ID: 479063
Sample Name: Covid-19 Data Report Google Checklist.exe
Cookbook: default.jbs
Time: 15:29:22
Date: 07/09/2021
Version: 33.0.0 White Diamond

Table of Contents

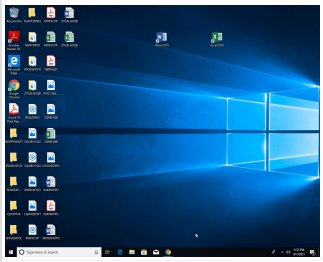
Windows Analysis Report Covid-19 Data Report Google…

Overview

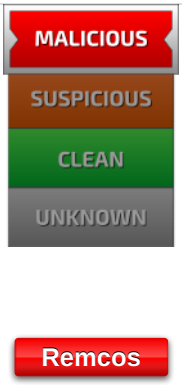
General Information

Sample Name:	Covid-19 Data Report Google Checklist.exe
Analysis ID:	479063
MD5:	704320b0ab5d2f2.
SHA1:	286e65e21dc0ab..
SHA256:	64c32d82c0dd86..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

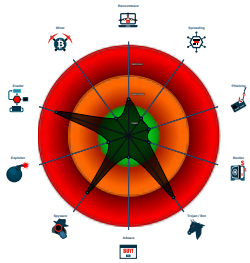


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 doma…
- 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…
- Contains functionality to inject code …
- Drops PE files with a suspicious file…

Classification



Process Tree

- **System is w10x64**
- Covid-19 Data Report Google Checklist.exe (PID: 6380 cmdline: 'C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe' MD5: 704320B0AB5D2F24EC101CFDA39589C7)
  - xdhqeufpq.pif (PID: 6624 cmdline: 'C:\84086963\xdhqeufpq.pif' fqficjon.emu MD5: 957FCFF5374F7A5EE128D32C976ADAA5)
    - RegSvcs.exe (PID: 6824 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- xdhqeufpq.pif (PID: 6992 cmdline: 'C:\84086963\XDHQEU~1.PIF' c:\84086963\fqficjon.emu MD5: 957FCFF5374F7A5EE128D32C976ADAA5)
  - RegSvcs.exe (PID: 5084 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Remcos

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000003.418699902.0000000001867000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000004.00000003.386707521.0000000004991000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000004.00000003.388209243.00000000049B1000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000006.00000002.614438289.0000000003630000.00000004.00000040.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000003.418686304.0000000004D51000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.xdhqeufpq.pif.4a112a0.1.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
4.3.xdhqeufpq.pif.4a112a0.1.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 ...

Source	Rule	Description	Author	Strings
4.3.xdhqeufpq.pif.4a112a0.1.raw.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:$str_b18: Uploaded file:
8.3.xdhqeufpq.pif.4d70a88.4.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
8.3.xdhqeufpq.pif.4d70a88.4.raw.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$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 37 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 domain / URL

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

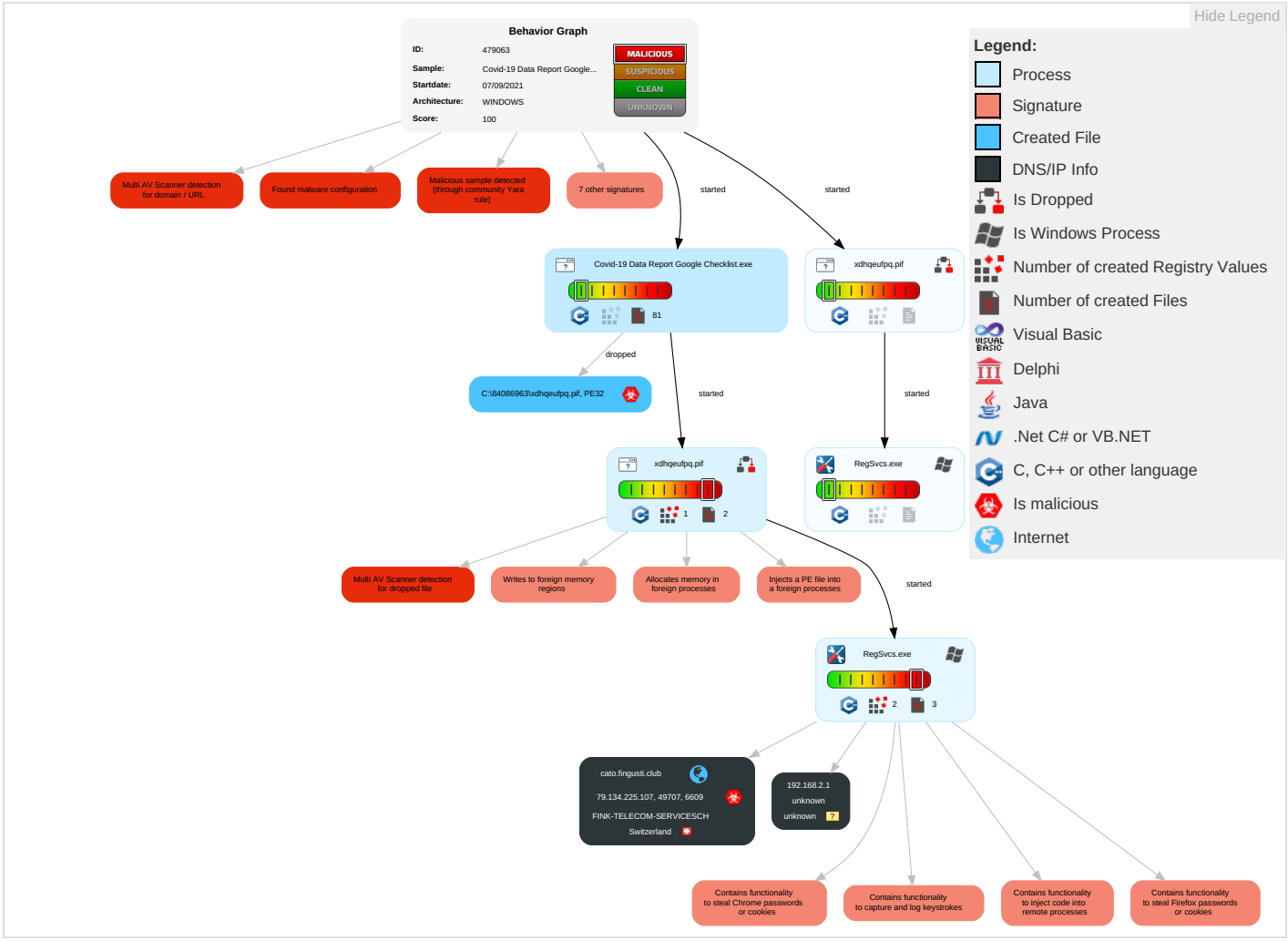
Detected Remcos RAT

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	DLL Side-Loading 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	Application Shimming 1	Obfuscated Files or Information 2	Input Capture 1 2 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 2 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 2	Windows Service 1	Access Token Manipulation 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)	Windows Service 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	Process Injection 4 2 2	Masquerading 1 1	LSA Secrets	System Information Discovery 3 5	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	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

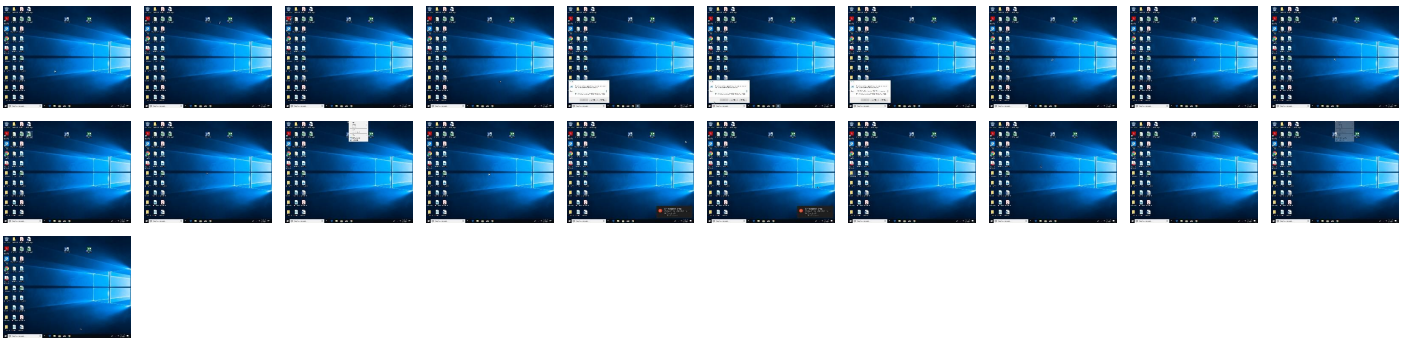
Behavior Graph



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 Google Checklist.exe	49%	Virustotal		Browse
Covid-19 Data Report Google Checklist.exe	57%	ReversingLabs	Win32.Trojan.Woreflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\84086963\xdhqeufpq.pif	55%	Virustotal		Browse
C:\84086963\xdhqeufpq.pif	31%	Metadefender		Browse
C:\84086963\xdhqeufpq.pif	50%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.3.xdhqeufpq.pif.49d0a88.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.xdhqeufpq.pif.4d70a88.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.xdhqeufpq.pif.4d30a78.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.xdhqeufpq.pif.49d0a88.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.2.RegSvcs.exe.13b0000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
12.2.RegSvcs.exe.b00000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
8.3.xdhqeufpq.pif.4d70a88.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.xdhqeufpq.pif.4a112a0.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
8.3.xdhqeufpq.pif.4d70a88.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.xdhqeufpq.pif.49d0a88.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.3.xdhqeufpq.pif.4db0a98.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.xdhqeufpq.pif.4990a78.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cato.fingusti.club	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
cato.fingusti.club	7%	Virustotal		Browse
cato.fingusti.club	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cato.fingusti.club	79.134.225.107	true	true	• 7%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
cato.fingusti.club	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	479063
Start date:	07.09.2021
Start time:	15:29:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid-19 Data Report Google Checklist.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:	24

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@8/80@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 44.3% (good quality ratio 32.2%) • Quality average: 55% • Quality standard deviation: 40.6%
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
15:30:40	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate c:\84086963\XDHQEU~1.PIF c:\84086963\fqficjon.emu
15:30:42	API Interceptor	882x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cato.fingusti.club	Notice to submit_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	Notice_to_submit.exe	Get hash	malicious	Browse	• 79.134.225.92
	IM0003057615_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	Notice to submit_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	Rules & Regulation (IRR)_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	wNxb2V5PKj.exe	Get hash	malicious	Browse	• 79.134.225.92
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	SecuriteInfo.com.Trojan.Win32.Save.a.31706.exe	Get hash	malicious	Browse	• 79.134.225.92
	10UNv6Ul0W.exe	Get hash	malicious	Browse	• 79.134.225.92

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	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
	qQ2SuVsWVP.exe	Get hash	malicious	Browse	• 79.134.225.44

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\84086963\xdhqeufpq.pif	PDA_pdf.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\84086963\afpukhvau.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	546
Entropy (8bit):	5.513325500509442
Encrypted:	false
SSDEEP:	12:0vliPh/DE1rYaG4uTh+mRiMdDyXQN2k06Ev8Uigr47Kgl/f:0vEpber9Nu9+uX7Fuigr4egl/f
MD5:	BADC3BAC3CB07596DDB4E9F55FAB409E
SHA1:	6C0DFCE7E92F5EB498416094B25E78FBDB7A58EF
SHA-256:	DFBBF55CB02264D1791251D6AB8F3F7AA678B9CE450C81A237358E3325AE2B0F
SHA-512:	2CABCF707365751DDF3839C3F2BD0E75721045A2B3050F55F56E6C08E105B68F45677E61A3E752D3C7E23F27A1DE1CA90EEC23A18F716E1AB0C253FE278603B
Malicious:	false
Reputation:	low
Preview:	cpxj8DdE1s3Eb0Xpz6..uTZ5s91lx00N7Xcs2k8cNAy6g8a83M7ToI3Lx80S8gT998uJV4Pf9y370zD9q20z1KyC24Goa4607l6q0w50mlRBhk77koMsV0U9ZJqpxr4P8m 1OTY5cR2J8t12..24B7c0x84590y479B1c26Wm31M9Yw0u2tm61..36w9MY15WBP02XaXhOsksbDS06z1g8l1u4..0c08b7hoX6lys5jb1Iz3v96YfLa7964nJ17t3F6Y3 219Ge7g9n0x4g26u251t547E110TlJtG386K153uZW992U3sc4hQWo2K61F27FWft29342nr44r..oPZ1lu734115txIn5rn86j3nrW53t7XZ6U793o7613g578w4WC6sl 6x3G721W47y6wWBrV242v796oa705YCZ18lkedKC28378397..9P79cn7102F6h14i0woLt07N079uSg366nEC0aW61KA27lzzxiJ209m3eAk7N8324BAD74YQRT9BT587 664WimZZs205rc0TpM24m921..

C:\84086963\arpja.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators

C:\84086963\arpja.icm	
Category:	dropped
Size (bytes):	616
Entropy (8bit):	5.5409688853949115
Encrypted:	false
SSDEEP:	12:8Hkk8P8MybV1Ua8q8NdmYW+qjUKHfr9FdKoZuX+H+cqTTMV3Gu1Vz0mf3ei8/sq+:8Hk5ybVDEN6+qAK/LdKQuX+HwTTM1Z0u
MD5:	E4A5818D0CC191A0C2BFADB16E6BBA6D
SHA1:	1E0254C21802099C6C07937344DEC725E7C81790
SHA-256:	84F6A5D5C69BD450CBB51835054977B4467E9E9421E589F97322551E6BAB2503
SHA-512:	A451C6FBDFD4D0AC33FB030348F403EFD80E26960C66DDC2E34EDD46EA2E9BC3F8E45C75B62DA82D3EDD7A1259EA4E73FC747182BE627C698FB06541295F1243
Malicious:	false
Reputation:	low
Preview:	9vH6oyQ61Zw539A90401x1wP2AaL96QNe9D54718456VoXWM091aoQP3s47029G8b3eEP30uS7b4gW73fQVAB666059ZJKT8Kn52uH3158800Mr9d61HizBl 0t3ky72IuO204XO7D70kc97bY83L82w9p120862KA6Yfm085a849Q4..m8NwRCVlIz1xlp0Et3dG232T1YH4007q4803999C3z6FO80..137b34rS43963d7cq..9Wn9i. .q4B0a29513jylYg2CN52909B62SNr0i9u0w10FotXTB37D2D1Xrj..4S0tmE60p373FRA0OZ7et6L14A5NM610rNH8qbk74i029hgO1Rk5bW42V8JwZJO8bP5xvZ9Df2. .33Z51P70X677m0c93..o967fR3pmuHx1O8LpX96896wwg4NLL2jsEX660L5345H4Z7O31qLBCC5250Tu655k1bg80l5o5yY2SawPY73ng5..b26C23KmYv53o0148438G 53cL23QeSh6Q8TSyZ0AJf8542KvKRmV6H7wB7mr0t47ZmxQ1F18s0W32v2Es2K2s7349s7n60365KIxZ36qmeGZMdDsTEey5DQ612Dl9..

C:\84086963\awcpm.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	516
Entropy (8bit):	5.419775893386141
Encrypted:	false
SSDEEP:	12:igiMsV1D/yKFG70MRMZ+4iqUUPTWPXFhPjO2JMTLy:2r1NE0zZXaV5jOUEy
MD5:	B13F7B0957A4C2943598D93BA56E16F2
SHA1:	CAC7070FE1AEB2EF13D83EFC39F82B38385017C8
SHA-256:	0875CA5488594E1E7D2E9551C6A7E2EC7BDA5F8E84D19DA1E747AFB9539F5AFA
SHA-512:	27D592B6353CA79740B677EE1AD378EAF2ADE86CB41791DACB45E0B0E463B899165E1C9A4B0144310AAB8DFDFE4ED5A2EFC65DDC30B7F1703AA4E55CAB617772
Malicious:	false
Reputation:	low
Preview:	05g2B345963iHk919ZZ9GnHFh9m126hH5F923b040ggvXg6oM4567pbg74lG8gb32s2..70p64i0XHw46of2q4n7c0z762F72d06cmWx8xtu004l713xo1F69m4ny78UF4 Uni8Ly2133V377MNDm68e8992G1o6211LnqR..55q4C19P6Ji049xr1uj1e5Z6913Nxs2118v0I60Aro9xTK7227zkO1LERi962H07nv2RR68wih4Q13B474P3O17m8048 1aj162M0kqM7Jb965N5..6hU7WWx30753ty7o6896JV655Ud9TI80CU7827k46K6B135639Ot8Y6259g70vF1O8vM1r9NaGIm8283cxNJm03VP012PSABIX07Jv5sHlg7Z k684880d3266u6h2HZ8..tY1mt6kq86d2x4giN0dd8X6VjnyYw592kBt222R1Z8r611kK93lQjy42c2nO0S79u0xPp7387562eFh03K913982oyrV878051xYX7D..

C:\84086963\bdrigsrhuf.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.505520204369817
Encrypted:	false
SSDEEP:	12:yrWqGvdQX8Cv8vNl/GL9DxQnAdxtq84tPJ5VgwrRjgjSznyN+pbvV:0WqGvdQX8CvuNlyynAdlyJteuu6bN
MD5:	3BF4F088C97D5358C0EA43F56C1EED48
SHA1:	71963715BDF4B5FD710053C346D46C182B5984CC
SHA-256:	9C790F569691DC42561431156E857D8EDC98FF1AFEEA0E10D5EB1AE4C0C253CD
SHA-512:	84461500EED5A993878564C0B87421774B3C9F950935BE02DBD29F04565F0684111B3609E937C1E66CD411222D6572A043073575B3B867A6D8B00AB136C5DC60
Malicious:	false
Reputation:	low
Preview:	b59S921eH1n1H..U11uz7K9y194H0LI8MCmU2uuo3s2H4spQh14q2Ye811191uR3i1CXyB8T37x0EONH557q2N527s..61AND3J07A7c8nS4yVz71VriI93Y1l9q2Cu2x8 4071l3d93O1q4le7D022914b2O8est4N541HN6P693eD6J9C32..6mAa69549N0XGfX6972J458FGFTc2nd3h229h312PF2F2uv03z849o441ocBd8w28398ww4N8507S8 9032x7T64h82e69la8Dm285..U8aWT19b3145O3VIdn131l3q05afeg8He61Xy32l8NXE9X12dw3iT59lpJ..A3SqLTWK4t9vjT21sUcd257lb23OyY..0t15Sf9882iWq EE4S7EhUZ8ml14E48t5C82hk9cz8896Df4RooX36D4074o165l66r9V4iObw1qPn5E3P7OF8gJS9t0868T3E734DoVa7V0h98f4xj..52St62XtWEAhgViSun4k622gD3i 2lb9lOfRm60390PfTZVCc885jV120I39SP5a6lYBMb8m95v..

C:\84086963\bpcfr.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	534
Entropy (8bit):	5.536234103479081
Encrypted:	false
SSDEEP:	12:IP4cs9rx4GT7yLRX0bQwWEAdTm7vgt7KHdlUARIvZ:qWyeyyEwW3dC4IvUAKvZ

C:\84086963\bpcfr.cpl	
MD5:	FC4F14DEC173BF5B13E9426E52B36963
SHA1:	504D8235FD860BC8E6BABB40488561F3D5F3DB82
SHA-256:	88775FCC858945DFAE71815DDE7FC14ABC036BCEBFAD385FABF86EA9165D1AB9
SHA-512:	01FEA00424B4F83A192FB04AE0038D234D4214621B8E73F5258A675FDF19CDA74EE8C24D20A982FCA0E2EE9707E73B3A72CF24A26F6C975E90E225122FB14AA8
Malicious:	false
Reputation:	low
Preview:	58KiI3D442bIR40s318JSY885n0bh27W9D..5Kp2D299vQ87A5Gpb4lC160l9Z797rcw4Z3ug37322Oa58EyBm9S9aJaYMv1Rw39uUpC0Vp0QkSj562pR1gMFi0B392Up8 5L8a010j9Gw9MzN..6QkE3y54q093F09jg5Jd5M19res0rJiO7007ij1Oc310R27u1j7C4844L8x7n9XD2zy19651P8Du75a83UwUD71XI5XbA6317Sgt7z4f4vF4c9d59 0eK87617F665hvvwK..47Bkyv35Z9t127V17QS34o9y8A4C5adO836J9Cm98..06bJ24s4V1b2qf7352CeYdnv5Y1H6ZU883WO5xBQdWI39U7PYN12cIg583cXC8wMCcY3 3r8N5eFmdz591FS6kb16SL6f89T36f83..22b484ik2i1699O00ChgzDe2l4X6JwaNpL44UO5xo45EO97JN24479371rB8f..902icu2i9CLRNJ20J51Bicc7A7xdR939A XW2THaJ21988..

C:\84086963\bvtxvncl.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.434340036552141
Encrypted:	false
SSDEEP:	12:40NkWD/VadL25qWjJTVzVIGE0q5l1JyRfF8G0MblQOEl:40qV25qGTVzxq5li3ZfEl
MD5:	5332AEA2F5A6A2FC6BDB82B8D57B7D25
SHA1:	8E605EBF5C2A4D10D40088C1E0D08AEBE82D0E3B
SHA-256:	F684669415866AED08165966EBDF9D74EF4B0753583F6B8C1CB62ED7AFE6703D
SHA-512:	524AC046727C4822C8FEE65A1D13A9694096FF5450886EA83AE5B820BA2F2343A32A4EDCB940DEE50E249DFD225F52D4036D3ED970081B52D71A19AAA5C6A27
Malicious:	false
Preview:	66400Y7d702A51728u5w11y142305586w04D0WK267t3sD44..y60i2CQ5c7979vDbYN521DnHp78JE4U5005Gxn715y24gSDVO7COKM7..m0w123tpBu4X68cf9X56b8K Bao1Om9wV54XIc7sbb29c3tDA2mJA0U4x4259946JED555kkMUp6JekWU48n764v2bjj408f92026944u709P21541t..CI5VA1K67MU3SxT9m627d69182KAd104EGX5x 909q4BqwvSr6Kz8qy..188F309g809136..772277g938oSMyAhGSqgyzk324VX937R1791g2q09z..7KL9848X320sxZr7r52qrn7jI2LL..lw29K1f29T7R890ZX8Da7 Gyf19q0eLC..q619igau0qEkTsz358U4Z730Bw556a8O599c792B1mUS6djB0H6C6260IW77227SS753L6H9N38N1D190OWf1L5B6L..1e426DEsS718BCR3BTM5s636FI P2..

C:\84086963\bwct.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.439107527197963
Encrypted:	false
SSDEEP:	12:gYuVI4OCySSfo+bVH+3Znh0gJDx87LbnRlaSTOv+0zH8EZsOqpCiTQ9ATBzy:ruiqySSfrbVH+9Ubfamqj/B+TQOBG
MD5:	2E644D5400EF129A503D0871A62B91B6
SHA1:	590398CEECA298B6AF6943EBF6944624CF720E9C
SHA-256:	EAAC7DA6F8E158EF5E32728C3285CF8DF9FCC9E240F89A449BCC0C040D4A8718
SHA-512:	12B6F07541C9442B31887EC5E316E7F3B22812B929E2A7E42BB905C5D92DE57AB91C0C3519DD5CCCF728109F777E7F3AAF8D52188CFD9C876501B252EC6674D
Malicious:	false
Preview:	944sBp7c0475BK3588b0o7l55Rqym7J2eY2Z8dk3ea8ff1I4sL627VbK29831II1N0988rY852V3i3w1o2v0Z82849XJVm9B24G8r..02p4314IhUN1244..51x5fuu3b7 8849p1T84f81lHgr8Af0A259z7S711m12v6zF86qcNBc5l7c91Q9613n198926e9lm0..s0rn4I8Z71MWX2u72lZ5u50K58956YN5uMERE1GP3451Z4000tq0N18D0PWWx 148fim1r005bv370c4gZk8l5977mk401z1b41o78n5aB3Ns884q903Y895vWA..h2v2403AfI9nY4D2sR01H7S8nv47..crUl26Bd972A1HbQi128Lu5c905syiVg11C8V ob16d1W6o95R15e2GKJ9SN2B0h67x1i837S7oN92ae28T916L8E1675..L57R4zTdkKe6B7Kx7J701T3MNI5nV93s3p6c47y7m0BZC..iLi9..5091uH05645095KUdS8B FQ6H42i388793Ozh7G86PpZ203BZB2v2hf1x5RU0ZvD8b27l8Z7H9SJ4apKGV4274LTyh31Pv6f29tkdI19rL38g50Cb7Lu8l4688R3S1eGVHX5rp2ei5i4p9il6h..

C:\84086963\caxangvd.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	581
Entropy (8bit):	5.464117647486144
Encrypted:	false
SSDEEP:	12:eHCcvQOngypyb9A9EGT5rxU7XazgwNajKtDB6OWm11Xq+NLhu:HcvQOngycxaEGTDU7UgwNajqWchVu
MD5:	5176E0EFD1048F10944AF4780BDB7806
SHA1:	2948F0C3728B80B2BC34A05302791F4ADBD90EDC
SHA-256:	2344A23FC664E82E7241895DBF1651CF0D6B664E0B352300B80D35675A0763A0
SHA-512:	52A6A163E32E303FD2257209C8CB530ECED109FCA3B8FBBF7BF1BA1E43DB152A47F997C36385BD984F6FCE55F8EACC2FCA85A62AA011BAED5C7609CF302BF ACD
Malicious:	false

C:\84086963\caxangvd.jpg	
Preview:	0U077t10Qi4460v2RL4Z3F8B53P6M9p3757J9TdZ79086v221Hot3X4813v25Z4m7K6lq99111Y2F5z0nL040clZQ1bm1E28298K05MOp20iT23D66Wpp8jMx8y38805K7 jg91085w37zO02hU78IU3Np5g2SD9us1N78X56z..dbP4J9q164708N592gpg06WI6820Ue2909nqa082Vb81842Mrbo20e9h00yJs5Sd4Kt5y41096c61FU2zQj720S61 14Mrk37u50u6OV72W8QU7rG1hJ145gDp8R4wTdV9LqJH02J628RL6M525sb9491AB292Rv..19V9eX6Ozy72Ft261p9L5r5gcIW5N7mfF7A2A858236tgc1C57r77LgI1O o6L803SKafCAlSP2T4z85HAG86..Pu0H60z42TPba6aQFdeW09fny9eELv7h23U9MR8SKYm..HnB0395IH6013D5e2..5x1663y97d64on26u6tm06x11c3h9i71U0qy6f 8j13lR917e9f4i41eJ67O73NW6t8368bQwz6p8Q73r5OX5l4544560DGBh7..

C:\84086963\cjsqemh.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.538256434964563
Encrypted:	false
SSDEEP:	12:GVoMayFAFncTbjGvnAjSN90um9BdMryf8Pgfn3H:DyCFcTbjU5m9LMr8+gPH
MD5:	DC3725E9F0AE851EDB710C412B969C24
SHA1:	D674FE9530F13871D69A947EA40FE8D805D2A738
SHA-256:	625EA896AE8DAF6803B247D806921E48CED86611F58BF5719A3072525C8E54A0
SHA-512:	A36535754AA9A89F23E89CD75F514FB06B8AD3734B8F75295D3C90B349F993C1A7206AB764F7C7A377F20200083535F23A7072F29E36CC8F76E3A97922E8A0F6
Malicious:	false
Preview:	1US4nK9n047R43g199fap916mXw8QH2w87hr2oDtc8a4h86t22..0S83090Q7i431tJ2fVsSal204Z228G91a8PTw95y65Fv3w18wS9Y6m5311Y1m51coJ6zS9PnuKg5pG 6y64870g0ir8wB2709G9Evp03aW2Ol2oE1Wf..67j2Iyp7jM9DA743c7H6vs70V74U1Py8u80Cjbw301W3OW7..62j5MjGLtGWJM2LJLsC54P9I6897w6o782dO8Na9236 qGtup46gR2ckze59l79AD1970TC7..7KW5FleE0k0..Z20Mvyq20tz683011eYMg333r1Qc8j44E37II612A..81Yp1Y2h59..X63uN036Y02cy2u1ie5429h8e82N0W0Z 35h6nk7w8s13044xQUc3V9lZC79653Ebd7egtQ3P5g6t97lVKV5P0991Lryh6qn2y51163m4FGX1yY0J51d1Y2YVo2vH0kePRWe13X898..t1v17ar7uq053pN8xp1vSAa kUP574nP233d3gmTC9..

C:\84086963\cprgmsqr.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.496681948912632
Encrypted:	false
SSDEEP:	12:jSneKI0mTllBRV0h3/8sJYTnmD5BTsRSVyBTnWC/xcRj4bY:jSnlJTllBRCh3/8sJlYNsgsTWG6jB
MD5:	CCEDFE91BED4C52056015BA0A1A0D5C1
SHA1:	2102EFADF99180A8FCDD4DF8E45294BB2B661E1B
SHA-256:	96E77C0B86DD5CC9B7AD385359FF909A1C31FCE14DA48156B001A6877E027180
SHA-512:	BA43247150CB3809062502599E645E72AF0DC19305B92C82A69D917D59BDC00078A051D2E46B18DB2819418070ED981F929FA71FEE73A7E99C353BCFC6A7A72E
Malicious:	false
Preview:	MrOk0dr362S366K3j0Q341hf8Cqhgn5C89IGD281L3DQi029uiOf599s7860816MM99IhC1rEQLiX3K9Mpu8QFSHl7K74mb99n2t5c17657M0CsH2G545S4538qiwnU3v3 e1TBHqB1O9F7Zyv1yM6686uo06E7677aKmF87i1cUnS4n23R0M..516379or489u4cT808jP81xXfXYug873611CBf3624yF1h49w8nye402M9E7pe280cCl8EsL4t8w54 Y20km213zx74R8YYL31RXa67CLB5qCH7u4INfK95CH2kdi5fC247f..d9E5Rn..70a46DQ99G912e2A895O2r3OhH78d64m1cCW16cpH6050Ju0282H99q642536z1xs25 U4xwr51c..4lb4s08Tax4gF0fKr33r2V1621MQ52w4o18xyss6aZs41N4f870..f750Zxk29P34vAdReVj5X37B0NiF2738smwzx8yiXseU3I54446LrKA580fgB21Xc119337C7..

C:\84086963\ddbtbulv.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.443797013815
Encrypted:	false
SSDEEP:	12:Ef5Wjy22V9MTWx39JAzm2cqPb1AFeoWCAp15sdv:Ef5WusWx39JAq2cqT1CeoWnOv
MD5:	28A09CC4CC345C7D6E4A956CF2FD71D1
SHA1:	FBFBB038FA71A3842213F9083227E51FAD7C349C
SHA-256:	0698EC376B649131E51A81E26538D966CD07EE678272ED78A907EB70F6411B1F
SHA-512:	37F50C568101B003E87EF760AD4B57F912115E9CEAEA8E16CD3478C4B3F764F4563D6841B713F06C4519BD9FB2CDBCA3E548E646554442CF8FB1763BFF4FFF4
Malicious:	false
Preview:	Yp1x3r88N671yuOAGDV6hTR..1897zK6450H49mhg022C86F12EbZM301tX053G7O0Y07vL5TXt57PB99eU6in37q5e9ZsN6g4N0135Rm6EPA27bxNR1J6081D..83w46P 43V485ZSV84Tq3d90wC01C3O00tqr40C344Rf4gmH97i4514gg7756F7On3in0293K8pz95XN9G4iM1fX5yZWl..vZv997EJ41zn492..288N7pLu63p6V143123mvzG01 96HYnssb54h1N59VUhB8d2481b998n05GVP707gjMB10Q21R263vOSc9d734V08n7s4LFgh635z1ZI2r84031k5c3KH5590640d07507Dal04O7743v9q4..aAe877f58Y 72B9ls50cFFSzdHYg0nh28xKc5fjw2iqtQB2i91ANyT946J3044E23617pb8P34872IwDs576Q599U83U65..J7240v4x5itTa319fGp4B402504V2FCz5jDc2mm9E9j16 8srg9dL0cd256Uc4n387..

C:\84086963\dpuanfml.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\84086963\dpuanfml.pdf	
Size (bytes):	518
Entropy (8bit):	5.533464997492796
Encrypted:	false
SSDEEP:	12:Q8de3lZFNq5ZZzH0mkjYdaiTupE7pjI2FkeEM99l85:nyCFgzQjYdDTupE7pM2ZJ+
MD5:	2E6C6DC67F8592408065870AD1A64E97
SHA1:	B169A212D6050FE7217E16C95B9895C83320E1CB
SHA-256:	DB6E38036E234CAF0EDBBEAE92CEE8FBD0B3AC4F165B4C8D041A7276BF211F9C
SHA-512:	FD0CC7C23F8143AD001AADA95225FCCC73BD178315C8A998941DAEB12193EADCD39E5B64797B4370FDCB9A915826916A22DF887E802683D4C7C3C6939AF5708
Malicious:	false
Preview:	Gfz579q9v2X08U56gXKA1X7X..HmCX463q224a52i602ern8Q4K54715h2H0hy8Q6rX5z865Eeh6p0B340za6DQ70PYlX01596HRW1ZM5o83jK97dwLdvHO4Hk..VLJYh56J2neG967544B64Q9841G7J774M161NU041694I6E0M40WHDQ31N1l16A2hvD1M31A8TWY6TWP079CI6..P5n585C3JyR8I444Kj0T9Pc98WYkXKq41Ip4iS1H0534crIT92W13l0030ECM12Y8pMEB..SgNV11jcVYH4C832NA62iy0638l886579X9..D51wR2paa51196ibQ3LfU8Um06te5Za9MCxvmOViV41e81i8T3903Ee3pituwm8y9A6B7NhPMJX0w58M85YGqx3L186wqdOUDoDKFA585BC32iUZc45e1355BAhlI072B3GR27Z8pbw56f2k8FJ0m4VT..672KYgRCE494e4..GA2X8d59cY2w0Q540InXZ14960..

C:\84086963\ehlstvqd.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.598448622073757
Encrypted:	false
SSDEEP:	12:ux5Mdg7efmzvDeUDljANsuabEALxeCUkAOjWW1o9Wkn:+Mdg74m//1l/eCd91Un
MD5:	CB99859554154D9C87E3581D8224DEE0
SHA1:	57DB444780C77B4EC1233BC6233E2BD313E5BA46
SHA-256:	CE96975E576F89FC2076B9C12A3D98AEE4982D85F6B7BFD718C55EBD3CC46ACC
SHA-512:	113E0D88ABBDC2EC281082413CB43B7D93336F7584D928F45B37A4013D763DE5E8F9E1DA7398698A8477B0F8043C464417A65FD59EB26A8CFF76C346D350B9D(
Malicious:	false
Preview:	59C68F8lVXq4N5k6zDt8V51F4RB075K7X6ikSbsv3iTF2l5730lLQ..0J75h38vR62P4443816U1M56FO78h8bL8H399Zuqi74PiE3o44h939Erh8aS65N383TMM040XIgc3s6N768X5bEZ3Uw9Y6a49rdL0gU1fcHx60F339..361VN9E6w..GAtCNM5lt..qGUw27Yg53B7hrx790k4m7b67124Zf18ct35tqX84bI14IMp856vX568J9V77d1iPW86G3cCdX27u0L242cpc8HQUc1gNI2v12h66K72Zm98r3418iBh2P8x42Me00Y8M50a634rp2uKqG8v5ZffBje88AyBapp3G0JwMmZ0o06v2v8c8Qw17FgWK3..AngLhW1A7wLd96PdJu2l8101zi24SCy236..Q3Az6Wys948DMq0sn0RTa08d6E351yE3pL4LU4D2hz9IRo2pcFhx0q28Yx154ckRHR0F0mlSFAxy1yyoy2D31Ml727938rJ95q773W991..

C:\84086963\entnulrpup.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	514
Entropy (8bit):	5.408371409752931
Encrypted:	false
SSDEEP:	12:7keCzskjrg/oF4JHtbyyWOsRwykl3QLqL+1:7IsQk/UqtvsA1S1
MD5:	0834A11E2CEDDE6E8EF898236F5FDFA0
SHA1:	D90836C711B4C84048775390CB541A15B628EF46
SHA-256:	D4C46C5676A40E04CC55A8391F91751BF5F7F70503F91E2914B5F6CA904A1D8A
SHA-512:	53D51AFBFDEDEA40A1809F4235A2463E408368BAE2F0E769EEEA4AC2FCFFB293FF5117EAF0C2953E05091CF6927D94F7F8AD02F0FAC6BFE9B5E901A9994F55A0
Malicious:	false
Preview:	T685513X0vlE7op34Mo29T9v709fbXm69tS03G0R7Cr5dr9OX8Tn76Ehg36999W400FTY7493k455v2lLTZr7gu4emS2453mWr35c2r3..7e838h..Mw165Mh293j741n46n7ja..8Jh21c8j1eZQ953v137a298z47r2Nj0vbVjd7JC1I69v5qE8Id10xZJ302VN685T4zX85emx84386Q8pJrz3wb401XNIXgx85d3176972548337SZL1wD3M96942w3v1e9Pu..4Pi8z2Ek00Rn8cLN7B62zow51PSmx0008L6er5qX79F46ly3T9h3z633xAZS6vgEPRH24..s5475K7g07a465I514V153U9d5971x73tej6T6oF5uKyF7qsO66OU67L27gb49O62f4g5GhW0746FD11g7a32FwT88E65hqkFZo33cN5K6O2B70E7630..8o881w98Z3N68227jW4096062K8E2a953NPRMtFGM3d181967H9R..

C:\84086963\facqhk.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.601256233916398
Encrypted:	false
SSDEEP:	12:uvrdNyqBAD0eBhSh4D7ca8RIK4oVHovxNSCNpv6CC6YAgfZwJ:uv7bq3Sh4chhzVSLSCNErmJ
MD5:	EF44DD9DA222299AF358F4B51C151DBA
SHA1:	94AE0F3F591069607F39D1D6D1DFFCA25AAB08BE
SHA-256:	DB8BA5A88DD3867FC088EE24CBED5F53DE354FA54C04CB0FFD7F2C9C87DE14B5
SHA-512:	AA3DC0B5189D4B516B2AF918BCD0674165615987413605 92A269083BD116A3C5AE8B4B8FCE346692EEDE060C6A1E8D05E7230AC4CD6ADA5A24F3FCE862A576A
Malicious:	false

C:\84086963\facqhk.xls	
Preview:	1173gJ5Q4io87747tnpSlP780mCm6B7148cKk6ua7D6iRf4m8c8Dv75dBY1fO0099E3794v4f32GX3nOx4Uv3F0Wl543b..ulA44006Hh468ZDt168cJ3Le1t4WFcH4wqR P133..Sc025kaB2jM41Z938Y714895MG4jgH4DMS4wS53RE890Y50..8CgK0..6ZzhUiJi0kS08679zsv7733k28e5PS5tW8005RF9UK9asQ27KYkq959n62Wrr5JV8mGO K32r22o3O2dXC9..E25U50lbL7MO77u1Ptu2P3359x5b49nLk8mU3091wMDjM89fEYl5551Q9..h1gf5jJY0alA91b14J7DV7261fKA9D2yT416YA39x698jeNLuFW656r oIMV92S9..8YJ2h8285d1..pys1RROt1UT7p0UjAi4Cs2Xl0D4R6mlb5r62byv1O5Ib0vuyrY6UaVonC4D90sv70mp44m554a0R044535Q6qzo0LXg1y2uf2SYfW057wog Z18t648N86a981qA4hw16IQD57EnAG5eo77Na9F0Mv722UW15U8W103W2BVo46jp..

C:\84086963\fhkrwrwh.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	606
Entropy (8bit):	5.446862383014172
Encrypted:	false
SSDEEP:	12:aXbcvcn6HVAExpVS/S7H96zl19AsocbCrg5Vo8bsj5Q5oWMdnEEZ8C3:aXbcvw6RI+Hm79T1Cyy9MMl
MD5:	60F2B5F5B09998A3051134C6DB2DA917
SHA1:	5E228EC1F5DB6CA678A2277D444D203022622366
SHA-256:	27661CF82AE6A5BE2D83D0FF76CB07C07682800B611090CCA4A7B9FBB0BC6FDF
SHA-512:	6D8880CFBF1F12EC7ACA097DCC46AF35321271E7E8D8F1E3553BEED3ABD12C6B35E7464BD573E72A30B6320E86D90EFBD922B0DD58774B2500F709463196505
Malicious:	false
Preview:	f0hO6Ge41t4Q35aS3m7g9..3Kx5m6m5x381F0d4gGT7iq43Io7499205167111GOO24RDz9s3A18P3..799Bguw6h901256Y0zf023q95016i597Ob967XS905091Ky1I6 28M72e5jB3I5968G1NUXvgaFt9..vdzM826uRJg910B763M463G6068Mb78G348968HVanlA1Dsv91q39Z3529h6FbTf4AmsuHB9S5LPdly9Y1xDS930sBV37X9z8x8..f A37q59845ZK1l47mj5GRliF0b4k4K2162yzg6E0F5091Sm75Xrr1Q64MZp318mX145V6G3Z77006tAByTg98cJk5ro581..d94f168EOulRuxs4Gd0057Tp1z5ynI8f..b 5JG75Ge6c6p2Iv5k8952SV7M12q1q022QGlw7xOKhX1s817bAS0Uch52E..6803087hwr4y8uql7wJf944FcT0mm6c693F98uM4z08h258T1Rl17199a6iw41tY02Plv23 BxZ3j7MD176VK4bg3UvVQ446ds7456U8Sdu12u1p9K18HDBD0w6p10H78911KsnNV552MbSL7931110LlO93..

C:\84086963\fqficjon.emu	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	data
Category:	dropped
Size (bytes):	197597108
Entropy (8bit):	7.092598836337755
Encrypted:	false
SSDEEP:	49152:aBLBnBPBOBIByBTBzBCBbBTBZBSBCBABmB6BXBABEBJBtBuBZB1BxBgBTBMBbBSU:e
MD5:	48F2E01CC5284AEEA84545BC2DD28D42
SHA1:	21A35E7AE31326BB947424629D987AD55842F38C
SHA-256:	E56192FBBEFE34A1C3D2A685224D3AF9A17BE3F02664DA5859368068FDDCEBFB
SHA-512:	15AE2385EB73A6D1F5EEA688078204BDE4D0818D4CB3737A5F50BB2FAD5F301E7A721EDA6D727227FE75B2796C450507F1123A497E6D65F4325C0C19BAB8A6D D
Malicious:	false
Preview:	..;..>...fN..S.,x.@.....?uG....Wq.d.bQ.Z.Y.H.....d;..mns.8YZ.}.1k.&...o.....?-fd....X...PF2...[>.r.....=...K.nLd..H.*\..L|de@.#>..Gkw7v2.....d(.....p.$b.L.....[...Y...M.{..b~0:..... ...#.c.s.G...q.FX1.&.N.5r.....R....=.O..L7....7.m.i.Ls.'..*..\|.@!....!...z...x.JP...CcR.n#../r.x~,0B*.3....wy.>.... ..2.A!.....Y.....$..7k<E..g.....].TB).....y.J....F.Q.....M.y2.....H....a 1z.*.@_.y.=.l..*yW. ..a..g.....M.6.R.u.8.7.W.....6.a.r.1.1.C.4.H.g.6.1.Y.8.4.....R.".9...T.....W.D.y.N..\:q..y.Ix>nb...h..,.E. ..X.....Uc...n.....<e.fnR.R;..|D:.{t#..3.#hwK....o.0.r.3.1. 6.Z.5.f.B.4.L.B.D.8.7.v.7.6.3.Y.3.9.0.3.4.5.7.S.....o.X.9.K.5.e.u.7.9.R.1.1.....x..n.P...cq...@..S7}./.2.....:C.R u.x.....PU..M.^C.....Ft... X....s.b....B.5.2.6.Y.2.x.3.t.C.u.A. 7.9.C.1.H.h.m.Z.I.0.2.m.p.q.3.M.z.k.8.7.7.6.S.....1.y.F.9.b.7.5.2.N.7.k.7.4.2.2.1.v.T.0.T.M.M.L.Z.3.Z.5.4.K.V.I.n.0.1.9.P.....r.0.z.D.Q.4.3.4.6.8.4.6.E.h.k.l.7.9.2.X.p.A. m.9.e.5.g.P.0.E.3.2.....#AO .4$m.C.pi...

C:\84086963\ghmpg.dat	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	521
Entropy (8bit):	5.462884504661737
Encrypted:	false
SSDEEP:	
MD5:	ABE809BE7DE12444306AB93851729A3E
SHA1:	472001DD80F12DF34E6F4342607A21116C57FD5F
SHA-256:	5E951724025469F34BD9378105462EE4159E25DB3C469AFF1A0EBCD71D588734
SHA-512:	3A3A59A908903E97BA9DF9C8FB9E0282B32FE97BF78C208F117360E355AD0EC2C3BF8206659DE1CEE8CDECD559437D47EAB6AD3E48169497B771D5FA48A4DD 11
Malicious:	false
Preview:	a081o263Cd9yWA0v6rjs5DM5Ax08wS7yb9f91Y89e1My6587Tx326I84XEwj1q8005EnP7o4A98K9sGsY8l2W13n0Y4Vg4352wCd7m3h0ExaQ19V87CHO1Q55c3648J2oe 847BeGTq6wmh745U50493l5l3..w6W0868v3Ou793l2l6zmzjzL4F548qem..58caqS6977ez6TvZwAad04828525JjIy4lNYow64446gu400G0l1y087MY5pYExp19tsQ u8z4675329276RFt77JO70po0wKN542q5KuL1z893PT56SK..ywWt5qo2V2r83rggFY249Z563f0809i4GQ347ZD7bY77675O24U94584VvMMzJaLip55LD6vKl9cG88B8 bsH4xkDQH73K9302Tb98Gu2W8R9044725u1hb936Nih96Fc64qoL7li7512FXxw588Q86..oF6o22E0409423H4lT2d07Gh1k1Q30545fh385L05Q9JPbg64M87GgW54G..

C:\84086963\gmktoect.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe

C:\84086963\gmktoect.pdf	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.510300564049379
Encrypted:	false
SSDEEP:	
MD5:	23F74D087A46EB7C37FF35CC770DCFFC
SHA1:	9A089C9D080C895ED88DD8429248E03C87974BED
SHA-256:	94B760BF5898B801B1E7FFAFDD0C2E0ADA3BEF8D250BD15DA7C780E79D05FE6F
SHA-512:	348F9C1971F4DB32768BE2522501AA5D7082ADB434710F07BBE4C5E737A30E69D89E93306706F9E1E116328BE9B4B5F38D21E8544C7430F0E13E9781623E78D7
Malicious:	false
Preview:	3OFJ60H5Oz11K3x31FbSc75023mXU6A7Y3l61dZL38w7OeA4428T6..2ZH4UC86924y972Oj4t6rEGfgLbIe6z573697IL068h5sbpTvMVjj6X9ao2L9j0d44zeUGJT1DH Do7PhA42QXoB3a3mcD3o7zn2e7clK6q1G811c532L31bX04n5al7hF5..J21MB51622g67RU9v6D485..7w544E568862iLC1A35g4Ei81B20Kb3EV7i77D6C50J1u00k3 Rg9yR9378s32a183i4d6sAGeWmnXnP0KiaD91ZO8NFx2KuN16gKk526G2E9i1gnsw07m648697qZ5kW6Y5le9D94Olv..39p7LLa24m3CSg3m2i5N9D62f1c81190l63E6 rUr77d5B6K19ew7agde5K61Yes09..I646YK28kY2925ttTqO80706YHr5o60k3v07P6f4IL5FB7t0p782Rt45i1151HY74V6t87DEpJV5Ee683N9h4B448r910yf146..

C:\84086963\gnqknrkuff.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.431892714534565
Encrypted:	false
SSDEEP:	
MD5:	59FD4C0AC4EC228EB46DC54D4D05BABF
SHA1:	E8E34DFD798A8EC2B13951AE7189979A00DFEA0A
SHA-256:	37489AD0B39AB133E569237105882A0E5130E308992F6D0E10F7B3E363D045EC
SHA-512:	CCE2FA1FD16B09F492E648302B575A2D43CC26C46769D2068B089BB0029CD8746A2FC2DD52FCBCB40CD1DB34D86EE491A593F8194B42ADBF49D85A727147D5 C
Malicious:	false
Preview:	0jPdEFmU4fm334T0h6752219GNO8o3IC29E49P82oMorS2nDS825rEHTF221S6532bsC7318rNpVW854vWHl944336G30818lPSz25em1HB..2Gw22O75Y78 00e693n7aK342Uj8Q97hK0506P5at98mwQ6960118155oo588J1Y7z4l9SN..o9JE6R79i9T0f5m36f9d74hgm4x2mswt8Fi2X155q96n9tJ3g823ow7Hn94B2ym29iB8d 7f6y42R5WE42bsE3M65b1f3Uo82PyJqI7fb9nVjF6X13E5NL74D0D480j7Wf82lt2K9R06ZCzbYy4Yd..88q2g9kl3J3K4xC545Fv40pu8cF8N939ADFRqKG14zZ67m18k x5Eg6ilBo54H1x3jC8NF71560P1z4l4kok6330z52888K84a8l3Q5V71Qz0I7DP960F8JT9Y5n8l4EIjv0GU7P04f420wt3V2534..P43f482668KV5z10714o7..

C:\84086963\gulmmhfj.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	5.454725356689082
Encrypted:	false
SSDEEP:	
MD5:	678ECBB89707E9381F6C13C2BAABF8B0
SHA1:	56A9680B0C9B041F2959E2E1113DCC4C4FBB3F88
SHA-256:	8592C75AE2A7DA218FF8BF9A573143E64C88709A8A9AD987F018621B06B1E0B2
SHA-512:	025CB65C45F60A6469C61D592DE7D58514FE6D283E824C7CF7984931BFBD4E6299521CFD7D7EFE08DCC734C34EF958775FB28A49A1FFF3BCD11052E37F69508
Malicious:	false
Preview:	d4055ivyqO94W0kQ838KP48W7CT4939ZERd50953t4sLcX402999FoAb5973btv581FG96S1WH2xB4502O0D79L7J64l84tT542Z1528jf..98Gm6I49..x0JX31hy3k72 GEr81215Um9626kQ6sqO60h0L520i2L8n9p14f6b0v3SMN5H3NIHdcs3044zP199C9zaUK4649T5f57..891124S2g722M09469779KiS0S71RD7iz3F52w3qpwvPz1259 q16iXcoh47g6J5AL061Y01TV28j33334j7z8RS72Bu3x1aA10RZKaT9t7MU4Ya9d099C998ayA435V84nWb4K4qTL..x23Oz2wf511FWO8745WEAh1ilU1NYTS74f76L6T Ff53qC935Otbz6u2k1..p2d26fLM5J2w5420t0q0343v43B0r4f7QM74Ta1RiP4Kt83LnxVl2NL67g2j64L412Dc2w60kCLR65tV9v1Ic1298J35ko4Ju3o4701SbDifd4SIr57rEK..

C:\84086963\gwqibdlqs.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	547
Entropy (8bit):	5.580061349750094
Encrypted:	false
SSDEEP:	
MD5:	6369B9AEF7FA372655C522998BF7C3BA
SHA1:	B377C3D756383F83270A126BA76DE48BDA81ADAB
SHA-256:	49383B9EF5A52AAE781EDEFC0E417393C5BF94766326280BBA98F6CA1F828AA4
SHA-512:	4AD0A39D28F603B47F38223ADDD44DEBE50696B5AC1C3CF2495689F9CD552F40B186B43C986F840BC91331EE91E52A7B9A6BC28F0035FF31B83F3AD671D91E9

C:\84086963\gwqibdlqs.txt	
Malicious:	false
Preview:	19j9t391Y2WO04XX5JCv1h6R4w0f0WN6it088tHD558C4yaqi7is4Bf2ML093r21Tv0vZM7w635yU6GowoBj9l6K07RJhQKo6KZ6wl15r5270f7Q37V6zfU8j2266T9Mh0 0D5xM7dQ2H081220iJrM88d..wh02qhO34ZD3F2cLd0t592Hs7ZE9I2..e05C71J795TF0jT16PSD70lRqv10ZLGx0d8yG7nC9kD8C312wUOeTxnLV9451X3N30T9780C2 j6D27v56m0r8876g..71SA6Bp1Yr8oOLHlDN7Wc34rb62Y7OsC01uU6BYRUR1O0S47pNRr2mKTA53Ci3pt8O04q8x7B6j2B3H1J89m818EPqN56n1oT9SezL3..k81Fh9F 5Lf8w9YMHiLcUz7K330W9w4gs6W..0MTy1Rzvsxa8Y3G141ND22H0x4k9S21247Z472DF45324e522P059OZ43n1Q70g8UIVex6do7LJ860sjl7xXf35r5dPq2s35X7Y46 Ot441w1QXp493A54OXU8r4a3t..

C:\84086963\hdwv.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	553
Entropy (8bit):	5.527928689562825
Encrypted:	false
SSDEEP:	
MD5:	F95E0A74D1F5E310381CF73256A75E8A
SHA1:	D1BCC351C5D704B4C2F320F3BF1189CE4B4CCA43
SHA-256:	696E60A0E1BA16CA2DBC51046BCFC10BBB7FEB08E22775DC3291250870D4D9D2
SHA-512:	25F62AD573A4BAAD9B9994B78B8C02F5D5D0D938A938CF10BC47288F7DDB985936B751E63E04009F2BEC18E9588B40712221FA81EA6330336AE6ED254CE32E7
Malicious:	false
Preview:	V752468waY5v05y7dsQ7d2E8Xhu917..3VO06b9LEX8Ib61S2J7..7H94s4H6z3D449Qhfn3O15Af4F8Nh9Y66nGQHNEPS7oQ0bWjx6TI1wC7525at50b94632N2vxP80y SM15a8nO06..1G15609610l598xOs0x..1830Sjof6747Hr20GZq31d3h60oVTy2v0hEy5G8J57saavxe56O9334XV8349rTo08FD237n96M206lTf1lT7Y7d0e40mHZoz O2d93nENTkQlu31K4Mo5l2H6qPo1..2G95414H1607w2..8Z3K51484M..6k2G632hi8k9h4VmG4051T2HJg6Agk9KZda20Kf7Pqw5..75B3KYM7XmLV1Q3Q368VRS7i3I 3Rg47L8ELI0UQfg767nrZ0c71wh0k467mlX183A51SJ57j3AQIVx20b8O3lZ78MQ1Y47J..J219cfVBnV751560K09yptZN0D5Oa0f4eiQ..43x16swxDG69276F6AM73y q56z81AhaT92PnzOVd1Mi6z2M0ip55k..

C:\84086963\hfohbsolju.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.488399112677618
Encrypted:	false
SSDEEP:	
MD5:	5250E9A9314FB47F79881BCCFF36E2C2
SHA1:	B966AAB8141F9F1CCB5FDE5FD15D42C588ED5295
SHA-256:	FD8F54D5C1E8739F38D0F08C1DCD82DE8E1E2A1B5B672492BA35F625D22B753C
SHA-512:	290962436328BFB781EAF51188BE5ECF7BB6349D8CE79BA0D7EB84E6BA2C8D5C3047415E69F38F1961E78FE76A9AF2ADE8B75BAAC1A142304274DF179E1CB28 0
Malicious:	false
Preview:	2r4288IXS3V16l78x4w36HL5c02itUtqfWLZYS0x4P16239p88u71n07s69..cgvt3b4A34539..56dG1DCi06Y1u3HRY4Z4789429P5E7615VN2A058aCJg11xrYpXR3P SL7Y7164T3U6994Qp290P7u4T4309i257m4G65m0..6rL2G3qg682P20i6536zqd376OACyF32384KslHKM6bADGf7OfTH002pXZ83R9n3i636R1ogC1h2fco25l721jPl 9q0ap73E0wtO4s7u2v..4cpQI3840753t8Ke8Pa0nh77u663VlF4O5955S1qu5y..C8m9V36jCb2lY7WG10848m8s8w29tQ14F41e..I5i6tO5W275T6lZb7q1fZbUf8Gr 8s79831KK3K0R4m7c4j3s6fG233b1kR772B88i68wnz876p480Jv1XlyxT9h9XX6W6873of03O3zz25nY801Owq67ad1N371T3djbTB2ywe3Vhc4..

C:\84086963\hnhm.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	531
Entropy (8bit):	5.43831352703004
Encrypted:	false
SSDEEP:	
MD5:	3EE4FFD172372E6EBF0B9CC05FA574B3
SHA1:	EE447A5DBBED57E86059C33AD9330F63548A5120
SHA-256:	7DCF83DF74DB0173EE3CBA63F61A560DCE2D40A3F7BE552B902199F0BE10586A
SHA-512:	E38FA5BA8880B42A22D8C88A14588980AD5617117EDF3A9054F9B789295BC9B5572A8ADDDA2B0F0F61AA024BFA1232F6529D7CCDDC6B4A3306BAFFEFFB5702 E8
Malicious:	false
Preview:	7V9Lz93t4ed21FjuEY68sqj3N8K5ZI7T665545D60LO6OW0DAC5Mvb990wbt698qB4dzD916m37y1Ipmt6ll79hAt708i6sT4N8U643p8v0v2Se6703Ix6nN3G8..q1ueH dr9nXuc3O0H2G7TQ189c86HQz35532u0V2PvZ05n24D9A8P96BDy9T8875yi2KG6Jun..50MJ0759e..o061qE1eOFG12h5O6G..954w980841zuK8H12dS31856R87t4j 6g11X..r812520Q7h17y51817SA9V811156690B078559y7EeYXS190060335BD9705rO..5dDgh02p188Y69067x3p12..11S2..007TU78ajI11L7808068ZfEvvime8 29OUJ2IZ529LkQ8DD9NC151Bn0W71Z9T263l6o1D2PGx72N76LJLrKeW50c9xfG9Z4i0ULS53Mc48QPH07d64a77527o3ZIC03t8PtzJeU2iRdN78Ih5T8ey5584qrQpu2 20rm11Rds..

C:\84086963\iiukcjdl.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.419640087050579
Encrypted:	false
SSDEEP:	
MD5:	28A9CA32C49E8D55B242247601B7FACE
SHA1:	7F2F61FFA07D965D31C458B3CCF2A84CF89D4854
SHA-256:	20089DFC3B975AD1A4935F60EAFC6B23D107D958230F40E8C2B21F06A111879D
SHA-512:	91B156324DD82DC8F98804AC5D83F17E365CD651297BD1B827822A31B71013178C51227F0BDEBF7286488913E91C0474505E754A28777DE84EB14F6C5A1B92F6
Malicious:	false
Preview:	40Byja117427L70c796w0op..c32dfIK80Yz5YH224o6J0mQSHV1Ds5ien3178bn1bde71f25Y326391R708tBGUa9..9HD337S522ms42b1z0762G0U9vYU64re814FAz se99Jw924y2v664uCU7024U028Hd930I8V8IbNX1ZD2h72TB2..xNo8Hmg1835eI925740i2PHf3Y606T95X44764XbJR6ZM7U812FM88OVv5Rm68KWkQC02 DG9U717635t..3753155u..C7eq29349Gk8L163324210s5S8GAD2Xp5naF7RBT8z4OhRK5E47v60i3R42..L40y62LcQ4A327r9281847KfOU400090WgB8z..VJ3yO9F X42713D925L..36T2v00J769yZS8rUsQpO1H01O4352cp305UAb49V5s4Zo2Kf05CMdxNU..XH22KBAl95470892xJ81l5q1kFTjrU17G2Wy07155HH4M3515K539Wod5S 3cpRp07w6T262t6w6B279bc4M57174237fHr7nqo4O48949480ahlCT869F..

C:\84086963\ilpgatrp.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.525847487225451
Encrypted:	false
SSDEEP:	
MD5:	B6806E3AB728CFE56D41F1255EAA180A
SHA1:	F2DA1229EBC4E007F7265ACEF559ABF3937FAC12
SHA-256:	4737DA62BEDC07DC857A87AB00A59826188106073 91C448237A6B01168E5AD40
SHA-512:	83556B7FC555BB96E1AD4458992EEDC695F61CF2158AB605FF7A9DB051D0925CC69426E039CF3D74E6A086F3652F6DF96E87F37D3AD82A7C138968139822C312
Malicious:	false
Preview:	hAZ2wdVH101S9h8v9ic2KK73EWFKUU1e04O0872477E4a56fB607R7y7h824c30g87X0355B8520297h059c2..686j01E7la4Gi5mU2783q50G71rb164i4571k1HVf41 986Q2WMAn445mFWaaqZ3y6O1xptSx1cXjf9H88S967t4ut3jZ38m44tR629J9902U72rXWkb758H8tUN13P308V..81Zo999v2..LW8wdIK3run61620..bsR1D1J73YHS S25rH07OfZP8C9s..2z30Prc6pP7EcvoC8W8R06H4h6df84m88HFD70VQt08SGv87W53F..9ZhTo3389vQ2sY77f8PwQI7FaD3G69gQqDG66Kb5zjA9ixvM9QhXQN7WPB1 I0IC8CtprUmM4DveZ9w17sb68..1Gk494K2MH9734f69OZ5x3R52u7513dXm2039..vyx0Ud72nWGHbX8E4u7nwwZcg2313K806QT20G401u95b22T06GD..

C:\84086963\ipontssug.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.526772857335459
Encrypted:	false
SSDEEP:	
MD5:	241CDBD9D0E438C83A2CAB69A991CEC9
SHA1:	389ED4A1E58E5F4CF992AAB0B6E78A086BBF7AED
SHA-256:	F552A05AD6B5B29C34114A4658FEB7D84B18C446052E668B46E7F9A239342F2C
SHA-512:	15E38573B7FD81793E9F4EF88E812A434E895D9986E1E18469CEFD9DA32C212907F051BFD8C4E12367E6CA86F330E4ED463951E0A1ECA9C9088C830C76D7712
Malicious:	false
Preview:	c68VCQVRN9U8hI279AGP7HA744u6H5ww0U6i3e23v2mP35sb2U9A95YJFv1a423mW..bqQ84P5KqUw7OpXLx9u7c083562g9HC9896368077Z517FT1iXnUn fol3c1gU6e867hT14V7..44t12H7Xb7k..2U6M581X..wt616hIGM8z7293gKJYMxIF2jqlj35Fm403AYxDPS46yN4VA148V874SI272189ojgC3754827pZzlyG01wT0p 1YDgB9H6f8xmDTWh1555vIoD549Yi263LrE45iQ732J98VChwd03w97852g6..7P2Ysu6I18POTAET1ngNS96188u3J1057ERSksCK88Hc5t2E70468dNRSfk2YV752Y2B i3F5B884RRn7J5684mT0E0VNRgv59JEb52hUl907j6M06y8Q3S1..52P6780J2p4JnB7u600DM189i7p7fZh3O880rTS278g5a86WZ4I380U89412Q6918L975NiIZu5GJ 00h4z1CGA6V5VTL0..

C:\84086963\iqfcgawc.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.576922223356181
Encrypted:	false
SSDEEP:	
MD5:	1B1C5C629A134083995DE4E672A748FC
SHA1:	DAF58F88444316D6B68552D2FE5B7FA3C2B2653C

C:\84086963\iqfcgawc.mp3	
SHA-256:	07F0AE3F0A93F15441A315B4C58E5609DB9963180A2D7722290683AF53C9967D
SHA-512:	97ACB9A5CD8990A4D3D733F20F93AD53D7DA1B44AD5803411B9E72D6C64ADFAE5C9C4751A680DDFE13BEBA7189D8CF40EECEC2CCB7983BC161BCA3835F2D389
Malicious:	false
Preview:	F76zGXtj9D2rnKrFw2B3r264M90mUff1792EH3..14gr151xlPhUX8pWDKZl6R7BH8tnd3L531Y6972lQ8k3L9VT77kpaI8..8Ua1Wj84vDZ4dH76nc851kswSH7RY094F35K64z0pKe32idd..96E0a74zAyf405xG740182i505U2122RXr03IHbp34V494693644e3utS2ynC3Q5kL944H7VE..TN22vw3h1o74G5y1a4w62wN4ht68YW0X40dT4t4115BV49MYiSX4uE673658sW5g98HofE2xbSgH1h1ui5Y022..58hVK90OMTo38jC45O9HSy8h5GBXyCA8vyqm9mN4ksi66nCN6p1L1V028yu10NyHgg05l1lidY..yZ430G70imd88Y0Yxl1xABac59e8XM710sL05b4T..9t8R428i0Ko263Ap31239d56g2cJ11C18VL7g62O010s6q3487fE3uwIIX5yWRq9557bU9Se860H82m5DG7t42Z6v2CS51M57UdO05O96Cs8jK5HCF2a75A..

C:\84086963\jicbdmo.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.530307634342483
Encrypted:	false
SSDEEP:	
MD5:	2E93E6AC6A7FBD1199A5BAE64F1CBB41
SHA1:	AA1A4D3C9360360DA75DC57D11D6D9AD9E16223D
SHA-256:	2931869EE1FE06482D3010B08F6AF7C146E6A5D50DBB82C68DFA3937E8DA1A80
SHA-512:	CFC3B3EAAE299FB9AE042CC446DDCB45A6BAF7C56D82CD00F8F843AEDEA825600B34A26D0281E3967B14CF9CB089A8CBB6860613943B0768DEE1D375FD271F5
Malicious:	false
Preview:	Mmjx2H8839955eFvu038a7s58LA6A3z24v971jRfTMRfwmW0Ui57r18YUJnX7Ri5fIf67..CYr3588g42xG52324K9XK729K9wKb5shJk76773lvqP26h0SrUI61ePb4990Z4u8b692PE7bMgg001ZUk7Y158272Q001DwZ040..N38AvV5508HP8A687658OLW720vyF0G1hb65z65x2X064r49d24r478q57cx5c44jluN7e2j9TMp69itr33c90152U3iH8SL56147Q643lGFuJAb8T4v58J044bT69362QaXtbF993V1E43s..207gkPPJ967b0505MO3Lu0J6Tsm93MXO5T14AyDW31CdoaL24xZ1pSpQ4K55RvXnRTT24dTK4DL9q6oc58s4323678gqsXL9cJROGFZT786IjV8hjw46X5e18rn8DHS8E1m4Dn303y..69MAm3HS6gw741dm8BG720n1b8d283PA853720bIsZWy83SWt7Z8PH15Yp..

C:\84086963\kbwqo.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.4373930643360024
Encrypted:	false
SSDEEP:	
MD5:	76E5AB326536B0E07A406ABF89BCA651
SHA1:	EFD5A3710F7929BB83039E7FCD3246873C0E9F15
SHA-256:	1BB05DA11DDBE5D12E27425BF9EB86553F2389CE0B8651FFA8F6738EF428AC12
SHA-512:	7CB2AA76D3D280C8D529C4F229BA8E11CF7CB9F08787515BD9EFB2029A7BE6925EAFA2AAA17227500481D2ECF65F027743BECD962484DC7ECF931AE6F4369F3
Malicious:	false
Preview:	j911S853636kgi18548..0cVdc3X..T3Ay3xcd48e5J5g9YnW10cr6085c35..G1j5629vea6946109Kc592N69f38J6677koN1S1wK5uZ429sW83K7t50S8513222zNoU..N4uWXKj6C25Ubb6B3JSR0N1fJY8y686rQ1I6Z2F9uQ4..5r25gY60213y6UDE..3w541Q114r240H6P5VH32Tm3Nh52Mi73265S5473Ws4430qck989em2PX2Mr8o89c8s73Oe7u1vr2W99f9I89SVTwboTbK00H03xV8gkKD42679N260I77D3RL..3x88vHA71m3N4z68L1883Y38f2V12Vb1NL1491v2EXyF7Qo4b07N0oMjWVw3ombhlZIB9zKI92WJ92uaL8KgM0244w3698c..16wEl2x37h9JCy2917x2va125W30f15766e44rVuJaN84ux4a85379NQ65Yp830qUk9VM8ex4WBM1j43fF0WTw345Hw5q7KstVR21g1R..

C:\84086963\keiv.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	327849
Entropy (8bit):	4.588913972555565
Encrypted:	false
SSDEEP:	
MD5:	C0A840407476DEF688DC7ADFCF31F4B4
SHA1:	B803063D8AE0CDDC18739E7D554B1A81AD9CD3B0
SHA-256:	678AFDFD84359BEB5FB2267A1B62D2B9CED9C0788DA91FDCC0D84F09CAC9CC17
SHA-512:	DCA4EC69779B83A6A1D9FA64219642B780A2607306C074BBE30C1E211A1C589FB42AEB9E00251130F0E42A420421C02465B01155911D696BDC4478DE7ACE0791
Malicious:	false

C:\84086963\keiv.bmp	
Preview:	291771jF1mM28850Pn19N8598E599790tMu20W0iDvc5O..nqc1137c708s7d3l9J5jk82c81juT030bz4sP886GKpkwo7Z711Kesc3c..F368y7d110392rtL6LGDrQwB f152841x7297Ru6142BE9839n4omUl1..oi847x8341tPW68TBY9KG6j254Z7guQo85ux7e0382NU9M2UK7l5JqhxSN3t9036je7B4a642ocPda15..6u5j4P376kV6dbT 5QtaMKC10sG7U8513..7SGMgA6F01V55o9LK585k8z9Sr6sI8mh6R092y270LL4Bz3..5b1t7RnN15fWtV1I9ZHs43zzR66d40WR8h64w6H564X2OGJ5..8D0sP4721A92 9837x0011d35..Xm1e90Be82WyXgP3c41..9N8VCI27fsdm1yL7nWXa2M7AlNCC79WQc72L52X87J5T5mxO126Dyw4l3nD9w6430do..kB590dNq98S8yT76vqXVbv0O8C 3o65p4I5M50j10v7T90055K83WR1F2d6Umwf6..9194r2l1x5y57K85NqpO2S1OEtdtXx582nA60sM..v8Na54i2B225ud02c6k41cysF21ph91545WRl9HT12y3m4125A 0xJk5493mpN2966S93zGz5M22..2k33r9Px0f6K7YI543KpU2V91s1616n77c9V3752m1Jj3l1745794Ip5N9f2..33zay5g1I09604P64a9v2N667W3K769IFMAa959Cm C21697FIM..0lz30q14137flE6i724oGx..9X0Wl96480s65m0R3l1W648QKy9131LzK7T8363905nPiU01405a3UM465Zdp4G146Qw17..N13l085Uk7Fd1z9iw6pNM84 652x4072ull4se6UE37y4Ng5sHR4xnODS89161ir35uNQ9hBTrEzKnQ1l30..7r750W7YJSg9591V8228ztaZ6GgO9

C:\84086963\kveisjkad.xl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	611
Entropy (8bit):	5.502498007400371
Encrypted:	false
SSDEEP:	
MD5:	6D06ACD34425A0D457A583A00C56442F
SHA1:	5974CB401440F0DF775770E2D26EA95798F958DE
SHA-256:	734EE4299A7971D10087AC9B1FFDD811F3E7F53F5D7EDA129780FB11DA8AEF98
SHA-512:	717FB305C4DE6C221014C34E569DB5D348B8B21793619E034EB9909B462B5F967EBFF1E00707B216712B79FBBC8FA77ADC6E587ED0DBFA14692F7F71A2FD81A
Malicious:	false
Preview:	tiR27h1S9290W88zCUB5o102V1Pc5A186Otgu55gV1186s4KBAsc9N34850895WJZ8VK99vt88W645gz..r1hI7z6V7479HK0G79DeI1lx61f6cYnG3954087SKr0I8FMa 43D273LMm15ZYx3r2f1313j7978n4N4C4NsfA38oJnnBD3651757E6539vV00Mt569wBByUT5hFlv0t54..pb87RT6a3487J3943p4fi081g00BR4479q06kqO21u72huY 87x..X7qmMG13C9VmAg88A880SOQ86918OT8iv5n3Pk3km406H7y3bDr2Q167488i5f5I9rF9165r89D3AS2H0Ic6veDG13Emv4986iWOcksGkP21at943A9O8S75093. .FU51azMXe3w59dM096b8uz10l0YGRJ9q4H5006W50X579G17554053..3fqr1u9yW4Cn92YDPDN648741fL7J2t6radC3138x307JL3S35RQAP7130H2Tj239y3Q0s2Bl E0befM17z69lA58e369Iv484d9p6XrA1gYh5g16nJ45AByLrdjY5alxN1P31S1OPJ0445tw787z06mbT2xGpBo2D0..

C:\84086963\kwjwpm.pdf	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.6074431131094284
Encrypted:	false
SSDEEP:	
MD5:	7C7BA25B6A000090A3C645B7D3027693
SHA1:	53314D9BF5C85E283C42BAFBD7F626BF7BD2AE0F
SHA-256:	57DAE0337E28545245FD1762AA820C1D512E2078069C448F9508915AACD077B4
SHA-512:	4049B50061DF2EFD8D3BE8A1C62D16372B9FE6A7430D8E8C28FC65AACDD8964732E6F93B810949169FFF046DAB07BABE62FDF439764E35C039098E7682E03F6
Malicious:	false
Preview:	761Xp11o12Q8lfuE6mi0V8k88Nj11j2xxV7O09M79f..PSdjog1a8cx8736dqX1m..13n8au67176kC2RM214yY8044z08s4dQ6sq577qm84A96nGU7FK183BF07SdkGAX 6Hs9x45eI52P729Qr2bL18c4I1dS3GV6G4cIS4BC75NB98DU7g233A03e96Y2l0E5w45F6488f33OjCj..k9M5FX873bJ7li00Z2p2g3Blp7116163Ae7A6F5Z6wL568N7 4N5iYa069r9N6KW2aBA506Kkc8sO9VATUjh69vK94duZ0r6CuId0IdiiMZHU5VVO4400kjS06f7a4k32Z75r63I55zK4167V3z7RWQ7O3v1ul7a78wiaTc..ik4Wl56k9i 59cuC1Ws8s6nG7Sf9p280J79545M4ycz7QK7j1C94RlhT..WJIPwF4AHmVD8l8JIL2y2p8AFm3777y1Po6w4b10aZvNloab93kocaS9i9es10S9K4sn05EHRh55nyteFW1 UXulY5..

C:\84086963\kwkcsr.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.3530223467242095
Encrypted:	false
SSDEEP:	
MD5:	62B3B4E207CA4471F867730E95455766
SHA1:	318EA50BE56A5E0B2D204D5683EF632ECB3776C3
SHA-256:	C5DB519D407493AAAEDA9F1FDD777D656717A6C6ED8E4ACA30DB7D7233BBEF16
SHA-512:	32D321251829D96D410424697E4B3188533F70AE0A28192384A7EA32F213A95B22BFF1B5B42CFBA2D79E0789F4B44DEDFC3EBAABC67CF7E5EB899069A602B1A A
Malicious:	false
Preview:	156RHb1jd48l276s4lKh82c6u2sT293H38AcvP5674i5h6223WSM8Zj8A1gboe9aiF16L5KK6X0779..P8cR8797724V9v400S699i971T7000c53t9Q6T8M68R80V255F A42UWe229Q285d863..9w152Nk0uVY03t96gCw676889cy9fRb17xIe0v8H8q2LmFs0FR..82ntwha127nqr9UPZ3d1aA8PSI40P39gw2329152luRtqMAwBDT7082t138 60cv906c873X82Te6V8Syf1f096s15Lk..S7h800924Vq43e50U6E0v01Z0vA6618b4Tl4H778d036c5Ri78086m9ZZV7l1W1gr92j2442ZMk9K0843291V8164w03FO32 mkK7L6532M86106jc28aCz0..o9h8W1JO852LJM93MbL6WhL71uPXqE45t6N45646iVY4Z49X9446r24qXsUTR6L237D8306867ru6ew42GaNe8SN5A51F969zGeH92693 RnW5q3406A9y8a563hcd4jnf8MrP51ifI640..

C:\84086963\lbmqoquhgo.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	501
Entropy (8bit):	5.531395657002091
Encrypted:	false
SSDEEP:	
MD5:	30FF1EF2CDF98239A8F51F88470EF205
SHA1:	3CC584E5F708A4376284E2900B73D010170F7667
SHA-256:	DB5DB507C5A87A4DF866EDB2FE49862E34C0CB0927C07DB2AECB503C8D3BDEB5
SHA-512:	FB16DB4AA06D516F0EFF693EC046B89A05619A8D141B3E629264726EA5FBC829EC81E21234515AD83E715ED35A7D9E00B9A684F6D6240423739158E09F08B0CF
Malicious:	false
Preview:	W9d1NPeOvwS3707B2y7c7iAE4jJ77o28668MHYRrK7f64n8Vxk123dY4359i2yT201741r74t88k128L6y0372l11OeZ7l0zCs70E5QmH858GHrn7l3266tO31R56HWpP9 J5Ne56O4bd4669xhL6y..qN60694qK9iRmFD98Cq14c63JZbT7h73uMZqO14ts56h47XwGj1060gUI6575Ihp770155QP7BL8oZ81wK4Tc85W819h4EFaXw43Z94G6X93f 91NU2sJG38UyUFSW5jj1Uc0M..08NIdJ694270914d3GlKg5DSlkO68OU0PW3vI8Fy0033m99L9I05gtWjO59U0bNy4747u34GPBNn61Ok3iQZq4Y..0S6581koG2z35hL tUs0ul6W23g4oWa7537O1mNnrp7r3612fncs7A9WPN8v8aLa2nSxEP909D839D1xQl5N6s95s0016FaR9tt5F291e40A5383x59w9239Lup41..

C:\84086963\ldcauue.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.582739191372483
Encrypted:	false
SSDEEP:	
MD5:	38A3EF198AE45CA8BB98250D007988DC
SHA1:	5B3DC5BF005BB67D5FFB203D1A3E5C02DD37356F
SHA-256:	A419F40E93D04AA5F842078EBABD177A20CF8779B3398808BDF46C189C775155
SHA-512:	A48F06D7E2098571DD9C1D291B632300E3ACC4A5D6FEBD281C32FC43D6EAF4FD302018E3CAC59F05BA5A8A995F285CFAC2DBA44683BC630C0C68843378FCB F0
Malicious:	false
Preview:	80Ke54dEG068f3H656gu69F312w03F7Ft2Y696m241528u31HG7z1tT209KZ4X9W0BQ3G5Mh3WPlg8cV5ET28uQsc429610Kp1Q..g11Rs1LnO280oko86Zb0SzKB4228i 5UXf89yr5..O9L7037X1xWS138SC89sZ6uvqrvkyF1T30x5i9C37z0Nvx7R..K8U4i80nh31p0v6q8bX69891H8W5S206YB3355L06Q1WOE29Z733l4d06KN4N5G72aE70 0N36qC23k6Zv8..V2AOh819F7Qk7cj248vS3g8dRE96A0QM1TV1417sK11C1d6F95oHIn03Lz90ne1ijy4Pn4XF9e4ShgPaNCow4gmZLc3t..11FUjAz8140S6LvkY47FZ FI82Q..vNY8am5bk8S827..LK5nMZx7ZcA77Lbh1AAsx11i0CsN3l6B1b4L4VPtFstvi06Qeex75TISR7t519bod1Xw0v1U4O0P2C4N744lz302D0mEwYncDEx53IF..

C:\84086963\leqbikmpjv.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.446202058195729
Encrypted:	false
SSDEEP:	
MD5:	54240DB398CB62FD2444B9B1DAA16733
SHA1:	3D66693129AE59AE3EB9355B665B5C67F1B575C5
SHA-256:	8133BF66689277BC254C140B4D06462ED5A5AA3F92D6ECD86973698E095726F3
SHA-512:	6D58EBACD43945E97C08338F49E65698BD236E785AB7BA39E9AE708730711CA84E8D6522AE8F43DE3670561BB25992AA7B62D64839DEC155B9F609382398AA88
Malicious:	false
Preview:	5WY4Mv2X7U3x4z8M7h10B09x23pcK297dR99558196936x0yx84H488tw13..3h8wO69p44qTqO6gpL36189xkjp6nz08smrN10N3q30n0Co98a6HaPm4N7Q6121Zzu5kL 97uEcFJfV710Jj5g6368A5vE2szmr25hx87cq29gBxC99dB2v05ye9WXDe6P452122882WCrVbcog55a705U3E1T87KSoZHfH1ti70v80TB16M28..zQ72KP812619Al11 kvM9b2aqK7L31Q956u90H2plPgOcQ35M1w2yB55446Pca29c326CX4O6j6k7410V17fSex1i2EU6m0NP381vP6M9052Asd54886WJyW4..82AD09oq9Sg06r294627F917 FjLBW99ED8j5k5440KpNLvJgT8Y3i8YqTlJ25Jd16143808A12hvo44v01AwH1WksKm487V598x589E267hhBQa8DUC885f00461j7K12d35W1Kt30Uh65p77286249LwR xNa9745S7509JiHai..

C:\84086963\lngpuluvo.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	550
Entropy (8bit):	5.379913664668419
Encrypted:	false
SSDEEP:	
MD5:	DF094B07D5496BCC157C03EB4282256B
SHA1:	DA764D0117FFAD70B120615A222294BFFAFFA8EC

C:\84086963\lngpuluvo.jpg	
SHA-256:	4463D70105F48D9D90BB96B007DAF924EBD33CA7C23FC6F398C97A4956EB1E44
SHA-512:	48A2F7AF97A560D52C1BFAEB042C6CF0DEFEF1DED46566D360A36B59722F95EE2255185784229497109A34ECC7C1BB6623648D31133BA0E9D8A43BF0D0C0BF8B
Malicious:	false
Preview:	9287601W6I5X9O380E7194N4VSJV53L42nr292cj8mjgjl2ec3Fz895886BCd..6IeW7bfB..EsfL84Wq273AMv9w24ZVLJ0GO4sRk209b002W08M0j9396V4287No3323T2293QQ5J24St9932c7cs1xm29EW64Z93381027ZEQ4z7ZPeTt1o997g96Z97..R5O751T2u3sCn7162j3EqT52594Uj7763787Q416Evh88HCw78t37u1E60906hT..0PE8312PYsW9w08W957BFS8cpaQkXA6JF6cm5mCF1adg20mE1n8dlm411EevJ6sn9432o4N33..2H8O8Qqc5QP518ff55XeC67p06Xmj58Cp1NS4Edw7Wk50ksES3G7eb02899Y4821r561I1285s6327t1G0373IMl75j3U575..23h49EonP3C50O9d6430z8J97KH8e0I2J33T6kMx08PD5HWe4m076AeZ4PQgI9385wB1766HXX57296GHmMr492r3467R6Tkqh2kT35m7345S2QbV3u15..

C:\84086963\lrpb.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.513639799361316
Encrypted:	false
SSDEEP:	
MD5:	F3D529E84DE78AE012CAFB6EF7E5231F
SHA1:	57ED29D31B32A8A2915C4334C801E3FF70418617
SHA-256:	DD624C949CF52DDA01559D8042B87B3472849D687AC6ECD3317E53A3187CAB81
SHA-512:	FEDF3DD6C3E9AEF361C3BED76FA1601C53C39CBECADA4D949D762CC267AD33904CF0CCA3FFDEA014FE145098A4A1FE2B963AB1062C22DE4E25A82488C188412
Malicious:	false
Preview:	HTkMzLUSqjNv92NW181L967Zx7QXZzK8XZMtY99N854517U8YF5LP3GaO12640d21G3alb770S9tbJ4buw2SO0Y2g..5223tn8x9x077F97n4609cvS4kr49969limNKk3z17s40mi33R6hKR2736CS881X..bmqKe5PL900f9511869V43d7884dJo2FPd76IdGWlQkbY561y44629d2T7142296e1L7996r887..JtGkSFHfw65Zws180P434uCc1394GPr21IGy792O62aj5Kc66TNw0..772F3kb98J1999M3s3106U5N3qX4Eh0q90XT0e986R4J5uxg4M25cM1Or930lg2v9EF13k0v1VHa365p2L697EB0i07k0YC68BT34..Plt232C..Yy8TQ5390R7P3w3tD9xOr5RrS7u28375HsjzZd0r00045ftqsYa95N8w875786wpLc4L67PM4n5484CwU245Ly8dRm799..Rh02our5226qk94a5ti7FXQO3w0HtA870ed44Km5gobU2IoChW2..

C:\84086963\mgbpw.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	511
Entropy (8bit):	5.432216359805171
Encrypted:	false
SSDEEP:	
MD5:	38449361C530C346CADF8C2082689CDC
SHA1:	4C6BDD97449299DAFAA6CBD0C6DDB46733E05EE2
SHA-256:	9D4D1538D1BD993485043A251C9BCE9F2E8C38C35C5744429234E2567DE8D0F2
SHA-512:	7792DE8E71D0455B5F1E11E768D7D949519AF75E84122A27FFEF046CAFD2F775F2DEB670A5575F522A38E6A491BECC622FF6D1A63F2E4578F2FEF0323B43A54F
Malicious:	false
Preview:	Nl2c1q14eGKD966NeDF9206t1I4UR01gqD70G21084l82DTI0Rf0H823L2m5s8647ZYQ09G0831g9..9a3654X2i9WQa07350hAxLr1C595J89..Ok38Lv3N0y67h28L03gX5hwuCTtEm18p93fr1q5ttselrmn0jz4fw4t9083YpS305s1acI830675rOJ984b26eEGI..S0aF87jkDTG383nfgXlM207a4499v..91I07JqrJ5P..w5C364y242ZS8084tY0T7Gv58F363Qr956n4Uf21z549612802IbAaY758Qh76R28vSd6966h5Ehbt7lp5c77YG096L1g016fb1eJ6hF0too298u0i3Y8723..AfU825aoualeOKh5c90Ti371J56e0Lim7877I7000y3bKdq571847c5525n0cL35C7S55MIf6ss65Rp186jn6kG290915..7KxcR42f..Fgp4y4Qw7DD77MmTU898g87xA014542uEZ7..

C:\84086963\mjxanpqa.ico	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	5.50010539956505
Encrypted:	false
SSDEEP:	
MD5:	5D9F1E143A2D39BA6259C368391A2D6F
SHA1:	51E68AA403FBCDAC9F3300C5D4B3704A62E7618A
SHA-256:	B7E181B1F0F0646731A5DA28E73237AA702F61EF85F7EEACC6B6ED8D9E9FED75
SHA-512:	76A9F423A21DF16764481A4AC0FC39934E925B548F964060910DD96E87FDBFF8091FB40B9629A15CBCDF8BED8086E586C0185A5619A957D949C4B38A5E4ED1B(
Malicious:	false
Preview:	83580381034Ed8Ma0497gHRx2Yp0O0Pr8777M63I3536c96431l6AI391423rp77p9q1M5zC6O4cF019L11On498B55Y..4oQ0234j9RxpfdeotnqC8V612v402Fohko06eL21c960TA..Rj0b063k5780ZA9U47vQ72H6U7zv1SR2H1kKZ7u16089m14z8V18C83OVHm688181Kk71l7318Wuy8rI1K1G763634UDyCGxV194Kh06Kg3h7i23qtV69dAjxK5Ao3UYJfz912k61Yi5gr96o5K65jic0..i796j7t2Mr68d2C3228j5A12W..YhUuD7LZWK4Lnm079c10KjB35vr4zWkH72GvQE5O105y6N1ow44RO7829A3S9u29DL328E8gOY12gEbF640fe3Lv3ihs9p380l87B4JOY7437kXW..d2SlwFZ5h8wHluP6Pyb886J9o5Vo952y475lOn0949glE29zj8642C1CgR24JzqT4W9wQT0501Lw9lkq5Z6d5C5pPa..

C:\84086963\mmaihjbaf.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	506
Entropy (8bit):	5.490009992764989
Encrypted:	false
SSDEEP:	
MD5:	6DF6F66071BCF1ABA880786F52C38116
SHA1:	56CE4D71D7F99906CDFE31AC57D07CA0B5AE9244
SHA-256:	4D59E342145B37DA948DEAE6EFB005B7DB97A790ECF8DD3C1B68C2634A727049
SHA-512:	599F99DB21E1A1D24C021F7B2E7F80C08170D27920809DA3C906E704996A942435AFE05F4790B318876812209C81F9390F35E30EC80209ECB4064A251B214004
Malicious:	false
Preview:	4gC5055Q1dHtkzs6Dr2xz8at2..cy0q02T8clEgQ352oPi95979Oe16D75Wzsi9..53Z5R9JVY465bR1y30ghFp850Wy54oD5Zj82h7FH092zWSVys252dq4W29SG48LWa B..9rn6J6i8u9x64e51247184a83gl535Z4..632Vo2Uk0r928tBl9r4s5Y97QO009P79awF..t55PcEL6mJ61..910TvmIDs9Bs67y98Oy0444813K4IWlj..HJ42jp5Vq3G5hQ09yj KR94..67S183L6IP5rNs1X347256GmvaP26h51232Fz264T9IPM9b5099R6d7LP3R..82XRV1nD3i5A9l28f95Ti7s6bcO2e6R596d7e4dXe301SxR7W82M8248gO31jT7 11c941MS21i790359Pr8TDMm82jcK496636L88j695JhW2E3xhq99nbBW2TXL2KH11SjRVcCtP0aialq71..5DciS430H66Jm80f7QAd..

C:\84086963\nbwuai.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	516
Entropy (8bit):	5.443127175988351
Encrypted:	false
SSDEEP:	
MD5:	18AD63B82339D36CD20DB61EF95C5E14
SHA1:	CE74170411F52FADD880816FFF10097BB9D1FDAF
SHA-256:	46FA400C83A7B6B02F34827EE4F25791EE9545D3086159EDB9468F33848FD2E4
SHA-512:	BBFD0F8009307E555223373B6F44A47114C827F6BE20915C066600BD6ED3E2E94D5F27DFAEDC84FBCAE84EE68130A2FBB72991C75C48EA9A54967C72F6A5D47
Malicious:	false
Preview:	4R5d6Cv1sj7hFo9733K854f6I6566..4973373AOjY7zXAmtzFDL4h4zhQ0uCR4T770v4..F00fsh6w987Pl397fV92uP60OWUZ162d2ofAg6i6K705o9j5r934t726X81 660o43O33R3qzU9y5UNz03..8FmBU3kTo3115gaU8tAG43PxMB2584594H1jFr5xc9ie2225n17217GH72824k..Wq2846remv1e358053o77X2z4LJ0F0o63UG6d25Lt7 RF0vv38ij1RNsUJx5T112E9W7eQ2987g8Md06b94mC..3gXv42nBvETf640126XbozD688F3h4PCsZ24P936549HX12dHO99p50..4Eu9535670q4q08P0j6kx5A86l5eQ 1Q8vu8gA6Y84U14019R3OU448iM40An9a42iV7D1c877nZb..113iaq9qvBJ9G..889On651793671j022557eN6kbeweD2s5x3Z0032YST29GGnJq1Y6C8156Gp..

C:\84086963\ndctgkwvr.ppt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.420059389876511
Encrypted:	false
SSDEEP:	
MD5:	6FA5867ABFACB30F8669414894D7F8F5
SHA1:	83104376EA580707E38D29AE206A3908E3C2D02A
SHA-256:	32C21933839D9B77BDE59525C9F4B5A35E55C389CDB9A07C9D400D9212478E0A
SHA-512:	A140D70B0E593418C9BE3DA665C33B5844333AAB2676F4747E5A883E4A3EBA7F088A11041A4FF2D68EBFEA4240A8103033F3E61DCA09F82781B9228A46B95948
Malicious:	false
Preview:	x9q3j9S14..2lc3C97atdzX67737103w20F38S42mG97O73771I5i4ys4p748iW68a0foEM60AqLuoaH3R87U5o46Jda7B240..3079nPttalE4EH5S53O4luKg2317GJz OxP..c5R8k713omO3l2e7LTp3HnN9Wm757YqFbv..qB34S4800004zt1203iWp6208lhriva75aXOS25690s67014Q169R118mF51U1QU24k2N4MZ46r276JU95s72Efh2 q6E777h31W71..T47Q6uP813PK0175be373F1pDR2l66aKl8F73lY3tg3en8406uplC6ep5K8pRJ780Owv4O76f80rZY94B..oKW7f30bN7122qL27WMlVV0p9nVII0H27 8SJn8666s184F7672aODh5106536in6PFJFn673LRO6y2Y695759p6..na2Z1yj48451I07iG30LyS5y987M1YAw36726d5c165b8uO16OO084l953z0n49408o1R3300V hb36x59z0uBh9Sn..

C:\84086963\nhatsaem.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	568
Entropy (8bit):	5.544308795182827
Encrypted:	false
SSDEEP:	
MD5:	FEFAE78A159DA68B06E944743082580E
SHA1:	5C23A616BC39853A630422DA943DFD0E07013C8C
SHA-256:	BBC62A56930ED6E1717D4AA038E4FFD580FA7A7B32833185C7922B06F0320574

C:\84086963\nhatsaem.ini	
SHA-512:	62658C501A9FD66C5281844C24042996AC452D013835BA907A3C674B8C4478B410B1F2E71FB9A9462F4F5ABC09BBAC01CBAB6E19341429D2C44891FD471E8F04
Malicious:	false
Preview:	Z21rUF55d20r44576HR91s51180WKz9IMa09SOx0Y3du3Z5qq6UroA4V4Y0YS643d02wg3Kv8176aI1XRi8u79p4G02dRrmiD869914vj235h576C182A6q1Z6tLno0Urm SAD..x94Ap9aE1n9ns5s2VS55dEGg52mIk74kr8zb34iv1wiQ24pzwyM324Z9zOYdP9i..O0k8q44..h6c4Fk5t7C3Y74i3fsF0q603dJ20Unuqx89H63nIZI7B555327l 71l045Cu306m36wgCcQT69nS8rWV1D432C53yG61uG9cZX89I8898SK3D0p93x426j4B9u59vS7Xj15fh04V8..I7274v7Vh14e9m0N7bNSN291zDzwF5y643S..3o5g25 nncv698DA7Jv..7rB3dU1Y3N90N1P2kf445rbFZ689D8a..aTsZ1G48Jg90F5e4d8Tzc7o9T7wy0LZAOK241t..6jjpTB2GR30k9p47u49mf7f6631J3b3b34928T6etU8 lQ8i01CU6V16zw6a63Wz81S0340r4IJa567Y1toS203Q95..

C:\84086963\nkcutginn.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.549320494372432
Encrypted:	false
SSDEEP:	
MD5:	21BF01371567E54A638E86CDBAEDE926
SHA1:	DD17559E1894ED08FAA372BB131AA5A5827D923D
SHA-256:	FC319107B16B8D6BE70291966B796BB4C64C37354B5E48C19E0E3E429F216D45
SHA-512:	9F8DE3773E7D515A347D06728DDABF84178857770D3346D48636C2115AAAEF6C4B0068C9582D61A39AF3E5F860E5F0DE73AAD5A668E2E0B5FA16030E23B9EA9
Malicious:	false
Preview:	29S5iN722033ZQ6Ch0s2ZwRM1kZ9OnAFmFHk036wg36A646494rzm583m690W867IwRoR0RY45Z91h957Tn727VDb0..9OyZ4x5A17kFj4wp3tp4ft976Nem BZ0D7WYp8bj3s3o78u0i4C1Spx1n68kTqB096j8M3r8a680729859n2AwWwku94sxJdjh1x2yq9pHuB35e652176z7mhw0K194866tC40Q21b84tKLd5teV2kFR2812h3i o5Rn8nQIVav404v3wO7Y7c..708h06o7g3Aal9i943lgAvyOzLx0Q5QY1p58335Bg1nDEO6BZC7QNAF408V8c24Wl16QQ21iwjS1Z..Azu6hX1D6z9uH0t5G05F0Z23UUy zrKBd5M4jXVc7I25R14h1KsD3M2jK6axmP4vb4w8jjI718168k4u0ekB6h846z5biWb06MZd7Y15i8528LgCiF6C626I0tV4x66A75e2q53121a5NI6f6P123wHyhW8a2O ne4oq0p085..

C:\84086963\nuhwt.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	535
Entropy (8bit):	5.528314857368201
Encrypted:	false
SSDEEP:	
MD5:	7836CFD1B9AA255A90E290D8B78DEC31
SHA1:	1B0B57AD243F6A2D0DA0214F4D8E525E5EBC739B
SHA-256:	C7DA0C2C0A738D64D5D28B6FE30E2214FFABE0129D261B83DFE8EAB235B49082
SHA-512:	75486430ADB140DB65E667E9A626A89843DB65457FE7AE7DCC5D9B0AF5AB6CDCF969A2D1D16297769DF0AFABF53E600CE3DDAC45CFE51E87A4671DFEFCE45 AB7
Malicious:	false
Preview:	96iRv0Mz30BCz6kJ08INCW05KN92696Nt91UQU0i72769H6Ft8CjdFKx10JpD7t7FI7I87V513e4u6Mj98ZD89p39Xm2m67PTr8Q3b1Ar7CmXw648Wu4o9W215YYrl36S3 R9bi979G188344gYBE0i..727qwe0722440h5f2d1s5239E30Ei9p231nyeh2204493dG5W8..Qm29OPRx0068uLq9416lLc27u00llV5212o821O9n892Tzw292lPn72M 8q..tCCR8..N3bxOc8d8995ZR42p3ZkB30DN0EHL9Kc3k8uBR61SO3gU2339h1Bm050510DTfr44j..IP69F051hCN35283K76Gcnaz2T094Go771NWB8V0q6ETepXq8pt 9kZWxnscyq40WlHPv410hkrmWO7dx6W4aw77x31390m760..g614784c8Xz4w7iJ..JC91D52x750nra3aw8mzj180gRW4m2Xi3N2y..d47Yxu7nPoK2341P3qdA3033kq 622jU491kRZ2G..

C:\84086963\odsgpb.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	5.505720771474401
Encrypted:	false
SSDEEP:	
MD5:	E9DC79C25308CEF856EF4D3AB1EB8885
SHA1:	4DC4D904374E1C6CC616DAFCB0879569AEA06A75
SHA-256:	D649739031D04918B09E43A0005636AFE4550E34E97D8DC057975FEE75AA40CC
SHA-512:	7BC8843221F338BABB9C76C4B5302664EAB86AE6F08172D921DC9DE65F3E93707D4AD22A56E31D160B3F47264BAC963ABE28BA03BDD440FDD6C405CFA8C2D5 2D
Malicious:	false
Preview:	L2mj9555Pck6j9MgctG7AMI81TJJtj3T8Hn8fBSbbF1xb40F2o6Y8Q6Pq03744a3A9A246667423w8395je726oD53HyBF2N2Zr3cCHr0882Pv01QG0RM1w04an8h39001 07s1sP2Yy6Yh5GGS7r25udJ9u670Wj3RkF6QP..my834295D7A260f9SCZa9G..78EJ29N3I58019456Ik6IR42n159T1CuX15C0ki5q40EZ537x17S62Az76rC9j2ph.. N9550E49gfG5j4ag3l794OyO14Sp3Vv74E94374r6mQ771U1OSz74TsQsq0r9FkA39d..9IP91m5H9Et62vW8i9WGkAkj3da2850iKQZz8C7p48mduxc7YuEt2PX66al67 022H4W49gYc59Z390x1H2M32t098t084Q071LS0Br3h51J0o496Q40D56uc3024HJg5854DUg8UFkE1091..83J22VPG8ody73xObS8iWB974695CRw29x4W 9xVG8W1723y43b8Of23a0D1VOk7hEu0C17b33e9819298V3s5I5CIP95225K25k4cG31xb04Q3WDaTnX1z7B370x8j88b8w2020H511bPUVM5Qubsp6138iH G7QV0x645CTKe50L4VTahXNc89R1vb0s18DV1TH..

C:\84086963\onhdxftk.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	557
Entropy (8bit):	5.525598843935324
Encrypted:	false
SSDEEP:	
MD5:	2F14798CE79B63741C105A9666767F77
SHA1:	9E32729025EA0F5C3AF63E7C0AB500FFC21F86ED
SHA-256:	2B63F693728DDF990EB6AC25EDE8ED5451CBBB04B685FB05CBE3287DB76EBA35
SHA-512:	661C44AE98FA0A2EBB2580DFD70109848D7EF57B4B84E3353BDB69818796ECA0A36A8FB7920A7470C058A1E95EA6E843E408372A6E3187C28CB9C02FD6C9F96A
Malicious:	false
Preview:	0MFseLn2bWz8EuN1b38UWnQ8we8S7eWpJ1n43BOC8465WZj0T11F36rjpRYs000iZ92Mm5068s7943l6J44475W96CB3Y17U7z0UR72Q..5e580905bo68ea a7HXdeMO3v42Z46A790ax19e0I2P13ph111pCJ4YKO3M8750rgwt24qJ0sh6d5Jr1KYw782zY34T72G6..4eaJM1B35H1VT77159XGy73h1455r989wp0n82TE7TC89i9a 58n49IC4L4..r3Kn560RAV9dnEF3M2zSC9ZxKisU6t50413B61OX45ZGmji8r48d1E4q6t55g0K65n1jy73l35OPm2qcLG5qP3zB43V2qXh1NU7064XE93g9l53De5j68z dVgi6I6S3CH6699w4KByHp95R..4C2N63Af0q2416TDc8fHZa6a9eBCI04qrIHmZ3dh..8Pvk62e74cHA4gr76EcPs4123lG86lFE..p16oXDW41523zE4r543O7ChYO17 nKx4Rn9W5H5BOG89371r4w93148T9890Z9tq59j95D373..

C:\84086963\onnw.bin	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.524600536989471
Encrypted:	false
SSDEEP:	
MD5:	15F78D300ECFFBA88FBFC6F1DF7FD5F9
SHA1:	F176F2F7F83D29D72FC2BB2CEDED90D084DF86F0
SHA-256:	DD7A54FADD296322781F4FE6B48581FAF83434731565EC368AC53A087A7181AC
SHA-512:	4FA75CF98019D0AC51698BB0496A968CA16FE8ADBAF8ED8B4A222CF014C81F7D2F2A119107379B40923CC04485161B55F6D6CC11569CE8C51F409AAAA5E4C885
Malicious:	false
Preview:	iqfX2mU941k119p1Euq00z4k90iKKtEh4XL998gX55i1Z01768K5Z9vG48394E2yCfej0MsF90C4O8s014Qw76Mh14H2ha632nkx7IeC218Je1921i85bi53TWx8546ut6 S0781IR4CUg10DUc643506Bm5v7..cN1y3s3EPR09t2M0CMs23Syml7u6GNT91Hjj19s8ip5B3O5PF9VdUX8Pb3X48S0mgy015BzzhTW0mVn11Y40mv..52UD33d3G2lKA 955D69tIWOT7DSFDElD0X7E9n584h3z92FncM22l58S57342G746vsJwv9ndUl0MG..C4t84Dbps361Xf654p04L17fG838..984201boZ52f5Wy..1vVP2VMa7J3D099U 91r9V2yk1018PJ3lvTv9749x9wz05skS0140A66Zm4zNdE8cu81s3y75m085d053KuoY367Qq0Q1WGTa7Xjh3VhLUL0142k29B2aT0U51F74793Bk77..

C:\84086963\oqcijplm.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.495167284436742
Encrypted:	false
SSDEEP:	
MD5:	2BD68D8ADB4F64CB59C04F0E272E5BF2
SHA1:	3AE6BE3A030AA6F007780F7B1D495B67BE0AC414
SHA-256:	C3712B831BED9E8897D7F43E6E310E3E0AC2C1FE8215688E9AC0E6729C8E7641
SHA-512:	DD1B1C30ADA20568AEBB4940F89F039CE0A7EE77842272E2E415B8E685237865185FCEAB8F93233B22BC32412132144E9A58E5BE986D443D22183FC628F903FC
Malicious:	false
Preview:	97x90ZBE3940kQzf776S6s0f8r77cn2H6o2pOKf4YnM7jYVc2U3tz76Z1tF485PL..91dya6U877QCntPah1013t12y5HlvGRC79X0836kgY4Lf97t1vDFHzeX88m726UE 53914e4Nff68N81j80LM9Qzf8t236t0JV38W..WD8jrk31QSHO9YLC9i9lKiQ70290xNaM728bZp1Cn89p2753t0WgXE3u82mA12f2429oJ6fU9q7P5a3pdeFzZF00k6Tb y6015pE6oF978Qr757i658yvh9Xq52N19697J7X9J24H4tN43wTh2141v33xSb2IjLuDb501B49U6b6116zv68..ji3e0Bd75aZTm03177q84DHiCk4538u61X..rS01D2 7V81l8uES84Z58686td4VgN2CQX9j1H8u4HmiB9A295B4890X22zj9aR22k0HN37270Y14R7oZy406WY3n237Lx2sM82o071Y5e1234Y1E7..8vc52kC468MgS31K5l..

C:\84086963\peqltkff.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.481444804363421
Encrypted:	false
SSDEEP:	
MD5:	2603A2188626FE5EC35C4F8B5DFE3D08
SHA1:	1F3BC8505D52B2F78CDB37740F80FFAD8C4E3482

C:\84086963\peqltkff.xml

SHA-256:	C3CBAF8296CA7901EF4F61CFA7514581CC14FCE097E0B8C147436A4471FE844D
SHA-512:	2E1C9B6D90BFB7B43A65903606CAD392C3707A8210E4BCE4A2D730123465F19B89A7C26983D7A03BAF64D37B7B490B2256088E47C92541A07F2C73F6D0A82E8E
Malicious:	false
Preview:	1C2058mmgl24hSL5J9a6LE8Sqw29571M65FSsOeqKi..7M1r05316h51t5hNIw47B100sGkVDbuYhG9Q2iGdLrZpQ6F53TAe0096J7z5P5..0lSkoK8Qg1n1kX9xL9227V fY7iw334JT14i321z9ynI21Ay8SOX788m90xhN271528qH2Ej8..x5S769gCh1kebeKp8j5BH21J35G9nz9iKlT0g4vD4FB2n0S728V157Nd8cH5Od0K78VFy35t74..cF 25cF992p525t5u7642R2H5Ds71ofG99828884p2G2OOX63C3n342TG233g5..2793lp58IZ3Npd1I3U326Q754Kl13i3DT4529yCd84385A51391zj18AL8mJH6rU3G9iL 8u797E8884986inzL4o34vb323P9je5r9bY64SL6dyim8u37mO94IU7Uh2a459BO1eU5w1886vt7d1b71w4685z2..ean9n1L2126HiW02ooi88FA6W6l71z3YU0B160ez 23183h1852p6snRK1n442s9CBnmi4mYHEjnLI57a80RI9N9m350J6479vP45mHm5319103a1tRX8W80Bw2840BZ3ZZ97It1z..

C:\84086963\pvoppkotp.msc

Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	5.408265240664928
Encrypted:	false
SSDEEP:	
MD5:	175EAE979DF4EAFD3448007B2FF4EF14
SHA1:	C84754CC44FE81A6270FBF43221EC95FB4AB079E
SHA-256:	C0DF880E92E8B572DA504AB7647DE507EC29C7C7D46A6B21AD55EEB39DA607A8
SHA-512:	5E24E2049C445D7C2C755A66B554A9A1ED359D222D93B1BFC5AED21F5143FFD3D18A7B205AF508CC8B0BFE830414BD99FABE49BF0C07777C7909B53BC5D6B4A
Malicious:	false
Preview:	N9J6v6765Z59W6fza58jwS3S01j74M2C7..732meJ89u34RV9r3Lf3S4B4v4Rh1P75p5o46TyF891428ZBZ64OeN2Di65N1fC6i12kuFwQcww9D4yC91Z59N2epi0Aq92t 5440B4a0JpdZ7M7jmg5Ylx1Z8543825nb625P..I3293a20j65D3Kq1Ow41461hz08221i2U647wFE92Z2E883s29e58g17ko5SW36nrA9R4FrI64O5589EV10z284py2D 47CZz5c40t3Z03W84WS..62S4up5w1Pf2jPA8QeD21W8y10cN8jumo3376p6597dr6VhA6jn47p5n20U0Eo8i27586jvL16J6liD749NH4160252122iDlQL1i517W4oSg bO12L04p02s3gv6cJ..t810ow0234UHfs3qmQ79424WF405KY4j6z37n76B700Bj56Cd43d65PScE4W7009V53QL2EuGj63HmDZ..99x47s2652oWo15J3173132j4oU10 3845wI91oI40kD91b08E56pf4U36G0cu550GNQ9XFg62Wo9H583BDj8328D8ja9JYVP1kp3f66Ek7uWn8..

C:\84086963\qhfoer.ico

Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.399524498098625
Encrypted:	false
SSDEEP:	
MD5:	20302EC29E6C56FCD4C357F07C11FDAB
SHA1:	BC1EC3C18922BA99831B24AFFF2E547C634E491E
SHA-256:	A6699FFE364F16D3DC17B7C7F278B0A64C8CBC07D0AE92BD7F45630B86C57E70
SHA-512:	174BA6EBC04F72B6CDC3AC7F5C9387098120CC4B2C36619D618816FB7E974E632183BCAC98ED0624B4163F164C257F7F289946A9A8A3A51A9AB3D046CBCFCDA
Malicious:	false
Preview:	4KA966O2j8Yu4n9P7z94n8Q20t60y6n3t7o1497Yy..b5R194..4mfP4j9AWGpY7D4O02p15XYy60AF17j9Yo372225893G2plHQ7P621t39J995n1SUJ95tN2R5N1..sP p3oR9cywWbfG4oDVfq0UK430v9v286452g4pr8PxkdfV7421Y97s037izE457pHCz93OdwWs1av41c3119152S26L4L9W418u5hM1Oa221..mO83y5R29T7qdG6jA760WU ouq55Ch6VoP4907vb3JEC83S5egbUh161qU3664MK34sz1V565syf2GM49283pz49t48SeBo3HO5422943..7O6654Wlru87734756HRl18s03L337KJ8N4U93SO71tU4T 25BJ65oQ59I1z88N839Y7p51Dmwnj7cNq0ZPr8r6A5J7Wm8673d0U..430E16960P2so7P43263e95cONk871to859m32ty70n41JYr00q28T0426iupp3C04w71G02019 8iE4H5..

C:\84086963\rjcenldrnw.xl

Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	570
Entropy (8bit):	5.454536992205009
Encrypted:	false
SSDEEP:	
MD5:	60812709A0A8B986FFF96A81D389700F
SHA1:	2B9A5E2314EB525D8E452E3BACA3C5BB7A5236FB
SHA-256:	2F92CEDC1984929611A67E15CFC9F002242F7883D72DB5F820C90B4712224518
SHA-512:	22FE6E95636D8198188E86232C7B2657F9045AA24038B985E468889028BFC25DFAB002A4869D842B88929ED092938DC95D652F171381062FB6EDCC63A7D88BA8
Malicious:	false

C:\84086963\rjcenldrnw.xl	
Preview:	9kOHZPv4tF4c14d79VAg43XL0ch44n24G4n91cFs7A173zpfV0u7mii36aK7079z1HKa6713B4Stn13W11726Q7TMJ11W47044mj3l342c..3i112I70bXcf988tTc3olC PS69VWG92y257454UypgvmfS7nPMH7Y5S4x9o67201u8F2OB00gyleISm1V6p1k681V01Xi1D89BLh7SRM1n0NMs0m2150..5D724QQl874en4LHAj23VS378G5d2864x7 4L474j0H1b48Pq4TM237y4iY5P77mVP7d23A7983R7298zVhHlCm764o6T0P0W44..O9722G6193PA2876SKOg59PaL029u24x5ww9Uzj818DD9eOHW7t9W2 2r746oF9uo04dhhVe15v916e5qKv7BY21A9K49oyF79Yk4It8kk..A9z7Gq2GpSRrMl034..9D41E7CW2m33O71e32rX4wUN9r701d8131y4nbmw7h54MPrk3537a4Oeom 548Z8T7037N0pP8Hgo23iW94C96X92kt285h616p79PL2b22YMz9mam4a2..

C:\84086963\ruqhqaxk.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	602
Entropy (8bit):	5.482113858910446
Encrypted:	false
SSDEEP:	
MD5:	A845B8E8EE89EF9B7C794835E421C258
SHA1:	7182746E72E878BCD9B1211C14F154D0FB021358
SHA-256:	FD050DA401C19EBBB052BB7A9D2A0A4150DA13DC0772DA6F79F66739F093894C
SHA-512:	AAA557735228E9B770FD2DCF156F4D730597D4211F2575D1F8BD0994F2D4F7B865766BEE4EAAD9BA32976342160A896F2A07454A0C2ECF6D837FB0D14279360D
Malicious:	false
Preview:	wEgM1861..gi06t2O43aF7dbA890F949MJ292..sx80gOw43oHEtc22S0J3s893Ym0540Sd63D5a390dU1Ps4j5rr487kYG7U94I28RINS2..A9W03590wlTd96M18S0s4 2550w302f7mU19842EPq99b2V9982rkE5F48pH3t4rm75mSwoS2M3k15r0H1NdnZN1SLG1P6e204647156n9X1r1R85vSH7eM0lNBpJqDnBS9X9X80tLU9A1LZf9t9lU3a 03P..nKrn3pK..8j2486070q1Ds50g08rA03Qh8Ra44CFNChF9hv..46igT3Q5ODR9w9E462L16N7175100053n2lCe4580Z9yC47GLoU98A90Sx4R1IAwu25MT1oApW11 191qwQg5ZU44H9BQ7Y63XJ936..5o04H5033aYZT92K7WphGH8f4x098854wDgNg88K318929Y75kf..R539i8B8Tp02rOE8krRYWUQ0WGD1DN45QQ04h56W 94qmZ2LU2ej7UgR99Q31I703981H83y548861161PZR0L6ROY8938N5FmlX4AG242aV2S5CHG125A8vUtA183zuz5k..

C:\84086963\suvq.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.47997493722099
Encrypted:	false
SSDEEP:	
MD5:	3A3EDB6F34422710680E830E8971282A
SHA1:	AD36E4CE7DC4485EA060537C4D34633666BF49D2
SHA-256:	B7B8AAC83F13AB7CD8836912E6E6E7C8C076D976BB6D945D5347A80B077C40D5
SHA-512:	000C4645EE2D895F21A536671884A09250E757D1290829ACDA6DF3E244ADBE82B82A3C19CAA86065465A86F2D4459E6B2CF159AED4E472FCF34977E8D4136BB
Malicious:	false
Preview:	0Y01471E8p26d84PG9g4Do03C297GAqk95qZ4Z12m0JJ8vs2877y96Y27770..e2g8YCl7mQ71dJ1Z4x6P257tm08S56E7Ie1vl8c35P6Qun57au6G9G9r2RQY6z58CP5x mIo0gYv970522F9bN8Y0v3b8pc661..07Ms86H9va9U50N7v5GPwk924u5xEOJEL8a9fyUqe49Uz5TBm779FIPhV65vAE55ba8yG9f7jSHs..7C8o851y8v4Ud5uq4k881 Q0lRP5z7tXe9frA7KQJKoiZD070UWcV91C5x6e7X6B27TjE31vd06477N5PrJ5X346577cic87v022S3859euUPcaP5xB8Q..3x7N0ujgh299zW37H2p091Zv18th32co7 0968kK9eL27dP04wx4Q52LH0y95DU5716A1FOj449HDF2k15W683Gt6fbzs6UH8V6981506501q030QxqQ718qhQ61c214618Kz47LX9b8C22c600OKl910vNmH529K5ti oPq2C7S2nhtfj27..

C:\84086963\thummq.log	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.525071060081313
Encrypted:	false
SSDEEP:	
MD5:	C2A3FD1A529544E7E78EEA8DCAF37736
SHA1:	D69CB795A97A8E1CD3B1B114834229A0E86A014E
SHA-256:	DD78F8E90E403EF4503289331572638468ED6D484A493C2689B6EC78BD9566B3
SHA-512:	B440EA479BB7A786CF07F320DF5D0F46F26396426EDA4C4E5855399EA8685711C5EFFCC5CBE1D8BC51F3ADEBE2C6841C4952D7656F61CFAA8AA7D045794E7B CC
Malicious:	false
Preview:	2Vh14if5G544yE940Z4ik3v57qMYdtXZP7q11j8lG34ub25axIbFeeIv155Op6l8S11130..4y9f6iUzeAh1jj5Hv174Q10g1v685J513E4O21gsW2NbpD72VF4nu5U915..S27Pal1z Fn76395t14KNv7w2e1aLLsdytLKbTZy99skJ2cRbut1189x726..57al9ujq4tA2DF7D4caFu08W66EPKL409830dc1kRs6Vu7LPeMJ762axKD1S1799f4Q05f9O91SuX6 VxP7822vR240440UOl8ce2lQ0w2Mt57IWAfW6G28..5WOPf0372766f63374nFgrw28mo8b288p21c6Zp31kXPJ73F9r21ias64GX916Vv81h2a547608X7Mw4vxw77532 8krV4P4Su373..53p42X35T6q1U1g5499fpz9gyE2v1q4Wn69M0KK1T77NHoL823Xb703qL4898nT7775m8717hKB87Cg..MKh6657xdI6rH3jN8lc9..

C:\84086963\tsewhsbwlk.mp3	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators

C:\84086963\tsewhsbwlk.mp3	
Category:	dropped
Size (bytes):	585
Entropy (8bit):	5.545025988403711
Encrypted:	false
SSDEEP:	
MD5:	5DAB4033A97F366976B897E46EB24151
SHA1:	E249DE0649733E3CFF2E5528C90D6E7DEFC046F4
SHA-256:	D6A9C6E5CB8A2BB4DACC7D86531B764EFCD0A247C485A137BE576E8832790688
SHA-512:	7A0B8D26BC7854637E4DACB7F115E6458AE411F26557A544D368C9E34E7225ED5B0FD479398CDB2007C7D182F8744AFE06C3FB993F6B3D7CC5C67C0EA3BEBE7
Malicious:	false
Preview:	4YPyZ98iNqqlJ81jG6LvDYv65f3r1zpF3Fo98909xvz531P9VhSDx..L1gy8hx4Gje91DvbB..774X1PI3AU952905992gd43yauy5T6c7l9I451Tf344O4PMdGY512d7k qba2lW0o88730oH7t01Bo5tvHX1n4c6Wz6Yf34gi9I6S49..Z538sRskRD370aPl0PqNO10Bm16K90Y3emLOoNmyn6g86P79..KQaD5D15Q28I44xv0J93PY9By30j5WT9 p40b64c18rxzmt5fU898870Y1B918wZ2fDbx7Y6a5l6LdR82uG9Ze331dpx0C3..5r8xk38230Ze9h4i63JGK537J84sbe436D86S161339553I4V9hf0hBW4c802w50o4 01Ds02V2c3A9C0F6P0igh9E..RP9zE13ot3CD89j9U21z4nt08kVM5nTPP9jj93cCW4T6SwV72QSoq3C52QW67qN9g9Su..30O9BW2m1iU0v6tY18g9y951366Z6gQZ1V4 r0M89w35C7H783JSDD4YGgT984P2UV7G5C9563S3OH00462p6Ck768tb8pw5q53..

C:\84086963\tspet.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.58470838230856
Encrypted:	false
SSDEEP:	
MD5:	6EA9A9B2B11690E9E3B869030A3ED30C
SHA1:	D0BD36830C6BCEB11D147C6757DF79AAD1C3A97C
SHA-256:	4B973C2BF7EAFB4781C47113B0AFCB779AC917AE0346C1794AE5264C45E21FD9
SHA-512:	9F8D1A0D6DE57C934E2DF1E3C3B5A59388256CE80DD08347AFD5530DC5CD4CF235FD24B7A2860018B92EE4967F860D96238A785DC5E55AB6139BE2D6A1FB2A3
Malicious:	false
Preview:	81e7PuQ4S24Z31z1aE65sBDw433913T3O5k351E38X3cH..2VAL9uXsrS253ofw..cVzLTV9vHW402caoCU6X41v5754827s85nt06A..4GFWY9si2947..39LQ9s873Z3 hOC3h19wj6LCY2CGQ3rr33988WQ06o0781SYUp74aL134s8cLu3i2Y99r1562BhjYC5RNMK2HUah6V4K775s84iEam7Y2ulr53QLHgvb90tYf1a991950tgSCV0K..xI7X RK30LP8OI866wxGfPuz..Ulr6e5yPvLp2Abn1sn54703m84ibo6I6dBvJh5GxhlkovqI0o528kJ8aO9OrvKn07xWMt9x74g464DPf1VHi4v4P4JofAa9SP8766nP2rsJH3 ..9Q52h8o8eCcQRa53x25KRi1K0Mg24FSQet102h8EB65ip0so5Ef54407hI1Kr411Bn4a8vRGvK6154276x68957377I7ozNk5f0p1ok3KxI7003..

C:\84086963\tvat.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	515
Entropy (8bit):	5.612604697200153
Encrypted:	false
SSDEEP:	
MD5:	3E81B6312BFB5170E0D5C7DB38EFE2F6
SHA1:	4369FA15A7EC69289D9E3A58EC551C5D2FE0FB73
SHA-256:	F5513BFFA231E7706D0A8F17F415DB1B5C0A2716E331EADF7C271AE4F3B219A9
SHA-512:	7329FF39FE9D9B233A27F000CF1992849912B56AD1629217D069D151F6006EB9D82AE0B5E43A8BEAA39242557B78F098159DA6773E96A27D5B1901E92B6F9421
Malicious:	false
Preview:	6N393gJxD1YX196P1uq7w93061Pg1GmF6KM9t3y9Fkn9a1r6E9c0..9BH994Mb366ztC6N8L1A1cUa8oU655j7Pb3J02B33WmTJO5evZDc6s977TEz207UC733U6xz9dv1 QcA5k8Ls4t32..14lq0CL668skxq32522fkrMyjV4m49G46kC13rF9mBHG78492kQbWTtN1AS6T34u324e3MPSVo65ZMDo76N0Jx3L9U..84e7U932I46o3FPW94Jez43T V40M1ruv4GHJZW42h7Slnu6G6UTI75n3xru..99z3t79G97B96342df7408T5jOD6R2Vybs4d0SCsU78PvD5zEDRbGs5c1H2lU0v2Od0621r55LEmnYir6Gh9m6kYoc8.. 785I0108660Wlz594r73yhH5Q4XdbY2P0sptgR43pL1u0m31U805c8BE5eMsrQ7e8E..R8K3Uf9B37j53v0h6I7WWZ7fcwla8pR9i4E48p04dD9p3kP92nx4vC6..

C:\84086963\uhwaulbhaj.ini	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.535701019505548
Encrypted:	false
SSDEEP:	
MD5:	3C7782675094A1A72BA467E2AD72E544
SHA1:	D3CC43E9069AB7FD660A74EAD396E825FC800BD9
SHA-256:	9175A75D1F5129ECF1C97B76413021D969A4A42F2F19E12DC57660841B4108F6
SHA-512:	EA212904EDDC1012CA1C478AA0CC7ED8B9531F48F987B49655DA693DC654B48C341C9FDF95066CE8E06EE1E8F0C92E3091F430AD57EA165F359882517581CBE

C:\84086963\uhwaulbhaj.ini	
Malicious:	false
Preview:	A0m1H0TtZ5P7pJ532..94fV3T3SxkZ9..32YNfR5511xh4yc0l9j224Y7Iqg5449Y38YR82C69789Ko5r7z055V097oT64a537..T9CfnFi59t1o44IBEjoyB2uG244vG5 Dx5CEG841He033b416h5uQ6V3190MLcBE707s66E3zt4713..55936w3704yzp87H4I9gl79yo9uF1br050K3X2HmyLzqZ91kM88z2s8YaP7A04ujY1nR45067582AP95j 5g5838b3853wa79Q4BxzLc4I2dbUOA0p2Q701F21saIvIqe660r246u..3u600c50..q2O7TV7NY14mQY54pnwOE5V19Mx9qr6zG31541N07n2vy1O322818r71I1g8aH7 fE3WB8vrF9Xd6mY..xh3gpQo251DmJ6942T9v5Wa5t411068okSO143V7bl4v7Cb0fGLDQ6HLAFEayeNF7FqiC7908yg1JCK6m1901LVKwVR7Jnu93C..

C:\84086963\ujfjsealdj.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	552
Entropy (8bit):	5.5200539853409385
Encrypted:	false
SSDEEP:	
MD5:	EA4C4D4C4B4E1522BC7CB643F915A1F2
SHA1:	705535D56E94B09BC62AABE5E4B666859D70B348
SHA-256:	3C54B0FB2173908401760C6D41CDF4984B0ECAC8800EEEE217479C16F9E4FE7D
SHA-512:	41D7B528CB7F5FB0921756BDF00ABE5F3B7ED7032CC68F0CA69AD2A05166BFC8547EA2D08ACBE920894483D0BB284853451C87553AC0F65FCD0CA25AC05C44 2
Malicious:	false
Preview:	01I27KG093pk6hfhc95e1J01Z0K399Jz04OBhgKFY77..n1o4sWb28Zw27lU9507g2e6N0k9j38096pRo22fM38Ig09b5P34T6kLoyAT676W6957Rt3dkLrEo5AWhb7R9A D1mpt0559i11s6Q7114y212VUECU50mgAo51Y075..r15056e3kWwwjO8i0ne9VgF4V8m57rhA94x249Nv3e4kv0S08h956ne7E19Q1S5r37Zv4IPQA6Ju7823Qb0v8GP8 qwi0889MAM1134aos3mI23p6dB2sB2zafR74g6i92..k8PKvqp8687o367622dPD1F33H6uv0j19oX5j4VpC285UDaKp999Q463375u4FFoPJ72xmVcMEYY48p3LBXf283 Go6o3oydWQ9e285Y5uSZ8N382Dt714wC3Xs84GCY6..jt01Y8DVLT4Y690666x5k9sUO7lr626oUZ2w10i682..2F925526o7t0r927QiC2i42eJX2lYyij04857pK6Xj0 3jk9FFsq558z80CQ9e4y75198uox42..

C:\84086963\ujqwpom.msc	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	614
Entropy (8bit):	5.528625724425723
Encrypted:	false
SSDEEP:	
MD5:	098314D0E33E12701A8313CD91D77D45
SHA1:	5296EEEF877EF9AC70D7FFB5326DA46A7590A678
SHA-256:	A84005224532E72B8C3A035418FDEC0C6EBE552928427F56133F1568099790BA
SHA-512:	EEC398730027B9A0DCF701FEBA66775F6E8987FD07C584857404137B632C73B0CAB65DA24DBD9B41C978722DA6A9ACA5AF199B401B86E75A7968957A7DA4B0E 3
Malicious:	false
Preview:	25H7457nKoM744j29vP1GMJU6Y02EEG2sOU0Qhuf4n6ZaD2g..4Q2053Ri0WeJmDjQ7vLf6U95K3s2R29976s958rjR6A8hh7HI1m251y7181ps40..k6v3xYWxl1d923g 0wTp5217248o8nXj7PmmQAuFg56k034ugaaq61VN0Uf851348e2528jQO81R03d06D335Ii210D92Ub..N2K2Lar2OP224Y8rn46vd6D1xJg7AkgLt0fwEitZMAO26W858 647pv13i93rOS3V3R8Uc233S..10l78fc34IGnN753hx29U9n05W7587t8s9RyzA9l9jB3IjS3675cex4jF76jA2z49n9624324444LM8kec1J4..p2Z5BCy2PkLf2s7RFFI12l12Y49 Ia2k199I826t394wZyTS..0l4Rxn2g4brDt0493e7r016v96PY89fX42j8i7U49b393598r4xW59njxLoY806857U7110s7085SluY88K41a0Pd5v78Um1G17dd1Wd4guY n4ee7Ek66j85V03tqvq607pjR324S5N00FdEm7Cw48rFwJ50B8wOHNU4jgc4273fF24U6wkpZ1lE46NzSW..

C:\84086963\unsdkvxll.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	5.520168614508109
Encrypted:	false
SSDEEP:	
MD5:	204150CC5EEBE21EBF05292FBFDD4E12
SHA1:	2F717BB029F7376AE43ACAA27BF10926B909EC9F
SHA-256:	82C198F6D99DAF9ADB28433F67E2B4B938393F1568273F9E2098850BD94C8CC6
SHA-512:	8A27FE9B0A2384BDDD0F3E80CE715721483C66486DBB1B1501198C2E6FDA3D8CE38B1A211B058F324669D82C6A5E2A2DA31C3B2A3539422639639AAA6AD3951
Malicious:	false
Preview:	5Y3538499992jw2zEJQ6461YGo5FO30455CME34LnSEZH5F1h75l0tt5955gzf82QyG1fIh9TceuT4exFo2MRL2SiX1F2A0o811c58zkhq95l620q..67933h5i4A2Q6p8 2RbdSiaNj5xN87KSI1738F03It158189d55Q0e9e57UnT671H1RFZT126U31Cr48381771677UaQVn6A16AX7dFq07t..84h31rRV3u219Z8P444t81S77AO5yu25k67XR DdUOAH4KnMrZ07yvu1V007BDid389G0bR54E3mz28Dn4Uh660z1j48W4u93201DnwJbz669o2HVMcw54402zbr645s49MVDHUZ80..H81w0C1z050052eO1S 0Z5vLhO5sK19v03cMrwUaz9Ud4m7QG61EA8Lq4jY5x76Oqh3XRJpd85219oO043..2t70rHdl40R0U9NMtIR8EF6L8264m09s9F88H7u4SFrf5o78s6R460E5NJ620014O iHkLTv7g9egX1j39Em7t257ygV8C45b2TOmI4V6oa5b86o24IpK813Rscv13..

C:\84086963\uqai.bmp	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.469651540544045
Encrypted:	false
SSDEEP:	
MD5:	465189370EC3BDE0E30A20C043977627
SHA1:	FDCE1041C78335E3C8C7FB2A4E93DB43A81CF3D6
SHA-256:	8110FD82D0875176FA5D436317F3358866C20F2D96A1809C163F68CD2F5C315C
SHA-512:	C22CCD432B29C03C6DBCF63D17EE3F186DFC7D0A2C0C37CB69A4A3183C06E0D6B44733729C83205F7878A6F9A707117B358DE462C8470F207A02A0A0DAA4BDC
Malicious:	false
Preview:	6SgR450V7CVsC69Iz793i6Z6Ynh3Z9bhE189OF4I9dNmN926I4JKdUBI8Ig514216I7wG738z81dN4P41L4e12VW962Jzc4786xFC8132554JI2Qj7o9lYY1r18R3F8Ax5 KT8fM6R2h7523hCn9660253MjjFe6YL19haZ0606..7W6QJ57Tc137c23sE68h02O9s75lR83o95lJ93303nC57FCb85..W86Xqk1o3I24m5kQP81b3904gh496r9e2KU1 99h430k2WpTk08vt2412BN23kS21S85os0U48nbM495f013Egc2fxY71QOJMCZrG288h61T6k9u54yPXAggY32320tvBX24RG9kaoPF9gs9v7220vQrMKG2INy25R0O495 pu5h3fWy9jX16EV2017194r..sB00d7245NNdC3FjY49KIcw9e65M4800F1Wa547fZ3f8Q727tm917bT..E18jy23QqStK2M380L10E5614A..v7Uwt6A9..

C:\84086963\vihccpv.exe	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	584
Entropy (8bit):	5.432846232360661
Encrypted:	false
SSDEEP:	
MD5:	5C288EE7FEC35B7BA0746120B0C9C176
SHA1:	DF5AF987BB05245153499C926984F3373BBBAC23
SHA-256:	905CC9E8DC5A7C1A6EDA552757BEBD3D97AEED925984FC80DA05892F9F6E92A8
SHA-512:	7CD2C549577D321C1A4C020DFB7196DA1A87F97F114183373E24D34E9FBA8491B28899676F8010E2662A86791F42A5E03C43638D985E53DBCA82749D822C1D4B
Malicious:	false
Preview:	DF6T70850pQ0s1lewW96L720R9E7x568412fh3Kz985z082Y2bp26zzS8O43US321e324800V2G49S2wq0540R6..1t2V80w8Rb0pA5AFVg3sfUgCn2692l7y97vxEc490 L5298697v..69606L9YIM1PY6I970037hZ663539U6Q6NM0p7qRJj2649D..l3gFV208Z0Cx6F1826G3yHY4tT2H4mry5ftxd92jd412u7Y8vav6824OA4548..0pQd6er 146u4561jr7b0h0Q86B2m02G118J8BB5JC3FUTkSPx025hYqlG8l96YIXflt37XZW015975Lj8Slc95UM6g5..pfbz9VB074Md2nWh6sKm41x4N293515468Iqd219xK84 EW22r713aT3I1XBrij59f0J68Nw452dIEM394MB3m6B9b075SaJTH3K51e6sv5U9C9T2b..960uw07G2Q9X4N574sP8e9539..i1F71Wbzw91571a77RO06fB620yL2j74 47h90R53u5Z7w8B6627W54Eh6PY9xHahh3q56610yh1977I0907gp5dvIWb76n..

C:\84086963\vilxemlqie.txt	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	557
Entropy (8bit):	5.52837233955466
Encrypted:	false
SSDEEP:	
MD5:	8523D150BB595B191A38F956BF92C498
SHA1:	A4FE55E00792B7E838D4557A5DD5F69ECB945895
SHA-256:	9888C8D6AED250A05AFB480B7872EC8008FF0EAABE4D4BABB17C5C7EB53FE511
SHA-512:	D127AF7F33FBCE315E23F2EF9248E36732591BC90EA52157ADD6CAE35097E86ADE7973C8B59FC31D88CB26C507218372857CA34943AE246A48923370739C8EC
Malicious:	false
Preview:	G4Y0cU43aJEStE53t5n3..n8COc1a4923OZ2xr132Ku0f6s7FHJpu93F1B459sky3195Pep14245174G187Yt1060L7v58p95kx9hA7JZ60l56433l23543uK5o3MN83zY bMnkD650656jAEhE4..7h00..5m1GjoY4m98M7xr8g4W33b2r5q9gFB14P4zc9u76v8UZpxXm6211je8h2185m..E229oV3k90cIh5Sj66P12xtKZInbwtn3Npi9j0hyS81st0r8l824 8l6jO98iC1q7e..8GtJE4T74642ce16989r5878k8gf015Yiyji9AeQkfvD3274iK..1H581e5x30H57b4a0R5x6DIDc99QYr5VM0uWQg..2xFm2Y2YkA9Hldl1AR10q37 C315H6kQPJ9W143WY9..60tY0Fj0059qNe96s63XS5yRL840kCqwnK6EmV4703T17584J38j33h9O62Y6t35K69b0Tc1..L140tFvSup9039m61c6B0493mT2121xRQ7HM k8Q9963foPKtCyATJ6Y6kA4UI..

C:\84086963\vioefncov.cpl	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.515683621328262
Encrypted:	false
SSDEEP:	
MD5:	FF28D604C4F77D14D914F34932B79EA4
SHA1:	62F0142B68902C4CDA59D3E6F9D4DACD630A52D1

C:\84086963\vioefncov.cpl	
SHA-256:	822FE6C4F4149FEA2323F9355F50C1D7449D44F7068720D4D2D0DEB27B031DDA
SHA-512:	97D09C7A6C2D3516CB95CE875E94AD2AF0A10B13CA18CAFFFA01F3EE9D023BB734F51434E635CB51CC59EF4544FC8F8F770C69F9A2DA8B5BE3BAFCB2DD78E2B2
Malicious:	false
Preview:	T3m6823pO523h37xzlRW0a49k10Y6EM7kLAAngJzC3641eEZ5a2JY4qEcM8kAFtzXD4NoR176fl787J0866k24nZc40..prK4vwd9g5yX538Azb320761oU01CWIm62FZG893MiC611mq911T87Fah3go4d154ch213E0XjL7ux8tG9dY71qene..Nk0T9w7duP66122TsL4W61oh3Mca7Os6d2K8T02f12E8j41Wq1vW6ap2M195AOi642R0CH6r21vHM67m731588lppkjqI715488jK104Z4709kZ3Q4cAAj08GZJ..7Vq605K54z191v3Qr35K8fb480Ziw48U6Z3313L358I1K765vtd4023vhm56JY4St0o5c5Sa540yjm04qYb3f39I8U6i88f46P7HABcl7DjT45M..7115N2973Gs2Cy84364N08xnucEc01T20Y9A0GW..M5S40m4e3BM51U7iC3v6MU2737067n0DaX2kVA4KAlg66cl4w584i47Q75k0B4639M536E5hq0jR55397VNiP66FCdRk6y67Yb18veqFo1aZ0ZG2AdsN3h70SSiZ7dwT28708d6..

C:\84086963\vjbwupem.docx	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.455500727748887
Encrypted:	false
SSDEEP:	
MD5:	145DE41EFEAAD2F8F381EA8E3C707AB6
SHA1:	EFFA5BF68678AA351FFABCF297FF3041080F23FE
SHA-256:	98677BC9FF191C1A0DC9375C643EC524C83C117A1006FB19E92B48126DD7BD2F
SHA-512:	EAC583E80DB3D15C27017165A0BEFA5EF738CFC5EF6F8F007AF0487B17368D39F56A0FF161E61B5C4334C4E9BAE536F11C91641DA3AC835EB013EBE61AB5CEFF
Malicious:	false
Preview:	s7a2149mL61H21458979zSP7FZ2e03Idw1X99..g7F26q042708NhTNKhk188mlKacn3GB56eN1IRdi50z5IDTU439411D1190w41Hr8dx4wV7248dk279WHB166466g0T87YN17L6k6491947MK5g042v9J8b9SnB..4J4XDl1fZ7nQ63dSMH871d0a4vp6f8U0rn4L1Y8a9O962E4Uk03iMr9oaLtfvpl893Z2g4ttKq86wH0uRK56YnYz3cIQ8Xoz0BLn743sl5c9g3..L7N2i3597HzWb55u88bnUT625134K6sxL3A694rh95Zad9nqh8496mG154F60699318985U35T37771..AX8L4S53c2582R5Aj0O600n18Hk61d8B7van6rr4ZmvP6nB094048650r6ctQpt0A74q1B5op3PGvnw771y3Wk3941d4Ji7X9e2H486kT639t65cjN131F2obsD7Y4xbas8870wphV17vC8rg0uV..

C:\84086963\wcxrx.dll	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.641654857494775
Encrypted:	false
SSDEEP:	
MD5:	CE11ED836F2538E430058444C39FB10B
SHA1:	AD6133FF3F1E3FED2185055FD254E225504944A7
SHA-256:	D18E2F6563EA2849AE6966FFF3BA947005CE91C86464C00A3F2016DBC52993D9
SHA-512:	6AA6C847B9123DC758AB0EA71AA1E1B979EFDA44FA440E9E498B871DCC4ED7FE6B50EF47A769DE637774066C842E51ADD1D08F2026B10403D1755DCA36CC2A99
Malicious:	false
Preview:	ls4840Rp86Ery2c2zsPA6bIJmD..Alxu50XX2kq55qiC5qkEPdw2ZW77MlN65SGq8xYWIoU44066FsFfue91a9904U15hiutA6JP89o4R..165573LZx6SONzr3K87Su7197O8IRis94qW422v9F5b2zZqenPbu9tA..Tx9geAaVf0i6BTQAl413G6384uj93vUm2MzbymI4qwM..P4F3R2p98qP58FPFd82HTDWD40895X41CFV3NjEuG5y691n27hO49Jio6k4PMD03c9i2C5f253wWK6hn9H2285S844Nj3A13hu409R4dG474np8q7u86y34Mt3HFBg64z04j39ZaKRk92A58S06a09N..a0cdgaOx4k82H85q1K1vQAi9IM24V08K9v3YU03809CdQczsh6dk94i77l7O8W1KiD5h2j30bMqn3mW6748UGni215AxrlaTP75HzTLmy9E1p173Rl69F734000m9qKvL3nPeOirm06Oc8a..

C:\84086963\whuphgwhd.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.524768458887234
Encrypted:	false
SSDEEP:	
MD5:	EF92C75DEAA5D03B87442B4B624B1E9D
SHA1:	02A443D06663D6CEF5E9FA6BACD6BC17AECB4B41
SHA-256:	80098C60C20F19A6B85A99D0AD10C8DBB82A3E0136DE8DFFA31AA767ADAFB49E
SHA-512:	33544754EE9DB9ACB591B5D1CC134FC99E1DAB3F076FF792C230E28304F28F29BD9541CD1E64FBF1C04B7704CCF1C4CAD6E4631910F1DFF577EB7FBDA43C0FA9
Malicious:	false

C:\84086963\whuphgwhd.icm	
Preview:	n9zDl4B2K9qn8gGt6tPxW0rb5F5j798d0U6p101YoJ240711lB16Tfah26UxjCK08E4J9TK5700B54k3hb1VPi4D90EHc3P61C10063U7q7d6h3W87OQ9xg37hJ5qvd3p7 I2ZP2iO2wDZ7TkN..v37Wh0B6yE6Lxo14E65627bz31j032..hb63v35572681KSs5SKF8..2R87IHZ91818QbBL14Kq4413hS6l5L6wrr07DI75uN6TXgPhX0Iyr147o9 6953xlg5C2TO1C6g07648Ela1R8R9yQ8..Or212L6uQrezJeQ578Y92z7Z6xC3595u..VqIv1h27Fp73518Q2QGe5dYp39LPl1R6..66Y40S5tkMOMYBlR4N090T9151w9 td07oSiUQO9728f6LU..2A6mlmn38h117K872V7yj52224Ki8x79GG20cQ7b3R11uk48853jc2n2lh8L2247SJ8vpG2dgXW45e25mz3l2v4ziFz1lHx6i022E0781..

C:\84086963\wnjepqgt.xml	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	MGR bitmap, old format, 1-bit deep, 32-bit aligned
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.522948201942726
Encrypted:	false
SSDEEP:	
MD5:	5BE37A6EED05E60FF6946196CFDB0829
SHA1:	026B96D1A0B65063159E99B698CAB0BFE6820B8A
SHA-256:	BAF615CFD2666A9A55BB370275EC639021AACC5612A6AD34547AA33201EF666D
SHA-512:	26591FAF0051DE6A09C094E63A74D6BAB923E72EEACE2F303226D0AF2AC8D23CCAA47388330513B68C5A1BC67138177AB7B00EDB384C61265DB34FC8887E833 B
Malicious:	false
Preview:	xz74sG565bkq3X3H0D4Db83608483s4Den3csP6062n2A908n227C303Ez44K3nJI8N6602a9ZN8PHgJ0MP4lg6sM1l51d0K1O6Xx420lAx3w6a9R2dyK2Qc31vm67u6Ja d193mv327Q4h1..D11n83WLa39..n1DlZ633rLv38W521222hEEc9CDuk690N22eyzKnP61A1lG711yo25n293xg16J1uN..2R70tNYxVtb2dl3v3wt00f553sL11l2907 i7G..wp2oqKlf5sL4xBiXHEywq19s806XsrR34nF684ej7g8PBU4079292LU4P8ldz44Vb..3HVNN3670Ib3L7002v4PQFVM2w67awuP75c5TP9a4bws5HzcK3pk6cU9xf 3GYvka9Tj5670423R2..k34iP72RYRD1uJ89s17y258WYCqEa753vy26OZ3r1..1l87PJ049R443Cp891cC5905I8m1fk0iqU2N0IDGgL4uHw64KN98..

C:\84086963\wtranbfvgl.jpg	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	502
Entropy (8bit):	5.463862210286423
Encrypted:	false
SSDEEP:	
MD5:	1936BD3D226B73CFEA950034D3A9B4C8
SHA1:	D72CE40E67AF08E026CF6777402CC9F39785A4D1
SHA-256:	FC04BB0DC3B2C6B8961AC3B27E045B5FB76A8265E83DD87AB9260980F83E87D8
SHA-512:	30703952D73824ACAC4E325C109D6F0A77F952FD683B024AF2E0A07495450567DC22C697F279382B5681422C930146A1F007DF462F9152BE0A33D2568DF2B8D6
Malicious:	false
Preview:	8t1J1O973yR25Z2S7hgqsr64930l8EzhdPFjzarTSU9110xO0gR78gl93p2zu57106c5jny07g53qv5W38VP0y0r83lI6OL0H38AHUjH4z7985K4S8x6n5f8f96124161t 7JvEeZ41zhlgW292a4m23m17jexL0mWx244M05p7Pa8bX8D33t5464u..7d4ZgO1532H92Z3UB..Z5uc9Y12Vfp7n0Jo96xic9f41s83cIK4l693f9865lc482SGS8213l 4296ev3H258..1NmIb4dhGHv029C7D998f71p0v4Lm8..0A469q0419WEFToSXi43l4SvOh1sE4OTz805F05d4D6T0B2E8xliU8Mb792E9cZ32606x3Iy2C5e8tS8307t5 TO8462t532Y9s0Z6x910H8d5V5U0w69Aw83026l397R087W5637APf4v19883wGQ2u7Tp3436lw4686GhK22Jl6nek9NuMfnqER9Q6g31xJY00..

C:\84086963\xdhqeufpq.pif	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	661744
Entropy (8bit):	6.575295279326677
Encrypted:	false
SSDEEP:	
MD5:	957FCFF5374F7A5EE128D32C976ADAA5
SHA1:	72A4CC77337D22B5C23335538C62BEA7ED9CBB93
SHA-256:	699534A988A6AA7C8C5FF4EB01AC28292BE257B0312E6D7351FB4CACAA4124D5
SHA-512:	E9DC65FBB964CB64CFCBB1C9B5C53595B0F0304A7179710DDAC5AEFA2F0F40BB67271B7AEB39654254C2FE68FCD62B77A94674B8E9C3A57AD3497197EDE87C A9
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 50%
Joe Sandbox View:	• Filename: PDA_pdf.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g....Rich..... .....PE..L....%O....."..... .....d..... ....@.....p..... ....@...@.....@.....T.....`_1.....D.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc...`_1.....2...R.....@..@.reloc...u.....v.....@..B..... ....

C:\84086963\xfunubfgqn.xls	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	5.382025219937329
Encrypted:	false
SSDEEP:	
MD5:	F505C30D2DFD661FDCE3DAF0ECE6E52F
SHA1:	2F6B4AF22457FA04606FD8C519D8F88048D73635
SHA-256:	74DF8F0F6EAADFE4771625801D0341C511B693A7ABE6720A35859C0C5F18EDFD
SHA-512:	CDF6162D8757902C6F533046CA758B0A582DFF62F66B1B23A0103800416513CF2FFECF13AA69B6F19581E95AB2824B3142D4C5DE2A9995D8058F08CFD2F3B15D
Malicious:	false
Preview:	Xl3k7Yc757RU38..61m7L3U97d4938KL9cnl76A1U026Pt32K2yh6o53Z98438t0X6a4GRDW1If5841G90T13R7g64r935qEy..6A0T80lT4y4k96iM91366fx42f3U917 ZbH90762Se3a7toIw575kh19J8..0KzbZ6S3ny25O68p18b77A301b5561XVCp11b14979e18jm4vN587109543s1C3JrxXTa05y223yZ30W910WLO85364sdO9M245883 Qy420L1S9803v2524G4856J01S7098wnc2ig18SZ02q7WNp25z2bjz0eW17..33j1N68TrhQND97Sg2OUH3o5d2wpMfZ11rd443600E669K0gxk1zB2OJrz4o7EeU07F27 Y9Or15UQeok40253t1097G1A6M9J1s9948XD6..f43432E4RMYl7r8r4o38F7E45c4307U7l5650WnpF1t9346713gJX0398Xp33obyEtZ57lqZK9A4P8S10t9gyHdK9UYu..

C:\84086963\xgtowcke.icm	
Process:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.4621900096684675
Encrypted:	false
SSDEEP:	
MD5:	CFE1BE4D6CADE1701329295E15775372
SHA1:	9D0885591AA3BFB6F2679950A97A34E09C10B0FF
SHA-256:	B0A197AD6F56B276A63F63DB6210BC2659041E12CB73D70A6E09B99550262671
SHA-512:	872D18ADB7DAABCC49EBAB8E2A3BFA949C72FDBA28B52D2D28DEC0C0F45464DD78B7111DF68F2210C99D6C08EB505AAB46EBE30BCB759775BD2BFBA2CD8 B5508
Malicious:	false
Preview:	J420v1DE6s14jcud3..p3k6fk52A4876Gn05C4cPa2o4j850274n9XV98T0v5Xb4G15q64C8f21x3fJthl36los33wCAsrYhu5Dn1q3PI07GxOaUZZ9D58z959Us9Iq1aW 825z708YJ8TWy9az..2uYBEArIegY97OJ1b1aR613Of1HV866..m35B4184004z5LCM76Z6M0N20614723Uf0PjQ6v6637yM7K6F936tdz019Sazi2e15X8z7f56D644dR J1X7M19P5A09lR1B55199wO5F161iC99y979f..03vJj2WDu44rY9av6y7b5300z6h8696r03X9e4M1141Sosrz9z96961X5y3cAZ3bj7qW79127z104M09O..87v58C0u 2Lh7pq9290Y8f9OX8m2g4W872763PpIz5R052GIFY9i1k9z5L086J45243Pz55L9k5b57SLmX9697hpHn7Q2y1ntj34jK9L7JaMo5UV2l3R656b11p3SpPA7tvF2Q9nR8c..

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	85
Entropy (8bit):	4.764829689324031
Encrypted:	false
SSDEEP:	
MD5:	4F045072EA548C517A12DC2883656D0F
SHA1:	D4A47C53587FF02226500A0B3A2C205092336C72
SHA-256:	45E73F9C9CEBC31B9CD6989B06BEBB895496BD572B359EB7C422D502A5527948
SHA-512:	6F8FBCACE7B8DC3F086CA6A4BBE55F488B4F3E6B1883A8725D3433EFB8DA6DC0C59955D31B21F7413BF65523AB31FD6A4DD8E4BB8806D28FE2EDDE7E5C1F2 8EC
Malicious:	false
Preview:	..[2021/09/07 15:30:42 Offline Keylogger Started]....[Run]....[Program Manager]..

C:\Users\user\temp\keiv.bmp	
Process:	C:\84086963\xdhqeufpq.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	90
Entropy (8bit):	5.121205913704214
Encrypted:	false
SSDEEP:	
MD5:	FF24EA6595DD486113A7C13A8731CFFB
SHA1:	FF510F41E9FF029BD237A85FA804DA7D3CED776E
SHA-256:	F8322186B2997F00482C6B192456D13662441B5B1065820D9BA56CA841796DAE
SHA-512:	B9805FD92796690037659BF9FDD09B07C9A1285A84C7BF15EF49449E277E7BF45EA5B26ECEB77BC5050AC32E86742C1716F9D4ED6CD92B63030DED1C1D7282C

C:\Users\user\temp\keiv.bmp	
Malicious:	false
Preview:	[S3tt!ng]..stpth=%homedrive%..Key=WindowsUpdate..Dir3ctory=84086963..ExE_c=xdhqeufpq.pif..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.456525029612192
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 Google Checklist.exe
File size:	1218155
MD5:	704320b0ab5d2f24ec101cfda39589c7
SHA1:	286e65e21dc0ab4199484c948527bb3d20c4039b
SHA256:	64c32d82c0dd8612a93831055d36ba9b2767c213b27062 12545fc80b34a4d900
SHA512:	e497642e91992dbb8c53f86998c05ae859229206e5a8ffb 6a99c8b817d12b5654bd054b207f69be8e0f3f760a7254a 6fed9d73b938d92c2602dd11a2e53f8b56
SSDEEP:	24576:5AOcZ9Z++WzSRUHcjOtgzDJ1ZoRWS+TUl3fO +veifWtU:z8W2RUHsWgzDHyRWSJkzUU
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
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 15:30:42.191059113 CEST	192.168.2.6	8.8.8.8	0x9385	Standard query (0)	cato.fingusti.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 7, 2021 15:30:42.239233017 CEST	8.8.8.8	192.168.2.6	0x9385	No error (0)	cato.fingusti.club		79.134.225.107	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Covid-19 Data Report Google Checklist.exe PID: 6380 Parent PID: 6128

General

Start time:	15:30:21
Start date:	07/09/2021
Path:	C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Covid-19 Data Report Google Checklist.exe'
Imagebase:	0xc30000
File size:	1218155 bytes
MD5 hash:	704320B0AB5D2F24EC101CFDA39589C7
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: xdhqeufpq.pif PID: 6624 Parent PID: 6380

General

Start time:	15:30:31
Start date:	07/09/2021
Path:	C:\84086963\xdhqeufpq.pif
Wow64 process (32bit):	true
Commandline:	'C:\84086963\xdhqeufpq.pif' fqficjon.emu
Imagebase:	0x12f0000
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: 00000004.00000003.386707521.0000000004991000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388209243.00000000049B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.386521048.0000000004971000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388439070.0000000004971000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388390294.00000000049D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388650467.00000000048A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388336916.00000000049D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.386874226.00000000049F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388305317.0000000004991000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.388273489.00000000048C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.386594878.00000000049B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.386755735.0000000004971000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000003.386645318.00000000048A9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 55%, Virustotal, Browse • 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: 6824 Parent PID: 6624

General

Start time:	15:30:41
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:	0xfe0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000006.00000002.614438289.0000000003630000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000006.00000002.611727246.00000000013B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000006.00000002.611727246.00000000013B0000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000006.00000002.611727246.00000000013B0000.00000040.00000001.sdmp, Author: unknown
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: xdhqeufpq.pif PID: 6992 Parent PID: 3440

General

Start time:	15:30:48
Start date:	07/09/2021
Path:	C:\84086963\xdhqeufpq.pif
Wow64 process (32bit):	true
Commandline:	'C:\84086963\XDHQEU~1.PIF' c:\84086963\fqficjon.emu
Imagebase:	0x12f0000
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: 00000008.00000003.418699902.0000000001867000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.418686304.0000000004D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421704593.0000000004D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421834849.0000000001867000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421773839.0000000004D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.418832919.0000000004D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421808057.0000000004D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421744141.0000000004D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.418729526.0000000004D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.418713297.0000000004D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.417154110.0000000004D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421731075.000000000188B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.421790934.0000000004D70000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: RegSvcs.exe PID: 5084 Parent PID: 6992

General

Start time:	15:30:56
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:	0x690000
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: 0000000C.00000002.422168272.0000000002FA0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000C.00000002.422028916.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 0000000C.00000002.422028916.0000000000B00000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000000C.00000002.422028916.0000000000B00000.00000040.00000001.sdmp, Author: unknown
Reputation:	high

Disassembly

Code Analysis