

COVID PASTO.exe (/sample/ac23c17dc1b58aab52dcca0a8344692d379...

malicious

This report is generated from a file or URL submitted to this webservice on April 25th 2020 23:19:25 (UTC)

Threat Score: 100/100

Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1

AV Detection: 48%


Falcon Sandbox (<https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/>) v8.30 © Hybrid Analysis

Labeled as: Trojan.Generic (/search?query=vxfamily%3A"Trojan.Generic")

#msil (/search?query=tag%3Amsil)

#phishing (/search?query=tag%3Aphishing)

#ransomware (/search?query=tag%3Aransomware)

 Overview (/sample/ac23c17dc1b58aab52dcca0a8344692d379224353721a83d338c9f8a8fac590)


 Login to Download Sample (101KiB) ()


 Downloads ▾

 External Reports ▾

 Re-analyze ()

 Link

 Twitter (/sample/5ea4c57a6f5c262966304397/twitter)

 E-Mail

 Hash Not Seen Before (/search?query=context:ac23c17dc1b58aab52dcca0a8344692d379224353721a83d338c9f8a8fac590&from_sample=5ea4c57a6f5c262966304397&block_redirect=1)

 No similar samples (/search?query=similar-to:ac23c17dc1b58aab52dcca0a8344692d379224353721a83d338c9f8a8fac590&block_redirect=1)

 Reportar abuso

Incident Response

Risk Assessment

Fingerprint

Queries kernel debugger information


Reads the active computer name

Reads the cryptographic machine GUID

Evasive

Marks file for deletion

Network Behavior

Contacts 1 domain and 1 host.  View all details

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con

 MITRE ATT&CK™ Techniques Detection

los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

This report has 17 indicators that were mapped to 12 attack techniques and 7 tactics. [View all details](#)

Indicators

i Not all malicious and suspicious indicators are displayed. Get your own cloud service (<https://www.falcon-sandbox.com/>) or the full version (<https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/>) to view all details.

Malicious Indicators

6

External Systems

Detected Suricata Alert

Sample was identified as malicious by a large number of Antivirus engines

Sample was identified as malicious by at least one Antivirus engine

General

The analysis extracted a file that was identified as malicious

Network Related

Malicious artifacts seen in the context of a contacted host

Hiding Malicious Indicators

Para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)

[ACCEPT](#)

All indicators are available only in the private webservice or standalone version

Suspicious Indicators

19

Anti-Detection/Stealthiness

Queries kernel debugger information

Anti-Reverse Engineering

Creates guarded memory regions (anti-debugging trick to avoid memory dumping)

Environment Awareness

Reads the active computer name

Reads the cryptographic machine GUID

External Systems

Found an IP/URL artifact that was identified as malicious by at least one reputation engine

General

Opened the service control manager

Reads configuration files

Installation/Persistence

Drops executable files

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)

[ACCEPT](#)

Detected increased number of ARP broadcast requests (network device lookup)
Sends traffic on typical HTTP outbound port, but without HTTP header
System Destruction
Marks file for deletion
Opens file with deletion access rights
System Security
Modifies Software Policy Settings
Unusual Characteristics
Installs hooks/patches the running process
Reads information about supported languages
Hiding 4 Suspicious Indicators
All indicators are available only in the private webservice or standalone version

Informative	21
Environment Awareness	
Queries volume information	
Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)	
External Systems	

Detected Suricata Alert**General**

Accesses Software Policy Settings

Accesses System Certificates Settings

Contacts domains

Contacts server

Contains PDB pathways

Creates mutants

Loads the .NET runtime environment

Logged script engine calls

Overview of unique CLSIDs touched in registry

Spawns new processes

Spawns new processes that are not known child processes

Installation/Persistence

Connects to LPC ports

Dropped files

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

Network Related

Found potential URL in binary/memory

System Security

Creates or modifies windows services

Opens the Kernel Security Device Driver (KsecDD) of Windows

Unusual Characteristics

Matched Compiler/Packer signature

File Details

All Details:

 COVID PASTO.exe

Filename

COVID PASTO.exe

Size

101KiB (103424 bytes)

Type

peexe

assembly

executable

Description

PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con


Architecture

WINDOWS

los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

SHA256

ac23c17dc1b58aab52dcca0a8344692d379224353721a83d338c9f8a8fac590 

Compiler/Packer

Microsoft visual C# v7.0 / Basic .NET

PDB Timestamp

04/22/2020 03:25:01 (UTC)

PDB Pathway

C:\Users\diego\Desktop\12345\MARIAJOSE UV - copia - copia\winexec\obj\x86\Release\ctfmon.pdb

Resources

Language

NEUTRAL

Icon



Visualization

Input File (PortEx)



(/file-

inline/5ea4c57a6f5c262966304397/main/visualized_sample.png)

Version Info

Translation

0x0000 0x04b0

LegalCopyright

Copyright 2020

Assembly Version

1.0.0.0

InternalName

ctfmon.exe

FileVersion

1.0.0.0

Classification (TrID)

- 62.0% (.EXE) Generic CIL Executable (.NET, Mono, etc.)
- 23.4% (.EXE) Win64 Executable (generic)
- 5.5% (.DLL) Win32 Dynamic Link Library (generic)
- 3.8% (.EXE) Win32 Executable (generic)
- 1.7% (.EXE) OS/2 Executable (generic)

ProductName

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con ctfmon

ProductVersion

los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

1.0.0.0

FileDescription

ctfmon

OriginalFilename

ctfmon.exe

File Sections

Name
.text
Entropy
6.14425930324
MD5
4a5f9bc60753d62384e9174ad8549c4d

Name
.reloc
Entropy
0.101910425663
MD5
91bd6d1cebc1ce250315597fbd324242

Name
.rsrc
Entropy
4.94205180373
MD5
Oaa15f84f46fffd7c605dd79ca37d01

File Imports

Este sitio web

mscoree.dll

utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con

los términos de nuestra Política de protección de datos. (/data-protection-policy)

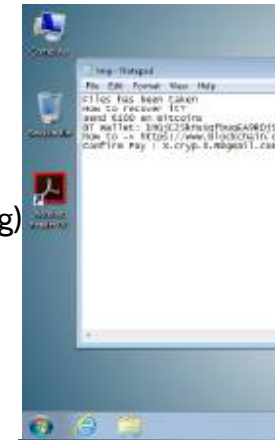
ACCEPT

_CorExeMain

Screenshots









(/file-inline/5ea4c57a6f5c262966304397/screenshot/screen_0.png)



Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 3 processes in total (System Resource Monitor).


-  COVIDPASTO.exe (PID: 3972)   12/73
-  powershell.exe /c Start-Sleep -s 1;Remove-Item -Path C:\COVIDP~1.EXE (PID: 360) 
-  notepad.exe %LOCALAPPDATA%\tmp.txt (PID: 2348)

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

DNS Requests

[Login to Download DNS Requests \(CSV\) \(\)](#)

Domain	Address	Registrar	Country
n2019cov.000webhostapp.com OSINT	145.14.145.179 TTL: 3599	Hostinger, UAB	 Netherlands

Contacted Hosts

[Login to Download Contacted Hosts \(CSV\) \(\)](#)

IP Address	Port/Protocol	Associated Process	Details
145.14.145.112 OSINT Show SSL	443 TCP	covidpasto.exe PID: 3972	 Netherlands

Contacted Countries

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy) [ACCEPT](#)



HTTP Traffic

No relevant HTTP requests were made.

Suricata Alerts

Event	Category	Description	SID
8.8.8.8:53 (UDP)	Not Suspicious Traffic	ET INFO Observed Free Hosting Domain (*.000webhostapp .com in DNS Lookup)	2026657
145.14.145.112:443 (TCP)	Domain Observed Used for C2 Detected	ET MALWARE Observed MSIL/n2019cov (COVID-19) Ransomware CnC Domain in TLS SNI	2029735
145.14.145.112:443 (TCP)	Domain Observed Used for C2 Detected	ET MALWARE Observed MSIL/n2019cov (COVID-19) Ransomware CnC Domain in TLS SNI	2029735
Response on port 49250 (TCP)	Not Suspicious Traffic	ET INFO Observed SSL Cert for Free Hosting Domain (*.000webhostapp .com)	2026658
Response on port 49251 (TCP)	Not Suspicious Traffic	ET INFO Observed SSL Cert for Free Hosting Domain (*.000webhostapp .com)	2026658

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con

 ET rules applied using Suricata. los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

Extracted Strings

Q

Search

All Details:

Off

Download All Memory Strings (3.1KiB) (/file/5ea4c57a6f5c262966304397/main/mstrings.zip)

All Strings (1096)	Interesting (230)	ac23c17dc1b58aab52dcca...	notepad.exe:2348 (82)	notepad.exe (1)	COVIDPASTO.exe:3972 (136)
powershell.exe (1)	screen_4.png (12)	screen_0.png (4)	screen_2.png (6)	SSL (6)	PCAP (1)
"3D9B94A98B-76A8-4810-B1AO-4BE7C4F9C98DA2#					
\$f3ce5c23-6ede-4898-8af3-d99b9c98b014					
%GUID:"Computer"%					
%LOCALAPPDATA%\tmp.txt					
.NET Framework 4					
.NETFramework,Version=v4.0					
/c Start-Sleep -s 1 ;Remove-Item â□□Path C:\COVIDP~1.EXE					
4System.Web.Services.Protocols.SoapHttpClientProtocol					
<?xml version="1.0" encoding="utf-8"?><asmv1:assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v1" xmlns:asmv1="urn:schemas-microsoft-com:asm.v1" xmlns:asmv2="urn:schemas-microsoft-com:asm.v2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/> <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2"> <security> <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3"> UAC Manifest Options If you want to change the Windows User Account Control level replace the requestedExecutionLevel node with one of the following. <requestedExecutionLevel level="asInvoker" uiAccess="false" /> <requestedExecutionLevel level="requireAdministrator" uiAccess="false" /> <requestedExecutionLevel level="highestAvailable" uiAccess="false" /> Specifying requestedExecutionLevel node will disable file and registry virtualization. If					

Extracted Files

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

i Displaying 20 extracted file(s). The remaining **292** file(s) are available in the full version and XML/JSON reports.


Malicious

1

 WhatsApp Image.com

 Download Disabled ()

 Extended File Details

 VirusTotal Report (<https://www.virustotal.com/#/file/ac23c17dc1b58aab52dcaa0a8344692d379224353721a83d338c9f8a8fac590/detection>)

 Hash Not Seen Before (/search?query=context:ac23c17dc1b58aab52dcaa0a8344692d379224353721a83d338c9f8a8fac590&from_sample=5ea4c57a6f5c262966304397&block_red)

Size

101KiB (103424 bytes)

Type

peexe **assembly** **executable**


Description

PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows


AV Scan Result

Labeled as "Obfuscator.BM" (12/73)


MD5

94062018fe8c640d9946cb5c52c928d0 

SHA1

4cae18ca17bdad3fbb2819e2841ece02f907f19f 

SHA256

ac23c17dc1b58aab52dcaa0a8344692d379224353721a83d338c9f8a8fac590 


Informative Selection

1

 tmp.txt

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con

 Download Disabled ()

 Extracted Streams

los términos de nuestra Política de protección de datos. (</data-protection-policy>)

ACCEPT

 Hash Not Seen Before (/search?query=context:1ea9f5d44103d709213d3d78fe31f245f0b4d2ccf65de61622a5354c6359de24&from_sample=5ea4c57a6f5c262966304397&block_redi)

Size

238B (238 bytes)

Runtime Process

COVIDPASTO.exe (PID: 3972)

MD5

d7a43845ed4208ea38b182e9006b3110 

SHA1


ea603f87b8fa3501d17bf24d70af76e06f02cd88 


SHA256


1ea9f5d44103d709213d3d78fe31f245f0b4d2ccf65de61622a3354c6359de24 

Informative

18

 SKWBHYIPMSGYPF81MR4.temp

 Download Disabled ()

 Extracted Streams

 Hash Not Seen Before (/search?query=context:8160ef06e7acc627f672a78c7218e28146487a19912f90eb3024d4d3ad950e84&from_sample=5ea4c57a6f5c262966304397&block_red

Size

7.8KiB (8016 bytes)


Runtime Process

powershell.exe (PID: 360)


MD5


c6286e390bbd1a055cc2400cbc60f8f6 


SHA1


50c0ac7f5c67dd375612fedd15ae0029e82d6cb1 


SHA256

8160ef06e7acc627f672a78c7218e28146487a19912f90eb3024d4d3ad950e84 

 adc6cee3-a5b2-45a4-8a0a-a1ba04062f50.lnk

 Download Disabled ()

 Extracted Streams

 Hash Not Seen Before (/search?query=context:adc6cee3a5b245a48a0aa1ba04062f50&from_sample=5ea4c57a6f5c262966304397&block_red

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

Size
830B (830 bytes)

Type

Ink

Description
MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Mon Jan 1 00:00:00 1601, mtime=Mon Jan 1 00:00:00 1601, atime=Mon Jan 1 00:00:00 1601, length=0, window=showminimized

Runtime Process
COVIDPASTO.exe (PID: 3972)

MD5
43b37257a3d24812ab278c3ec5b6b35a

SHA1
20c7c774240dbc66a50889192c11a8e0327d61b1

SHA256
ff17c4a97ad4542f4597b393e08051d3922c42b995c62f03a3735014063eef12

AlbumArtSmall.jpg.P4WN3D

Download Disabled ()

Extracted Streams

Hash Not Seen Before (/search?query=context:d115f548b152197fb2b1bb01688b3f6e7e372998417b18a6892d56377544c785&from_sample=5ea4c57a6f5c262966304397&block_redir





Size
5.1KiB (5216 bytes)

Runtime Process
COVIDPASTO.exe (PID: 3972)

MD5
10774279519381c47437aec0f1ceab27

SHA1
f29afc576ee06885cdefc91fb4d30b850615d054

SHA256
d115f548b152197fb2b1bb01688b3f6e7e372998417b18a6892d56377544c785

 Chrysanthemum.jpg.P4WN3D Desert.jpg.P4WN3D Hydrangeas.jpg.P4WN3D Jellyfish.jpg.P4WN3D Koala.jpg.P4WN3D Lighthouse.jpg.P4WN3D Penguins.jpg.P4WN3D Tulips.jpg.P4WN3D adc6cee3-a5b2-45a4-8a0a-a1ba04062f50.lnk.bin P9Cptr.jpg.P4WN3D HiFL.pdf.P4WN3D YhSGz6pY.gif.P4WN3D

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con

 1fdX8.pdf.P4WN3D

los términos de nuestra Política de protección de datos. (/data-protection-policy)

ACCEPT

 SrO3glOEN9SPZi43.doc.P4WN3D

Notifications

Runtime

Community

❗ There are no community comments.

❗ You must be logged in (/login) to submit a comment.

© 2020 Hybrid Analysis (<https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/>) — Terms (/terms) — Data Protection Policy (/data-protection-policy)

 (<https://twitter.com/HybridAnalysis>)

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra Política de protección de datos. (/data-protection-policy) ACCEPT