Report #6444

Creation Date: Feb. 17, 2020, 2:31 p.m.
Last Update: Feb. 17, 2020, 8:41 p.m.
File:
Download_01629264864.exe
Results:

Binary

DLL	**False**
Size	93.00KB
trid	**93.4%** Win32 Executable Borland Delphi 7 **1.9%** Win32 Executable Delphi generic **1.8%** Windows screen saver **0.9%** Win32 Dynamic Link Library **0.6%** Win32 Executable
type	PE
wordsize	32
Subsystem	Windows CLI

Hashes

md5	0dfca88b93a9c6e6616022d06bad0816
sha1	37364bb7015a7db1e3ce8ee04cdf54cfa2fcbeeb
crc32	0xa8b03f40
sha224	dc882606db503852ca329e3dffd4ea2fcb97843aa007aec0c8cb7064
sha256	c95caae20195f49e07adb8951abd6e78bd07089aaf1e39234310298c8a6b91af
sha384	c7fe3ae9c6f2cbe5d83be3505824dd0f71729b6043cf81963857032ebd125e1626c5c16c6b9dbf16f24fa1479cc80616
sha512	ecd3fc0faea471fde81c9532bdf0c16125fe53c85d91adb02205b7112a2c94dea8add91e5da3e9274c0083be4b20f90127aab185aa3af2edf1cd162179e2f217
ssdeep	1536:9k+qQxQrzttUsaQizfzdlQ6RiUElAZE1/HDz0Qqb8ycVgKU:jxuzQIOrd264/7Zf0Qy5xKU

Community

Google False

HashLib False

YARA

Matches domain, Delphi_Copy, Borland, Delphi_DecodeDate, contentis_base64, keylogger, IsConsole, win_registry, Microsoft_Visual_Cpp_v50v60_MFC, Delphi_CompareCall, borland_delphi, Delphi_StrToInt, win_files_operation, IsPE32, Big_Numbers3, Big_Numbers2, Big_Numbers1

Suspicious True

Strings

List

t.Ht
P.rsrc
SOFTWARE\Borland\Delphi\RTL
Software\Borland\Locales
Software\Borland\Delphi\Locales
Apartment
Division by zero
August September
Too many open files
Assertion failed
%s (%s, line %d)
Privileged instruction(Exception %s in module %s at %p.
I/O error %d
ESafecallException
AF9425203FEE6BDB4BDD1E0105112D251632D16FF5
No argument for format '%s'"Variant method calls not supported
49D3043BD527C6A98FFA55A25D
Invalid variant operation%Invalid variant operation (%s%.8x)
Abstract Error?Access violation at address %p in module '%s'. %s of address %p
%s5Could not convert variant of type (%s) into type (%s)=Overflow while converting variant of type (%s) into type (%s)
Application Error1Format '%s' invalid or incompatible with argument
GetProcAddress
GetProcAddress
EPrivilege
Invalid class typecast0Access violation at address %p. %s of address %p
CF7504011C0D0979E87FF9252135C148F15EFD1B21
ExitProcess
OLE error %.8x.Method '%s' not supported by automation object/Variant does not reference an automation object7
Dispatch methods do not support more than 64 parameters
E620CF7A959E56ED02
FD23BB49D444C6B6ADBB3CE366FE1B17002C2B36CE

!'%s' is not a valid integer value
1B21C67EAF
FPUMaskValue
GetDiskFreeSpaceA
This program must be run under Win32
sActiveX
CoCreateInstanceEx
VirtualAlloc
CoCreateInstance
SysUtils
SysUtils
SysUtils
Variant or safe array is locked
LoadLibraryExA
GetModuleHandleA
GetModuleFileNameA
FreeLibrary
FindFirstFileA
WriteFile
RegQueryValueExA
RegOpenKeyExA
GetModuleHandleA
WriteFile
GetModuleHandleA
GetModuleFileNameA
CreateDirectoryA
OleInitialize
External exception %x
Sleep
GetCPInfo
1 1$1(1,101H1U1]1l1y1
1#1)131<1E1O1\1g1y1
0"0&0,00060=0A0[0d0m0y0
4&4.464>4F4N4V4o4{4
=!=%=)=-=1=5=9===A=E=I=M=Q=U=Y=]=a=e=i=u=
24383<3@3D3H3L3P3T3X3\3`3d3h3l3p3t3x3|3
2#282M2034383<3@3D3H3L3P3T3X3\3`3d3h3l3p3t3x3|3
t%HtIHtm
Interface not supported
101H1T1\1s1
80888<8@8D8H8L8P8T8X8l8
EInOutErrorlY@
3 3$3(3,3034383<3@3D3H3L3P3T3X3\3
4 4$4(4,4044484<4@4D4H4L4P4T4X4\4`4d4h4l4p4t4x4|4
80<0@041<1@1D1H1l1p1t1x1|1
$VarUtils
EVariantBadVarTypeError(
2<2D2L2T2\2d2l2t2|2
ERangeError,[@
7"7-727=7
Exception\X@
59CA74A14DDC0439C870EA38F21031EF
EVariantBadIndexError
3Messages
Control-C hit
EVariantDispatchError
P.reloc
EVariantArrayLockedError
EVariantTypeCastError

PACKAGEINFO
;>=F=S=^=h=r=
ZTUWVSPRTj
$*@@@*$@@@$ *@@* $@@($*)@-$*@@$-*@@$*-@@(*$)@-*$@@*-$@@*$-@@-* $@-$ *@* $-@$ *-@$ -*@*- $@($ *)(* $)
Runtime error at 00000000
EVariantArrayCreateError
EVariantInvalidOpError
EDivByZero
EOleSysError
EControlC
EIntError

Foremost

Matches	0.exe, 93 KB
Suspicious	**True** ✅

Heuristics

IPs	**hasIPs**: **False** ❌ **Allowed** **Suspicious** **hasAllowed**: **False** ❌ **hasSuspicious**: **False** ❌
URLs	**Allowed** **hasURLs**: **False** ❌ **Suspicious** **hasAllowed**: **False** ❌ **hasSuspicious**: **False** ❌
Files	**Allowed**: user32.dll, ole32.dll, advapi32.dll, kernel32.dll, oleaut32.dll, shell32.dll **hasFiles**: **True** ✅ **Suspicious** **hasAllowed**: **True** ✅ **hasSuspicious**: **False** ❌

Binary

Sizes	**RVA** **RVA:** 16 **Suspicious:** **False** ❌ **Code** **Size:** 16384 **Suspicious:** **False** ❌ **Image** **Address:** 4194304 **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: 0
Suspicous: True

Sections

Allowed: code, data, bss, .idata, .tls, .rdata, .reloc, .rsrc
Suspicious
hasAllowed: True
hasSections: True
hasSuspicious: False

Versions

OS
Version: 4
Suspicious: False
Image
Version: True
Suspicious: 4
Linker
Version: 2.25
Suspicious: False
Subsystem
Version: 4.0
Suspicious: False
Suspicious: False

EntryPoint

Address: 77316
Suspicious: False

Anomalies

Anomalies: The header checksum and the calculated checksum do not ma
tch.
hasAnomalies: True

Libraries

Allowed: user32.dll, ole32.dll, advapi32.dll, kernel32.dll, oleaut32.dll, shell
32.dll

	hasLibs: True **Suspicious** **hasAllowed**: True **hasSuspicious**: False
Timestamp	**Past**: True **Valid**: True **Value**: 1992-06-19 19:22:17 **Future**: False
Compilation	**Packed**: False **Missing**: True **Packers** **Compiled**: False **Compilers**
Obfuscation	**XOR**: False **Fuzzing**: True

PEDetector

Matches	None
Suspicious	False

Disassembly

hasTricks	True
Tricks	
pushret	**none**: 16
pushpopmath	**none**: 2 **.reloc**: 7
garbagebytes	**none**: 16
hookdetection	**none**: 2 **.reloc**: 1
software breakpoint	**none**: 4 **.reloc**: 2

programcontrolflowchange	**none**: 16
cpuinstructionsresultscomparison	**none**: 2 **.rsrc**: 1

AVclass

banload	1

VirusTotal

md5	0dfca88b93a9c6e6616022d06bad0816
sha1	37364bb7015a7db1e3ce8ee04cdf54cfa2fcbeeb

SCANS (DETECTION RATE = 67.65%)

AVG	**result**: FileRepMalware **update**: 20180716 **version**: 18.4.3895.0 **detected**: **True** ✅
CMC	**update**: 20180714 **version**: 1.1.0.977 **detected**: **False** ❌
MAX	**result**: malware (ai score=85) **update**: 20180716 **version**: 2017.11.15.1 **detected**: **True** ✅
Bkav	**update**: 20180716 **version**: 1.3.0.9466 **detected**: **False** ❌
K7GW	**result**: Trojan-Downloader (00509ea81) **update**: 20180716 **version**: 10.54.27765 **detected**: **True** ✅
ALYac	**result**: Trojan.GenericKD.4709409 **update**: 20180716 **version**: 1.1.1.5 **detected**: **True** ✅
Avast	**result**: Win32:Evo-gen [Susp]

update: 20180716
version: 18.4.3895.0
detected: **True**

Avira

result: HEUR/AGEN.1020350
update: 20180716
version: 8.3.3.6
detected: **True**

Baidu

update: 20180716
version: 1.0.0.2
detected: **False**

Cyren

result: W32/Trojan.EKHM-3039
update: 20180716
version: 6.0.0.4
detected: **True**

DrWeb

update: 20180716
version: 7.0.33.6080
detected: **False**

GData

result: Trojan.GenericKD.4709409
update: 20180716
version: A:25.17796B:25.12737
detected: **True**

Panda

result: Trj/GdSda.A
update: 20180715
version: 4.6.4.2
detected: **True**

VBA32

result: Trojan.Inject
update: 20180716
version: 3.12.32.0
detected: **True**

VIPRE

result: Trojan.Win32.Generic!BT
update: 20180716
version: 68156
detected: **True**

Zoner

update: 20180716
version: 1.0
detected: **False**

AVware

result: Trojan.Win32.Generic!BT

update: 20180716
version: 1.6.0.52
detected: **True**

ClamAV

update: 20180716
version: 0.100.1.0
detected: **False**

Comodo

result: UnclassifiedMalware
update: 20180716
version: 29357
detected: **True**

F-Prot

update: 20180716
version: 4.7.1.166
detected: **False**

Ikarus

result: Trojan-Downloader.Win32.Banload
update: 20180716
version: 0.1.5.2
detected: **True**

McAfee

result: Trojan-FLDW!0DFCA88B93A9
update: 20180716
version: 6.0.6.653
detected: **True**

Rising

result: Malware.Generic.4!tfe (C64:YzY0OkztpfgawxG/)
update: 20180716
version: 25.0.0.20
detected: **True**

Sophos

result: Mal/Generic-S
update: 20180716
version: 4.98.0
detected: **True**

Yandex

result: Trojan.DL.Banload!5W8IfY7tjVA
update: 20180713
version: 5.5.1.3
detected: **True**

Zillya

result: Downloader.Banload.Win32.75653
update: 20180713
version: 2.0.0.3594
detected: **True**

Arcabit

result: Trojan.Generic.D47DC21
update: 20180716
version: 1.0.0.831
detected: **True**

Babable

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

Cylance

update: 20180716
version: 2.3.1.101
detected: **False**

Endgame

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

TACHYON

update: 20180716
version: 2018-07-16.03
detected: **False**

Tencent

result: Win32.Trojan.Generic.Kqe
update: 20180716
version: 1.0.0.1
detected: **True**

ViRobot

update: 20180716
version: 2014.3.20.0
detected: **False**

Webroot

update: 20180716
version: 1.0.0.403
detected: **False**

eGambit

update: 20180716
detected: **False**

Ad-Aware

result: Trojan.GenericKD.4709409
update: 20180716
version: 3.0.5.370
detected: **True**

AegisLab

result: Troj.W32.Inject!c
update: 20180716
version: 4.2
detected: **True**

Emsisoft

result: Trojan.GenericKD.4709409 (B)
update: 20180716
version: 2018.4.0.1029
detected: **True**

F-Secure

result: Trojan.GenericKD.4709409
update: 20180716
version: 11.0.19100.45
detected: **True**

Fortinet

result: W32/Banload.XWN!tr
update: 20180716
version: 5.4.247.0
detected: **True**

Invincea

result: heuristic
update: 20180601
version: 6.3.5.26121
detected: **True**

Jiangmin

update: 20180716
version: 16.0.100
detected: **False**

Kingsoft

update: 20180716
version: 2013.8.14.323
detected: **False**

Paloalto

result: generic.ml
update: 20180716
version: 1.0
detected: **True**

Symantec

result: ML.Attribute.HighConfidence
update: 20180716
version: 1.6.0.0
detected: **True**

AhnLab-V3

result: Malware/Win32.Generic.C1882991
update: 20180716
version: 3.13.1.21452
detected: **True**

Antiy-AVL

result: Trojan/Win32.TSGeneric
update: 20180716
version: 3.0.0.1

	detected: True
Kaspersky	**result**: HEUR:Trojan.Win32.Generic **update**: 20180716 **version**: 15.0.1.13 **detected**: True
Microsoft	**result**: TrojanDownloader:Win32/Banload **update**: 20180716 **version**: 1.1.15000.2 **detected**: True
Qihoo-360	**update**: 20180716 **version**: 1.0.0.1120 **detected**: False
TheHacker	**update**: 20180716 **version**: 6.8.0.5.3372 **detected**: False
ZoneAlarm	**result**: HEUR:Trojan.Win32.Generic **update**: 20180716 **version**: 1.0 **detected**: True
Cybereason	**result**: malicious.b93a9c **update**: 20180225 **version**: 1.2.27 **detected**: True
ESET-NOD32	**result**: a variant of Win32/TrojanDownloader.Banload.XWP **update**: 20180716 **version**: 17722 **detected**: True
TrendMicro	**result**: TROJ_BANLOAD_GD04005A.UVPM **update**: 20180716 **version**: 10.0.0.1040 **detected**: True
BitDefender	**result**: Trojan.GenericKD.4709409 **update**: 20180716 **version**: 7.2 **detected**: True
CrowdStrike	**result**: malicious_confidence_60% (D) **update**: 20180530

version: 1.0
detected: True

K7AntiVirus

result: Trojan-Downloader (00509ea81)
update: 20180716
version: 10.53.27764
detected: True

SentinelOne

update: 20180701
version: 1.0.17.227
detected: False

Avast-Mobile

update: 20180716
version: 180716-00
detected: False

Malwarebytes

update: 20180716
version: 2.1.1.1115
detected: False

TotalDefense

update: 20180716
version: 37.1.62.1
detected: False

CAT-QuickHeal

result: Trojan.Inject
update: 20180714
version: 14.00
detected: True

NANO-Antivirus

result: Trojan.Win32.Inject.emwkhc
update: 20180716
version: 1.0.116.23366
detected: True

MicroWorld-eScan

result: Trojan.GenericKD.4709409
update: 20180716
version: 14.0.297.0
detected: True

SUPERAntiSpyware

update: 20180716
version: 5.6.0.1032
detected: False

McAfee-GW-Edition

result: Trojan-FLDW!0DFCA88B93A9
update: 20180715
version: v2017.3010
detected: True

TrendMicro-HouseCall	**result**: TROJ_BANLOAD_GD04005A.UVPM **update**: 20180716 **version**: 9.950.0.1006 **detected**: True

total	68
sha256	c95caae20195f49e07adb8951abd6e78bd07089aaf1e39234310298c8a6b91af
scan_id	c95caae20195f49e07adb8951abd6e78bd07089aaf1e39234310298c8a6b91af-1531748092
resource	0dfca88b93a9c6e6616022d06bad0816
permalink	https://www.virustotal.com/file/c95caae20195f49e07adb8951abd6e78bd07089aaf1e39234310298c8a6b91af/analysis/1531748092/
positives	46
scan_date	2018-07-16 13:34:52
verbose_msg	Scan finished, information embedded
response_code	1

File

Trace

17/2/2020 - 19:45:42.653	Open	1480	C:\malware.exe	C:\malware.exe
17/2/2020 - 19:45:42.653	Unknown	1480	C:\malware.exe	C:\malware.exe
17/2/2020 - 19:45:42.653	Open	1480	C:\malware.exe	C:\
17/2/2020 - 19:45:42.653	Unknown	1480	C:\malware.exe	C:\
17/2/2020 - 19:45:42.653	Open	1480	C:\malware.exe	C:\Monitor
17/2/2020 - 19:45:42.653	Unknown	1480	C:\malware.exe	C:\Monitor
17/2/2020 - 19:45:42.6	Open	148	C:\malware.e	C:\Monitor\Malware

53		0	xe		
17/2/2020 - 19:45:42.653	Unknown	1480	C:\malware.exe	C:\Monitor\Malware	
17/2/2020 - 19:45:42.653	Open	1480	C:\malware.exe	C:\Windows\Globalization\Sorting\SortDefault.nls	
17/2/2020 - 19:45:42.653	Unknown	1480	C:\malware.exe	C:\Windows\Globalization\Sorting\SortDefault.nls	SortDefault.nls
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\ProgramData\AVAST Software	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\ProgramData\Inteltecnolocis	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\ProgramData\Inteltecnolocis	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\ProgramData	
17/2/2020 - 19:45:42.700	Unknown	1480	C:\malware.exe	C:\ProgramData	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\ProgramData\Inteltecnolocis	
17/2/2020 - 19:45:42.700	Unknown	1480	C:\malware.exe	C:\ProgramData\Inteltecnolocis	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winhttp.dll	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winhttp.dll	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\webio.dll	
17/2/2020 - 19:45:42.700	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\webio.dll	
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\pt-BR\KernelBase.dll.mui	
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\cryptsp.dll	
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\cryptsp.dll	
17/2/2020 - 19:45:42.7	Open	148	C:\malware.e	C:\Windows\SysWOW64\cryptsp.dll	

47		0	xe	
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\credssp.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\credssp.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\credssp.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\mswsock.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\mswsock.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\WSHTCPIP.DLL
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\WSHTCPIP.DLL
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wship6.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\wship6.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\DNSAPI.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\dnsapi.dll
17/2/2020 - 19:45:42.747	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\dnsapi.dll
17/2/2020 - 19:45:42.856	Open	1480	C:\malware.exe	C:\IPHLPAPI.DLL
17/2/2020 - 19:45:42.856	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\IPHLPAPI.DLL
17/2/2020 - 19:45:42.856	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\IPHLPAPI.DLL
17/2/2020 - 19:45:42.856	Open	1480	C:\malware.exe	C:\WINNSI.DLL
17/2/2020 - 19:45:42.856	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\winnsi.dll
17/2/2020 - 19:45:42.8	Open	148	C:\malware.e	C:\Windows\SysWOW64\winnsi.dll

56		0	xe	
17/2/2020 - 19:45:42.903	Open	1480	C:\malware.exe	C:\rasadhlp.dll
17/2/2020 - 19:45:42.903	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rasadhlp.dll
17/2/2020 - 19:45:42.903	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\rasadhlp.dll
17/2/2020 - 19:45:43.122	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FWPUCLNT.DLL
17/2/2020 - 19:45:43.122	Open	1480	C:\malware.exe	C:\Windows\SysWOW64\FWPUCLNT.DLL

Process

Trace

Analysis

Reason Timeout

Status Sucessfully Executed

Results 1

Registry

Trace

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**: False

Deleted **Identified**: False

Browsers **Identified**: False

Internet **Identified**: False

DNS

Query

💻 localhost → 💻 gateway:49551 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:50273 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:54285 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:50043 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:51595 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:49222 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:59829 ‹› www9.lordstark.dynamic-dns.net.
💻 localhost → 💻 gateway:DNS ‹› www9.lordstark.dynamic-dns.net.

Response

💻 gateway:DNS → 💻 localhost ‹› www9.lordstark.dynamic-dns.net. ↩ 10.1.1.1

TCP

Info

💻 localhost:65198 → ⍰ 10.1.1.1:80
💻 localhost:65192 → ⍰ 10.1.1.1:80
💻 localhost:65193 → ⍰ 10.1.1.1:443
💻 localhost:65191 → ⍰ 10.1.1.1:443
💻 localhost:65196 → ⍰ 10.1.1.1:80
💻 localhost:65197 → ⍰ 10.1.1.1:443
💻 localhost:65195 → ⍰ 10.1.1.1:443
💻 localhost:65194 → ⍰ 10.1.1.1:80

UDP

Info

💻 localhost:51595 → 💻 localhost:53
💻 localhost:49551 → 💻 localhost:53
💻 localhost:55394 → 💻 localhost:53
💻 localhost:53 → 💻 localhost:59829
💻 localhost:54285 → 💻 localhost:53
💻 localhost:53 → 💻 localhost:51595
💻 localhost:53 → 💻 localhost:49551
💻 localhost:50273 → 💻 localhost:53
💻 localhost:49222 → 💻 localhost:53
💻 localhost:53 → 💻 localhost:50043
💻 localhost:53 → 💻 localhost:50273
💻 localhost:50043 → 💻 localhost:53
💻 localhost:53 → 💻 localhost:54285
💻 localhost:53 → 💻 localhost:55394
💻 localhost:59829 → 💻 localhost:53
💻 localhost:53 → 💻 localhost:49222

HTTP

Info

Summary

DNS	**True** ✅
TCP	**True** ✅
UDP	**True** ✅
HTTP	**False** ❌

Results

BINARY

KNN (K=3, NFS-BRMalware)
confidence: 100.00%
suspicious: True

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

SVC (Kernel=Linear, NFS-BRMalware)
confidence: 86.70%
suspicious: True

MalConv (Ember: Raw Bytes, Threshold=0.5)
confidence: 96.96%
suspicious: False

Random Forest (100 estimators, NFS-BRMalware)
confidence: 64.00%
suspicious: True

Non-Negative MalConv (Ember: Raw Bytes, Threshold=0.35)
confidence: 36.20%
suspicious: True

LightGDM (Ember: File Characteristics, Threshold=0.8336)
confidence: 92.38%
suspicious: False