Report #6830

Creation Date: Feb. 19, 2020, 3:03 p.m.
Last Update: Feb. 19, 2020, 5:01 p.m.
File:
ondriveexplorer.exe
Results:

Binary

DLL	**False**
Size	5.14MB
trid	**100.0%** DOS Executable Generic
type	PE
wordsize	32
Subsystem	Windows GUI

Hashes

md5	a97ab5b7ba4ea3e2d1a52531a8db9e25
sha1	907124b20b633f60e46d8dcac94d63222de3b532
crc32	0x8e96a318
sha224	177dab2b0b313bc05d9f140773e7bfdf40d3e743e33cbcbf282a51c7
sha256	40fa321dd7b9195a234952d0da809dfca670b4493071db31f441254b42103b6c
sha384	df187255c46e6ee3db43d6b0fe6212dbcc2184b7c5290ad0b651fe5e9052438cfddb83ea92d80e5e2cf2023d0d23d4c5
sha512	6933e11036faa4c134a330d0ae233ae07f056288a4ac31cfeeca33cbca5ccd18b50fee1c541067ef444b4b1221accd973835b21f541a956a2054949c3b273b7d
ssdeep	98304:KUc+/s8+1YIttttttttttbF1ypWl7F/1qCNOL3iADnrZKisCStQinmfxVKY:KN+/s8+1Htttttttttjy27SviADnrV

Community

Google	**False**

HashLib	**False**

YARA

Matches	maldoc_getEIP_method_1, HasModified_DOS_Message, url, IP, FSG_v110_Eng_dulekxt_Borland_Delphi_40_50, contentis_base64, IsPacked, HasOverlay, network_ssl, IsPE32, IsWindowsGUI, possible_includes_base64_packed_functions
Suspicious	**True**

Strings

List

http://ns.adobe.com/xap/1.0/
http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
2"http://ns.adobe.com/xap/1.0/
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:xmp="http://ns.adobe.com/xap/1.0/">
xmlns:tiff="http://ns.adobe.com/tiff/1.0/">
xmlns:tiff="http://ns.adobe.com/tiff/1.0/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
xmlns:dc="http://purl.org/dc/elements/1.1/">
G.afl
Vcl.Graphics
Winapi.Windows

I.sC
e.ht
t.cO
g.RS
s.tC
a.bI
C.SA
DC.al
A.cH
BA.tg
Font.Name
Font.Name
Font.Name
Font.Style
Font.Name
Font.Style
Font.Name
Font.Style
Font.Style
Font.Style
Font.Style
Font.Style
Font.Name
Font.Name
Font.Style
Font.Name
Font.Style
Font.Name
Font.Style
Font.Name
Font.Style
Font.Name
Font.Name
Font.Style
Font.Style
Font.Name
Font.Name
Font.Style
Font.Style
Font.Name
Font.Name
Font.Style
Font.Style
Font.Name
Font.Style
Font.Style
Font.Name
Font.Name
Font.Name
Font.Style
Font.Style
Font.Name
Font.Style
Font.Style
Font.Name
Font.Name
Font.Style
Font.Style
Font.Name

Font.Style
Font.Name
Font.Name

Foremost

Matches

734.jpg, 110 KB, 955.jpg, 106 KB, 1171.jpg, 78 KB, 1329.jpg, 85 KB, 1501.jpg, 108 KB, 1727.jpg, 165 KB, 2062.jpg, 56 KB, 2177.jpg, 47 KB, 2274.jpg, 58 KB, 2393.jpg, 55 KB, 2505.jpg, 36 KB, 2582.jpg, 38 KB, 2662.jpg, 36 KB, 2739.jpg, 38 KB, 2816.jpg, 56 KB, 2934.jpg, 52 KB, 3040.jpg, 59 KB, 3161.jpg, 42 KB, 3248.jpg, 50 KB, 3350.jpg, 44 KB, 3442.jpg, 20 KB, 3483.jpg, 31 KB, 3547.jpg, 18 KB, 3585.jpg, 34 KB, 3653.jpg, 16 KB, 3686.jpg, 15 KB, 3718.jpg, 27 KB, 3775.jpg, 98 KB, 0.exe, 2 MB, 24.png, 43 KB, 419.png, 16 KB, 453.png, 18 KB, 491.png, 18 KB, 530.png, 68 KB, 668.png, 30 KB

Suspicious

True

Heuristics

IPs

hasIPs: **False**
Allowed
Suspicious
hasAllowed: **False**
hasSuspicious: **False**

URLs

Allowed: http://www.w3.org/1999/02/22-rdf-syntax-ns#
hasURLs: **True**
Suspicious: http://purl.org/dc/elements/1.1/, http://ns.adobe.com/tiff/1.0/, http://ns.adobe.com/xap/1.0/
hasAllowed: **True**
hasSuspicious: **True**

Files

Allowed: user32.dll, comctl32.dll, advapi32.dll, kernel32.dll
hasFiles: **True**
Suspicious
hasAllowed: **True**
hasSuspicious: **False**

Binary

Sizes

RVA
RVA: 16
Suspicious: **False**
Code
Size: 2405888
Suspicious: **False**
Image
Address: 320077824
Suspicious: **False**
Stack
Stack: 16384

Suspicious: False
Headers
Headers: 1024
Suspicious: False
Suspicious: False

Symbols

Number
Number: 0
Suspicious: True
Pointer
Pointer: 0
Suspicious: True
Directories
Number: 16
Suspicious: False

Checksum

Value: 5435148
Suspicous: False

Sections

Allowed: data, bss, .rsrc, .crt, .ctors
Suspicious
hasAllowed: True
hasSections: True
hasSuspicious: False

Versions

OS
Version: 5
Suspicious: False
Image
Version: True
Suspicious: 5
Linker
Version: 2.25
Suspicious: False
Subsystem
Version: 5.0
Suspicious: False
Suspicious: False

EntryPoint

Address: 7512064
Suspicious: False

Anomalies

Anomalies
hasAnomalies: False

Libraries

Allowed: user32.dll, comctl32.dll, advapi32.dll, kernel32.dll
hasLibs: True
Suspicious
hasAllowed: True
hasSuspicious: False

Timestamp	**Past**: False **Valid**: True **Value**: 2017-02-05 23:10:26 **Future**: False
Compilation	**Packed**: False **Missing**: True **Packers** **Compiled**: False **Compilers**
Obfuscation	**XOR**: False **Fuzzing**: False

PEDetector

Matches	None
Suspicious	False

Disassembly

hasTricks	False
Tricks	

AVclass

bandra	1

VirusTotal

md5	a97ab5b7ba4ea3e2d1a52531a8db9e25
sha1	907124b20b633f60e46d8dcac94d63222de3b532
SCANS (DETECTION RATE = 77.94%)	
AVG	**result**: Win32:Malware-gen **update**: 20180723 **version**: 18.4.3895.0 **detected**: True
CMC	**update**: 20180723 **version**: 1.1.0.977

detected: False

MAX

result: malware (ai score=85)
update: 20180723
version: 2017.11.15.1
detected: True

Bkav

update: 20180723
version: 1.3.0.9466
detected: False

K7GW

result: Riskware (0040eff71)
update: 20180723
version: 10.54.27833
detected: True

ALYac

result: Gen:Variant.Razy.130976
update: 20180723
version: 1.1.1.5
detected: True

Avast

result: Win32:Malware-gen
update: 20180723
version: 18.4.3895.0
detected: True

Avira

result: TR/ATRAPS.Gen
update: 20180723
version: 8.3.3.6
detected: True

Baidu

result: Win32.Trojan.WisdomEyes.16070401.9500.9914
update: 20180723
version: 1.0.0.2
detected: True

Cyren

result: W32/LdPinch.N.gen!Eldorado
update: 20180723
version: 6.0.0.4
detected: True

DrWeb

result: Trojan.Siggen7.10958
update: 20180723
version: 7.0.33.6080
detected: True

GData

result: Gen:Variant.Razy.130976

update: 20180723
version: A:25.17860B:25.12791
detected: **True**

Panda

result: Trj/Genetic.gen
update: 20180722
version: 4.6.4.2
detected: **True**

VBA32

result: TrojanBanker.Bandra
update: 20180720
version: 3.12.32.0
detected: **True**

VIPRE

result: Trojan.Win32.Generic!BT
update: 20180723
version: 68318
detected: **True**

Zoner

update: 20180723
version: 1.0
detected: **False**

AVware

result: Trojan.Win32.Generic!BT
update: 20180723
version: 1.6.0.52
detected: **True**

ClamAV

update: 20180723
version: 0.100.1.0
detected: **False**

Comodo

result: UnclassifiedMalware
update: 20180723
version: 29396
detected: **True**

F-Prot

result: W32/LdPinch.N.gen!Eldorado
update: 20180723
version: 4.7.1.166
detected: **True**

Ikarus

result: Trojan.ATRAPS
update: 20180723
version: 0.1.5.2
detected: **True**

McAfee

result: GenericR-JSC!A97AB5B7BA4E
update: 20180723
version: 6.0.6.653
detected: **True**

Rising

result: Trojan.Dynamer!8.3A0 (CLOUD)
update: 20180723
version: 25.0.0.24
detected: **True**

Sophos

result: Mal/Basine-C
update: 20180723
version: 4.98.0
detected: **True**

Yandex

result: Trojan.PWS.Bandra!
update: 20180720
version: 5.5.1.3
detected: **True**

Zillya

result: Trojan.Black.Win32.49639
update: 20180720
version: 2.0.0.3599
detected: **True**

Arcabit

result: Trojan.Razy.D1FFA0
update: 20180723
version: 1.0.0.831
detected: **True**

Babable

update: 20180406
version: 9107201
detected: **False**

Cylance

result: Unsafe
update: 20180723
version: 2.3.1.101
detected: **True**

Endgame

result: malicious (high confidence)
update: 20180711
version: 3.0.0
detected: **True**

TACHYON

update: 20180723
version: 2018-07-23.02
detected: **False**

Tencent

result: Win32.Trojan.Generic.Lnoc
update: 20180723
version: 1.0.0.1
detected: **True**

ViRobot

update: 20180723
version: 2014.3.20.0
detected: **False**

Webroot

result: W32.Bandra
update: 20180723
version: 1.0.0.403
detected: **True**

eGambit

update: 20180723
detected: **False**

Ad-Aware

result: Gen:Variant.Razy.130976
update: 20180723
version: 3.0.5.370
detected: **True**

AegisLab

result: Uds.Dangerousobject.Multi!c
update: 20180723
version: 4.2
detected: **True**

Emsisoft

result: Gen:Variant.Razy.130976 (B)
update: 20180723
version: 2018.4.0.1029
detected: **True**

F-Secure

result: Gen:Variant.Razy.130976
update: 20180723
version: 11.0.19100.45
detected: **True**

Fortinet

result: W32/Generic.AC.3CDD71!tr
update: 20180723
version: 5.4.247.0
detected: **True**

Invincea

result: heuristic
update: 20180717
version: 6.3.5.26121
detected: **True**

Jiangmin

result: Trojan.Banker.Bandra.aa
update: 20180723
version: 16.0.100
detected: **True**

Kingsoft

update: 20180723
version: 2013.8.14.323
detected: **False**

Paloalto

result: generic.ml
update: 20180723
version: 1.0
detected: **True**

Symantec

result: ML.Attribute.HighConfidence
update: 20180723
version: 1.6.0.0
detected: **True**

AhnLab-V3

result: Trojan/Win32.Generic.C1774523
update: 20180723
version: 3.13.1.21452
detected: **True**

Antiy-AVL

result: Trojan/Win32.AGeneric
update: 20180723
version: 3.0.0.1
detected: **True**

Kaspersky

result: HEUR:Trojan.Win32.Generic
update: 20180723
version: 15.0.1.13
detected: **True**

Microsoft

result: TrojanSpy:Win32/Banker
update: 20180723
version: 1.1.15100.1
detected: **True**

Qihoo-360

result: Win32/Trojan.eb0
update: 20180723
version: 1.0.0.1120
detected: **True**

TheHacker

update: 20180723
version: 6.8.0.5.3439
detected: **False**

ZoneAlarm

result: HEUR:Trojan.Win32.Generic
update: 20180723
version: 1.0
detected: **True**

Cybereason

result: malicious.7ba4ea
update: 20180225
version: 1.2.27
detected: **True**

ESET-NOD32

result: a variant of Win32/Packed.Obsidium.AL
update: 20180723
version: 17760
detected: **True**

TrendMicro

result: TROJ_GEN.R002C0PBG18
update: 20180723
version: 10.0.0.1040
detected: **True**

BitDefender

result: Gen:Variant.Razy.130976
update: 20180723
version: 7.2
detected: **True**

CrowdStrike

result: malicious_confidence_80% (D)
update: 20180530
version: 1.0
detected: **True**

K7AntiVirus

result: Riskware (0040eff71)
update: 20180723
version: 10.54.27834
detected: **True**

SentinelOne

update: 20180701
version: 1.0.17.227
detected: **False**

Avast-Mobile

update: 20180723
version: 180723-00
detected: **False**

Malwarebytes

update: 20180723
version: 2.1.1.1115
detected: **False**

TotalDefense	**update**: 20180722 **version**: 37.1.62.1 **detected**: **False**
CAT-QuickHeal	**result**: TrojanSpy.Banker **update**: 20180723 **version**: 14.00 **detected**: **True**
NANO-Antivirus	**result**: Trojan.Win32.Bandra.elmkoc **update**: 20180723 **version**: 1.0.116.23366 **detected**: **True**
MicroWorld-eScan	**result**: Gen:Variant.Razy.130976 **update**: 20180723 **version**: 14.0.297.0 **detected**: **True**
SUPERAntiSpyware	**update**: 20180722 **version**: 5.6.0.1032 **detected**: **False**
McAfee-GW-Edition	**result**: GenericR-JSC!A97AB5B7BA4E **update**: 20180723 **version**: v2017.3010 **detected**: **True**
TrendMicro-HouseCall	**result**: TROJ_GEN.R002C0PBG18 **update**: 20180723 **version**: 9.950.0.1006 **detected**: **True**

total	68
sha256	40fa321dd7b9195a234952d0da809dfca670b4493071db31f441254b42103b6c
scan_id	40fa321dd7b9195a234952d0da809dfca670b4493071db31f441254b42103b6c-1532341866
resource	a97ab5b7ba4ea3e2d1a52531a8db9e25
permalink	https://www.virustotal.com/file/40fa321dd7b9195a234952d0da809dfca670b4493071db31f441254b42103b6c/analysis/1532341866/
positives	53

scan_date	2018-07-23 10:31:06
verbose_msg	Scan finished, information embedded
response_code	1

File

Trace

19/2/2020 - 16:45:44.340	Open	1480	C:\malware.exe	C:\wsock32.dll	
19/2/2020 - 16:45:44.340	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wsock32.dll	
19/2/2020 - 16:45:44.340	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wsock32.dll	
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\Globalization\Sorting\SortDefault.nls	
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Windows\Globalization\Sorting\SortDefault.nls	SortDefault.nls
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming	
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming	
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming\Obsidium\{7996E268-2E45773B-75A57AB4-2449A90A}.11924041074243746681	
19/2/2020 - 16:45:44.	Open	148	C:\malware.	C:\Users\Behemot	

622		0	exe	
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Users\Behemot\.obs32\{7996E268-2E45773B-75A57AB4-2449A90A}.11924041074243746681
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Open	148	C:\malware.exe	C:\Monitor\Malware

		0		
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Unknown	1480	C:\malware.exe	C:\Monitor\Malware
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rpcss.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rpcss.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\wtsapi32.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wtsapi32.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wtsapi32.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\WINSTA.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winsta.dll
19/2/2020 - 16:45:44.622	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winsta.dll

19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\Windows\Fonts\StaticCache.dat	
19/2/2020 - 16:45:44.684	Read	1480	C:\malware.exe	C:\Windows\Fonts\StaticCache.dat	StaticCache.dat
19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\security.dll	
19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\security.dll	
19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\security.dll	
19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\SECUR32.DLL	
19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\secur32.dll	
19/2/2020 - 16:45:44.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\secur32.dll	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\olepro32.dll	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\olepro32.dll	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\olepro32.dll	

19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\ntmarta.dll	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\ntmarta.dll	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\ntmarta.dll	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\malware.exe.Local	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_pt-br_59b90943c4d9db88	
19/2/2020 - 16:45:44.700	Unknown	1480	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_pt-br_59b90943c4d9db88	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_pt-br_59b90943c4d9db88	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_pt-br_59b90943c4d9db88\comctl32.dll.mui	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\Fonts\arial.ttf	
19/2/2020 - 16:45:44.700	Open	1480	C:\malware.exe	C:\Windows\Fonts\arial.ttf	
19/2/2020 - 16:45:44.700	Read	1480	C:\malware.exe	C:\Windows\Fonts\StaticCache.dat	StaticCache.dat
19/2/2020		1	C:\mal		

- 16:45:44.715	Open	4800	ware.exe	C:\Windows\SysWOW64\uxtheme.dll.Config
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\Windows\SysWOW64\uxtheme.dll
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\malware.exe.Local
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
19/2/2020 - 16:45:44.715	Unknown	4800	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
19/2/2020 - 16:45:44.715	Unknown	4800	C:\malware.exe	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Unknown	4800	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Open	4800	C:\malware.exe	C:\Users\Behemot\AppData\Local
19/2/2020	Op	4	C:\mal	

- 16:45:44.715	en	80	ware.exe	C:\Users\Behemot\AppData\Local
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming
19/2/2020	Op	14	C:\mal	

- 16:45:44.715	en	80	ware.exe	C:\Users\Behemot\AppData\Roaming
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Unknown	1480	C:\malware.exe	C:\Users\Behemot
19/2/2020 - 16:45:44.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local
19/2/2020 - 16:45:44.	Op	14	C:\malware.	C:\Users\Behemot\AppData\Local

731		en	80	exe	
19/2/2020 - 16:45:44.731	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local	
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History	
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History	
19/2/2020 - 16:45:44.731	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History	
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History\History.IE5	
19/2/2020 - 16:45:44.731	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History\History.IE5	
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files	
19/2/2020 - 16:45:44.731	Unknown	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files	
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\api-ms-win-downlevel-advapi32-l2-1-0.dll	
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-l2-1-0.dll	
19/2/2020 - 16:45:44.	Unknow	148	C:\malware.	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-l2-1-0.dll	api-ms-win-downlevel-advapi32-l2-

731	n	0	exe		1-0.dll
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-l2-1-0.dll	
19/2/2020 - 16:45:44.731	Unknown	1480	C:\malware.exe	C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-l2-1-0.dll	api-ms-win-downlevel-advapi32-l2-1-0.dll
19/2/2020 - 16:45:44.731	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat	
19/2/2020 - 16:45:47.825	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.dll	
19/2/2020 - 16:45:47.872	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.dll	
19/2/2020 - 16:45:48.153	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemcomn.dll	
19/2/2020 - 16:45:48.153	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbemcomn.dll	
19/2/2020 - 16:45:48.200	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbemcomn.dll	
19/2/2020 - 16:45:48.762	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\Logs	
19/2/2020 - 16:45:48.809	Unknown	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\Logs	
19/2/2020 - 16:45:48.809	Open	148	C:\malware.exe	C:\Windows\SysWOW64\advapi32.dll	

		0		
19/2/2020 - 16:45:48.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\advapi32.dll
19/2/2020 - 16:45:48.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemprox.dll
19/2/2020 - 16:45:48.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemprox.dll
19/2/2020 - 16:45:49.59	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wmiutils.dll
19/2/2020 - 16:45:49.59	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wmiutils.dll
19/2/2020 - 16:45:49.481	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\nlaapi.dll
19/2/2020 - 16:45:49.481	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\nlaapi.dll
19/2/2020 - 16:45:49.481	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\NapiNSP.dll
19/2/2020 - 16:45:49.481	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\NapiNSP.dll
19/2/2020 - 16:45:49.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\pnrpnsp.dll
19/2/2020 - 16:45:49.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\pnrpnsp.dll

		0		
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\mswsock.dll
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\mswsock.dll
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\DNSAPI.dll
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\dnsapi.dll
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\dnsapi.dll
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winrnr.dll
19/2/2020 - 16:45:50.137	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winrnr.dll
19/2/2020 - 16:45:50.372	Open	1480	C:\malware.exe	C:\IPHLPAPI.DLL
19/2/2020 - 16:45:50.372	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\IPHLPAPI.DLL
19/2/2020 - 16:45:50.372	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\IPHLPAPI.DLL
19/2/2020 - 16:45:50.372	Open	148	C:\malware.exe	C:\WINNSI.DLL

		0		
19/2/2020 - 16:45:50.372	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winnsi.dll
19/2/2020 - 16:45:50.372	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winnsi.dll
19/2/2020 - 16:45:50.418	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FWPUCLNT.DLL
19/2/2020 - 16:45:50.418	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FWPUCLNT.DLL
19/2/2020 - 16:45:50.512	Open	1480	C:\malware.exe	C:\rasadhlp.dll
19/2/2020 - 16:45:50.512	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rasadhlp.dll
19/2/2020 - 16:45:50.512	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rasadhlp.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\CRYPTSP.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\cryptsp.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\cryptsp.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll

19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rsaenh.dll

19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\RpcRtRemote.dll	
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\RpcRtRemote.dll	
19/2/2020 - 16:45:50.606	Unknown	1480	C:\malware.exe	C:\Windows\SysWOW64\RpcRtRemote.dll	RpcRtRemote.dll
19/2/2020 - 16:45:50.606	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\RpcRtRemote.dll	
19/2/2020 - 16:45:50.606	Unknown	1480	C:\malware.exe	C:\Windows\SysWOW64\RpcRtRemote.dll	RpcRtRemote.dll
19/2/2020 - 16:45:50.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemsvc.dll	
19/2/2020 - 16:45:50.809	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemsvc.dll	
19/2/2020 - 16:45:51.231	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\fastprox.dll	
19/2/2020 - 16:45:51.231	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\fastprox.dll	
19/2/2020 - 16:45:51.231	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\NTDSAPI.dll	
19/2/2020 - 16:45:51.231	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\ntdsapi.dll	

19/2/2020 - 16:45:51.231	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\ntdsapi.dll
19/2/2020 - 16:45:51.653	Open	1480	C:\malware.exe	C:\SXS.DLL
19/2/2020 - 16:45:51.653	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\sxs.dll
19/2/2020 - 16:45:51.653	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\sxs.dll
19/2/2020 - 16:45:51.653	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
		1		

19/2/2020 - 16:45:51.653	Read	480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:51.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020		1	C:\mal	

- 16:45:53.434	Open	480	ware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020	Re	14	C:\mal	

- 16:45:53.434	ad	80	ware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.434	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:53.715	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\EUDCNZA
19/2/2020 - 16:45:54.372	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\BAOEIAZC
19/2/2020 - 16:45:55.403	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\BAOEIAZC
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Program Files (x86)
19/2/2020 - 16:45:55.918	Unknown	1480	C:\malware.exe	C:\Program Files (x86)
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Program Files (x86)\GbPlugin\bb.gpc
19/2/2020	Op	14	C:\mal	

- 16:45:55.918	en	80	ware.exe	C:\Program Files (x86)\GbPlugin\cef.gpc
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Program Files (x86)\GbPlugin\uni.gpc
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Program Files (x86)\GbPlugin\abn.gpc
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Program Files (x86)\Scpad\scpIBCfg.bin
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Program Files (x86)\diebold\warsaw\core.exe
19/2/2020 - 16:45:55.918	Open	1480	C:\malware.exe	C:\Users\Behemot\AppData\Local\Aplicativo Itau\itauaplicativo.exe
19/2/2020 - 16:45:56.575	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020	Re	14	C:\mal	

- 16:45:56.575	ad	80	ware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:56.575	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.	Re	14	C:\malware.	C:\Windows\SysWOW64\wbem\wbemdisp.tlb

887	ad	80	exe	
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.887	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:57.	Read	148	C:\malware.	C:\Windows\SysWOW64\wbem\wbemdisp.tlb

887		0	exe	
19/2/2020 - 16:45:58.356	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.	Read	148	C:\malware.	C:\Windows\SysWOW64\stdole2.tlb

356		0	exe	
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.356	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:45:58.637	Unknown	1480	C:\malware.exe	C:\Windows\SysWOW64\wbem\wbemdisp.tlb
19/2/2020 - 16:45:58.637	Open	1480	C:\malware.exe	C:\IdnDL.dll
19/2/2020 - 16:45:58.637	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\idndl.dll
19/2/2020 - 16:45:58.637	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\idndl.dll
19/2/2020 - 16:45:58.637	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Open	148	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll

		0		
19/2/2020 - 16:45:58.637	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll

19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll

19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
		1		

19/2/2020 - 16:45:58.637	Read	480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll
19/2/2020		1	C:\mal	

- 16:45:58.637	Read	480	ware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:45:58.637	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\shell32.dll	
19/2/2020 - 16:46:3.325	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	
19/2/2020 - 16:46:3.325	Unknown	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.325	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	
19/2/2020	Re	14	C:\mal		

- 16:46:3.325	ad	80	ware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.372	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.418	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.465	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.559	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.606	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.653	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.700	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.747	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.793	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020	Re	14	C:\mal		

- 16:46:3.840	ad	80	ware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:3.934	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.497	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020	Re	14	C:\mal		

- 16:46:4.497	ad	80	ware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.5	Re	14	C:\malware.	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll

12	ad	80	exe		
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\FirewallAPI.dll	FirewallAPI.dll
19/2/2020 - 16:46:4.512	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb	
19/2/2020 - 16:46:4.5	Read	148	C:\malware.	C:\Windows\SysWOW64\stdole2.tlb	

12		0	exe	
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.512	Read	1480	C:\malware.exe	C:\Windows\SysWOW64\stdole2.tlb
19/2/2020 - 16:46:4.887	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\WSHTCPIP.DLL
19/2/2020 - 16:46:4.887	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\WSHTCPIP.DLL
19/2/2020 - 16:46:5.231	Open	148	C:\malware.exe	C:\Windows\SysWOW64\wship6.dll

		0		
19/2/2020 - 16:46:5.231	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wship6.dll
19/2/2020 - 16:46:5.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\tzres.dll
19/2/2020 - 16:46:5.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\tzres.dll
19/2/2020 - 16:46:5.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\tzres.dll
19/2/2020 - 16:46:5.684	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\tzres.dll

Process

Trace

Analysis

Reason	Timeout
Status	Sucessfully Executed
Results	1

Registry

Trace

19/2/2020 - 16:4	Wr	14	C:\malwar	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet

5:44.715	ite	80	e.exe	Settings\5.0\Cache\Content	CachePrefix
19/2/2020 - 16:45:44.715	Write	1480	C:\malware.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies	CachePrefix
19/2/2020 - 16:45:44.715	Write	1480	C:\malware.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History	CachePrefix
19/2/2020 - 16:45:54.231	Write	1480	C:\malware.exe	HKCU\Software\Microsoft\Internet Explorer\Main	Use FormSuggest
19/2/2020 - 16:45:54.231	Write	1480	C:\malware.exe	HKCU\Software\Microsoft\Internet Explorer\Main	FormSuggest Passwords
19/2/2020 - 16:45:54.231	Write	1480	C:\malware.exe	HKCU\Software\Microsoft\Internet Explorer\Main	FormSuggest PW Ask
19/2/2020 - 16:45:54.887	Write	1480	C:\malware.exe	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	HD373DID

File Summary

Created **Identified**: False

Deleted **Identified**: False

Process Summary

Created **Identified**: False

Deleted **Identified**: False

Registry Summary

Proxy **Identified**: False

AutoRun **Identified**: False

Created **Identified**: True

Deleted **Identified**: False

Browsers **Identified**: True

Internet **Identified**: True

DNS

Query

localhost → gateway:DNS ‹› www.clinicadaspatas.com.br.
localhost → gateway:50273 ‹› www.clinicadaspatas.com.br.

Response

gateway:DNS → localhost ‹› www.clinicadaspatas.com.br. 108.167.188.154

TCP

Info

108.167.188.154:80 → localhost:65191
localhost:65191 → 108.167.188.154:80

UDP

Info

localhost:50273 → localhost:53
localhost:53 → localhost:50273

HTTP

Info

localhost POST www.clinicadaspatas.com.br /Adapter/teste/romano/master.php

Summary

DNS True

TCP True

UDP	**True** ✅
HTTP	**True** ✅

Results

BINARY

KNN (K=3, NFS-BRMalware)
confidence: 66.67%
suspicious: **False** ❌

Decision Tree (NFS-BRMalware)
confidence: 100.00%
suspicious: **True** ✅

SVC (Kernel=Linear, NFS-BRMalware)
confidence: 90.69%
suspicious: **False** ❌

MalConv (Ember: Raw Bytes, Threshold=0.5)
confidence: 84.52%
suspicious: **True** ✅

Random Forest (100 estimators, NFS-BRMalware)
confidence: 68.00%
suspicious: **True** ✅

Non-Negative MalConv (Ember: Raw Bytes, Threshold=0.35)
confidence: 41.39%
suspicious: **True** ✅

LightGDM (Ember: File Characteristics, Threshold=0.8336)
confidence: 75.82%
suspicious: **False** ❌