
SHA256:	6712498150d5e13d83aca08d5720f38e0bb17b63d9850a33f7f57b5b86401c09
SHA512:	d4c7d56e256b6f721db40c099b8d0e51fcc74b2cc1e808fef9595df65ad3cfe531d62099f85794e974a8fa5448050f44094030afb6946e5fbce15dccf84f4f72

General

SSDEEP:	24576:5AOcZ9Zo5Mhoz30xGjimPvIqyepC3fO+veiflL:zyhoAxMIqyaez5
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 7, 2021 15:40:48.065325022 CEST	192.168.2.3	8.8.8.8	0x844f	Standard query (0)	remcos.fin gusti.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 7, 2021 15:40:48.114670992 CEST	8.8.8.8	192.168.2.3	0x844f	No error (0)	remcos.fin gusti.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 .exe PID: 3296 Parent PID: 3376

General

Start time:	15:40:26
Start date:	07/09/2021
Path:	C:\Users\user\Desktop\Covid-19 Data Report .exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Covid-19 Data Report .exe'
Imagebase:	0x960000
File size:	1260641 bytes

MD5 hash:	F7B7D0144665B034190E826E035F9C98
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: glpmruvjds.pif PID: 2436 Parent PID: 3296

General

Start time:	15:40:37
Start date:	07/09/2021
Path:	C:\Users\user\53280493\glpmruvjds.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\53280493\glpmruvjds.pif' otggkjoob.bnv
Imagebase:	0x10a0000
File size:	661744 bytes
MD5 hash:	957FCFF5374F7A5EE128D32C976ADAA5
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: 00000005.00000003.270724186.0000000003C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.271079064.0000000004010000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269314350.0000000003C91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.270887890.0000000002FDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269290149.0000000003C91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269142650.0000000003C51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.271397021.0000000002FB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269094828.0000000003C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269387450.0000000003CD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.271157446.0000000003C90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269350761.0000000003CB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269227982.0000000003C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.270937496.0000000003C51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.271019743.0000000003C90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.271290186.0000000003C31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269119072.0000000002FB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000003.269002467.0000000003C31000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 31%, Metadefender, Browse • Detection: 50%, 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: 3508 Parent PID: 2436

General

Start time:	15:40:46
Start date:	07/09/2021
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:	0x400000

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: 00000007.00000002.492377010.0000000000800000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000007.00000002.492377010.0000000000800000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000007.00000002.492377010.0000000000800000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000002.492855959.0000000002AA0000.00000004.00000040.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: glpmruvjds.pif PID: 6556 Parent PID: 3388

General

Start time:	15:40:57
Start date:	07/09/2021
Path:	C:\Users\user\53280493\glpmruvjds.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\53280493\GLPMRU~1.PIF' C:\Users\user\53280493\OTGGKJ~1.BNV
Imagebase:	0x10a0000
File size:	661744 bytes
MD5 hash:	957FCFF5374F7A5EE128D32C976ADAA5
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: 00000011.00000003.317794056.0000000004800000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.314903867.0000000003AB6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.316020069.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.316748134.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.318319543.0000000003AB6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315218162.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315274051.0000000004791000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.316141009.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315298076.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315083483.00000000047E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315046193.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.317892072.00000000047C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315114343.00000000047BE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.318055782.0000000003A93000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315100780.0000000004771000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.314813363.0000000003A93000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.314881153.00000000047E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315347274.0000000004800000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.317556415.00000000047E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.315175094.0000000004771000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.314941565.00000000047C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.317942588.0000000004B60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000011.00000003.318006153.0000000004771000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegSvcs.exe PID: 6688 Parent PID: 6556

General

Start time:	15:41:08
Start date:	07/09/2021
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:	0x560000
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: 00000012.00000002.318294839.0000000002E70000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.318094476.0000000000930000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000012.00000002.318094476.0000000000930000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000012.00000002.318094476.0000000000930000.00000040.00000001.sdmp, Author: unknown
Reputation:	high

Disassembly

Code Analysis